UNIVERSIDADE CATÓLICA PORTUGUESA | FACULDADE DE ENGENHARIA

A importância dos controlos técnicos preventivos e detetivos nas redes de dados da Administração Pública

Ricardo João Duque Oliveira

Dissertação apresentada à Faculdade de Engenharia da Universidade Católica Portuguesa para obtenção do grau de Mestre em Segurança em Sistemas de Informação

Júri

Professor Doutor Manuel Barata Marques (Presidente)

Professor Doutor Rui Pires

Professor Doutor Tito Santos Silva (Orientador)

Maio de 2014

UNIVERSIDADE CATÓLICA PORTUGUESA | FACULDADE DE ENGENHARIA

A importância dos controlos técnicos preventivos e detetivos nas redes de dados da Administração Pública

Ricardo João Duque Oliveira

Dissertação apresentada à Faculdade de Engenharia da Universidade Católica Portuguesa para obtenção do grau de Mestre em Segurança em Sistemas de Informação

Sob orientação do Professor Doutor Tito Santos Silva

Maio de 2014

“Se o dinheiro for a sua esperança de independência, jamais a terá. A única segurança verdadeira neste mundo é a reserva de sabedoria, de experiência e de competência.”

Henry Ford

AGRADECIMENTOS

Um Obrigado especial à minha família pelo tempo que lhes subtraí, sobretudo ao meu filho e à minha esposa, pela força que me transmitiram e pela compreensão que me foram demonstrando...

Obrigado ao Professor Tito Santos Silva, pelas suas orientações e pela sua preciosa disponibilidade.

Obrigado aos meus semelhantes das tecnologias de informação da Administração Pública que, nesta época de mudança particularmente difícil, fazem cada vez mais com cada vez menos, contribuindo de forma determinante para a melhoria contínua e para esta forma de pensar.

Obrigado!

RESUMO

A evolução tecnológica e a constante adequação do "negócio" dos organismos públicos às Tecnologias de Informação e Comunicação trazem desafios ambiciosos. O facto de os seus processos serem, cada vez mais, suportados nas redes e nos Sistemas de Informação, abre portas a riscos que podem comprometer ativos críticos. As necessidades de interoperabilidade entre sistemas de organismos públicos, ou entre estes e sistemas de entidades externas, são também crescentes. Por outro lado, o descontentamento social generalizado tem promovido o aumento dos ataques especificamente dirigidos às entidades públicas. Todos estes fatores reforçam assim a pertinência da reflexão sobre a temática da segurança na Administração Pública. É por isso essencial existir no Estado, de forma normalizada, mecanismos de prevenção e deteção de ameaças, capazes de conter eficazmente o risco, sem que para isso se tenha que afetar consideravelmente os orçamentos dos ministérios.

Após uma contextualização sobre os conceitos envolvidos, a dissertação apresentará um levantamento de ameaças atuais inerentes às redes de dados, exemplificando-as com eventos recentes. Serão reconhecidas vulnerabilidades genéricas existentes nas redes dos organismos e será resumido algum do trabalho já efetuado neste âmbito. Serão caracterizados controlos técnicos preventivos e detetivos considerados essenciais, justificando-se a sua importância e exemplificando-se a sua existência com produtos *open-source*. Será proposto um modelo de segurança, recomendando-se o posicionamento estratégico desses controlos em diferentes zonas de rede, consoante um conjunto de critérios. Serão apresentadas conclusões e identificadas vantagens da implementação do modelo, sugerindo-se ainda a continuidade destas melhorias em trabalhos futuros.

PALAVRAS-CHAVE: Administração Pública; Redes de Dados; Sistemas de Informação; Tecnologias de Informação e Comunicação; Segurança; Controlos técnicos.

ABSTRACT

The technological evolution and the constant adaptation of the public organization's "business" to the Communication and Information Technologies brings ambitious challenges. The fact that its processes increasingly supported in the data networks and the Information Systems, brings forth threats that may compromise critical assets. The interoperability needs between systems of public organizations, or between these and systems of external entities, are also increasingly larger. On the other hand, the generalized social dissatisfaction has been promoting the increase of attacks aimed specifically to the networks and systems of public entities. These events then buttress the relevance of the reflection on the theme of the Public Administration network security. It is therefore essential the existence in the State, in a normalized way, mechanisms of threat prevention and detection, able of efficiently containing the menace without considerately affecting the Ministry's budgets.

After a contextualization about the concepts discussed, the dissertation will present a mapping of some of the main current threats inherent to the data network, exemplifying them with recent events. There will also be identified, generically, existing vulnerabilities in the public organizations' networks and it is abridged some of the already developed work in this ambit. It will characterize the preventive and detective technical controls deemed essential exemplifying its existence resorting to open-source products. It will be proposed a security model, being recommended the strategic positioning of those controls on different network areas, according to an array of criterions. Conclusions will also be presented and potential inherent advantages to the implementation of the model will be identified, existing also a suggestion of continuity of these improvements in future works.

KEY-WORDS: Public Administration; Data Networks; Information Systems; Information and Communication Technologies; Security; Technical Controls.

LISTA DE ABREVIATURAS

- ✓ AP – Administração Pública;
- ✓ ARP – Address Resolution Protocol;
- ✓ BPDU – Bridge Protocol Data Unit;
- ✓ CAM – Content addressable memory;
- ✓ CERT – Computer emergency response team;
- ✓ CGD – Caixa Geral de Depósitos;
- ✓ CISSP - Certified Information System Security Professional;
- ✓ CSIRT – Computer security incident response team;
- ✓ DNS – Domain Name System;
- ✓ DSL – Digital Subscriber Line;
- ✓ EMGFA – Estado-Maior-General das Forças Armadas;
- ✓ FEUP – Faculdade de Engenharia da Universidade do Porto;
- ✓ GARP – Gratuitous Address Resolution Protocol;
- ✓ GPTIC – Grupo de Projecto para as Tecnologias de Informação e Comunicação;
- ✓ HIPS – Host-based Intrusion Prevention System;
- ✓ IDS – Intrusion Detection System;
- ✓ IGFEJ – Instituto de gestão financeira e equipamentos da Justiça;
- ✓ INESC – Instituto de Engenharia de Sistemas e Computadores do Porto;
- ✓ IP – Internet Protocol;
- ✓ IPS – Intrusion Prevention System;
- ✓ ISP's – Internet Service Providers;
- ✓ IT – Information Technology;
- ✓ LAN – Local Area Network;
- ✓ MAC – Media Access Control;
- ✓ MAI – Ministério da Administração Interna;
- ✓ NIDS – Network Intrusion Detection System;
- ✓ QoS – Quality of Service;
- ✓ RCM – Resolução do Conselho de Ministros;
- ✓ SI – Sistemas de Informação;
- ✓ SNMP - Simple Network Management Protocol;
- ✓ UTIS – Unidade de Tecnologias de Informação de Segurança;
- ✓ VLAN – Virtual Local Area Network;
- ✓ VPN – Virtual Private Network;
- ✓ WAN – Wide Area Network.

GLOSSÁRIO

- ✓ Anti-Spam – Técnicas e mecanismos de prevenção do mail de Spam;
- ✓ Back-doors – Técnicas/métodos de ataque que visam evitar os procedimentos de autenticação no sistema, com a instalação de software maligno cujo intuito é vir a facilitar esses mesmos acessos futuros.
- ✓ Banner grabbing – Técnicas/métodos de ataque que visam a obtenção de informação do sistema, nomeadamente a enumeração de versões de sistemas operativos e aplicações, dos serviços a correr e dos respetivos portos abertos.
- ✓ Broadcast – Transmissão disseminada de um pacote que vai ser recebido por todos os dispositivos ligados à rede do dispositivo origem.
- ✓ Bruteforce – Técnicas/métodos de ataque que visam a descodificação de uma chave através do teste a todas as combinações possíveis.
- ✓ Buffer overflow – Dá-se quando um programa (geralmente malicioso), ao gravar dados num buffer, sobrescreve o limite previsto do mesmo, invadindo a memória adjacente.
- ✓ Cloud – Refere-se à disponibilização de serviços através de redes de dados, que aparentam ser prestados por um servidor físico (hardware), sendo na realidade disponibilizados por hardware virtual distribuído, sem que haja necessidade do utilizador saber onde reside fisicamente a fonte dessa prestação de serviços.
- ✓ Cracks – Processo de obtenção/alteração de passwords através de técnicas de Bruteforce.
- ✓ Data-Link layer – Refere-se à camada 2 do modelo OSI que, de forma genérica, é responsável por fornecer os meios funcionais para a transferência de dados entre nós da rede, podendo fornecer os mecanismos de deteção e correção de erros que possam ocorrer no meio físico de transmissão.
- ✓ Delay ou latência – É uma característica na transmissão que mede o tempo que leva um bit a ser transmitido entre dois pontos terminais da rede; É afetada pela distância, erros, congestionamento, capacidade de processamento dos equipamentos, etc.
- ✓ Dialup – Forma de acesso que utiliza a infraestrutura telefónica pública (Public Switched Telephone Network - PSTN) para o estabelecimento de conexão com o operador de telecomunicações, nomeadamente para acessos à Internet.
- ✓ Eavesdropping – Consiste na captura não autorizada de pacotes de rede, provenientes de outros dispositivos, e na análise do seu conteúdo com vista à procura de informação sensível tal como passwords.

- ✓ Exploits – Peça de software, bloco de dados, ou sequência de comandos que se aproveita de um bug ou de uma vulnerabilidade com o intuito de causar intencionalmente um comportamento anormal e inesperado num sistema.
- ✓ Flood de pacotes SYN – Técnica/Método de negação de serviço em que um atacante envia uma sucessão de pedidos para um sistema alvo com o intuito de consumir os seus recursos, visando causar indisponibilidade ao tráfego legítimo.
- ✓ Frame – É a unidade de transmissão de dados inerente ao Layer 2 do modelo OSI.
- ✓ Hub – Dispositivo de rede que permite conectar vários equipamentos Ethernet, através dos seus interfaces, num único segmento de rede; O tráfego que passa em cada interface não é segregado, sendo visto por todos os outros.
- ✓ Jitter – É a medida de variação do atraso (delay) na entrega de dados na rede, atraso esse verificado entre os pacotes sucessivos de dados.
- ✓ Man-in-the-Middle – Técnicas/métodos de ataque em que o atacante se consegue posicionar no meio de uma transmissão entre a origem e o destino, comprometendo a confidencialidade e integridade dessa informação.
- ✓ Personal Firewall – Aplicação que controla o tráfego de dados da rede para o computador que a tem instalado e vice-versa, permitindo-o ou negando-o consoante um conjunto de critérios (política de segurança).
- ✓ Ping of death – Técnicas/métodos de ataque que envolve o envio de pacotes ping malformados ou maliciosos para um sistema alvo; Por exemplo, o envio de muitos pings com tamanho elevado podem comprometer a disponibilidade do computador destino.
- ✓ Ping Sweep – Métodos/ferramentas de ping que permitem, após a definição de uma range de endereços IP, verificar quais deles representam hosts ativos nessa rede.
- ✓ Redes Mesh – Topologias de rede em que os nós da mesma estão diretamente interligados com todos os outros (Full-Mesh) ou com alguns dos outros (Partial-Mesh).
- ✓ Smurf (attack) – Método de ataque em que é enviado para toda a rede (broadcast), pelo atacante, um nº elevado de pacotes ICMP com o endereço IP de origem falsificado como sendo o da vítima, e cujas respetivas respostas lhe vão causar uma negação de serviço por esgotamento dos seus recursos.
- ✓ Switch (ou Bridge) – Dispositivo de rede que permite conectar vários equipamentos Ethernet, através dos seus interfaces, em vários segmentos de rede; O tráfego que passa em cada interface é segregado, representando por isso vários domínios de colisão.
- ✓ Syslog - É um padrão criado pela Internet Engineering Task Force (IETF) para a transmissão de mensagens de log em redes IP;

- ✓ TCP/UDP Port Scan – Métodos/ferramentas que permitem verificar, nos equipamentos ligados à rede, quais as portas TCP e UDP que estão a ser utilizadas na disponibilização de serviços.
- ✓ Trap SNMP – Tipo de unidade de dados utilizada para a relatar um alerta (ou outro evento) de um dispositivo ligado à rede, através do protocolo de gestão e monitorização SNMP.
- ✓ URL filtering – Mecanismos/ferramentas que permitem filtrar o acesso à Internet através da catalogação dos tipos de conteúdos e URL's disponibilizados por websites.
- ✓ Whois – Método/ferramentas que permitem verificar informações associadas a um determinado domínio, nomeadamente endereçamento IP e propriedade do nome de domínio.

ÍNDICE

1. INTRODUÇÃO 16
1.1. MOTIVAÇÃO 17
1.2. OBJETIVOS DA DISSERTAÇÃO 18
1.3. ORGANIZAÇÃO DA DISSERTAÇÃO 19
2. O ESTADO DA ARTE 21
2.1. CONTEXTUALIZAÇÃO 21
2.1.1. A organização atual da Administração Pública 21
2.1.2. Os Sistemas de Informação na Administração Pública 26
2.1.3. A necessidade das redes na Administração Pública 29
2.1.4. A Segurança nas redes informáticas e a sua importância 29
2.1.5. Conceito de Vulnerabilidades, Ameaças, Risco e Contramedidas (Controlos) .. 31
2.1.6. Tipificação dos Controlos 33
2.2. ANÁLISE DA SITUAÇÃO ATUAL 35
2.2.1. As redes de dados da Administração Pública e a sua evolução 35
2.2.2. Ameaças significativas nos dias que correm 42
a. Penetração em redes 48
b. Malware 50
c. Botnet's, SPAM e Distributed Denial of Service 54
d. Ataques web-based 59
e. Ataques de Layer 2 63
2.2.3. O Hacktivismo e seus impactos negativos 69
2.2.4. Vulnerabilidades genéricas nas redes do Estado 74
2.2.5. Trabalho já efetuado no âmbito das redes e da segurança da AP 76
3. CARACTERIZAÇÃO DE CONTROLOS TÉCNICOS PREVENTIVOS E DETETIVOS 86
3.1. A IMPORTÂNCIA DA GESTÃO DO RISCO E DOS STANDARDS INTERNACIONAIS DE SEGURANÇA 86

3.2. CONTROLOS TÉCNICOS PREVENTIVOS 89
3.2.1. Firewalls 89
a. Tipificação 90
b. Demilitarized Zones 92
c. Arquiteturas 93
d. Network Address Translation 94
e. Exemplo de Produto de Firewall open-source 95
3.2.2. Virtual Private Network's 99
a. Exemplo de Produto VPN open-source 101
3.2.3. Proteções de Layer 2 104
a. Proteção básica 105
b. Port Security 106
c. Proteções contra ataques ao Spanning Tree Protocol 107
d. Proteções contra ataques a VLAN's 108
3.3. CONTROLOS TÉCNICOS DETETIVOS 109
3.3.1. Antivírus 109
a. Métodos de deteção 110
b. Exemplo de Produto de Anti-vírus open-source 112
3.3.2. Intrusion Detection Systems 115
a. Necessidade de utilização e objetivos fundamentais 115
b. Métodos de deteção e tipificação de IDS 117
c. Arquitetura genérica 119
d. O uso de SPAN/ RSPAN 122
e. Exemplo de Produto de IDS open-source 123
3.3.3. Auditorias à rede para deteção de vulnerabilidades 125
a. A recolha de Informação/ Descoberta 126
b. A enumeração 128
c. A deteção 129

d. Exemplo de scanner de vulnerabilidades open-source 129
4. MODELO DE SEGURANÇA PARA AS REDES DE DADOS DA AP 132
4.1. PROPOSTA DE MODELO 133
4.1.1. Pressupostos e governança 133
4.1.2. Organização hierárquica da rede e tipificação dos sites 136
4.1.3. SITE Nível 1 – Site TIC do Organismo TIC do Ministério 140
4.1.4. SITE Nível 2 – Sites TIC dos restantes Organismos 142
4.1.5. SITE Nível 3 – Sites consumidores de recursos 143
4.2. VANTAGENS DA IMPLEMENTAÇÃO DO MODELO PROPOSTO E ANÁLISE DAS DIFERENÇAS 145
5. CONCLUSÕES 147
5.1. DISCUSSÃO 147
5.2. TRABALHO FUTURO 149
REFERÊNCIAS BIBLIOGRÁFICAS 151
SOBRE O AUTOR 156

ÍNDICE DE ILUSTRAÇÕES

Ilustração 1 - Tabela orgânica do Estado 24
Ilustração 2 - Organograma parcial da Presidência do Conselho de Ministros 25
Ilustração 3 - Visão arquitetural dos Sistemas de Informação 28
Ilustração 4 - B2C vs B2B 29
Ilustração 5 - Segregação da rede em zonas de segurança 30
Ilustração 6 - Componentes da Gestão do Risco 32
Ilustração 7 - Exemplos de Controlos 34
Ilustração 8 – Exemplo de topologia "Star" 36
Ilustração 9 – Exemplo de topologia "Full Mesh" 37
Ilustração 10 - Tipos de ligações WAN 38
Ilustração 11 - Frame Relay 40
Ilustração 12 – Exemplo de uma rede de um Organismo Público (IFAP) 42
Ilustração 13 - ENISA: Threat Landscape - Ameaças e Tendências 45
Ilustração 14 - ENISA: Threat Landscape - Relação ameaças vs agentes 46
Ilustração 15 - Caracterização de um ataque de penetração 48
Ilustração 16 - Footprinting: identificações por ambiente 49
Ilustração 17 - Total de Malware e Novo Malware 52
Ilustração 18 - Participações de Ransomware 53
Ilustração 19 - Mobile malware 53
Ilustração 20 - Denial of Service por SYN Flooding 56
Ilustração 21 - Spam vs Email legítimo 57
Ilustração 22 - Atividade de Spam das Botnet's Grum e Festi 58
Ilustração 23 - Exemplo de SQL Injection num formulário 60
Ilustração 24 - Teste de vulnerabilidade XSS 62
Ilustração 25 - Ataque "Man-in-the-Middle" por "ARP Spoofing" 65
Ilustração 26 - Ataque STP 67
Ilustração 27 - Ataque “VLAN Hopping” por "Double Tagging" 69
Ilustração 28 – Hacktivistas: características vs orientações 70
Ilustração 29 - Logótipos dos “Anonymous” e dos “LulzSec” 71
Ilustração 30 – Âmbito do Top 14 das Vulnerabilidades em redes e Sistemas 76
Ilustração 31 - Passos do Plano Global Estratégico das TIC da AP 80
Ilustração 32 - 25 Medidas das TIC da AP 81
Ilustração 33 - Implementação com Stateful Firewall 92
Ilustração 34 - Arquiteturas de Firewall 93

Ilustração 35 - pfSense: System Overview 97
Ilustração 36 - pfSense: Firewall Rules 97
Ilustração 37 - pfSense: NAT 98
Ilustração 38 - pfSense: Logging 98
Ilustração 39 - Túneis VPN 99
Ilustração 40 - Shrew Soft VPN Client: Access Manager 103
Ilustração 41 - Shrew Soft VPN Client: Definições gerais do site 103
Ilustração 42 - Shrew Soft VPN Client: Método de autenticação 104
Ilustração 43 - Modelo de avaliação dos métodos de deteção de mallware 112
Ilustração 44 - Interfaces do ClamWin 114
Ilustração 45 - Arquitetura genérica dos IDS's 121
Ilustração 46 - Implementação distribuída de IDS's 121
Ilustração 47 - Exemplo de configuração de RSPAN para uso de um IDS 123
Ilustração 48 - Elementos constituintes do Snort e suas interdependências 124
Ilustração 49 - Ferramenta de Whois 127
Ilustração 50 - OpenVAS framework 130
Ilustração 51 - Diagrama hierárquico de alto nível da rede da AP 137
Ilustração 52 – Diagrama da Rede Interministérios 139
Ilustração 53 - SITE Nível 1: Site TIC do Organismo TIC do Ministério 140
Ilustração 54 - Esquema de blocos de segurança: Site TIC do Ministério 142
Ilustração 55 - SITE Nível 2: Sites TIC dos restantes Organismos (não TIC) 143
Ilustração 56 - SITE Nível 3: Sites consumidores de recursos 144
Ilustração 57 - Modelo SWOT da implementação do modelo 146

1. INTRODUÇÃO

Esta Dissertação de Mestrado aborda, de uma forma geral, preocupações relacionadas com a Segurança da Informação no contexto dos organismos públicos e pretende definir um modelo tipificado, normalizado e unificado de organização de mecanismos técnicos para controlo preventivo e detetivo do risco de concretização de ameaças nas redes de dados da Administração Pública (AP). Em sintonia com as dificuldades financeiras que o Estado atravessa, estará sempre presente uma perspetiva de contenção de custos (recorrendo-se ao *open-source* como uma boa alternativa) e de racionalização e otimização dos recursos.

Tendo em conta que a informação é, mais que nunca, um ativo de extremo valor para os organismos públicos e que o "negócio" destes organismos é bastante dependente das infraestruturas de rede e das transmissões de dados sensíveis, revela-se muito importante que haja o devido conhecimento das ameaças existentes que possam causar indisponibilidade nos sistemas, ou mesmo que possam promover a captura indevida deste tipo de informação.

Nos últimos tempos, também devido a algum descontentamento social, tem crescido significativamente o número de ataques aos Sistemas de Informação de entidades públicas portuguesas. Por outro lado, tem sido cada vez mais difícil a estas entidades ter verbas disponíveis para a manutenção/gestão dos seus ativos de rede e de segurança com vista a evitar ou minimizar o impacto destes ataques.

Assim, torna-se cada vez mais relevante haver medidas de consolidação da Segurança da Informação no Estado como um todo, por forma a serem diminuídas as vulnerabilidades existentes nos seus ativos e, consequentemente, o risco destes serem explorados por este tipo de ameaças. Esta consolidação promove ainda a eficiência na prestação de serviços dos organismos públicos e a racionalização dos seus recursos, evitando-se redundâncias desnecessárias e diminuindo-se o desperdício neste âmbito.

Para que este modelo possa trazer maior benefício, deverá ser assente numa rede de comunicações única que interligue todos os edifícios dos organismos públicos que, por sua vez, deverão ser tipificados consoante alguns critérios de criticidade que os caracterizem.

1.1. MOTIVAÇÃO

A motivação intrínseca a esta Dissertação baseia-se essencialmente na constatação de aspetos significativos a melhorar na segurança das infraestruturas de rede do Estado e dos seus ativos críticos, tais como a informação. O facto de o autor desempenhar funções num organismo público e de experienciar a este nível também a realidade de outros, contribuiu de forma determinante para um conhecimento sólido dos processos TIC assim como dos ativos que os sustentam e das potenciais vulnerabilidades que lhes são inerentes. Assim, esta Dissertação é concebida com o intuito de vir a trazer valor acrescentado num cenário de reorganização das redes da Administração Pública, privilegiando a segurança da informação.

Acresce ainda como fator de motivação a atual conjuntura socioeconómica, que se entende tornar oportuna a determinação de querer fazer mais com menos recursos, promovendo também a eficiência na gestão da segurança das redes do Estado.

1.2. OBJETIVOS DA DISSERTAÇÃO

Os principais objetivos que esta Dissertação pretende alcançar são:

- ✓ Descrever, de forma genérica, a situação atual dos organismos públicos, em termos de segurança em redes de dados;
- ✓ Identificar o trabalho já feito nesta área (e os intervenientes envolvidos) e o que se pretende fazer a curto prazo para melhorar a segurança nas redes do Estado;
- ✓ Caracterizar alguns dos principais controlos técnicos preventivos e detetivos para as redes de dados, dando exemplos de produtos *open-source* e explicitar a sua importância para a segurança da informação nos organismos públicos;
- ✓ Estabelecer e propor um modelo de segurança para as infraestruturas de rede do Estado, recorrendo-se a mecanismos técnicos de prevenção e deteção de ameaças, tendo em conta critérios de racionalização das TIC e de otimização dos recursos;
- ✓ Aferir acerca da importância da segurança dos Sistemas de Informação no Estado Português, associando-a à diminuição do risco e ao aumento da eficiência do setor público;
- ✓ Contribuir com valor para a comunidade, essencialmente para todos os intervenientes ligados à gestão de redes e de segurança no setor público;
- ✓ Identificar trabalho futuro premente nesta área.

1.3. ORGANIZAÇÃO DA DISSERTAÇÃO

Em termos de organização, a Dissertação é, basicamente, estruturada da seguinte forma:

1 <u>INTRODUÇÃO</u>: Indicação breve dos temas a abordar e das ideias que se pretende transmitir.

1.1 MOTIVAÇÃO: Descrição dos principais fatores motivadores para elaboração da Dissertação.

1.2 OBJETIVOS DA DISSERTAÇÃO: Enumeração dos objetivos a atingir.

1.3 ORGANIZAÇÃO DA DISSERTAÇÃO: Descrição da estrutura e da forma como a Dissertação é organizada.

2 <u>O ESTADO DA ARTE</u>: Descrição da situação atual neste âmbito.

2.1 CONTEXTUALIZAÇÃO: Descrição da organização atual da Administração Pública (AP) e do papel dos Sistemas de Informação e das redes de dados na AP, clarificação da importância da segurança nas redes, definição de conceitos relacionados com a segurança e tipificação dos controlos.

2.2 ANÁLISE DA SITUAÇÃO ATUAL: Exposição genérica das redes de dados da Administração Pública, identificação das principais ameaças e de algumas das vulnerabilidades existentes em termos gerais, bem como elencar trabalho já existente no âmbito da segurança e das redes de dados da Administração Pública.

3 <u>CARACTERIZAÇÃO DE CONTROLOS TÉCNICOS PREVENTIVOS E DETETIVOS</u>: Identificação e caracterização de alguns dos principais controlos técnicos preventivos e detetivos, evidenciando-se produtos de código aberto (*open-source*) a serem aplicados no modelo a propor.

3.1 A IMPORTÂNCIA DA GESTÃO DE RISCO E DOS STANDARDS INTERNACIONAIS DE SEGURANÇA: Demonstração da importância da gestão do risco para identificar, classificar e mitigar os riscos inerentes aos Sistemas de Informação, às redes e aos processos TIC.

3.2 CONTROLOS TÉCNICOS PREVENTIVOS: Identificação, caracterização e exemplificação de alguns dos principais controlos técnicos preventivos.

3.3 CONTROLOS TÉCNICOS DETETIVOS: Identificação, caracterização e exemplificação de alguns dos principais controlos técnicos detetivos.

4 MODELO DE SEGURANÇA PARA AS REDES DE DADOS DA AP: Definição de um modelo de organização e de segurança para as redes da Administração Pública e enquadramento dessa necessidade.

4.1 PROPOSTA DE MODELO: Proposta do modelo de segurança para as redes da Administração Pública e tipificação dos diversos *sites* envolvidos.

4.2 VANTAGENS DA IMPLEMENTAÇÃO DO MODELO E ANÁLISE DAS DIFERENÇAS: Identificação das vantagens (assim como das dificuldades) para a implementação do modelo teórico a propor e demonstração das principais diferenças em relação à realidade atual.

5 CONCLUSÕES: Apresentação das conclusões decorrentes da dissertação e da própria pesquisa.

5.1 DISCUSSÃO: Concluir sobre como se conseguem alcançar os objetivos definidos no início da dissertação.

5.2 TRABALHO FUTURO: Sugestões para trabalho a realizar num futuro próximo (nomeadamente no que respeita ao processo de submeter a proposta de implementação do modelo a entidades competentes para o efeito).

REFERÊNCIAS BIBLIOGRÁFICAS: Enumeração das referências bibliográficas utilizadas na Dissertação.

2. O ESTADO DA ARTE

2.1. CONTEXTUALIZAÇÃO

O presente capítulo pretende contextualizar acerca do que é a organização da Administração Pública em termos orgânicos, qual o seu papel no que respeita a tecnologias de informação, de comunicação e de segurança, bem como explicar conceitos enquadradores que facilitarão a obtenção dos objetivos desta dissertação.

2.1.1. A organização atual da Administração Pública

Em termos orgânicos, o Estado apresenta-se atualmente estruturado conforme a tabela abaixo (PORTAL DO GOVERNO DE PORTUGAL, 2013):

PELOURO	ÓRGÃOS
Primeiro Ministro	Secretário de Estado da Presidência do Conselho de Ministros
	Secretário de Estado Adjunto do Primeiro-Ministro
	Secretário de Estado da Cultura
Ministro Adjunto e dos Assuntos Parlamentares	Secretário de Estado Adjunto do Ministro-Adjunto e dos Assuntos Parlamentares
	Secretária de Estado dos Assuntos Parlamentares e da Igualdade
	Secretário de Estado da Administração Local e Reforma Administrativa
	Secretário de Estado do Desporto e Juventude
Ministério das Finanças	Secretaria -Geral
	Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais
	Inspecção -Geral de Finanças
	Direcção -Geral do Orçamento
	Direcção -Geral do Tesouro e Finanças
	Autoridade Tributária e Aduaneira
	Direcção -Geral da Administração e do Emprego Público
	Direcção -Geral de Protecção Social aos Trabalhadores em Funções Públicas
	Serviços Sociais da Administração Pública
	Direcção -Geral da Qualificação dos Trabalhadores em Funções Públicas
	Caixa Geral de Aposentações, I P
	Instituto de Gestão da Tesouraria e do Crédito Público, I P
	Entidade de Serviços Partilhados da Administração Pública, I P
	Banco de Portugal
	Instituto de Seguros de Portugal
	Comissão do Mercado de Valores Mobiliários

Ministério dos Negócios Estrangeiros	Secretaria-Geral
	Direção-Geral de Política Externa
	Inspeção-Geral Diplomática e Consular
	Direção-Geral dos Assuntos Europeus
	Direção-Geral dos Assuntos Técnicos e Económicos
	Direção-Geral dos Assuntos Consulares e das Comunidades Portuguesas
	Embaixadas
	Missões e representações permanentes e missões temporárias
	Postos consulares
	Fundo para as Relações Internacionais, I P
	Instituto Camões, I P
	Instituto Português de Apoio ao Desenvolvimento, I P
	Comissão Interministerial de Limites e Bacias Hidrográficas Luso-Espanholas
	Comissão Nacional da UNESCO
	Conselho das Comunidades Portuguesas
Ministério da Defesa Nacional	Secretaria-Geral
	Inspeção-Geral de Defesa Nacional
	Direção-Geral de Política de Defesa Nacional
	Direção-Geral de Pessoal e Recrutamento Militar
	Direção-Geral de Armamento e Infra-Estruturas de Defesa
	Instituto da Defesa Nacional
	Instituto de Ação Social das Forças Armadas
	Polícia Judiciária Militar
Ministério da Administração Interna	Guarda Nacional Republicana
	Polícia de Segurança Pública
	Auditora Jurídica
	Serviço de Estrangeiros e Fronteiras
	Autoridade Nacional de Proteção Civil
	Autoridade Nacional de Segurança Rodoviária
	Inspeção-Geral da Administração Interna
	Direção-Geral de Administração Interna
	Direção-Geral de Infraestruturas e Equipamentos
	Empresa de Meios Aéreos, SA
Ministério da Justiça	Direção-Geral da Política de Justiça
	Inspeção-Geral dos Serviços de Justiça
	Secretaria-Geral do Ministério da Justiça
	Polícia Judiciária
	Direção-Geral da Administração da Justiça
	Direção-Geral de Reinserção e Serviços Prisionais
	Instituto de Gestão Financeira e Equipamentos da Justiça, I P
	Instituto dos Registos e do Notariado, I P
	Instituto Nacional de Medicina Legal e Ciências Forenses, I P
	Instituto Nacional da Propriedade Industrial, I P
	Centro de Estudos Judiciários
	Comissão de Proteção às Vitimas de Crime
	Comissão de Apreciação e Controlo da Atividade dos Administradores da Insolvência

Ministério da Economia e do Emprego	Secretaria -Geral
	Gabinete de Estratégia e Estudos
	Direcção -Geral das Actividades Económicas
	Direcção -Geral de Energia e Geologia
	Direcção -Geral do Consumidor
	Autoridade de Segurança Alimentar e Económica
	Autoridade para as Condições de Trabalho
	Direcção -Geral do Emprego e das Relações de Trabalho
	Instituto de Apoio às Pequenas e Médias Empresas e à Inovação, I P
	Instituto do Turismo de Portugal, I P
	Instituto Português da Qualidade, I P
	Laboratório Nacional de Energia e Geologia, I P
	Instituto da Construção e do Imobiliário, I P
	Instituto Nacional de Aviação Civil, I P
	Instituto da Mobilidade e dos Transportes, I P
	Laboratório Nacional de Engenharia Civil, I P
	Instituto Português de Acreditação, I P
	Instituto do Emprego e da Formação Profissional, I P
	Instituto Financeiro para o Desenvolvimento Regional, I P
	Instituto de Gestão do Fundo Social Europeu, I P
Ministério da Agricultura e do Mar	Secretaria-Geral - SG
	Gabinete de Planeamento e Políticas - GPP
	Direção-Geral de Alimentação e Veterinária - DGAV
	Direção-Geral de Agricultura e Desenvolvimento Rural - DGADR
	Direção-Geral de Política do Mar - DGPM
	Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos - DGRM
	Direção Regional de Agricultura e Pescas do Norte - DRAP do Norte
	Direção Regional de Agricultura e Pescas do Centro - DRAP do Centro
	Direção Regional de Agricultura e Pescas de Lisboa e Vale do Tejo - DRAP de Lisboa e Vale do Tejo
	Direção Regional de Agricultura e Pescas do Alentejo - DRAP do Alentejo
	Direção Regional de Agricultura e Pescas do Algarve - DRAP do Algarve
	Instituto de Financiamento da Agricultura e Pescas, IP - IFAP
	Instituto da Conservação da Natureza e das Florestas, IP - ICNF, IP
	Agência Portuguesa do Ambiente, IP - APA, IPInstituto da Vinha e do Vinho, IP - IVV, IP
	Instituto dos Vinhos do Douro e do Porto, IP - IVDP, IP
	Instituto Nacional de Investigação Agrária e Veterinária, IP - INIAV, IP
	Instituto Português do Mar e da Atmosfera, IP - IPMA, IP
Ministério do Ambiente, Ordenamento do Território e Energia	Secretaria-Geral - SG
	Instituto da Habitação e da Reabilitação Urbana, IP - IHRU, IP
	Entidade Reguladora dos Serviços de Águas e Resíduos
	Conselho Nacional da Água
	Conselho Nacional do Ambiente e do Desenvolvimento Sustentável
	Comissão Técnica do Registo Internacional de Navios da Madeira
	Direção-Geral do Território - DGT
	Comissão de Coordenação e Desenvolvimento Regional do Norte
	Comissão de Coordenação e Desenvolvimento Regional do Centro
	Comissão de Coordenação e Desenvolvimento Regional de Lisboa e Vale do Tejo
	Comissão de Coordenação e Desenvolvimento Regional do Alentejo
	Comissão de Coordenação e Desenvolvimento Regional do Algarve

Ministério da Saúde	Secretaria -Geral
	Inspecção -Geral das Actividades em Saúde
	Direcção -Geral da Saúde
	Serviço de Intervenção nos Comportamentos Aditivos e nas Dependências
	Administração Central do Sistema de Saúde, I P
	INFARMED — Autoridade Nacional do Medicamento e Produtos de Saúde, I P
	Instituto Nacional de Emergência Médica, I P
	Instituto Português do Sangue e da Transplantação, I P
	Instituto Nacional de Saúde Doutor Ricardo Jorge,I P
	Administração Regional de Saúde do Norte, I P
	Administração Regional de Saúde do Centro, I P
	Administração Regional de Saúde de Lisboa e Vale do Tejo, I P
	Administração Regional de Saúde do Alentejo, I P
	Administração Regional de Saúde do Algarve, I P
	Entidade Reguladora da Saúde
Ministério da Educação e Ciência	Secretaria Geral
	Direção Geral do Ensino Superior
	Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais
	Fundação para a Ciência e a Tecnologia
	Estádio Universitário de Lisboa
	Academia das Ciências de Lisboa
	Agência Nacional Proalv
	Direção Geral de Inovação e Desenvolvimento Curricular
	Gabinete Coordenador de Segurança Escolar
	Direção Geral de Recursos Humanos da Educação
	Gabinete de Estatística e Planeamento da Educação
	Gabinete de Gestão Financeira
	Gabinete de Avaliação Educacional
	Gabinete Coordenador do Sistema de informação - MISI
	Direção Regional de Educação do Norte
	Direção Regional de Educação do Centro
	Direção Regional de Educação de Lisboa e Vale do Tejo
	Direção Regional de Educação do Alentejo
	Direção Regional de Educação do Algarve
	Centro Científico e Cultural de Macau, I P
	Agência Nacional para a Qualificação e o Ensino Profissional, I P
Ministério da Solidariedade e Segurança Social	Secretaria-Geral
	Inspecção-Geral do Ministério da Solidariedade e da Segurança Social
	Gabinete de Estratégia e Planeamento
	Direcção-Geral da Segurança Social
	Instituto da Segurança Social, I P
	Instituto de Gestão Financeira da Segurança Social, I P
	Instituto de Gestão de Fundos de Capitalização da Segurança Social, I P
	Instituto Nacional para a Reabilitação, I P
	Casa Pia de Lisboa, I P
	Instituto de Informática, I P
	Conselho Nacional para as Políticas de Solidariedade, Voluntariado, Família, Reabilitação e Segurança Social
	Santa Casa da Misericórdia de Lisboa
	Comissão Nacional de Protecção de Crianças e Jovens em Risco

Ilustração 1 - Tabela orgânica do Estado

Para os efeitos desta Dissertação, importa ainda evidenciar o papel de alguns dos organismos com atribuições nas TIC e na Segurança da Informação da Administração Pública. Assim, ilustra-se ainda, de forma parcial, a estrutura orgânica da Presidência do Conselho de Ministros (PORTAL DA SECRETARIA-GERAL DA PRESIDÊNCIA DO CONSELHO DE MINISTROS, 2013) dando-se enfase à "Agência para a Modernização Administrativa" (AMA), ao "Centro de Gestão da Rede Informática do Governo" (CEGER) e ao "Gabinete Nacional de Segurança" (GNS).

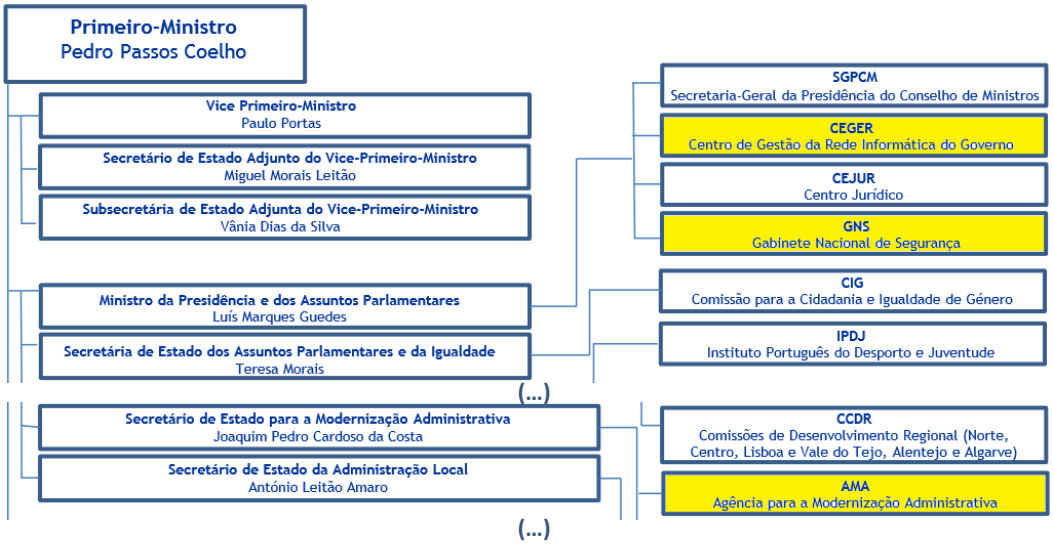


Ilustração 2 - Organograma parcial da Presidência do Conselho de Ministros

A *AMA* tem por missão "*desenvolver, coordenar e avaliar medidas, programas e projectos nas áreas de modernização e simplificação administrativa e regulatória, de administração electrónica e de distribuição de serviços públicos, no quadro das políticas definidas pelo Governo*". A AMA é a responsável pelo projeto da Rede Interministerial das TIC (RCM 109/2009) e pelo Plano Global da Racionalização das TIC na AP (RCM 12/2012) que será abordado mais adiante (AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA, 2012).

O *CEGER* é o organismo "*responsável pela Gestão da Rede Informática do Governo e visa apoiá-la nos domínios das tecnologias de informação e de comunicações e dos sistemas de informação*." Atua em diversas áreas estratégicas das TIC, nomeadamente e no que respeita à segurança, tem a seu cargo a Entidade Certificadora do Estado que providencia a emissão de certificados digitais para Sistemas de Informação de organismos públicos (CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO, 2012).

O *GNS* tem a missão de "*garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exercer a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que actuem no âmbito do Sistema de Certificação Electrónica do Estado - Infra-Estrutura de Chaves Públicas (SCEE)*". É dirigido pela Autoridade Nacional de Segurança que promove a proteção e a salvaguarda da informação classificada (GABINETE NACIONAL DE SEGURANÇA, 2012).

Existem ainda outros organismos com responsabilidades nas TIC e na segurança, no âmbito e abrangência do seu próprio ministério, como são exemplo o Instituto de Gestão Financeira e Equipamentos da Justiça, o Instituto de Informática da Segurança Social e a Entidade de Serviços Partilhados da Administração Pública. Noutros ministérios, estas responsabilidades e competências não se encontram centralizadas num único organismo.

2.1.2. Os Sistemas de Informação na Administração Pública

Por norma, os organismos públicos em Portugal sustentam o seu "negócio" fazendo uso de Sistemas de Informação desenvolvidos para o efeito, bem como recorrendo a produtos de *software* existentes no mercado. Os Sistemas de Informação desenvolvidos por estes organismos, embora sejam muito heterogéneos, constituem muitas vezes, de forma parcial, informação semelhante e que pode ser atualizada a partir dos Sistemas de Informação desenvolvidos por outros organismos. Por esta razão, os sistemas de diferentes organismos têm a necessidade de comunicar frequentemente e de forma autónoma entre eles, partilhando informação pertinente para alimentar os seus processos (exemplo de informação do contribuinte/ beneficiário/ utente /requerente). Na maioria dos casos, esta interoperabilidade imprescindível entre os organismos públicos é efetuada através da Internet, embora também seja praticada por via de redes privadas do Estado, o que reduz o risco de acesso indevido a este tipo de informação. Estas interações não se verificam, na mesma escala, ao nível dos produtos de *software* adquiridos "*as is",* embora possam também existir em casos esporádicos.

Um sistema bastante comum no universo dos organismos do Estado é o Sistema de Informação Contabilístico (SIC).

Este sistema envia dados contabilísticos para o Sistema Central de Contabilidade (SCC) da atual Entidade de Serviços Partilhados da Administração Pública, I. P. (ESPAP) e que é gerido pela Direção Geral do Orçamento.

Os pagamentos enviados para o SCC são submetidos para o Sistema de Gestão do Tesouro (SGT) da Direção Geral do Tesouro (DGT) que, por sua vez, os encaminha (através da SIBS) para a conta do fornecedor (TAVARES, 2007).

Noutro âmbito, para se suportar a aquisição de produtos e serviços no Estado, os organismos públicos contam com a plataforma SaphetyGov, uma ferramenta que promove a contratação pública eletrónica, possibilitando a gestão de todo o processo de contratação de forma simples, segura e transparente (SAPHETY, 2012).

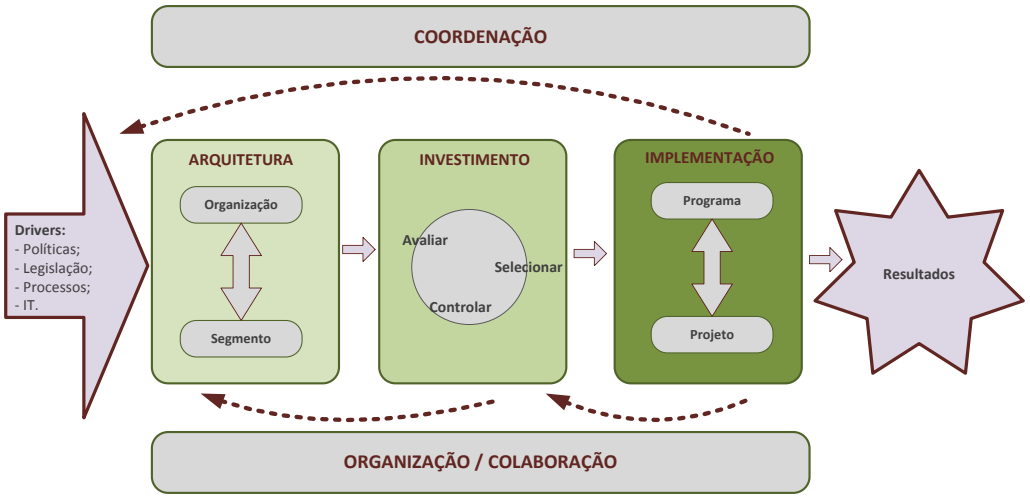
Outro sistema de informação muito importante para o Estado é o Sistema de Informação da Organização do Estado (SIOE). Descreve-se como sendo "*uma base de dados de caracterização de entidades públicas e dos respetivos recursos humanos, com vista a habilitar os órgãos de governo próprios com a informação indispensável para definição das políticas de organização do Estado e da gestão dos respetivos recursos humanos*" (SISTEMA DE INFORMAÇÃO DA ORGANIZAÇÃO DO ESTADO, 2012).

Ao nível de toda a AP, existe também o Sistema Integrado de Gestão e Avaliação do Desempenho na Administração Pública (SIADAP), estabelecido pela Lei 66-B/2007. Este sistema pretende "*contribuir para a melhoria do desempenho e qualidade de serviço da Administração Pública, para a coerência e harmonia da acção dos serviços, dirigentes e demais trabalhadores e para a promoção da sua motivação profissional e desenvolvimento de competências*". É composto por diferentes módulos (1. subsistema de avaliação do desempenho dos serviços, 2. subsistema de avaliação do desempenho dos dirigentes e 3. subsistema de avaliação do desempenho dos trabalhadores) que funcionam de forma integrada e que, no global, se articulam com o sistema de planeamento de cada ministério (GESTÃO INTEGRADA DA AVALIAÇÃO DE DESEMPENHO DA ADMINISTRAÇÃO PÚBLICA, 2012).

Por outro lado, os sistemas Enterprise Resource Planning (ERP) também são um exemplo de ferramentas informáticas utilizadas na administração pública. Compostos por aplicações integradas numa única base de dados, dão suporte, entre outras, às áreas de recursos humanos, financeira, património e gestão documental.

Podem ser extremamente úteis para o dia-a-dia de organizações que estejam frequentemente sujeitas a controlos e legislações específicas, como é o caso dos organismos do setor público.

Todos estes exemplos de Sistemas de Informação da Administração Pública, podem ser esquematicamente observados numa "visão arquitetural global" que nos permite identificar as suas diversas macrocomponentes bem como a respetiva integração entre elas. O esquema apresentado a seguir ilustra essa visão (TAVARES, 2007):



Baseado em: Visão arquitetural dos Sistemas de Informação constante em "O Sistema de Informação das Finanças Públicas: sua evolução e perspectivas de futuro" (TAVARES, 2007)

Ilustração 3 - Visão arquitetural dos Sistemas de Informação

Esta visão arquitetural possibilita aos organismos do setor público olharem para o que existe em termos de Sistemas de Informação, identificarem as funções comuns e específicas de cada, perceberem o que está por implementar e desenvolverem a melhor forma de colaboração e entreajuda.

A evolução dos Sistemas de Informação na Administração Pública foi feita, de uma forma geral, individualmente e sem levar em linha de conta perspetivas de racionalização e de melhores interações para um bem comum. Segundo TAVARES (2007), a falta de coordenação associada à procura de eficiência de cada organismo levou a uma gestão feudal dos sistemas e tecnologias da informação com a criação de verdadeiros silos informacionais. Para que se possa mitigar a existência destes "silos informacionais" e promover a adaptação e interoperabilidade entre os sistemas existentes, visando-se tirar melhor partido da informação que comportam, importa haver infraestruturas de rede apropriadas, tanto ao nível da performance como da segurança, capazes de dar o melhor suporte a estas interligações.

2.1.3. A necessidade das redes na Administração Pública

A existência das redes informáticas no setor público tem, assim, não só o propósito de disponibilizar os serviços e aplicações que suportam o "negócio" dos organismos aos utilizadores dispersos geograficamente (sejam eles colaboradores, parceiros ou utentes), como também de promover a interoperabilidade entre sistemas de organismos públicos, ou entre estes e sistemas de entidades externas. Ou seja, a razão fundamental da necessidade das redes informáticas na AP, não é mais do que a expressão daquilo que se traduz atualmente na forma habitual de se proceder à troca de informação entre partes interessadas – operações *Business-to-Consumer* e operações *Business-to-Business*. A imagem seguinte ilustra estes tipos de interações:

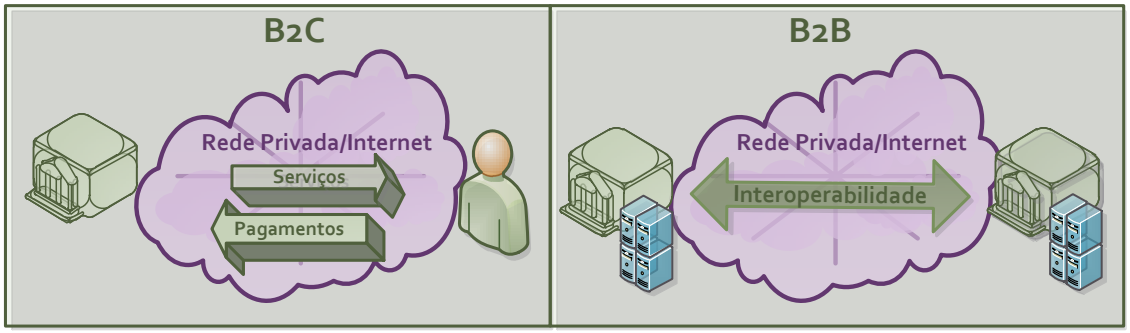


Ilustração 4 - B2C vs B2B

2.1.4. A Segurança nas redes informáticas e a sua importância

Segundo ESTRELA (1998), os requisitos de segurança da informação sofreram duas grandes alterações nas "últimas décadas". A primeira alteração foi relativa à introdução dos computadores e às respetivas necessidades de proteger a informação localmente residente, e a segunda foi referente à introdução das redes (e da computação distribuída) e às respetivas necessidades de proteger a informação em trânsito. Desta forma, acrescentou-se a segurança técnica às seguranças física e administrativa, já existentes até então.

Apesar do longo tempo passado desde esta afirmação, e da constante evolução tecnológica (nomeadamente do aparecimento das redes de alto débito) a importância da segurança nas redes informáticas continua a incidir na demanda pelas melhores formas de proteção da informação residente e da informação em trânsito.

No que respeita em concreto aos organismos públicos, uma vez que grande parte da informação trocada por rede entre eles, ou entre eles e outros intervenientes, tem carácter restrito ou confidencial (embora na maioria dos casos a informação não esteja formalmente classificada), as formas de proteção das infraestruturas de rede assumem um papel determinante.

Em primeira análise, o que a boa prática demarca, é que os sistemas e a LANs dos organismos do Estado que disponibilizam serviços para a rede devem estar devidamente protegidos e segregados. Tendo isto em conta, e com base no valor dos ativos para o negócio dos organismos (tais como a própria Informação que tem uma importância chave), um dos papéis fundamentais das áreas do IT no que concerne às redes, reside na avaliação e definição de agrupamentos de recursos que partilhem o mesmo grau de risco aceitável, bem como na análise se esses agrupamentos estão bem constituídos. Isto é, levar a cabo um processo, suportado nos requisitos de negócio (como a criticidade da informação, os níveis de serviço que são necessários oferecer, questões de conformidade com legislação, questões relacionadas com o custo da perda, etc), que implemente e delimite as chamadas zonas de segurança.

Esta segregação das redes, após a fase de desenho e na sua implementação é, por norma, realizada com o recurso a *firewalls* (ou outro equipamento com capacidade de *layer 3* e que faça filtragem de pacotes) que deverão ter regras de acesso tão estreitamente afinadas quanto possível. A figura seguinte ilustra um exemplo de uma rede local segregada em diversas zonas/ domínios de segurança:

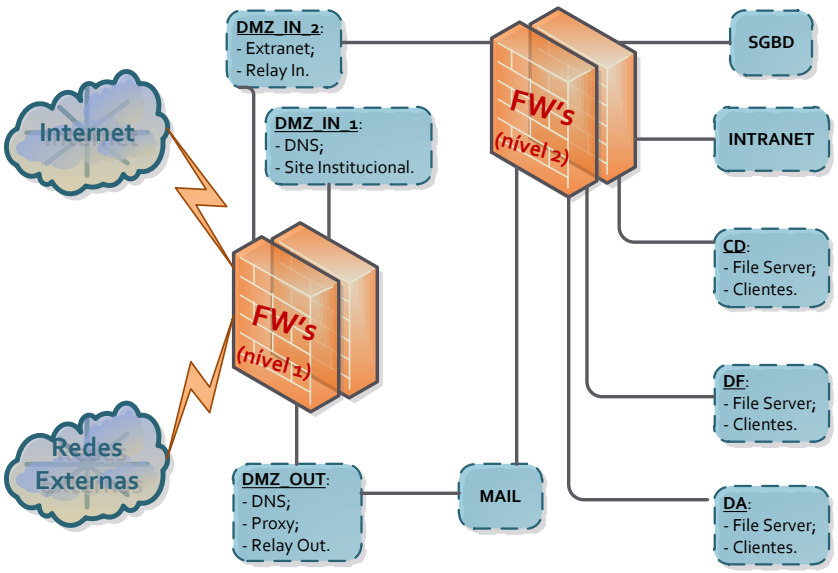


Ilustração 5 - Segregação da rede em zonas de segurança

Importa referir que a segurança destas redes informáticas não se deve basear apenas na defesa de perímetro que a figura demonstra, mas também, e com recurso a outro tipo de mecanismos, deve ser complementada com uma defesa em profundidade inerente ao interior de cada domínio de segurança segregado. Com a defesa em profundidade, utilizando-se vários controlos de forma encadeada, é possível criar-se e manter-se infraestruturas de rede com um cariz mais resiliente (ZÚQUETE, 2008).

Por outro lado, a segurança das *WAN's* que interligam os vários edifícios dos organismos públicos, apresenta um carácter igualmente importante. Para se proteger a confidencialidade e a integridade da informação que circula nestas redes deve-se recorrer a mecanismos que contemplem cifra e autorização (como as *Virtual Private Networks*).

Estes mecanismos poderão ser proporcionados pelos operadores de telecomunicações que disponibilizam os circuitos, ou poderão ser disponibilizados pelos próprios organismos com tecnologia apropriada nas *gateways* ou noutros equipamentos existentes para o efeito.

Para se garantir os níveis de serviço necessários aos sistemas de cada organismo, promovendo-se a disponibilidade da informação adequada a cada situação, deve-se recorrer à melhor forma de redundância para cada caso (de circuitos e de equipamentos), sempre que esta seja necessária.

Estas preocupações básicas de segurança visam a mitigação do risco e da exposição dos organismos do Estado às mais diversas ameaças (que têm crescido consideravelmente nos últimos tempos) sempre que estes disponibilizam serviços e aplicações nas redes de dados, sejam elas públicas ou privadas.

2.1.5. Conceito de Vulnerabilidades, Ameaças, Risco e Contramedidas (Controlos)

No que à Segurança dos Sistemas de Informação diz respeito, Vulnerabilidades são fragilidades na informação ou nos sistemas, de origem humana, processual ou tecnológica, que podem vir a ser exploradas por ameaças internas ou externas. Ameaças são quaisquer circunstâncias ou eventos com o potencial impacto negativo sobre a confidencialidade, integridade ou disponibilidade da informação ou dos sistemas de informação (GREGORY, 2010).

O Risco representa a probabilidade de uma ameaça específica poder comprometer a informação ou os sistemas de informação através da exploração de uma vulnerabilidade, expressando-se num determinado impacto negativo.

Desenvolver estratégias para o gerir ajuda no estabelecimento e na validação da eficácia dos mecanismos de segurança e importa, por isto, ser um processo que esteja sempre presente no seio dos organismos públicos. Estas estratégias podem ir no sentido de se transferir, evitar, reduzir ou mesmo aceitar o risco. A gestão da segurança terá de contemplar a identificação dos ativos, a documentação e implementação de políticas e procedimentos, bem como mecanismos verdadeiramente capazes de garantir a confidencialidade, integridade e disponibilidade da informação. (GREGORY, 2010)

Sendo o conceito de Controlos associado a um conjunto de políticas, de procedimentos, de tecnologias, de *software* ou de estruturas implementadas para reduzir o risco de uma ameaça se concretizar, é também importante que sejam devidamente avaliados e implementados nas infraestruturas de rede do Estado, para que se possa garantir um nível de segurança nos seus ativos tão rigoroso quanto possível. A imagem seguinte evidencia as componentes da gestão do risco, refletindo a importância dos controlos de segurança.

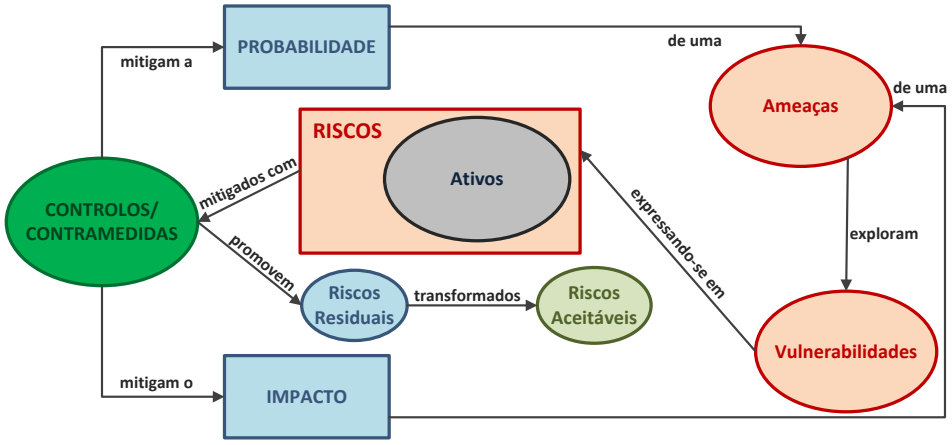


Ilustração 6 - Componentes da Gestão do Risco

Da figura, pode-se aferir que os controlos servem para mitigar a probabilidade ou o impacto de determinada ameaça poder explorar uma vulnerabilidade, concretizando-se num risco sobre um ou mais ativos.

A melhoria contínua (e a forma de se avaliar/ afinar constantemente as contramedidas ou acrescentar outras) promove a evolução dos Riscos inicialmente existentes para Riscos Residuais e, por sua vez, para Riscos Aceitáveis.

2.1.6. Tipificação dos Controlos

Como já foi referido, os controlos são mecanismos de extrema importância para se poder conter e gerir o risco. São seus sinónimos os conceitos de "Contramedidas" ou de "Medidas de Segurança".

Segundo o SANS Institute num documento relativo aos controlos críticos para a ciberdefesa, o objetivo dos controlos é proteger os ativos críticos, a infraestrutura e a informação, fortalecendo a postura defensiva das organizações através da proteção automatizada e monitorização contínua das tecnologias da informação, reduzindo assim os seus comprometimentos, os esforços de recuperação, e todos os respetivos custos associados. Neste sentido, a prevenção é o ideal, mas a deteção é imprescindível (SANS, 2013).

Os controlos podem ser tipificados em duas principais dimensões: em relação ao objetivo da sua existência (o que o controlo faz) ou em relação à forma como é implementado (como o controlo é).

Em relação à primeira dimensão, os controlos podem ser do tipo preventivo, detetivo ou corretivo (embora muitas vezes também se utilize o conceito de controlo de recuperação, quando se pretende recuperar de um incidente). Os controlos preventivos são os que previnem a concretização das ameaças, reagindo às mesmas e apresentando por vezes também um carácter inibidor.

Os controlos detetivos detetam a ocorrência de ameaças apenas quando estas estão a decorrer; Tentam detetar atividade anómala e responder de alguma forma possível, podendo essa resposta passar pela exibição de *logs* numa consola ou por cancelar uma ligação de rede decorrente da escuta de tráfego (ERICKSON, 2008).

Os controlos corretivos visam a recuperação da integridade, disponibilidade ou confidencialidade da informação ou dos SI, após se ter concretizado uma ameaça; Podem também vir a servir para a investigação de causas de risco.

No que respeita à segunda dimensão, podemos tipificá-los em controlos administrativos, físicos ou técnicos. Os controlos administrativos são aqueles que promovem as bases da segurança, essencialmente ligados a procedimentos de atuação, especificando os fatores humanos da segurança.

Controlos físicos, como o nome indica, são as medidas de segurança aplicadas a infraestruturas físicas a fim de se evitar, identificar ou de se conter acessos não autorizados.

Por sua vez, os controlos técnicos utilizam a tecnologia como suporte para se mitigar o risco, sendo muito diversificados e abrangentes nas suas implementações (INFORMATION SECURITY HANDBOOK, 2012).

Apesar de existirem estas tipificações de controlos para os agruparmos e melhor se perceber quais os seus objetivos e as suas formas de implementação, importa referir no entanto que, em alguns dos casos, os controlos podem ser simultaneamente associados a vários tipos, na medida em que apresentam objetivos de existência múltiplos (para prevenir, detetar ou corrigir o risco) ou, por outro lado, podem ser disponibilizados/ implementados em diversas formas (administrativa, física ou tecnológica).

A tabela apresentada de seguida enquadra nesta tipificação alguns dos exemplos mais comuns de controlos de segurança.

	ADMINISTRATIVOS	FÍSICOS	TÉCNICOS
PREVENTIVOS	- Sensibilização e treino dos colaboradores; - Segregação de funções; - Classificação da informação; - Plano de Continuidade do negócio.	- Câmaras de vigilância; - Porteiros e vigilantes; - Portas blindadas; - Controlos biométricos em portas.	- Criptografia (e VPN's); - Autenticação; - ACL's; - VLAN's (e proteções Layer2); - Firewall's; - Sistemas IDS/IPS; - Sistemas DLP; - Antivírus.
DETETIVOS	- Checklists de verificação de conformidade; - Auditorias a processos.	- Alarmes térmicos ou de movimento; - Câmaras de vigilância; - Inspeções à infraestrutura física.	- Sistemas IDS/IPS; - Software de auditoria; - Logs de acesso a sitemas; - Antivírus; - Auditorias à rede e testes de intrusão.
CORRETIVOS	- Planos de recuperação; - Procedimentos de atuação após concretização de acidente de segurança nos SI.	- Porteiros e vigilantes.	- Backups para recuperação posterior a um incidente; - Antivírus.

Ilustração 7 - Exemplos de Controlos

Pode constatar-se que, por exemplo, os sistemas IDS/IPS, uma vez que atualmente já são mecanismos de segurança integrados, representam controlos do tipo técnico e, simultaneamente, preventivo e detetivo.

Os sistemas de Antivírus podem também ser controlos técnicos do tipo preventivo, detetivo e corretivo, na medida em que previnem a entrada de *malware* no sistema, detetam-no no caso de o sistema já estar comprometido e removem-no automaticamente se a base de dados de assinaturas estiver devidamente atualizada. Por outro lado, pode-se também afirmar que sistemas de biometria associados a segurança física poderão representar simultaneamente controlos preventivos do tipo físico e técnico, uma vez que previnem acessos físicos ilegítimos, recorrendo a tecnologia para o efeito.

2.2. ANÁLISE DA SITUAÇÃO ATUAL

2.2.1. As redes de dados da Administração Pública e a sua evolução

O desenvolvimento das redes de dados na Administração Pública seguiu, de forma geral, o padrão evolutivo da realidade nacional. Com o crescimento dos organismos públicos nos últimos anos, incrementando-se o nº de colaboradores e de delegações (muitas vezes de longa distância à sede), bem como com a modernização e informatização dos seus processos de negócio, foi também fomentada a sua adequação ao nível das redes de comunicações. Desta modernização foi então resultando, à medida que os anos corriam, um crescente gerar de informação dos mais variados tipos, com necessidade de ser acedida por parceiros e por colaboradores dispersos geograficamente. As redes de dados no Estado tiveram e continuam a ter, cada vez mais, um papel determinante na disponibilização dessa informação. No entanto, para um estabelecimento tão assertivo quanto possível destas infraestruturas de rede (*WAN's*), levando em conta a especificidades tecnológicas e as necessidades concretas dos organismos públicos, deveriam ter sido sempre consideradas questões capazes de fazer antever o impacto após a sua implementação.

VACHON e GRAZIANI (2008) sugerem as seguintes reflexões para ajuda à tomada de decisão:

- ✓ Qual o propósito e âmbito geográfico da rede?
- ✓ Quais os requisitos reais de tráfego?
- ✓ O meio de transmissão mais adequado é público ou privado?
    - Sendo privado, deveria ser dedicado ou *switched*?
    - Sendo público, qual o tipo de VPN mais adequado?
- ✓ Que opções de conectividade estão disponíveis nos locais em causa e quais os custos?

Dada a importância desta análise prévia e assumindo a forma de complemento com ênfase na segurança, entende-se também pertinente a consideração das questões abaixo:

- ✓ Qual a latência admissível para o tráfego dos sistemas em causa?
- ✓ Existe necessidade de *QoS* na rede?
- ✓ Qual a classificação da informação a circular na rede?
- ✓ Que mecanismos de segurança deveriam salvaguardar os ativos dos organismos nestes circuitos?

Em termos de topologias utilizadas, os organismos do Estado foram constituindo desenhos de rede relativamente homogéneos.

Tendo em conta o conhecimento empírico do autor decorrente da experiencia profissional neste âmbito, é possível afirmar que os organismos públicos, com as suas redes locais (*LAN's*) previamente definidas em edifícios dispersos, apresentavam em regra, os "Centros de Informática" e toda a disponibilização de serviços centralizados num edifício específico, o que potencializou a utilização generalizada de topologias do tipo "*Star"*.

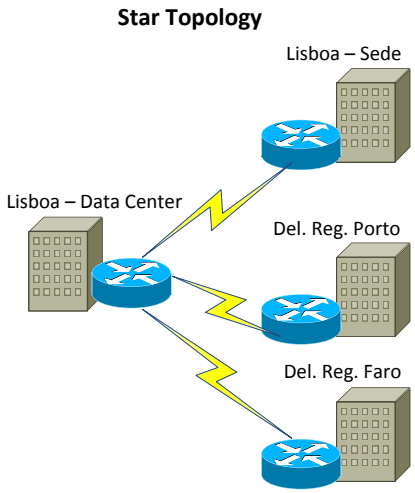


Ilustração 8 – Exemplo de topologia "Star"

Contudo, a experiência foi demonstrando que, para se fazer face a adversidades e eventuais quebras de circuitos que poderiam vir a comprometer processos de negócio, seria conveniente haver caminhos alternativos para o tráfego de informação que proporcionassem redundância e, assim, acréscimo de disponibilidade.

Foi então com o intuito da redundância de acessos que alguns dos organismos optaram por topologias do tipo *"Partial-Mesh"* ou mesmo *"Full-Mesh"*.

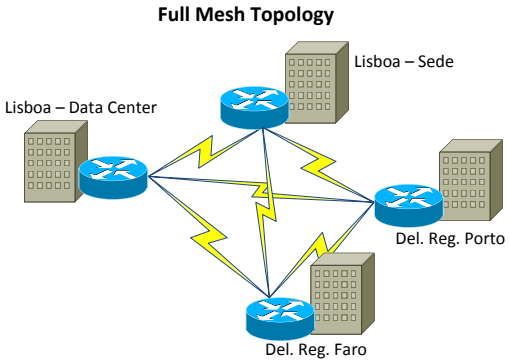


Ilustração 9 – Exemplo de topologia "Full Mesh"

Como estas alternativas implicavam um aumento significativo de custos de comunicações, não se expressaram de forma generalizada nos organismos do setor público.

Ao nível das tecnologias de implementação das soluções *WAN*, os circuitos de comunicações podem variar essencialmente entre ligações dedicadas, ligações do tipo *circuit-switched*, ligações do tipo *packet-switched* e ligações *VPN* Internet. Em ligações dedicadas, um *link* ponto a ponto entre a origem e o destino é estabelecido através da rede do operador. Nas ligações do tipo *circuit-switched*, antes da comunicação poder ser efetuada, é necessário pré-estabelecer-se uma conexão *dialup*, através da rede do operador, entre a origem e o destino (exemplo do *PSTN* e do *ISDN*). Nas redes do tipo *packet-switched*, os dados são transmitidos em *frames*, *cells* ou pacotes e é possível partilhar-se largura de banda com outras entidades a fim de se poupar custos (exemplo do *FR*, *X.25* e *ATM*). As ligações *VPN* Internet utilizam cifra na rede pública para se proceder à troca de informação entre os diferentes locais (exemplo do teletrabalho).

Os organismos do setor público, dentro das suas variadas necessidades ao longo do tempo, foram fazendo uso dos diversos tipos de soluções *WAN* existentes. Como apresentado por VACHON e GRAZIANI (2008), as diversas opções de ligações *WAN* podem ser agrupadas conforme ilustrado no esquema seguinte.

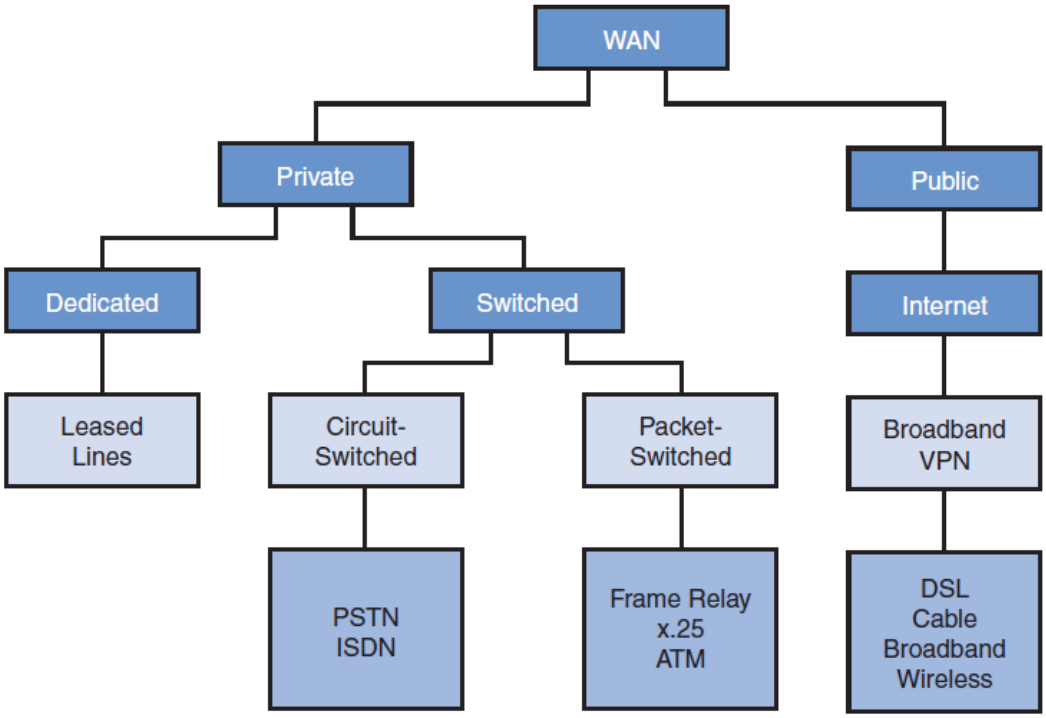


Ilustração 10 - Tipos de ligações WAN

As redes de comunicações que inicialmente existiam exclusivamente com o intuito da transmissão de voz (onde centrais telefónicas encaminhavam o tráfego), foram progressivamente dando lugar a redes com tecnologias *WAN* capazes de suportar adequadamente comutação de voz, dados e vídeo. O meio físico utilizado para as comunicações de dados era assim o cobre usado para a transmissão de voz, sendo apenas mais tarde preparadas infraestruturas específicas para o tráfego de dados, embora apresentando altos custos operacionais. Foi então que surgiu uma multiplicidade de tecnologias de comutação de dados, com base em padrões internacionais do *Data-Link layer*, com o principal objetivo de promover o multisserviço num único meio de comunicações.

Em meados dos anos 80, as poucas comunicações de dados utilizadas nos organismos do setor público faziam, em grande parte, uso do protocolo X.25. Com as ligações da rede analógica a fazerem uso do X.25 era possível criarem-se circuitos virtuais estabelecidos através de um circuito físico, destinando-se os pacotes das requisições a um endereço específico. O SVC (Switched Virtual Circuit) seria identificado por um número de canal e os pacotes de dados relacionados com esse número de canal seriam enviados para o endereço correspondente. Múltiplos canais podiam estar ativos numa única conexão (VACHON, GRAZIANI, 2008).

Com alguma frequência, era possível constatar que organismos do Estado utilizavam durante a década de 90 circuitos dedicados para estabelecerem ligações ponto a ponto com os seus *sites* remotos ou mesmo com outras entidades. Estes circuitos eram bastante dispendiosos e o seu custo era essencialmente "indexado" à largura de banda utilizada e à distância entre os locais. Redes com um nº de *sites* considerável, geograficamente dispersos e com uma boa performance em termos de débito, apresentavam custos muitas vezes incomportáveis para os organismos. Contudo, em determinadas situações que apresentassem exigências relacionadas com latência e *jitter*, os benefícios de um circuito dedicado poderiam justificar os seus custos. Um circuito dedicado do tipo E3 é o standard em Portugal (e na Europa) e consegue atingir débitos na ordem dos 34,064 Mbps.

Sempre que se pretendia transmissões de dados sem grandes necessidades de volume de tráfego e a custos acessíveis, os organismos recorriam ao uso de linhas de *dialup* de 56Kbps. Em transmissões deste tipo, os respetivos modems analógicos modulavam os dados binários na origem para um sinal analógico e faziam o processo contrário no destino.

Posteriormente apareceu o *ISDN* (Integrated Services Digital Network) que também fazia uso do mesmo cobre das comunicações telefónicas, mas conseguindo atingir melhores débitos, com base na conversão do meio físico em conexões digitais TDM (*time-division multiplexed*). Existem 2 tipos de interfaces *ISDN*; o *Basic Rate Interface* (BRI) que disponibiliza 2 canais do tipo B de 64Kbps e 1 canal do tipo D de 16Kbps, e o *Primary Rate Interface* (PRI) que disponibiliza 30 canais do tipo B de 64Kbps e 1 canal do tipo D de 16Kbps. Para transmissões que não exigiam grande largura de banda, o ISDN BRI podia fornecer uma conexão ideal. O BRI possibilitava um tempo de estabelecimento da chamada inferior a 1 segundo e os canais do tipo B proporcionavam capacidade superior à de uma ligação analógica. Sempre que fosse necessária maior capacidade, um segundo canal do tipo B poderia ser ativado, proporcionando um débito de 128 Kbps. Este tipo de circuitos, embora ainda inadequado para transmissões de vídeo, proporcionava para além do tráfego de dados, a possibilidade de várias comunicações de voz em simultâneo e muitas vezes podiam servir de circuitos de backup para as linhas dedicadas (VACHON, GRAZIANI, 2008). Ainda hoje é comum ver-se estas implementações em alguns organismos públicos. Com soluções do tipo PRI, já era possível disponibilizar-se videoconferência e transmissões mais exigentes, embora a existência de várias ligações (canais B) fosse equivalente a elevados custos nas grandes distâncias.

Ainda nos anos 90 foi introduzido o *Frame Relay* em Portugal.

Este protocolo sucessor e melhorado do X.25, que é uma especificação de alta performance dos *layers* 1 e 2 do modelo OSI, chega a atingir débitos na ordem dos 45Mbps. Revelou-se numa importante e vantajosa alternativa aos circuitos dedicados para os organismos públicos, na medida em que conseguiu fazer baixar significativamente os custos das comunicações, aumentando ainda a performance nas mesmas. Segundo LAMMLE (2007), o *Frame Relay* permite a criação de redes *mesh* eficientes:

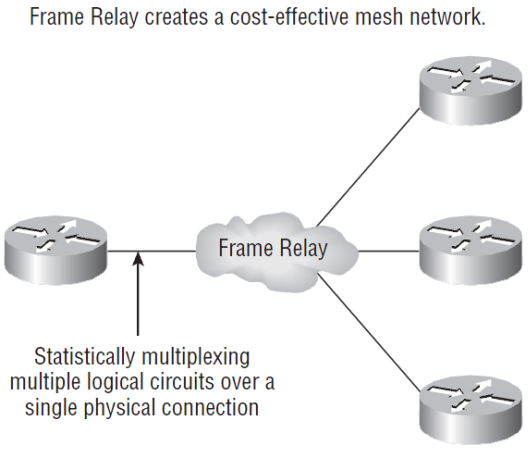


Ilustração 11 - Frame Relay

Por sua vez, a tecnologia *Asynchronous Transfer Mode* (ATM) foi criada para dar a melhor resposta ao tráfego sensível ao tempo, através de redes privadas ou públicas. Isto é, providencia a transmissão em simultâneo adequada de voz, vídeo e dados. Uma vez que o IP é a base da Internet mas não disponibiliza capacidade de qualidade de serviço no encaminhamento e gestão de tráfego mais exigente, surgiram as redes ATM como forma de suprimir essa necessidade. O ATM utiliza uma arquitetura baseada em células (em vez de *frames*) que têm um tamanho fixo de 53 bytes, 5 dos quais para o *header* e 48 de *payload*. Esta arquitetura de células pequenas e de comprimento fixo é a ideal para o transporte de tráfego intolerante a *delay*, como o caso da voz e do vídeo (VACHON, GRAZIANI, 2008). É um tipo de tecnologia muito utilizado em serviços de IPTV, não se tendo expressado significativamente em implementações nos organismos públicos; tipicamente, as mais comuns ligações *Frame Relay* são em grande parte executadas sobre tecnologia ATM (LAMMLE, 2007).

O *Multiprotocol Label Switching* (MPLS) é o grande sucessor do *Frame Relay*. Introduzido em força a meio da década passada, foi nos últimos anos generalizado na maioria das empresas portuguesas e, em particular, nos organismos públicos que têm vindo a migrar progressivamente as suas *WAN's* para esta tecnologia.

Uma vez que a tecnologia ATM apresentava alguns problemas de escalabilidade, o MPLS é exposto como representando melhorias dos métodos de encaminhamento de pacotes, fazendo uso de rótulos de comprimento fixo associados a pacotes IP, a células ATM ou a *frames*. Os rótulos são embutidos entre o *header* do *layer* 3 e do *layer* 2 no caso de tecnologias de encaminhamento baseadas em *frames*, ou embutidos nos campos VPI/VCI no caso de tecnologias baseadas em comutação de células. A sua principal vantagem recai assim no facto de poder ser utilizado em qualquer meio e em qualquer camada que possa transmitir dados (NAKAMURA, 2009). Os operadores de telecomunicações têm dado relevo às vantagens inerentes ao MPLS junto dos seus clientes e têm definido preços inferiores aos habitualmente praticados com o *Frame Relay*.

Existem ainda alternativas económicas caracterizadas por VPN's que fazem uso da conetividade à Internet para interligar *sites* remotos. Estas opções, estabelecem comunicações cifradas entre redes privadas através da rede pública e, em vez de utilizarem conexões de *layer* 2, utilizam ligações virtuais denominadas túneis que fazem o roteamento (*layer* 3) entre a rede privada do organismo e o *site* remoto. Estas comunicações podem ser estabelecidas com recurso a VPN's do tipo *Site-to-Site* que interligam redes privadas distintas, ou com recurso a VPN's do tipo *Remote-Access* que permitem a ligação entre diversos *hosts* remotos e a rede privada (onde reside um concentrador/ coletora de VPN's). As principais vantagens das *Virtual Private Networks* (VPN) são enunciadas abaixo (VACHON, GRAZIANI, 2008).

- ✓ Poupança de custos em relação a outras opções – Porque possibilitam o uso da Internet para ligação remota entre *sites* e/ou *users*, eliminando a necessidade do uso de tecnologias WAN mais onerosas;
- ✓ Segurança – Porque fazem uso de encriptação avançada e de protocolos de autenticação que as protegem dos acessos não autorizados aos dados;
- ✓ Escalabilidade – Porque utilizam a infraestrutura de Internet dos ISP's, sendo fácil a adição de utilizadores ou de mais capacidade sem necessidade de alterar de forma significativa a infraestrutura.
- ✓ Compatibilidade com tecnologia de banda larga – porque é independente do meio físico, pode fazer uso de tecnologias de acesso como DSL, cabo ou fibra-ótica.

Principalmente devido a estas vantagens e à conjuntura de contenção de custos e otimização de recursos, nos dias que correm a generalidade dos organismos públicos procede a contratações de WAN's com tecnologias VPN.

Com a massificação do meio físico em fibra ótica no panorama nacional, estas VPN's assentam hoje em dia essencialmente neste tipo de cablagem, embora se verifique em muitos casos, quer por constrangimentos técnicos/geográficos (quando a infraestrutura de fibra não chega a determinadas localidades), quer por questões de custo-benefício (quando as transmissões não são tão exigentes), a existência de VPN's com base noutras tecnologias de banda larga, nomeadamente com base nas linhas telefónicas de cobre utilizadas no xDSL. A imagem seguinte exemplifica a rede de área alargada de um organismo público (à data de Maio/2013) composta por duas VPN's MPLS e duas ligações à Internet centralizadas e redundantes.

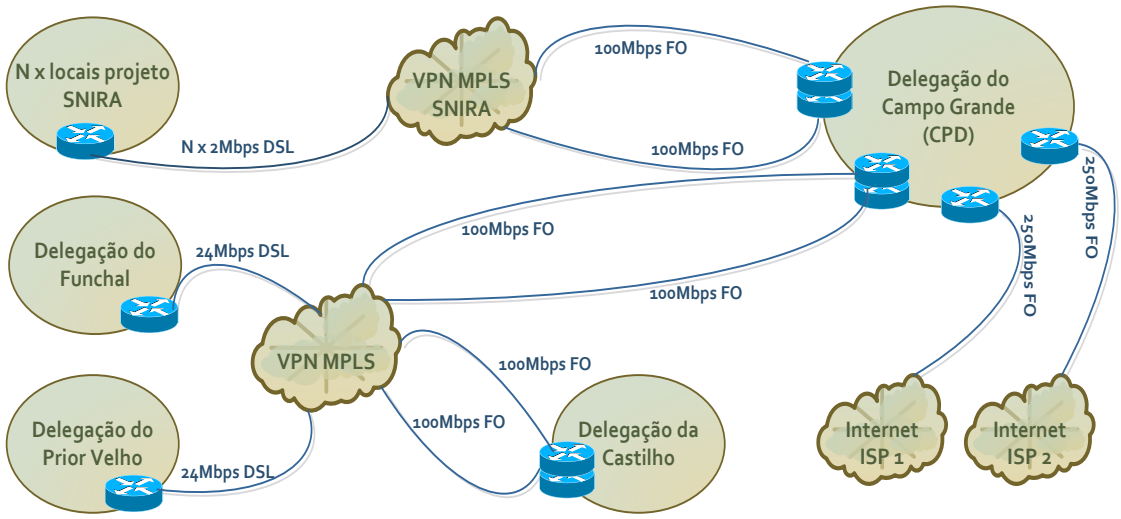


Ilustração 12 – Exemplo de uma rede de um Organismo Público (IFAP)

2.2.2. Ameaças significativas nos dias que correm

Existem bastantes tipos de ataques associados aos Sistemas de Informação e múltiplas formas de serem levados a cabo. Para simplificar a sua identificação, alguns autores classificam estas ameaças em categorias/ classes e, embora se denotem ligeiras diferenças de nomenclatura, em termos de conteúdo os conceitos transmitem a mesma mensagem.

Segundo SANTOS (2007) e RODRIGUES (2010), podemos categorizar os ataques às redes/ sistemas de informação da seguinte forma:

- ✓ **Interceção** – Representa o acesso não autorizado (pessoa, programa ou equipamento) a um recurso; Constitui uma ameaça à confidencialidade da informação. Exemplo: intercetar mensagens confidenciais de outrem na rede.

- ✓ **Interrupção** – Representa a negação de acesso a um recurso (por inoperacionalidade ou impedimento propositado); Constitui uma ameaça à disponibilidade da informação. Exemplo: corte de uma linha de comunicações.
- ✓ **Modificação** – Representa a alteração não autorizada das propriedades de um recurso; Constitui uma ameaça à integridade da informação. Exemplo: adulterar pacotes de dados a circular na rede.
- ✓ **Fabricação** – Representa a adição não autorizada de elementos à rede/ sistema de informação; Constitui uma ameaça à autenticidade da informação. Exemplo: adicionar registos falsificados numa Base de Dados.

Apesar destes tipos de classificação, os ataques a redes e sistemas apresentam-se cada vez mais complexos, integrados e combinados, dificultando o seu posicionamento num destas categorias. No fundo, o ataque propriamente dito pode ser constituído por vários ataques de menor dimensão e com um âmbito muito específico, contribuindo globalmente para a obtenção do sucesso nos objetivos do atacante.

Os anos de 2011 e 2012 foram particularmente difíceis para os organismos públicos em diversos âmbitos, nomeadamente no que diz respeito a ataques de *hackers* e à exploração de algumas vulnerabilidades ao nível das tecnologias e dos sistemas de informação. O descontentamento social generalizado e a facilidade de execução de técnicas de ataque e de acesso às ferramentas para o efeito, contribuíram de forma determinante para a evolução desfavorável desta situação.

Diversas notícias de ataques a sistemas de organismos públicos (e também de partidos políticos) foram neste período publicadas nos órgãos de comunicação social e em *blogs* na Internet.

A grande maioria dos ataques executados não detinha grande grau de complexidade, apresentando com frequência a forma de *Denial of Service* ou *SQL Injection* simples. O jornal Diário de Notícias em artigo de 05/12/2011 reforça esta ideia, referindo que "*o coordenador do Vigilis, que avalia o nível de segurança da Internet portuguesa, considerou hoje que os ataques até agora realizados pelos piratas informáticos são fáceis de ser executados*" (DIÁRIO DE NOTÍCIAS, 2011).

Um ano mais tarde, a Lusófona Online Conteúdos (LOC) na sua publicação de 14/12/2012, citando o Diretor do CEGER Manuel Honorato, refere que "*Portugal é, em 2012, um dos países mais atrasados nesta matéria*", que dá como exemplo as 30 tentativas de invasão que acontecem por minuto à rede informática do governo.

Manuel Honorato complementa ainda que "*o país tem, por isso, de se adaptar aos novos cenários de ameaça e aos novos conceitos de segurança*." A partilha desta opinião é também expressada neste artigo pelo tenente-coronel Viegas Nunes do Estado-Maior do Exército, segundo o qual "*os padrões de segurança atuais não estão aptos para esta nova realidade digital*" (LUSÓFONA ONLINE CONTEÚDOS, 2012).

Uma vez que os atacantes estão sempre um passo à frente de quem defende os sistemas, é assim imperativo compreender-se ao detalhe como são lançados os ataques e quais as suas especificidades, por forma a ser possível desenvolverem-se controlos para se evitar ou travar atempadamente o impacto negativo destas ameaças nos ativos dos organismos.

O relatório de segurança anual da SOPHOS (2011) deu particular ênfase a ameaças como o Hacktivismo, o *Malware* (explicitando o Conficker), as botnets e o spam, os ataques online, fragilidades dos sistemas operativos e riscos específicos nos locais de trabalho, tais como questões relacionadas com a mobilidade, as redes sociais e a *cloud*.

Por sua vez, os relatórios trimestrais da MCAFEE (2012) sobre as ameaças mais significativas respeitantes a 2012, incidiram especialmente sobre os ataques nos dispositivos móveis, o *malware*, o *spam*, as botnets, os ataques de rede, as ameaças Web, o Cybercrime e o Hacktivismo.

A European Network and Information Security Agency, num "*Theat Landscape*" de 28/09/2012 respeitante ao panorama europeu, faz uma associação extremamente interessante e de análise pertinente. Enquadra o top das ameaças nas tendências tecnológicas correntes e emergentes, espelhando a previsão da sua evolução conforme o quadro abaixo (ENISA, 2012).

Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Ilustração 13 - ENISA: Threat Landscape - Ameaças e Tendências

A ENISA realça ainda a ação dos agentes das ameaças e espelha as suas principais associações com as mesmas. O quadro seguinte ilustra esse mapeamento (ENISA, 2012).

	Threat Agents					
	Corporations	Cybercriminals	Employees	Hacktivists	Nation states	Terrorists
Drive-by exploits		✓				✓
Worms/Trojans		✓			✓	✓
Code Injection		✓		✓		✓
Exploit kits		✓				
Botnets	✓	✓		✓		✓
Denial of service		✓		✓	✓	✓
Phishing attacks		✓				
Compromising confidential information	✓	✓	✓	✓	✓	✓
Rogueware / Scareware		✓			✓	
Spam	✓	✓				
Targeted attacks	✓	✓			✓	✓
Physical Theft / Loss / Damage	✓	✓	✓		✓	✓
Identity theft	✓	✓	✓		✓	
Abuse of Information Leakage	✓	✓	✓	✓	✓	✓
Search Engine Poisoning	✓	✓				
Rogue certificates		✓			✓	

Ilustração 14 - ENISA: Threat Landscape - Relação ameaças vs agentes

No que diz exclusivamente respeito a previsões de ameaças para o ano de 2013, a Symantec dá enfase no seu *site* às seguintes tendências (SYMANTEC, 2012):

1. O cyber-conflito será recorrente;
2. O *ransomware* será o novo *scareware*;
3. O *madware* vai contribuir para a insanidade;
4. As redes sociais vão constituir novos perigos;
5. À semelhança dos utilizadores, também os atacantes irão aderir à mobilidade e à *cloud*.

No mesmo âmbito, a empresa de segurança Websense apresenta no seu relatório de segurança para 2013 as seguintes previsões (WEBSENSE, 2013):

1. Os ataques continuarão a incidir sobre plataformas Web;
2. Mais ameaças multiplataforma a incidir sobre dispositivos móveis;
3. As lojas legítimas de aplicações para dispositivos móveis vão alojar mais *malware*;
4. Os incidents inerentes ao hacktivismo vão diminuir;
5. Os ataques patrocionados por governos vão aumentar;
6. As ameaças tornar-se-ão mais "virtual aware";
7. As ameaças de Email vão evoluir para novos níveis.

Por sua vez, no relatório da Mcafee referente às previsões de ameaças para 2013, realçam-se as seguintes opiniões de tendências (MCAFEE, 2013):

1. *Worms* em dispositivos móveis que provocam a compra de outras aplicações maliciosas e promovem roubos às vítimas;
2. *Malware* que bloqueia os updates de segurança nos dispositivos móveis;
3. Kits de *ransomware* que proporcionam que criminosos sem grandes capacidades de programação possam extorquir pagamentos;
4. Ataques persistentes e dissimulados incidirão sobre o Windows;
5. Irá existir um desenvolvimento rápido de formas de atacar o Windows 8 e o HTML5;
6. Ataques em larga escala como da *Stuxnet* com o intuito de destruir a infra-estrutura em detrimento de extorquir dinheiro;
7. Outros ataques do tipo dos lançados das botnet's "Zeus", que fazem uso do *trojan* "Citadel", dificultarão o papel dos produtos de segurança;
8. *Malware* que renova as conexões mesmo após o desmantelamento das botnets, permite que as infeções continuem a crescer;
9. Spam SMS de smartphones infetados;
10. "Hacking as a Service": Vendedores e compradores anónimos partilham kits de *malware* e praticam serviços deste tipo em troca de dinheiro, negociando através de fóruns para o efeito;
11. A atividade dos hacktivistas Anonymous será mais reduzida mas dará lugar a atividade de grupos politicamente mais comprometidos e/ou extremistas;
12. Nações e exércitos serão mais frequentemente agentes e vítimas de ameaças cibernéticas.

Tendo em conta os principais ataques sucedidos recentemente, em especial os ocorridos em sistemas de organismos públicos, bem como os tops das previsões enunciados por entidades credenciadas, serão caracterizadas as ameaças que se entende mais prementes e que devem ser alvo de maior atenção e acompanhamento pelos organismos para que se possa evitar, dentro do possível, a potencial exploração das vulnerabilidades inerentes às suas infraestruturas.

a. Penetração em redes

Um ataque concertado de penetração ilegítima em redes e sistemas resulta da combinação de diversas técnicas. Tipicamente, a anatomia de um ataque de penetração segue um processo composto por várias fases com objetivos parciais distintos que, na sua combinação, visam um objetivo comum que pode ser expressado, por exemplo, num simples ataque de negação de serviço ou no roubo de informação crítica para o negócio. Esse processo é ilustrado na figura abaixo e descrito em seguida (BARRETO, 2009).

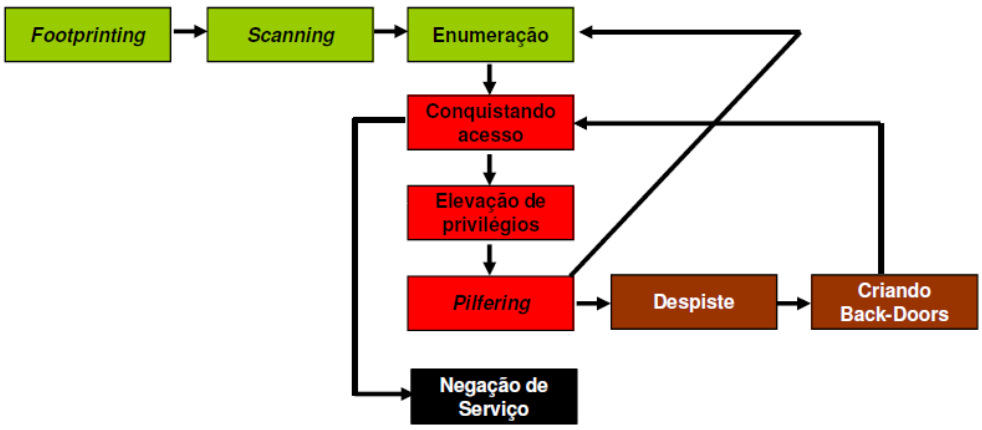


Ilustração 15 - Caracterização de um ataque de penetração

Na fase de Footprinting, o objetivo primordial do atacante é, através de fontes publicamente disponíveis e de forma insuspeita, obter a extensão do alvo, o respetivo *namespace*, bem como recolher o máximo de informação possível que lhe venha a ser útil para concretizar o ataque. Recorre para isso a diversas técnicas tais como pesquisas em motores de busca, ao comando/ interfaces de *whois* e a transferências de zona DNS, entre outras. Apesar de haver diversas formas de Footprinting, tipicamente destina-se à identificação de informação relacionada com ambientes de Internet, intranet, acesso remoto e extranet (MCCLURE, SCAMBRAY, KURTZ, 2009).

A ilustração seguinte resume, por ambiente, os tipos de informação que se pretende identificar nesta fase crucial:

Internet	Domain names
	Network blocks and subnets
	Specific IP addresses of systems reachable via the Internet
	TCP and UDP services running on each system identified
	System architecture (for example, Sparc vs. *x*86)
	Access control mechanisms and related access control lists (ACLs)
	Intrusion-detection systems (IDSs)
	System enumeration (user and group names, system banners, routing tables, and SNMP information)
	DNS hostnames
Intranet	Networking protocols in use (for example, IP, IPX, DecNET, and so on)
	Internal domain names
	Network blocks
	Specific IP addresses of systems reachable via the intranet
	TCP and UDP services running on each system identified
	System architecture (for example, SPARC vs. *x*86)
	Access control mechanisms and related ACLs
	Intrusion-detection systems
	System enumeration (user and group names, system banners, routing tables, and SNMP information)
Remote access	Analog/digital telephone numbers
	Remote system type
	Authentication mechanisms
	VPNs and related protocols (IPSec and PPTP)
Extranet	Domain names
	Connection origination and destination
	Type of connection
	Access control mechanism

Ilustração 16 - Footprinting: identificações por ambiente

No Scanning, o atacante pretende identificar os equipamentos e os serviços disponíveis para se lançar o ataque. Métodos como o *ping sweep* (fping), TCP/UDP portscan e deteção do sistema operativo (nmap) são dos mais úteis nesta fase. De seguida, a Enumeração tem por objetivo ser mais intrusiva e detalhada para se identificar os recursos disponíveis passíveis de serem explorados (como aplicações, *users* e partilhas); Para o efeito, o atacante recorre tipicamente a técnicas como o *banner grabbing*. Alguns exemplos de ferramentas utilizadas nesta fase são o Nessus, o OAT (BD's Oracle), o showmount e o rcpinfo (MCCLURE, SCAMBRAY, KURTZ, 2009).

Após já ter sido identificada a informação suficiente e para se Conquistar o acesso, o atacante recorre a técnicas como *eavesdropping*, *bruteforce* a *shares* ou ficheiros, *buffer overflow* ou exploração de alguma vulnerabilidade específica, com o intuito de concretizar o ataque propriamente dito a um determinado ativo. Para tal, faz uso de ferramentas tais como o Ettercap - spoofing, o Wireshark - sniffing, ou o Webscarab - proxy http (FEUCP, 2009).

O atacante pode então vir a promover uma *Negação de serviço* (*flood* de pacotes *TCP SYN*, *ping of death*, *smurf*) a um recurso vulnerável ou tentar uma Elevação de privilégios a níveis superiores (preferencialmente até root/ Admin), usando *cracks* de passwords ou *exploits* (getadmin, sechole). No caso de ser bem sucedido na elevação de privilégios, pode entrar na fase de Pilfering, onde coleciona informação adicional no próprio sistema, possibilitando a ampliação da área exposta ao ataque (FEUCP, 2009).

O ataque não é terminado sem antes, na fase de Despiste, se eliminar do sistema qualquer pista que possa indicar que houve uma intrusão ou, no mínimo, que possa indicar a origem do mesmo (eliminando-se *logs*, escondendo-se ferramentas, etc). Normalmente são ainda desenvolvidas formas de se poder operacionalizar posteriores acessos em modo privilegiado. Nesta fase de Criação de back-doors são concebidas novas contas, programados *batch* files, ativados serviços remotos, substituídos binários, instaladas ferramentas de monitorização, etc (utilizando-se utilitários do tipo netcat, rc, VNC, SubSeven).

b. Malware

A definição de Malware, ou código malicioso, contempla todo o *software* que é especificamente desenvolvido para danificar ou infligir alguma ação maliciosa e ilegítima na informação, nos equipamentos ou nas redes informáticas. Normalmente, estes produtos de *software* disseminam-se explorando vulnerabilidades conhecidas nos sistemas operativos e noutras aplicações ou, noutros casos, são involuntariamente instalados pelos utilizadores quando, por exemplo, pressionam em determinados *links* ou executam ficheiros de origem não fidedigna. Dependendo do seu propósito, o *malware* pode assumir diversas formas que lhe figura nomenclaturas igualmente distintas. Por exemplo, os Vírus e os *Worms* são essencialmente caracterizados por terem a capacidade de se auto-replicarem e de se propagarem (através da rede, mail, partilhas, discos amovíveis).

No entanto, enquanto os Vírus dependem de outro programa para se propagarem, os *Worms* são independentes neste aspeto. É essencialmente esta interessante particularidade que os distingue.

Neste contexto, SZOR (2005) considera as seguintes componentes como essenciais na estrutura genérica dos *Worms*:

- ✓ *Target Locator* (localizador de alvos) – Para que se consiga disseminar rapidamente pela rede, o *worm* necessita de mecanismos para encontrar novos alvos, como é exemplo a pesquisa de endereços no diretório de contactos para posterior envio de uma réplica por e-mail;
- ✓ *Infection Propagator* (propagador da infeção) – Estratégia que o *worm* utiliza para se transferir para um novo nó da rede e para obter o controlo sobre esse sistema remoto, por exemplo, atacando um tipo de sistema operativo através de linguagens de *scripting* apropriadas, formatos de documentos específicos ou código binário injetado em memória.

Por outro lado, os *Trojans* são um tipo de *malware* que, aparentando ser *software* legítimo, induzem os utilizadores a executar código malicioso, vindo a despoletar consequências prejudiciais no sistema, nomeadamente criando *backdoors* para futuros acessos ilegítimos.

Os *Bots* são outra expressão de *malware*, em que processos automatizados interagem de forma maligna com serviços de rede, fornecendo funções e informações e mecanizando tarefas normalmente só realizadas por humanos (exemplo da interação automática com *websites* ou com *instant messanging*).

Segundo CORREIA (2011, p.67) o primeiro *bot* a ser criado não tinha "*qualquer tipo de atividade maliciosa, jogava com os utilizadores de canais IRC o jogo Hunt of the Wumps*. *Este bot tal como os primeiros que apareceram, mostravam-se aos outros utilizadores como simples clientes normais de um chat IRC."*

Já com intenções maliciosas, este tipo de *software* auto propaga-se e é essencialmente programado para infetar computadores na rede que passam assim também a ser controlados de forma central por hackers, dando origem ao que se chama de Botnet's, cuja principal razão de existir são os posteriores ataques em massa a partir das fontes comprometidas.

Em relação a este conjunto de ameaças classificadas como *malware*, é de prever a continuação do seu crescimento durante o futuro próximo.

A Mcafee antecipa essa tendência no seu relatório de ameaças do segundo trimestre de 2012, evidenciando o número de amostras de *malware* na sua base de dados e identificando a evolução das suas novas formas.

A imagem seguinte permite verificar o crescimento persistente de amostras de *malware* bem como constatar o aparecimento significativo de novos tipos de ameaças a este nível nos últimos tempos (MCAFEE, 2012).

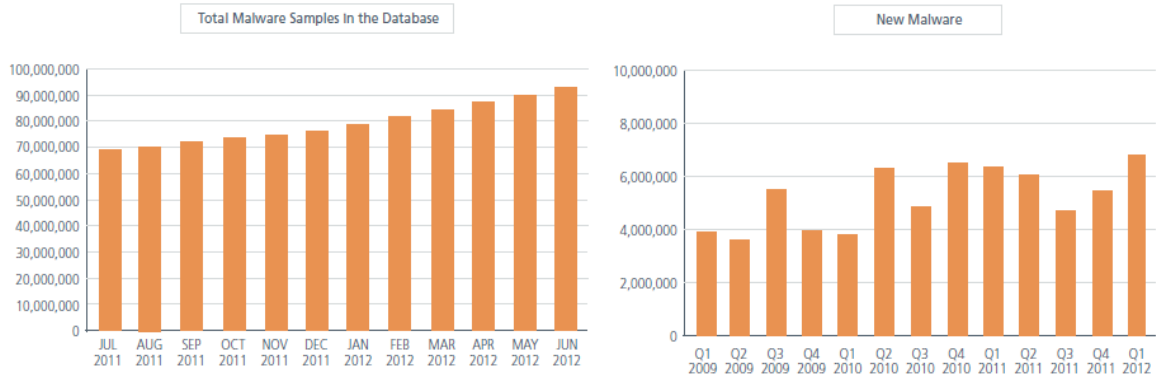


Ilustração 17 - Total de Malware e Novo Malware

No relatório de previsões de ameaças para 2013, a Mcafee chama ainda particular atenção para o facto do Windows 8 vir a ser um grande alvo de atenções para ataques de malware, apesar deste sistema operativo apresentar evoluções significativas em termos de segurança. Os *softwares* maliciosos para esta plataforma irão surgir muito mais rapidamente do que surgiram para versões anteriores do Windows (MCAFEE, 2012).

Por outro lado, prevê-se que a tendência de evolução do código malicioso com o simples intuito de causar estragos irá aumentar. Depois de um período de decréscimo em detrimento de ataques com objetivos mais ambiciosos relacionados com obtenção de ganhos financeiros ou roubos de propriedade intelectual, os ataques deste tipo irão voltar a crescer. Contudo, estas ameaças que poderão ser associadas ao Hacktivismo ou, simplesmente, serem consideradas ações com carácter malicioso, serão também acompanhadas por um crescimento significativo do *Ransomware*, ameaça em que as vítimas são defrontadas com a hipótese de pagarem um resgate ao atacante para que os seus dados sejam devolvidos ou decifrados novamente (MCAFEE, 2012).

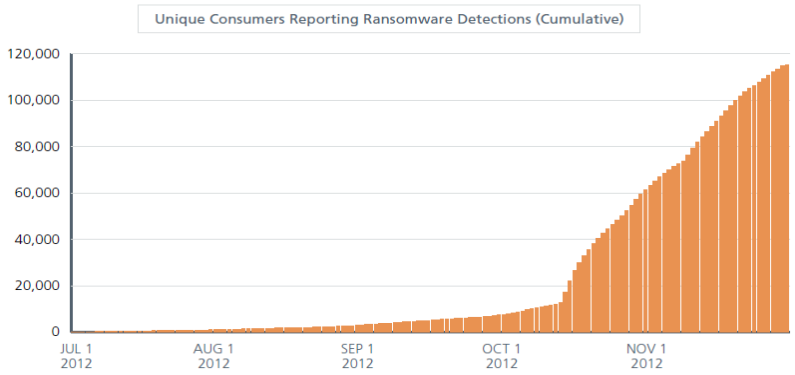


Ilustração 18 - Participações de Ransomware

Um exemplo típico destas incidências é o do Citadel Trojan/Ransom que esconde o desktop do Windows, trancando todas as aplicações e apresentando uma imagem com o logotipo de uma polícia nacional, informando que o computador tem conteúdo ilegal e que o utilizador tem que pagar um montante para ser restaurado o acesso.

A tendência de evolução dos diversos tipos de ataques de *malware* é vista com particular incidência e cuidado em targets de dispositivos móveis. Com a disseminação de equipamentos do tipo laptops, *smartphones* e *tablets* nas organizações, a partilha de informação e as formas de acessos são cada vez mais uma preocupação a ter em conta.

Em finais de 2012, a esmagadora maioria dos alvos contabilizados de ataques deste tipo foram equipamentos com sistemas operativos Android. A Mcafee continua a prever o crescimento expressivo de código malicioso deste tipo (MCAFEE, 2012).

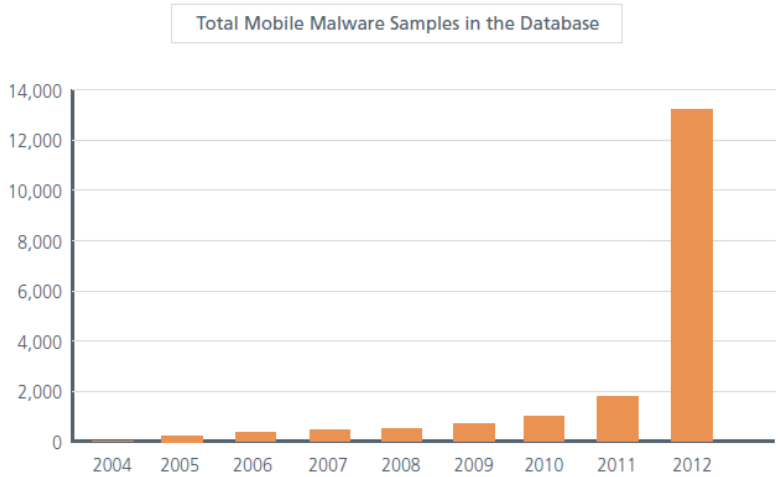


Ilustração 19 - Mobile malware

O *MadWare*, ou Mobile Adware (software que exibe *banners* de publicidade ou *pop-up's* enquanto está a ser executado) é também uma das principais preocupações inerente aos dispositivos móveis para 2013, principalmente no que respeita a sistemas operativos Android. Este tipo de código malicioso incomoda de forma excessiva os utilizadores, alterando a normal utilização dos equipamentos, podendo ainda comprometer dados privados dos mesmos, tais como detalhes de contactos, de geolocalização e de configurações do próprio dispositivo.

A empresa Symantec afirma em 8 de Novembro de 2012, no seu Top 5 de previsões de segurança para 2013 que, nos últimos 9 meses, as aplicações disponíveis com as formas mais agressivas de *madware*, cresceram 210% (SYMANTEC, 2012). A sua previsão de constante crescimento destas ameaças mantém-se.

Em suma, o *malware* continuará a crescer e a assumir as mais diversas formas, ajustando-se aos padrões evolutivos da sociedade. Permanecerá, cada vez mais, como uma representação das ameaças mais significativas para as organizações nos dias que correm.

Os organismos públicos em particular têm de ter a capacidade de ajustar os seus mecanismos de segurança para poderem acompanhar a dinâmica e mutação constante deste tipo de ameaças, por forma a serem capazes de conter a forte probabilidade de ocorrência e o impacto significativo destes riscos nas suas infraestruturas.

c. Botnet's, SPAM e Distributed Denial of Service

Como já abordado anteriormente, as Botnet's são redes compostas por máquinas comprometidas que estão sobre o controlo de indivíduos mal-intencionados. Utilizam estes computadores denominados de "zombies", pertencentes a utilizadores comuns espalhados na Internet e que estão infetados por código malicioso, para conseguirem lançar ataques em massa, com os mais variados fins. As Botnet's representam uma das principais ameaças na Internet nos dias que correm e são uma ferramenta muito eficaz para os *hackers* concretizarem ataques de *Denial of Service* (DoS), *spam*, *malware*, roubo de informação e extorsão, entre outros. Assim que infetada por código malicioso deste tipo, a máquina comprometida comunica com um servidor público gerido pelo *Botmaster* (hacker que controla uma Botnet). Muitos destes "Command & Control servers" (C&C) são servidores de IRC ou utilizam tipicamente portas HTTP/HTTPS e SMTP para comunicar, sendo a partir deles que são controlados e disseminados comandos para a Botnet.

Estes servidores estão constantemente a ser trocados a fim de se evitar a deteção e nunca são da propriedade/ registo dos hackers. Periodicamente é também enviado novo código malicioso para os Bot's que constituem a Botnet e são, sistematicamente, feitas tentativas para se acrescentar novas máquinas.

Um dos ataques mais frequentes de hackers que dispõem de Botnet's para estes efeitos, é o ataque do tipo *Distributed Denial of Service* (DDoS), ou seja, um tipo de ataque distribuído que pretende tornar indisponível para os seus utilizadores determinado recurso da rede. Contudo, o uso das Botnets está progressivamente a mudar o seu propósito, alterando-se as capacidades de ataques de DDoS em favor do roubo de informação dos clientes, como nos casos da Botnet *ZeuS* e da *SpyEye*, e em favor do envio de Spam, como nos casos da Botnet *Rustock* e das suas sucessoras (CORREIA, 2011). Os ataques de *Denial of Service* podem ser levados a cabo por intermédio de várias técnicas e métodos, nomeadamente SYN *Flooding*, ICMP *Flooding*, *Reflected Attack*, entre outros. Segundo FERREIRA (2010), os ataques de *Denial of Service* mais comuns são os de *SYN Flooding*. Estes ataques tiram partido do "*Three-Way Handshake*" do protocolo TCP para estabelecimento das ligações. Este processo de negociação do TCP pretende estabelecer um canal de comunicação entre as duas partes envolvidas, atuando essencialmente em três passos:

1) O endereço origem (SRC) envia um número de sequência inicial X com o primeiro datagrama SYN;
2) O destinatário (DST) reconhece o primeiro datagrama com o envio de um ACK de número X+1, enviando também o seu próprio número de sequência Y num datagrama SYN;
3) A origem reconhece o destinatário e através do envio de um datagrama ACK com número Y+1 completa o início da ligação.

"Neste ataque, o atacante cria um elevado número de meias ligações (half open connections) usando IP forjados. O atacante primeiro envia pacotes SYN com um falso endereço IP para a vítima, de forma a iniciar a ligação. A vítima regista o início de ligação na sua estrutura de dados e responde com mensagens SYN/ACK, mas nunca recebe a correspondente mensagem ACK para estabelecer a ligação, pois os endereços IP forjados pelo atacante não estão ao alcance da vítima ou são incapazes de responder. Apesar do registo de dados para ligações não concluídas ser limpo após um determinado tempo, o atacante gera um elevado número de half open connections sobrecarregando a estrutura de dados da vítima, levando ao bloqueio do computador" (FERREIRA, 2010, p.11).

A figura seguinte ilustra esta técnica de ataque:

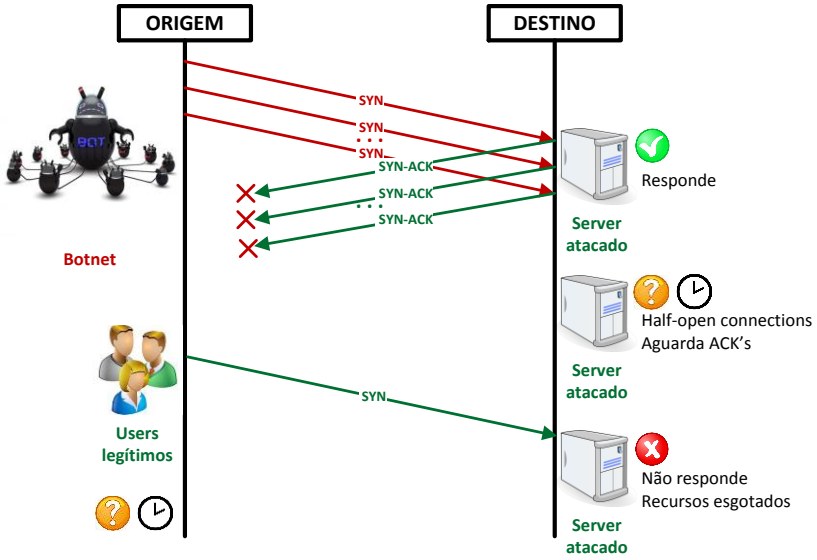


Ilustração 20 - Denial of Service por SYN Flooding

Outra forma comum de DDoS fácil de ser executada, é o ICMP Flooding. Nesta técnica, o atacante faz uso das vulnerabilidades inerentes ao protocolo ICMP para lançar ataques distribuídos com o mesmo objetivo de causar indisponibilidade. O "ping flood" é um exemplo disso, e é caracterizado pelo envio, a partir de várias origens, de pacotes ping alterados e de grande dimensão que poderão causar o esgotamento da largura de banda ou a falha dos recursos do sistema alvo.

Outro exemplo ainda é o ataque distribuído Reflected/Spoofed que consiste na disseminação de falsos *requests* para um grande número de computadores que irão responder às solicitações para o endereço origem dos pacotes, o qual já tinha sido falseado (IP Adress Spoofing) para o endereço da vítima a atacar; Desta forma todas as respostas serão dirigidas a esse ativo da rede que não vai ter capacidade para tratar todas as mensagens recebidas, esgotando rapidamente os seus recursos e causando indisponibilidade.

As Botnet's são também muito frequentemente utilizadas para atividades relacionadas com Spam e, de acordo com a Kaspersky, estima-se que cerca de 80% deste tipo de e-mail seja proveniente de máquinas controlados por botmaster's (KASPERSKY, 2009). O termo "Spam" relaciona-se com a utilização de sistemas de correio eletrónico para disseminação em grande escala de mensagens não solicitadas.

Tipicamente refere-se ao envio de mails de propaganda com links que podem conduzir os utilizadores a *sites* de phishing ou malware. Atualmente, cerca de 78% do total de tráfego respeitante a correio eletrónico é considerado Spam (TIME, 2009).

A empresa Mcafee espelha no seu relatório de ameaças respeitante ao segundo trimestre de 2012 a dimensão que o Spam pode tomar, comparando-o com o mail eletrónico legítimo:

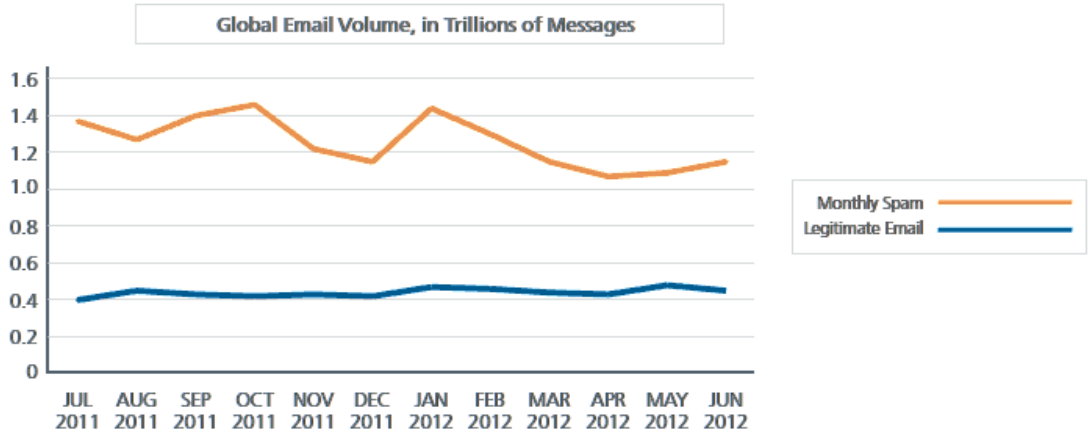


Ilustração 21 - Spam vs Email legítimo

Podemos classificar as mensagens de Spam, tendo em conta as suas temáticas, da seguinte forma:

- ✓ Publicidade (divulgam produtos, serviços, marcas, etc);
- ✓ Malware (mails que incitam os utilizadores a executarem programas maliciosos);
- ✓ "Scam" (difundem esquemas enganosos para efeitos de fraude);
- ✓ "Phishing" (iludem os utilizadores a fim de disponibilizarem informação confidencial com o objetivo de fraudes, transferências bancárias, etc);
- ✓ Ofensivos (mensagens que apelam à violência, propagam acusações infundadas, ideias extremistas, racismo, abusos sexuais, etc);
- ✓ Hoaxes (mensagens de boatos com o intuito de alarmar os utilizadores para a sua replicação urgente a vários destinatários, tipicamente temas falsos de pedidos de ajuda);
- ✓ Correntes (mails que garantem sorte ou outro benefício na sua replicação a um determinado numero de utilizadores, prometendo azar caso contrário).

Como se compreende, as Botnet's são o meio ideal para propagar Spam.

Para levar a cabo este tipo de ações, um indivíduo interessado e mal-intencionado poderá facilmente adquirir serviços de uma Botnet na Internet para este efeito. Se existe uma tipificação das Botnet's consoante o seu propósito, um dos tipos existente é certamente o das Botnet's destinadas ao envio de Spam. A título de exemplo expressivo para a disseminação de Spam, indicam-se as seguintes Botnet's (CORREIA, 2011):

- ✓ *Rustock*, sendo uma das mais conhecidas e com maior tráfego até ter sofrido a desativação da maioria dos seus servidores por parte da Microsoft em 2011;
- ✓ *Lethic*, correspondente a cerca de 350 mil máquinas infetadas para envio de Spam (essencialmente publicidade farmacêutica), chegando mesmo a atingir a fatia de 10% do Spam global;
- ✓ *Waledac*, que chegou a enviar cerca 1.5 mil milhões de mensagens não solicitadas por dia, o que corresponde a 1% do Spam global.

Outro exemplo interessante e particular é o da *Grum*, uma das maiores Botnet's de sempre que no seu apogeu foi responsável por cerca de 18% do tráfego de Spam, antes de ser desligada definitivamente em Julho de 2012. Este mérito foi de algumas organizações de segurança como a FireEye e a Spamhaus que em articulação com os ISP's que hospedavam os servidores de comando/ controlo, os conseguiram desligar. A *Grum* manteve-se no entanto em atividade durante algum tempo até os seus zombies ficarem desativados por completo. O gráfico abaixo ilustra a atividade da *Grum* em comparação com outra Botnet de Spam e DoS denominada *Festi*, precisamente no período de desativação da primeira, demonstrando em contraste, a notória evolução da segunda (SPAMHAUS, 2012).

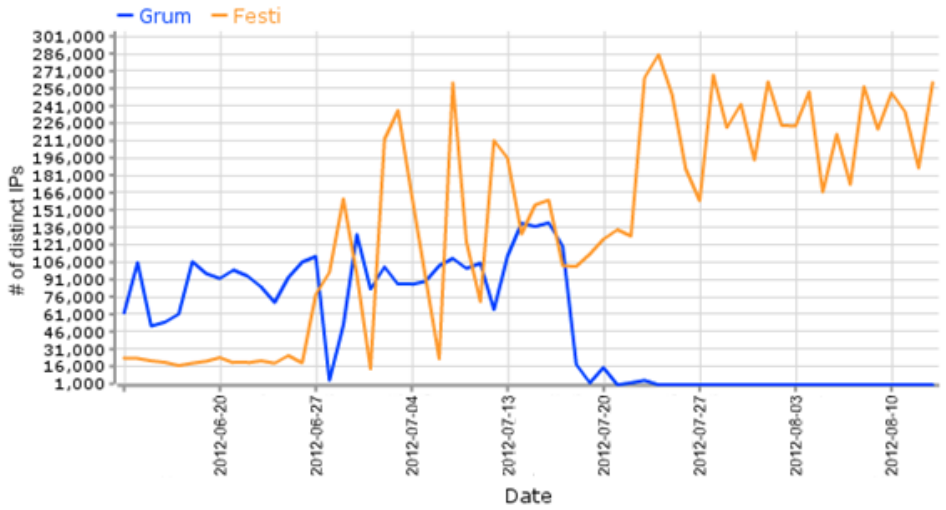


Ilustração 22 - Atividade de Spam das Botnet's Grum e Festi

Apesar das previsões indicarem que para 2013 o Spam representa uma ameaça mais ou menos estagnada, não deixa de ser considerado um dos principais perigos para as TIC dos organismos públicos, principalmente porque pode despoletar a concretização de outros riscos.

No que respeita às Botnet's em concreto, e tendo em conta as suas dramáticas potencialidades, a preocupação dos organismos ao defenderem as suas redes deve prender-se não só com as medidas a levar a cabo para que os seus ativos não fiquem comprometidos e sobre o controlo de um "Botmaster" mas, sobretudo, com a criação de mecanismos para se evitar a concretização de ataques em massa provenientes de Bots dispersos na Internet e que possam pôr em causa a disponibilidade, confidencialidade e integridade dos seus sistemas de informação.

d. Ataques web-based

Duas das principais ameaças a sistemas institucionais, que se têm verificado com relevância nos últimos tempos, são as técnicas de ataque web-based "SQL Injection" e "Cross-Site Scripting".

O SQL Injection explora vulnerabilidades em sistemas que interagem com base de dados através da linguagem SQL. O ataque verifica-se quando o atacante é bem sucedido ao introduzir, numa query comum, instruções SQL supostamente não autorizadas, manipulando os inputs de uma aplicação com formulários, por exemplo.

Na inteligência por trás de determinado formulário poderia residir um fragmento de código que definisse variáveis compostas por instruções SQL que posteriormente interagissem com a base de dados; Por exemplo:

```
(…)
{
var nome;
var sobrenome;
nome = Request.form("nome");
sobrenome = Request.form("sobrenome");
idade = Request.form("idade");
var rso = Server.CreateObject("ADODB.Recordset");
var sql = "select nome, sobrenome, idade from beneficiarios where nome = '" + nome + "' and
sobrenome = '" + sobrenome + "' and idade = '" + idade +"'";
(…)
```

Ora, não se encontrando o sistema devidamente protegido, um atacante poderia injetar código SQL no formulário de forma não prevista, alterando o impacto da execução da instrução. Veja-se no exemplo abaixo, como a mera utilização maliciosa de uma "**'**" e de um "**;**", num sistema não protegido contra SQL Injection, poderia remover a tabela de beneficiários da base de dados:

FORMULÁRIO DE BENEFICIÁRIOS	
Nome:	*'; DROP TABLE beneficiarios;--*
Sobrenome:	
Idade:	
(…)	

Ilustração 23 - Exemplo de SQL Injection num formulário

Assim, com a introdução deste texto específico no primeiro campo do formulário, a variável "sql" produziria um resultado não previsto decorrente da execução de 2 instruções:

1) *SELECT nome, sobrenome, idade FROM beneficiários WHERE nome = ' ';*
2) *DROP TABLE beneficiarios;*

Uma vez que à direita da segunda instrução aparecem os caracteres "--", tudo o que viesse de seguida ficaria comentado, não se verificando erros de sintaxe.

Outros exemplos típicos de SQL Injection são os casos abaixo, inerentes a campos de login (username), quando é solicitado username e password.

- ✓ Se o atacante souber o login de um utilizador, loga-se sem password:

admin'--

- ✓ O atacante pode-se logar com o primeiro utilizador da tabela de utilizadores:

' or 1=1--

- ✓ O atacante pode-se logar com um utilizador fictício:

'union select 1, 'xpto_user', 'xpto_password',1--

Recentemente, têm vindo a ser tornadas públicas bastantes ocorrências respeitantes a SQL injection. Alguns dos exemplos relevantes são:

- ✓ Março/2011 – A página oficial do MySQL foi comprometida através de "blind SQL injection", denominação aplicada quando os resultados da injeção de código não são visíveis para o atacante (SUCURI, 2011);
- ✓ Julho/2012 – Foram furtadas cerca de 450.000 credenciais de login do Yahoo!, através de "union-based SQL injection", técnica utilizada com recurso à instrução union do SQL (CBS News, 2012);
- ✓ Outubro/2012 – Foram publicados registos pessoais de estudantes e funcionários de 53 Universidades de várias partes do mundo, recolhidos com SQL injection, por um grupo hacker denominado "Team GhostShell" (BITS, 2012);
- ✓ Dezembro/2012 – Um exemplo recente português, onde foi divulgado e evidenciado por um grupo hacktivista que o *site* oficial da empresa de telecomunicações Cabovisão estaria vulnerável a ataques de SQL injection (TUGALEAKS, 2012).

Por outro lado, o Cross-Site Scripting (XSS) é uma ameaça associada a ambientes Web que, tipicamente, compromete os browsers dos clientes com vários intuitos, nomeadamente os de roubar cookies para autenticação, reencaminhar utilizadores para páginas de phishing e instalar malware no sistema.

Tem algumas semelhanças com o SQL Injection, na medida em que também se trata da injeção de código; no entanto o atacante em vez de se injectar queries SQL como inputs de utilizador (atacando as bases de dados), injeta *scripts client-side* no servidor aplicacional remoto.

De forma mais detalhada, o processo baseia-se na ação do atacante ao explorar vulnerabilidades num sistema web inserindo código não filtrado (normalmente javascript) na aplicação que, por sua vez, retorna um script malicioso no browser de utilizadores legítimos (quando estes fizerem pedidos à página) e executa-o. Os inputs maliciosos podem ser executados a partir de *script tags*, *body tags*, *image tags*, etc. A partir deste momento, o browser cliente está em condições de servir os interesses do atacante, podendo comprometer de alguma forma o normal funcionamento do servidor aplicacional.

Estas ocorrências são bastante comuns e verificam-se principalmente quando uma aplicação web utiliza inputs de um utilizador nos seus outputs sem os ter previamente validado/codificado.

Um exemplo típico de demonstração destas vulnerabilidades é a inserção de código em *script tags* nos campos de procura das aplicações web para gerar janelas com mensagens a passar. No sistema de testes para este efeito da InsecureLabs (www.insecurelabs.org), pode-se verificar que, se o utilizador em vez de fazer uma procura normal no *site* introduzir por exemplo o código *<script>alert("Teste XSS: Página vulnerável!!!")</script>*, é exibida essa mensagem/alerta no seu browser:

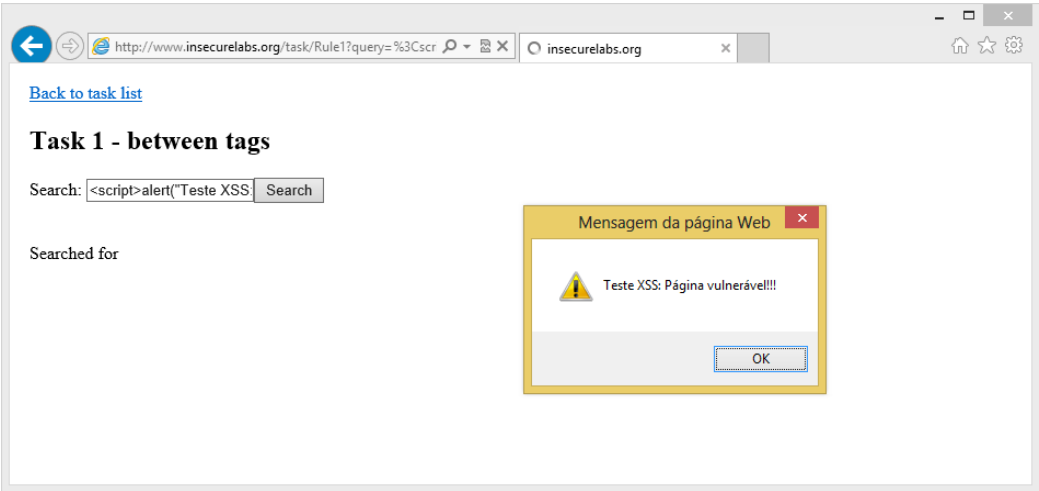


Ilustração 24 - Teste de vulnerabilidade XSS

O Cross-Site Scripting pode apresentar carácter persistente (*stored*) ou não-persistente (*reflected*). As vulnerabilidades do tipo não-persistente são as mais comuns e verificam-se quando os dados fornecidos por um cliente web são utilizados imediatamente por scripts de servidor, analisando e exibindo uma página de resultados de e para o utilizador, sem a devida "higienização"(filtragem) do HTML.

Exemplo:

- ✓ O *User U* acede habitualmente ao *Website W* que lhe permite logar-se e armazenar informação sensível;
- ✓ Um *Hacker H* sabe que o *Website W* tem vulnerabilidade XSS e envia ao *User U* um mail com uma URL a apontar para o *Website W* mas com código malicioso acrescido que o *Website W* irá refletir;
- ✓ O *User U* clica no URL e loga-se no *Website W*, sendo o script malicioso executado no browser do *User U* como se viesse diretamente do *Website W*, enviando o cookie da sessão ao *Hacker H* que passará a ter acesso à informação sensível.

As vulnerabilidades do tipo persistente são as que podem causar maior impacto e verificam-se quando os dados passados pelo atacante são salvos pelo web server e permanentemente exibidos nas páginas retornadas a outros utilizadores. Exemplo:

- ✓ O *Hacker H* publica mensagem com *payload* malicioso numa Rede Social;
- ✓ Assim que o *User U* lê a mensagem, o XSS de *Hacker H* rouba-lhe o cookie;
- ✓ O *Hacker H* consegue personificar o *User U* através da sua sessão.

Segundo a empresa de segurança Firehost, os ataques de Cross-site scripting estão em plena ascensão e, no final do ano de 2012, aumentaram mais de 160% na Europa e nos Estados Unidos. (FIREHOST, 2013)

Um exemplo português e mediático é o ataque ocorrido em Março/2013 ao *site* http://sonae-industria-tafisa.com (e outras tentativas a *sites* do grupo) reivindicado pelo coletivo hacktivista "*Sud0h4k3rs*", após o Presidente do Conselho de Administração do grupo Sonae ter proferido declarações polémicas referentes a mão-de-obra barata (PPLWARE, 2013).

Estes ataques contra o *layer* aplicacional requerem uma atenção particular por parte dos profissionais de IT dos organismos e necessitam de análises muito específicas no que concerne aos mecanismos de segurança a adotar. Isto porque, independentemente da robustez das políticas de segurança da Firewall e da credibilidade da própria rede, se as boas práticas de desenvolvimento não forem cumpridas, estas ameaças vão explorar diretamente transações que utilizam porta típicas como a 80 e a 443. Ou seja, sem mecanismos especiais para o efeito, todo este tipo de atividade maligna é entendida como legítima. Assim, é imperativo que os organismos públicos sejam capazes de desenvolver controlos técnicos preventivos e detetivos capazes de mitigarem o risco de concretização destas comuns ameaças.

e. Ataques de Layer 2

O conhecimento empírico revela que, em grande parte das organizações e nomeadamente nas públicas, o foco de prevenção de ataques de rede está centrado na segurança de perímetro, em particular em mecanismos como Firewalls e outros métodos de proteção análogos. A estratégia da segurança é quase sempre pensada para proteger as infraestruturas de rede internas dos ataques externos, muitas vezes descorando os potenciais riscos provenientes do interior da própria organização.

Os agentes responsáveis por ataques internos são particularmente difíceis de controlar não só porque têm acesso direto e imediato à rede da organização como também, muitas das vezes, esse acesso é legitimado por atribuições e funções profissionais; nestes casos, acresce ainda como fator de agravamento da situação o facto de existir conhecimento relativo à informação sensível e de maior valor para a organização, assim como conhecimento de outros ativos críticos para os processos de negócio.

Um estudo recente da Universidade de Carnegie Mellon revela que, do total dos crimes eletrônicos identificados, 21% foram levados a cabo do interior das organizações e sugere que estes ataques apresentam um impacto superior ao dos ataques provenientes do exterior (SOFTWARE ENGINEERING INSTITUTE – CARNEGIE MELLON, 2011).

KREICBERGA (2010) revela que, as ameaças internas causadas por colaboradores das organizações inerentes a negligências, a descuidos e a erros cognitivos são os mais expressivos e os principais a endereçar, justificados essencialmente pela falta de sensibilidade dos colaboradores e respetivo treino nas questões da segurança; no entanto, os colaboradores também se podem sentir motivados para a realização de ataques intencionais, motivação essa que vem diretamente associada ao descontentamento profissional, nomeadamente associada à possibilidade de virem a ser demitidos.

Por outro lado, importa referir que a camada de ligação de dados (o layer 2 do modelo OSI) difere dos layers superiores também por ser assumida como uma camada confiável por defeito. Ou seja, enquanto nas camadas acima é frequente utilizarem-se mecanismos de filtragem de tráfego em listas de controlo de acesso, autenticação e controlos aplicacionais para limitar/restringir acessos, por norma, no layer 2 não é comum haver preocupação relacionada com a prevenção de ataques.

A este nível assume-se que, no envio de determinada frame, apenas o sistema que contém o MAC (Media Access Control) Address de destino o vai processar. Desta forma, pode-se afirmar que um dos principais problemas do layer 2 é não ter sido pensado em termos de segurança.

Assim, e como a arquitetura em camadas foi projetada para que as mesmas funcionem individualmente sem o conhecimento da operação das outras, se o layer 2 for atacado, as comunicações são comprometidas na totalidade sem que os outros layers se apercebam da ocorrência de algum problema.

É tendo em conta estas premissas que se consideram críticos os ataques de layer 2 e se evidência a possibilidade do forte impacto que os mesmos podem assumir nos organismos públicos e nas organizações em geral. Dos diversos tipos de ataque que se têm verificado a este nível, serão neste ponto caracterizadas algumas das técnicas mais típicas e comuns.

No caso do *MAC Spoofing*, uma técnica extremamente fácil de ser executada, o atacante adultera o MAC (Media Access Control) Address de um dispositivo de rede com o intuito de tirar proveito dessa ação. Na verdade, o MAC Address é *hard-coded* no interface de rede e não pode ser propriamente alterado, mas existem formas de fazer com que o nível do sistema operativo entenda que o MAC Address é outro, recorrendo-se a software para o efeito. As motivações para esta alteração à identidade de um dispositivo de rede consistem, tipicamente, na necessidade do atacante evitar listas e controlo de acesso ou de personificar outro dispositivo para concretizar os seus fins ilícitos. A grande maioria dos ataques de layer 2 passa por uma fase em que se pretende explorar os pacotes ARP (Address Resolution Protocol) que são um elemento de fronteira entre os endereços MAC e os endereços IP. Este protocolo, com o devido recurso às tabelas existentes para o efeito, é responsável pela tradução dos endereços IP (layer 3) em endereços MAC (layer 2); todos os dispositivos de rede têm uma tabela atualizada em que é feita esta associação. Se houver dúvidas de qual o endereço MAC destino para determinado pacote, o cliente antes de o encaminhar, faz o broadcast de uma mensagem ARP questionando qual o MAC para o referido IP. No entanto, pode-se também dar o caso em que os clientes forçam o envio de mensagens ARP sem que tenham sido solicitados para isso (Gratuitous ARP Messages), tendo os dispositivos destinatários que fazer os respetivos updates às tabelas ARP, passando o futuro tráfego a respeitar esses novos endereços. Ora, são estas mensagens gratuitas a génese dos ataques de ARP Spoofing (ou ARP Poisoning) em que o atacante pode proporcionar a alteração das tabelas de ARP de outros dispositivos, fazendo determinado tráfego passar por si (Man-in-the-Middle) antes de chegar ao destino. O *SANS Institute* exemplifica estes tipos de ataque com a ilustração seguinte, identificando o dispositivo do atacante como “ADVERSARY” (OCONNOR, 2010):

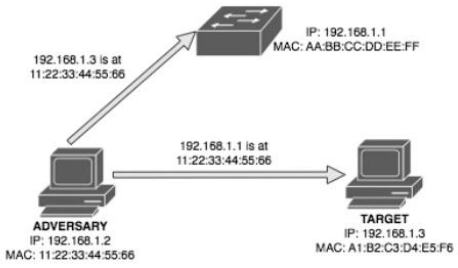


Ilustração 25 - Ataque "Man-in-the-Middle" por "ARP Spoofing"

Neste caso concreto, o atacante envia os seguintes pacotes GARP:

- ✓ Ao switch, indicando que o MAC Address correspondente ao IP da vítima é o seu endereço;
- ✓ À vítima, indicando que o MAC Address correspondente ao IP do switch é o seu endereço.

Se a vítima ficar algum tempo sem receber tráfego, ela própria vai enviar pacotes GARP para a rede o que, juntamente com os pacotes GARP do atacante, poderá provocar aquilo a que se chama uma *ARP Storm, o* que poderá vir a consumir todos os recursos de rede nestas transações, causando um denial of service aos dispositivos envolvidos. Desta forma, o atacante fica numa posição privilegiada nestas comunicações, podendo vir a comprometer a confidencialidade (através da inspeção do tráfego), a integridade (através da alteração do tráfego) e mesmo a disponibilidade (através da negação de serviços dos dispositivos) da informação que passa nesta rede. Para evitar futura identificação na deteção do ataque, o atacante tipicamente altera o MAC Address da sua placa (MAC Spoofing) para um endereço fictício, neste caso para 11:22:33:44:55:66.

Por outro lado, se não existirem as devidas proteções para o efeito, a CAM (Content Addressable Memory) table dos switches é também um alvo de ataques a este nível que se podem expressar num impacto muito negativo para as organizações. Estes dispositivos de rede agregam uma tabela que mapeia as portas do switch (e as VLANs correspondentes) com os MAC Addresses através das quais estão ligados. Assim o switch sabe para que porta em concreto tem que encaminhar determinada mensagem sem que tenha que fazer broadcast da mesma. Contudo, esta lista de associações tem um limite que varia consoante os tipos de switches. Ora, um ataque de CAM table overflow (ou CAM table exhaustion), também sem grande complexidade de ser executado, explora os limites destas tabelas por força da injeção por parte do atacante de novos mapeamentos Porta/MAC até o switch não saber a que porta destino deve entregar as frames e começar a fazer broadcast de todas mensagens, passando a funcionar como um hub. Não havendo autenticação a este nível, qualquer utilizador pode enviar os seus (falsos) MAC Addresses e fazer-se passar por quaisquer outros, "poluindo" assim a CAM table.

Desta forma, e com o inundar da CAM table com estes MACs falsos aleatórios, é possível ao atacante "escutar" todo o tráfego" (por VLAN) que passa neste equipamento, comprometendo a confidencialidade da informação em causa.

Por sua vez, os *ataques STP* (Spanning Tree Protocol) são ataques mais complexos de levar a cabo mas que podem ter um impacto gravoso. O princípio básico do STP é evitar a ocorrência de loops de layer 2 na rede, sempre que existam caminhos redundantes para os pacotes percorrerem. Para tal, este protocolo faz uso de um algoritmo que cria uma base de dados da topologia, encontra links redundantes e remove-os, fazendo as frames circularem apenas por um caminho definido. Só se o link principal falhar é que um dos links redundantes entrará em funcionamento. De forma genérica, este mecanismo é gerido com a atribuição de prioridades a switches e com o bloquear/levantar de portas de forma automática, consoante as necessidades. Uma das fases cruciais do STP é a eleição do Root Bridge, o switch que será o ponto principal da rede; Este processo é feito através da troca de BPDUs (Bridge Protocol Data Units) para se determinar qual a prioridade (quanto mais baixa, melhor) de cada switch/bridge da rede. Num ataque STP, o atacante pretende ganhar acesso à rede introduzindo um falso switch com ligação a pelo menos 2 switches legítimos da rede, para que consiga capturar e analisar o tráfego. A Cisco exemplifica o ataque, ilustrando o normal comportamento de uma rede com STP e a posterior colocação do falso Switch (BOYLES, 2010):

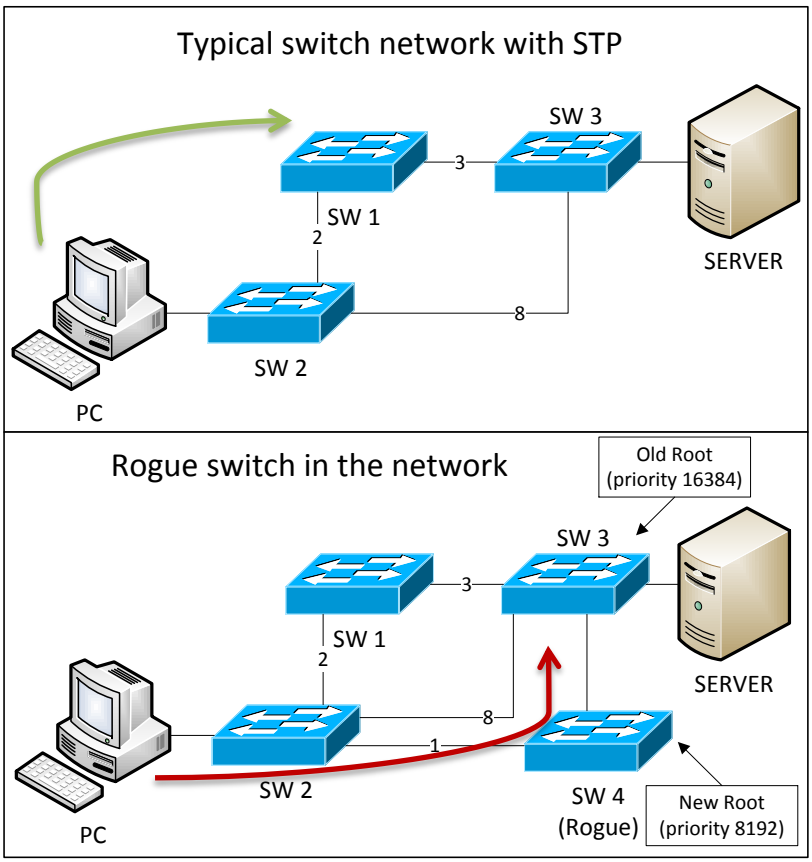


Ilustração 26 - Ataque STP

O primeiro cenário ilustra o comportamento normal de uma topologia STP, em que o SW3 é considerado o Root Bridge e o tráfego do PC é encaminhado pelo SW2 e SW1, também por força do custo dos links (normalmente associado ao débito dos links), em vez de fluir diretamente do SW2 para o SW3 e daí para o servidor.

No segundo cenário, o atacante insere na topologia o seu switch (SW4) e altera-lhe a prioridade para uma inferior à do Root Bridge, trocando de seguida BPDU's com os restantes switches para que possa ser eleito o novo Root Bridge da rede e, consequentemente, conseguir capturar o tráfego destinado ao servidor.

O *VLAN Hopping* (ou VLAN Jumping) é outra técnica de ataque associada à camada de ligação de dados. As VLANs (Virtual Logical Area Networks) são redes logicamente segregadas no mesmo meio físico e são disseminadas pela infraestrutura física de rede através de interfaces em modo *trunk* (normalmente através do protocolo standard 802.1q). Ou seja, os interfaces dos switches assim configurados permitem o fluxo de tráfego de/para diversas VLANs. Por norma, sem haver equipamentos de routing pelo meio (layer 3), os dispositivos de rede apenas conseguem comunicar com outros dispositivos pertencentes à mesma VLAN. Mas para que seja possível comunicarem naturalmente dois utilizadores ligados em swiches físicos distintos mas pertencentes à mesma VLAN, as frames ethernet são também compostas por uma *tag* (ID) que identifica a VLAN respetiva e que é inserida imediatamente a seguir ao MAC Address de origem. As frames são então encaminhadas pelos interfaces de trunk e a *tag* é retirada (stripped) da frame antes desta deixar a porta destino do switch.

De forma genérica, num ataque de VLAN Hopping, o atacante está ligado em determinada VLAN e pretende ganhar acesso ilegítimo a outra VLAN. Para o efeito, pode recorrer a duas técnicas específicas:

- ✓ Double tagging;
- ✓ Switch Spoofing.

Na primeira técnica, um dispositivo ligado na VLAN 1 (VLAN nativa, que não se deve utilizar precisamente por estes motivos) adiciona uma segunda *tag* à frame. Antes da mesma ser transmitida para o switch seguinte, a primeira tag é removida. Quando a frame chega ao switch seguinte tem uma *tag* ativa e pode ser perfeitamente encaminhada para uma VLAN que está disponível nesse switch, através de uma porta de acesso.

No exemplo seguinte a frame é encaminhada para a porta onde está ligado o servidor alvo do ataque (BOYLES, 2010).

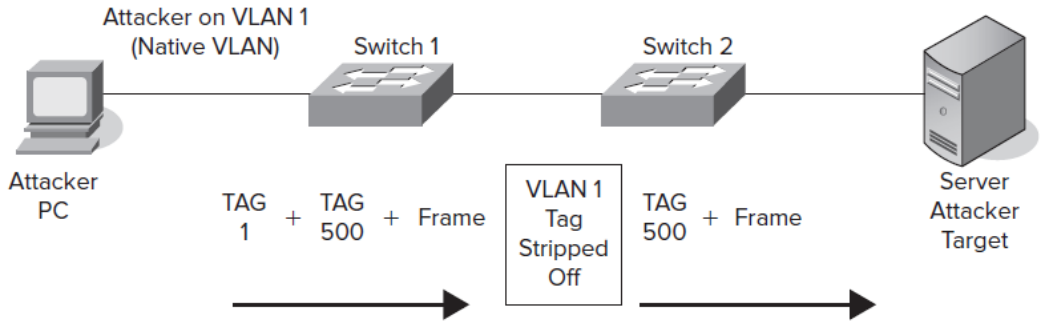


Ilustração 27 - Ataque "VLAN Hopping" por "Double Tagging"

A segunda técnica de VLAN Hopping baseia-se na ação do atacante em forçar a ligação entre um switch seu (ou software que o emula, fazendo uso de protocolos de trunking) e outro switch da rede, utilizando uma porta em modo trunk para enviar mensagens DTP (Dynamic Trunk Protocol). Isto é possível acontecer porque os interfaces dos switches, em norma e por defeito, estão em "auto negotiation mode", o que proporcionará a criação de um link trunk entre os dispositivos. O atacante poderá assim ter acesso ao tráfego de todas as VLANs, comprometendo a confidencialidade da informação desses fluxos.

2.2.3. O Hacktivismo e seus impactos negativos

Os ataques explicitados nos pontos anteriores são, em grande medida e nos dias que correm, levados a cabo também por grupos hacktivistas. Por esta razão, entende-se importante a abordagem deste fenómeno com algum relevo.

O termo Hacktivismo provém de 1996 e foi atribuído pelo grupo de hackers "Cult of the Dead Cow" (CDC, 2012). É qualificado pela realização de ações de intrusão, alteração ou indisponibilidade em redes e sistemas informáticos com o propósito de chamar a atenção para ideais políticos, sociais, de direitos humanos, de liberdade de expressão ou outras motivações éticas.

Um hacktivista faz uso das mesmas ferramentas e práticas de um hacker comum mas entende legítimas as suas ações porque levantam a bandeira da causa social. Uma das principais convicções dos grupos de Hacktivismo é a do direito fundamental à informação.

Os hacktivistas acreditam que o recurso à tecnologia é uma arma importante para o protesto e para a desobediência social e política. Tipicamente, as suas ações são materializadas em ataques de denial-of-service, invasões e alterações de web *sites*, roubo de informação, entre outros. Segundo SAMUEL (2004), as características dos hacktivistas são distintas consoante a sua orientação seja criminosa ou meramente de transgressiva:

		Orientation	
		Transgressive	Outlaw
Characteristics	Legal risk	Legally ambiguous	Illegal
	Accountability[7] (naming practices)	Real names, traceable pseudonyms	Untraceable pseudonyms, anonymity
	Group size	Medium-size groups, dependence on mass participation	Solo, small groups
	Transnational cooperation	Multinational (working with hacktivists from multiple nations)	National (vs. own country) Multinational (cooperating across boundaries) International (mirroring international conflicts)

Ilustração 28 – Hacktivistas: características vs orientações

Em Portugal, o fenómeno do Hacktivismo obteve o seu expoente máximo em finais do ano 2011 e princípios do ano 2012. O forte descontentamento social e político, nacional e internacional, foi razão determinante para a ocorrência de um conjunto de eventos desta natureza. Neste período verificaram-se frequentes ataques reivindicados por grupos hacktivistas a *sites* e redes institucionais, alguns dos quais foram tornados públicos, tais como os ataques ao Ministério das Finanças, ao DCIAP, à PSP, ao SIS e a alguns partidos políticos, como o PS, PSD e CDS.

De acordo com o website da Panda Security, estes "*ataques e a forma como são feitos demonstram que proteger e controlar o tráfego Web gerado pelos utilizadores empresariais, deixou de ser uma opção nas organizações e tem que ser abordado de forma séria e efectiva. É uma necessidade incontornável. A questão reside em saber qual a melhor abordagem para enfrentar este desafio, de modo a conjugar o melhor controlo possível sem onerar demasiado os orçamentos. A verdade é que estes ataques aumentam fruto da instabilidade social, mas também porque a redução dos orçamentos muitas vezes deixa de fora aspectos que deveriam ser considerados essenciais*" (PANDA SECURITY, 2012).

Dois dos principais grupos que têm atuado a este nível em Portugal são os Anonymous e os LulzSec. A figura abaixo exibe os dois logótipos hacktivistas que estiveram bastante vincados na nossa sociedade durante esse período e que, de alguma forma, ainda continuam a marcar a sua presença:

Ilustração 29 - Logótipos dos "Anonymous" e dos "LulzSec"

Os Anonymous são um grupo hacktivista que teve origem em 2003 (no *site*/imageboard 4chan - http://www.4chan.org/) e que difunde ideais de liberdade, representando comunidades online que atuam como um cérebro anarca e global. Apresentam-se como não tendo líderes e o seu conceito base reside no facto de qualquer pessoa poder fazer parte do grupo. Intitulam-se uma organização de vigilantes que procuram o bem comum. Os Anonymous encontram-se disseminados por todo o globo. Na variante portuguesa, apresentam na sua página do Facebook: "*Os Anonymous não são nada em específico ou concreto, são simplesmente uma ideia, uma ideia de um mundo livre. Se também tiveres essa ideia tu também és Anonymous. Nós estamos a lutar numa escala mundial como um só, está a ser um momento histórico mundialmente. A Anonymous não são apenas hackers, Os Hacktivistas Anonymous lutam pela liberdade de expressão seja ela online ou offline (…)*" (ANONYMOUS-PORTUGAL, 2011).

Estabelecem-se contra a "Nova Ordem Mundial", definindo e difundindo planos de atuação conjunta. Em termos resumidos, elencam-se de seguida algumas das suas operações com maior impacto a nível mundial.

- ✓ Abril/2009 - Ataque coordenado de DDoS ao "International Federation of the Phonographic Industry", após os réus responsáveis pelo *site* "Pirate Bay" terem sido considerados culpados de violação de direitos de autor.
- ✓ Janeiro/2011 – Ataque de DoS a *sites* oficiais do governo tunisino, erguendo-se contra a opressão e a censura da informação.
- ✓ Julho/2011 – Roubo de cerca de 1GB de informação confidencial de sistemas da NATO e publicação da mesma na web.
- ✓ Julho/2011 – Ataque de DDoS que desligou o *site* da PayPal depois da empresa bloquear os donativos dos apoiantes do Wikileaks; Foram ainda divulgadas mensagens no Twitter apelando os utilizadores a deixarem a PayPal e a considerarem alternativas; Nos períodos imediatos, a PayPal foi perdendo 4 utilizadores por minuto.
- ✓ Outubro /2011 – Desligaram o website de pornografia infantil Lolita City e divulgaram informação pessoal dos seus membros.
- ✓ Janeiro/2012 - Ataque coordenado de DDoS ao FBI e ao Departamento de Justiça americano (assim como a outras entidades envolvidas), após o *site* do Megaupload ter sido desligado pelas autoridades.
- ✓ Janeiro/2012 – Ataque a *sites* de grupos Neo-Nazis, expondo inclusivamente informação pessoal (contactos) dos seus membros.
- ✓ Fevereiro/2012 – Ataque ao *site* da CIA, expondo informação confidencial de vária ordem.

O grupo hactivista LulzSec, apresenta afinidade ideológica com o anterior, operando inclusivamente e por diversas vezes em conjunto (como no caso do ataque à CIA). Contudo, alegam que também têm motivações baseadas em obter satisfação e divertimento pessoal ao atacar os seus alvos, o que demonstra que na sua génese não reside exclusivamente o carácter ativista que os Anonymous publicitam. Um dos seus principais membros e fundador é um especialista em segurança informática (que utiliza o apelido na Internet de *Sabu*) e que, após ter sido detido, colabora em acordo judicial com as autoridades para a deteção de outros hackers, inclusivamente de membros do grupo LulzSec.

Dos seus ataques com maior relevo e impacto, explicita-se o ataque à Sony Pictures, em Junho de 2012, em que se verificou roubo de informação sensível de contas de utilizadores, incluindo nomes completos, passwords, e-mails, moradas e datas de nascimento dos clientes. O grupo utilizou estratégias de SQL injection e foi motivado pelo facto desta empresa interpor uma ação judicial contra um utilizador comum por este ter "crackado" uma Playstation 3 (alterar o estado de origem do dispositivo com o intuito de tirar partido de funcionalidades não autorizadas).

Por outro lado, e em alinhamento com as previsões, de diversas entidades credenciadas, acerca do aumento significativo do *cyber conflict*, que se estima vir a ser cada vez mais comum entre organizações e entre nações, existem opiniões de que o hacktivismo pode ser uma arma para servir interesses promíscuos. Segundo PAGET (2012), o hacktivismo é um movimento amorfo que pode agora estar a esconder um leque de motivações mais obscuras como a criminalidade e o "phishing" patrocinada pelos Estados; O colaborador da Mcafee agrupa o hacktivismo em 3 distintas motivações:

- ✓ os que procuram a propaganda (como os Anonymous);
- ✓ os "ciberocupantes" (que considera os verdadeiros ativistas), que lutam contra a corrupção e procuram a verdadeira democracia;
- ✓ os "ciberguerreiros" (tipicamente de países como o Irão, China e Rússia), que reivindicam agir a favor dos seus governos suportando movimentos nacionais e extremistas.

Sugere ainda que alguns indivíduos podem estar a fazer jogo duplo, escondendo atividades ilegais sob a bandeira do hacktivismo político e conclui que a falta de ética em muitas operações aponta para que alguns movimentos hacktivistas podem ser despoletados e controlados por serviços secretos de governos (PAGET, 2012).

Independentemente das motivações destes movimentos, a agência europeia de segurança das redes e da informação, ENISA, identifica os grupos hacktivistas como sendo um dos principais agentes de ameaças a este nível nos dias que correm. Relaciona-os essencialmente com os perigos das Botnets, Denial of Service, injeção de código e comprometimento de informação sensível (ENISA, 2012).

Com base nestes riscos e previsões, é imperativo que os organismos públicos, em particular, estejam atentos ao fenómeno do hacktivismo e se mantenham precavidos. Apesar dos ataques que caracterizam estas ações concertadas não serem na sua generalidade dotados de níveis de sofisticação e complexidade elevados, têm vindo a demonstrar o quão vulneráveis poderão estar as redes e os sistemas das entidades públicas. Assim, à medida que os organismos forem reconhecendo a necessidade premente das medidas preventivas e detetivas a este nível, menor será a probabilidade de sucesso destas ameaças mais básicas de DDoS e Code Injection que se têm vindo a verificar com bastante regularidade.

2.2.4. Vulnerabilidades genéricas nas redes do Estado

Este ponto não pretende elencar de forma detalhada ou exaustiva as vulnerabilidades existentes nos ativos e nas redes dos organismos públicos, uma vez que a exposição dessa informação, só por si, poderia constituir uma falha gravosa e representar riscos acrescidos para estas infraestruturas do Estado. Pretende-se no entanto, com base na experiência existente das realidades de organismos públicos e de supervisões efetuadas a infraestruturas de rede do Estado nos últimos tempos, enumerar alguns dos problemas e limitações existentes nestas infraestruturas que se encaram como vulnerabilidades de alto nível, uma vez que podem pôr em causa a confidencialidade, integridade e disponibilidade dos sistemas de informação:

- ✓ Apesar da situação ter vindo a melhorar lentamente, nos organismos públicos ainda se verifica alguma insensibilidade para a problemática da segurança;
- ✓ Com os orçamentos cada vez mais reduzidos agrava-se a tendência de não se atribuir a importância devida às componentes de segurança nas redes do Estado;
- ✓ Grande parte dos ativos críticos para o negócio não contempla mecanismos de redundância, representando um ponto de indisponibilidade em caso de falha;
- ✓ Muitos dos ativos de rede apresentam antiguidade excessiva, encontra-se mesmo uma parte considerável num estado de *end-of-life* e *end-of-support*;
- ✓ Acresce que alguns destes e de outros equipamentos críticos não têm contratos de manutenção associados;
- ✓ Em certos casos, existe um excesso de dependência em relação a fornecedores de serviços no que respeita a intervenções/ gestão de ativos críticos TIC; Este desvio de conhecimento pode representar uma falha grave, principalmente quando estes serviços críticos são cessados por questões orçamentais;
- ✓ Existe muito pouco controlo no tráfego que circula nas redes dos organismos públicos;
- ✓ A grande maioria dos Centros de Processamento de Dados não respeita as regras de segurança física e lógica enunciadas pelos standards de boas práticas, nomeadamente nos mecanismos de controlo de acessos;
- ✓ Grande parte das infraestruturas de rede dos organismos não é segregada em VLANs distintas, proporcionando que os sistemas e ativos em causa partilhem o mesmo domínio de broadcast e o mesmo grau de exposição ao risco, independente da sua criticidade e valor para o negócio.
- ✓ A função informática descentralizada bem como a inexistência de uma rede única de comunicações levanta questões de governança e de gestão, potencia a multiplicidade das vulnerabilidades e dificulta o controlo e a contenção do risco.

Por outro lado, importa exemplificar determinadas vulnerabilidades comuns nas redes e sistemas das organizações atuais. Vários autores têm vindo a desenvolver esforços para exibir algumas das mais típicas e recorrentes. Os profissionais com certificação CISSP, MCCLURE, SCAMBRAY e KURTZ (2009) identificam o Top 14 das vulnerabilidades a este nível:

1. Controlo de acesso inadequado nos Routers (ACLs mal configuradas) pode proporcionar acessos não autorizados às DMZs;
2. Ligações remotas não seguras e sem monitorização são dos meios mais comuns alvo de exploração para acesso não autorizado a redes de dados;
3. A fuga de informação pode dar a conhecer ao atacante conhecimento crítico como versões de SO, versões de aplicações, users, grupos, partilhas, DNS info e serviços a correr;
4. Serviços desnecessários a correr em servidores podem ser facilmente comprometidos (nomeadamente FTP, RPC, SMTP, DNS);
5. Passwords fracas, previsíveis e reutilizadas nas workstations podem comprometer também os servidores;
6. Contas de utilizador e de teste com privilégios excessivos podem representar vulnerabilidades graves;
7. Servidores de Internet mal configurados, normalmente scripts CGI e ASP em Web Servers, FTP servers com diretorias contendo permissões de escrita para o mundo e Vulnerabilidades XSS;
8. Firewalls ou ACLs de routers mal configuradas podem proporcionar o acesso direto a sistemas internos ou comprometer servidores na DMZ;
9. Software em estado default, sem os updates/patches mais recentes ou vulnerabilidades conhecidas, nomeadamente em web servers;
10. Demasiados tipos de Controlo de acessos a ficheiros e diretorias.
11. Relações de confiança excessivas, como Windows Domain trusts, UNIX .rhosts, host.equiv e ficheiros SSH podem proporcionar acessos não autorizados a sistemas sensíveis;
12. Serviços não autenticados como o X Windows permitem aos utilizadores capturarem keystrokes remotos;
13. Monitorização, logging e capacidade de deteção inadequados ao nível da rede e dos hosts.
14. Falta de políticas de segurança, procedimentos, normas e guidelines aceites e devidamente promulgadas.

A ilustração abaixo enquadra de forma mais clara estas vulnerabilidades nas infraestruturas e nos ativos de rede mais comuns das organizações (MCCLURE, SCAMBRAY, KURTZ, 2009):

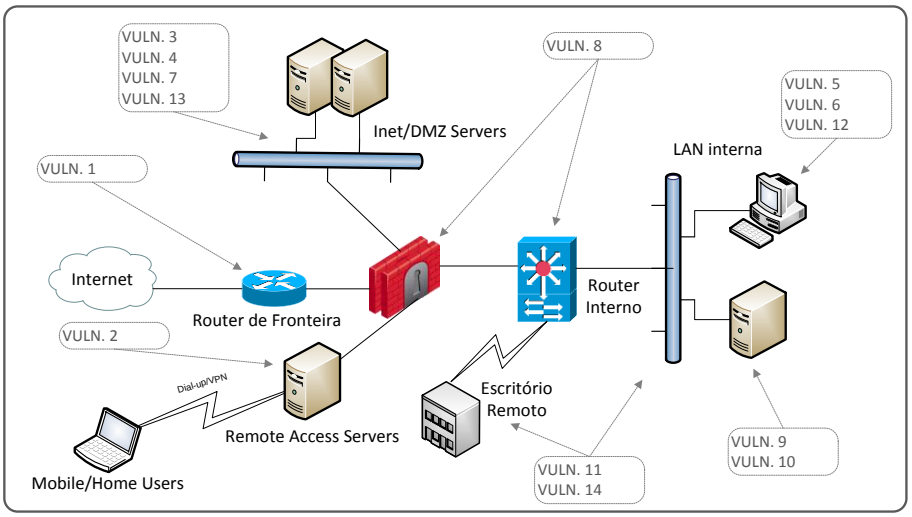


Ilustração 30 – Âmbito do Top 14 das Vulnerabilidades em redes e Sistemas

Apesar destas vulnerabilidades que são apresentadas como problemas de alto nível e generalizadas na Administração Pública, é importante referir que, naturalmente, existem organismos em diferentes graus de maturidade a este respeito. Alguns deles seguem inclusivamente modelos de referência em termos de segurança dos sistemas de informação, encontrando-se em conformidade com os mesmos, apesar da necessidade constante de melhoria contínua. Desta forma, entende-se que seria pertinente encarar o Estado como um todo em termos de TIC e de segurança dos SI, nivelando-se os padrões por cima, isto é, aproveitando-se os bons exemplos existentes, generalizando-os.

2.2.5. Trabalho já efetuado no âmbito das redes e da segurança da AP

Este capítulo pretende identificar alguns dos recentes contributos existentes no âmbito das redes e da segurança na Administração Pública.

Em 2 de Outubro de 2009, a Resolução do Conselho de Ministros (RCM) nº 109/2009 definia que compete à Agência de Modernização Administrativa, IP (AMA) "estabelecer orientações comuns em matéria de TIC na Administração Pública e coordenar a sua execução, através da dinamização de uma rede interministerial de agentes das tecnologias de informação", dando apoio ao governo na definição de políticas transversais (RCM nº 109/2009, 2009).

Segundo a RCM 109/2009, a rede interministerial "permitirá uma articulação mais eficaz dos vários agentes para definir normas e directrizes TIC e de interoperabilidade que sejam utilizadas e seguidas em toda a Administração Pública, potenciando a existência de serviços partilhados e integrados, aumentando a segurança dos serviços públicos electrónicos" (RCM nº 109/2009, 2009). Desta forma, nasceu a Rede Interministerial das TIC (RITIC), que é uma sub-rede de intervenientes integrada na Rede Comum de Conhecimento e que se constitui como um conjunto colaborativo de agentes do Estado para as tecnologias de informação e comunicação. Tem o intuito de vir a definir normas TIC e de interoperabilidade a ser aplicadas no âmbito da Administração Pública depois de serem devidamente aprovadas em Conselho de Ministros.

O âmbito de trabalhos da RITIC foi separado em grupos de trabalho com temáticas prementes no que respeita às tecnologias de informação e comunicação da Administração Pública, dos quais se destacam para o efeito desta dissertação, o da "Segurança da Informação" e o da "Racionalização das Comunicações".

No que respeita à **Segurança da Informação**, a AMA apresentou em sede de RITIC as seguintes especificações (AMA, 2010):

Missão

- ✓ Criação de políticas de segurança aplicáveis a toda a Administração pública garantindo a integridade, disponibilidade e confidencialidade da informação manipulada internamente e inter-organismos e a disponibilização de serviços seguros ao cidadão e empresas.

Objetivos

- ✓ Estabelecer as principais linhas de atuação para a Administração pública, de acordo com critérios de premência, transversalidade e ponderação custo/benefício;
- ✓ Criação de políticas de segurança a aplicar de acordo com o ponto anterior, de forma a criar um patamar aplicável a todas as entidades.

Principais resultados esperados

- ✓ Linhas de atuação para a Administração pública;
- ✓ Relatório de políticas de segurança.

Entidades de coordenação e dinamização

- ✓ GNS – Gabinete Nacional de Segurança;
- ✓ SGMD – Secretaria Geral do Ministério da Defesa;
- ✓ DGAJ – Direção Geral da Administração da Justiça;
- ✓ AMA – Agência para a Modernização Administrativa.

Entidades externas/especialistas

- ✓ FCCN – Fundação para a Computação Cientifica Nacional.

Relativamente à **Racionalização das Comunicações**, a AMA especificou o seguinte (AMA, 2010):

Missão

- ✓ Desenvolver e implementar um modelo de gestão integrada das comunicações para toda a Administração pública, de forma a uniformizar arquiteturas, infraestruturas, racionalizar recursos, obter economias de escala e consequentemente a redução dos custos associados a aquisição de hardware e software, recursos e infraestruturas.
- ✓ Delinear iniciativas de incentivo à utilização de mecanismos de videoconferência e messaging dentro da Administração Pública.

Objetivos

- ✓ Levantamento da situação atual, contemplando a análise de iniciativas anteriores já desenvolvidas na Administração pública;
- ✓ Proposta de modelo a adotar, contemplando um calendário e metodologia de implementação.

Principais resultados esperados

- ✓ Modelo de gestão das comunicações.

Entidades de coordenação e dinamização

- ✓ SG MOPTC – Secretaria Geral do Ministério das Obras Públicas, Transportes e Comunicações;
- ✓ AMA – Agência para a Modernização Administrativa;
- ✓ CEGER – Centro de Gestão da Rede Informática do Governo;

Entidades externas/especialistas

- ✓ FCCN – Fundação para a Computação Cientifica Nacional.

Como fio condutor da RITIC, foi constituído o Grupo de Projeto para as tecnologias de informação e comunicação – GPTIC (RCM 46/2011, 2011), responsável por elaborar um plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública e cuja implementação resulta de uma obrigação assumida pelo Governo Português no âmbito do Plano de Assistência Económica e Financeira.

A meta de implementação foi inicialmente apontada para o final de 2012, o que se verifica não ter sido possível cumprir. Com os objetivos finais de se obterem ganhos de poupança e de eficiência, bem como de se promover, em termos de TIC, a visibilidade do Estado como um todo, a RCM 12/2012 resolve, de forma genérica, o seguinte (RCM 12/2012, 2012):

- ✓ Aprovar as linhas gerais do plano global estratégico;
- ✓ Determinar que em cada ministério é identificado um organismo responsável pela coordenação das TIC;
- ✓ Determinar que o GPTIC identifica sistemas operacionais críticos que ficam sujeitos a regras específicas de salvaguarda;
- ✓ Estabelecer que será dada prioridade ao cumprimento e implementação do plano global estratégico;
- ✓ Estabelecer (no Anexo à RCM 12/2012) os cinco eixos de atuação e as 25 medidas de racionalização das TIC enquadradas em cada um dos eixos e especificadas no plano global estratégico.

A figura seguinte resume todo este processo.

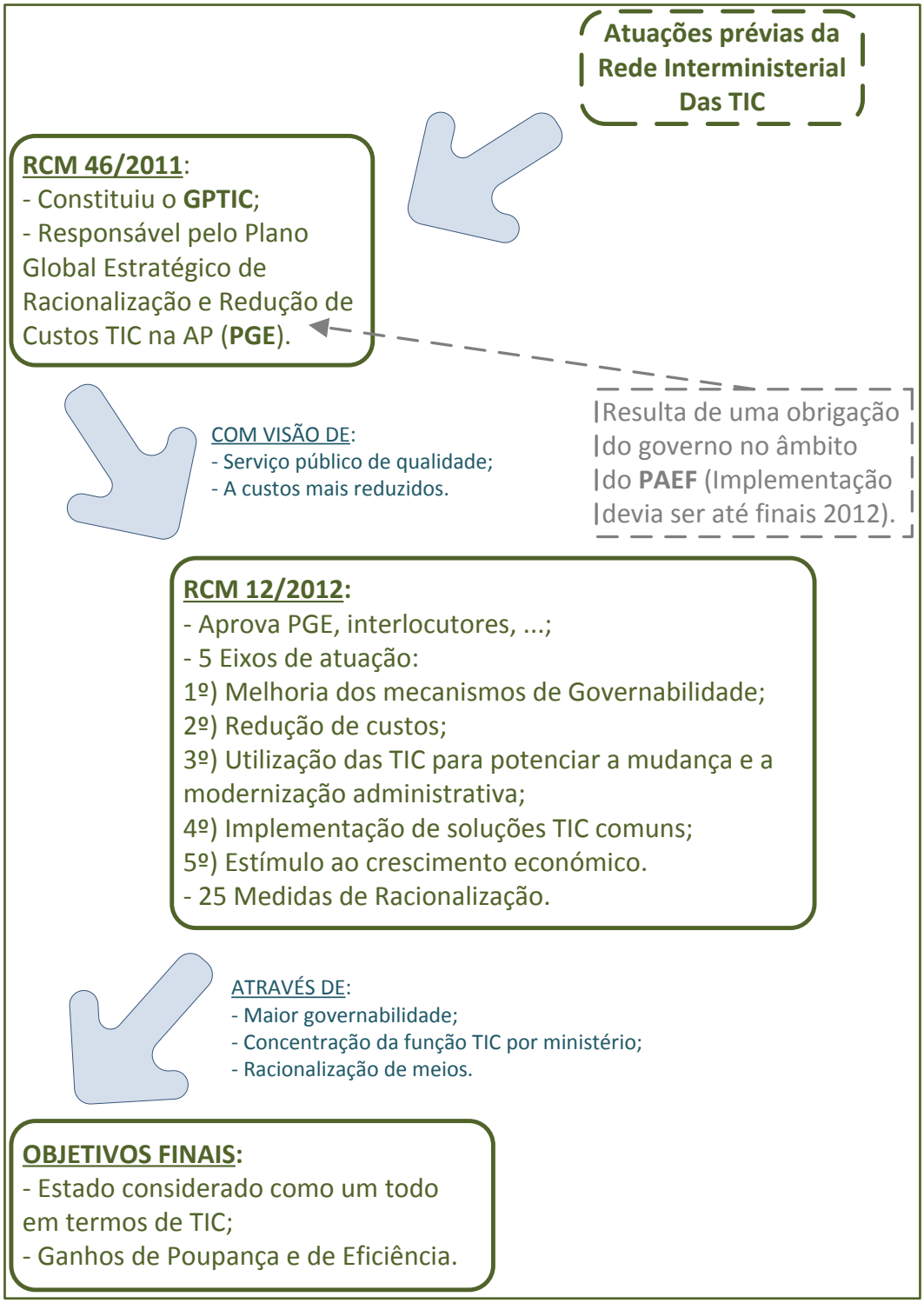


Ilustração 31 - Passos do Plano Global Estratégico das TIC da AP

As 25 medidas de atuação, enquadradas nos 5 eixos definidos (identificados na figura anterior), são descritas na ilustração/tabela seguinte.

Eixo	Medida	Descrição
1º	1	Definição e implementação da *governance* das TIC na Administração Pública
	2	Racionalização, organização e gestão da função informática
	3	Arquitetura, normas e *guidelines* de tecnologias e sistemas de informação
	4	Definição e implementação de uma estratégia nacional de segurança da informação
	5	Definição e implementação de planos de ação sectoriais de racionalização das TIC
2º	6	Avaliação de projetos e despesas TIC
	7	Racionalização de comunicações
	8	Racionalização dos centros de dados (CPD)
	9	Plataforma de comunicações unificadas
	10	Medidas de racionalização transversais potenciadas pelas TIC
3º	11	Interoperabilidade na Administração Pública
	12	Autenticação e assinatura eletrónicas na AP
	13	Racionalização da prestação de serviços públicos por meios eletrónicos.
	14	Racionalização das TIC e modernização administrativa dentro dos organismos públicos
	15	Central eletrónica de arquivo do Estado
4º	16	Catalogação de recursos humanos
	17	Catalogação, partilha e uniformização de *software* do Estado
	18	*Cloud Computing* na Administração Pública
	19	Plataforma B2B
	20	Diretório de boas práticas TIC
5º	21	Adoção de software aberto nos sistemas de informação do Estado
	22	Aquisição de bens e serviços de TIC
	23	Administração Aberta e novos canais de atendimento
	24	Internacionalização de metodologias, soluções TIC e conhecimento publico
	25	Divulgação e prototipagem de projetos inovadores em *clusters* de competitividade

Ilustração 32 - 25 Medidas das TIC da AP

No âmbito desta dissertação, as medidas que se entendem mais pertinentes são a "Racionalização, organização e gestão da função informática" (medida 2), a "Definição e implementação de uma estratégia nacional de segurança da informação" (medida 4) e a "Racionalização de Comunicações" (medida 7).

Em relação à medida 2, pretende-se vir a "garantir uma efetiva centralização da função informática em cada ministério, incluindo a gestão das infraestruturas tecnológicas, das comunicações, dos sistemas de informação (agregando a manutenção e desenvolvimento de todas as aplicações verticais do ministério), da gestão de aquisições e licenciamento e do apoio aos utilizadores" (RCM 12/2012, 2012). Quanto ao calendário estimado para esta implementação, o referido regulamento aponta para que os ministérios efetuem esta centralização até ao prazo limite do fim do ano de 2013, o que se verifica não ter sido possível cumprir. Entende-se que esta medida é extremamente importante e pertinente de levar a cabo, antecipando-se que venha a trazer melhorias no desempenho e segurança das TIC dos ministérios, não só porque promove a racionalização dos recursos como também porque proporciona um maior controlo na informação e nos ativos críticos dos organismos públicos.

No que respeita à medida 4, pretende-se consolidar uma Estratégia Nacional de Segurança da Informação (ENSI). Para o efeito, a RCM 12/2012 define a necessidade de contemplar nessa estratégia, nomeadamente, os itens seguintes:

- ✓ Os objetivos nacionais para a segurança da informação;
- ✓ A responsabilidade na segurança da informação;
- ✓ A organização da segurança da informação;
- ✓ A gestão da segurança da informação;
- ✓ Os serviços de segurança da informação.

Decorrente da ENSI, prevê-se ainda o seguinte conjunto de atuações (RCM 12/2012, 2012):

- ✓ A criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNCSeg);
- ✓ O aprofundamento e melhoria das condições de operação do Sistema de Certificação Electrónica do Estado (SCEE), com vista à sua adequação aos requisitos internacionais mais recentes;
- ✓ A criação e certificação de uma solução de criptografia forte de origem nacional, bem como o desenvolvimento de soluções para a sua utilização e promoção junto dos potenciais utilizadores;
- ✓ A revisão do quadro legal para a segurança das matérias classificadas.

O prazo de implementação desta medida, liderada pelo GNS, foi definido na RCM 12/2012 para um período máximo de 12 meses, o que se verifica não ter sido possível cumprir. No entanto, existe já publicada no website do GNS (GNS, 2013) uma proposta de ENSI a aguardar aprovação final (ANEXO I), da qual se evidenciam os três principais objetivos a alcançar pelo país:

- ✓ Garantir a Segurança no Ciberespaço;
- ✓ Fortalecer a Cibersegurança das Infraestruturas críticas nacionais;
- ✓ Defender os Interesses Nacionais e a Liberdade de Ação no Ciberespaço.

Foi ainda constituída uma comissão instaladora do CNCSeg, a fim de se dar início aos trabalhos de implementação do referido centro (RCM nº 42/2012, 2012). A definição da ENSI e a constituição do CNCSeg aproximam-nos de outros países em termos de posicionamento estratégico na esfera da segurança dos sistemas de informação da AP, devendo por isso ser encaradas como prioridades nacionais.

No que concerne à medida 7, pretende-se definir uma estratégia para a implementação de uma rede de comunicações única ou um conjunto de redes de comunicações interligadas que sirvam a totalidade da AP, com gestão centralizada e global e integrando todos os serviços de dados e voz (RCM 12/2012, 2012).

O prazo de implementação estipulado no regulamento aponta para um período de 12 meses inerente à definição e divulgação de um modelo, o que se verifica não ter sido possível cumprir. Em complemento à medida 2, também esta medida traz ganhos de eficiência e de maior controlo na informação e nos ativos de cada ministério, promovendo assim a segurança nas TIC da AP.

Por outro lado, iniciativas menos recentes que as anteriores mas com evolução significativa nos últimos tempos, têm vindo a trazer contributos extremamente úteis para a prevenção e deteção de ataques nas infraestruturas de rede nacionais, em particular nas da Administração Pública.

É o caso dos contributos que derivam do Serviço de Resposta a Incidentes de Segurança Informática – CeRT.PT, dirigido pela FCCN, e da sua rede nacional de intervenientes para resposta a incidentes – CSIRT's.

O CeRT.PT tem, no panorama nacional, a missão de "contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal" (CeRT.PT, 2013).

No sentido de dar cumprimento à sua missão, atua basicamente da seguinte forma (CeRT.PT, 2013):

- ✓ Presta apoio a utilizadores de sistemas informáticos na resolução de incidentes de segurança, aconselhando procedimentos, analisando artefactos e coordenando ações com as entidades envolvidas;
- ✓ Reúne e dissemina informação relacionada com novas vulnerabilidades de segurança e produz recomendações referentes a potenciais riscos de segurança e atividades maliciosas em curso, no sentido de formar uma consciência de segurança junto dos utilizadores;
- ✓ Promove a criação de novos CSIRT em Portugal e a sua cooperação.

O CeRT.PT responde a incidentes de segurança informática no contexto da comunidade utilizadora da RCTS - Rede Ciência, Tecnologia e Sociedade.

A Rede Nacional de CSIRT's, com elo de ligação e coordenação CeRT.PT, tem como principais objetivos os seguintes (CeRT.PT, 2013):

- ✓ Estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança;
- ✓ Criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contramedidas pró-ativas e reativas;
- ✓ Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão;
- ✓ Promover uma cultura de segurança em Portugal.

De entre os seus membros, exemplificam-se o próprio CeRT.PT, o EMGFA, a FEUP, o IGFEJ, o INESC, a UTIS-MAI e a CGD.

Em Dezembro de 2012 a Rede Nacional de CSIRT's desenvolveu uma *framework* de tipificação dos Incidentes que pode ser utilizada não só pelos membros como também por outras entidades, uma vez que o documento foi tornado público e disponibilizado no website do CeRT.PT. Este output é apenas um exemplo de um dos contributos dos CSIRT's para a sociedade.

Outros aspetos relevantes são também os dois workshops de segurança por ano promovidos pela rede, a Informação estatística e os indicadores disponibilizados, o fórum técnico para troca de ideias e os alertas de segurança de forma constante ou sempre que se justifique. Contudo, e apesar de todos estes esforços que têm vindo a ser desenvolvidos para a melhoria da segurança nas redes e sistemas da Administração Pública, ainda prevalece alguma desarticulação entre os organismos, denotando-se, para além do risco inerente, algum desperdício na gestão das tecnologias de informação do setor público.

Da análise efetuada neste âmbito por SANTOS (2011), referente em concreto à governação da cibersegurança em Portugal, advém nomeadamente o seguinte:

- ✓ Não existe, dentro da estrutura funcional do Estado, nem no plano político, nem no plano estratégico, um ponto focal para as questões relativas à cibersegurança;
- ✓ Existe um vazio de responsabilidade e a ausência de uma estratégia abrangente para esta área;
- ✓ Num plano mais operacional interessa eliminar duplicações e preencher as omissões existentes.

No que respeita a esta problemática da Segurança podemos antecipar, teoricamente e em certa medida, as melhorias que o Plano Global Estratégico TIC trará para a AP, mitigando nomeadamente as preocupações anteriormente identificadas, uma vez que visa a definição da ENSI, a criação de um CNCSeg e a unificação das redes, dos centros de dados e da função TIC por ministério, entre outras medidas importantes (GPTIC, 2011).

No entanto, não existe por enquanto a definição de um modelo mais operacional e detalhado que explicite a melhor forma de interligação das redes dos ministérios e que, a partir dessa organização, identifique estrategicamente os mecanismos tecnológicos de contenção do risco, as suas localizações físicas e lógicas e os procedimentos básicos da sua implementação e gestão. Como forma de complemento aos contributos já identificados para a melhoria estratégica das redes e segurança da AP, esta dissertação pretende definir esse modelo de segurança que disponibilize alguns controlos preventivos e detetivos importantes para as infraestruturas de rede do Estado.

3. CARACTERIZAÇÃO DE CONTROLOS TÉCNICOS PREVENTIVOS E DETETIVOS

3.1. A IMPORTÂNCIA DA GESTÃO DO RISCO E DOS STANDARDS INTERNACIONAIS DE SEGURANÇA

Antes de se abordar a temática dos controlos técnicos preventivos e detetivos, faz sentido evidenciar a importância da gestão do risco e dos standards Internacionais de Segurança, bem como assinalar a forma como os poderão condicionar.

Como já referido, em Segurança dos Sistemas de Informação, o termo "Risco" representa a probabilidade de determinada ameaça comprometer a Informação (ou os sistemas) através da exploração de determinada vulnerabilidade. A gestão do risco é um processo que pretende avaliar e medir o risco, desenvolvendo as melhores estratégias para o gerir. Estas estratégias podem ir no sentido de evitar, reduzir, transferir ou mesmo aceitar o risco. É importante termos sempre presente que o risco e a segurança podem ser condicionados não só por estas ações que os intervenientes das próprias organizações podem tomar, como também por atitudes estratégicas que os adversários das organizações podem levar a cabo (SCHECHTER, 2004).

O processo de gestão do risco assume assim uma relevância nuclear na segurança dos Sistemas de Informação das organizações, não só ajudando a estabelecer os controlos de segurança mais adequados para mitigar cada risco, como também validando a sua real eficácia. Contudo, importa realçar que o objetivo primordial da gestão do risco é proteger as organizações e a capacidade de levarem a cabo a sua missão, e não apenas proteger de forma indistinta os seus sistemas de informação (BOWEN, HASH, WILSON, 2006). Daí advém a importância da categorização e valorização dos ativos do sistema de informação, bem como do seu alinhamento com os processos de negócio.

A gestão do risco pode ser, tipicamente, subdividida em 3 principais fases:

1) Avaliação de Risco
    - Identificar o âmbito da análise;
    - Identificar os ativos a proteger e valorizá-los;
    - Identificar os riscos (vulnerabilidades, ameaças, impacto e probabilidade de ocorrência);

- Identificar as oportunidades de melhoria
  - Avaliação Quantitativa (*Asset Value, Exposed Factor, Single Loss Expectancy, Annualized Rate of Occurence, Annualized Loss Expectancy*);
  - Avaliação Qualitativa (Baixo, Médio, Alto, Muito Alto, Crítico).

2) Mitigação de Riscos
   - Seleção da estratégia mais adequada (evitar, reduzir, transferir, aceitar);
   - Seleção dos controlos mais adequados (relação risco vs custo);
   - Recurso a Standards/ melhores práticas (ISO 27001, CobIT, etc).
3) Avaliação contínua
   - Monitorização constante;
   - Garantir que o sistema funciona permanentemente de forma tão segura quanto possível.

Em termos de avaliação do risco, podem-se então ser seguidos dois modelos distintos - Avaliação Quantitativa e Avaliação Qualitativa. O primeiro modelo utiliza informação objetiva e mensurável para determinar o valor dos ativos, a probabilidade da perda e os riscos associados. O segundo modelo utiliza uma medida mais relativa para medir o risco e o valor dos ativos, baseando-se em categorias descritivas, tais como risco "baixo", "médio" e "alto" e ativo "não importante", "importante" e "muito importante".

Segundo MACEDO (2009), ambos os modelos apresentam vantagens e desvantagens, devendo as organizações escolher cada um deles consoante entendam ser mais vantajoso. No passado recente a avaliação quantitativa dominava a gestão de risco em Segurança dos SI, tendência essa que mudou recentemente dado o grande esforço e dificuldade que apresenta, em relação os poucos benefícios alcançados quando comparada com a avaliação qualitativa (MACEDO, 2009). Independentemente do modelo de avaliação a adotar, e tendo em conta as ameaças cada vez mais complexas e constantes dos dias de hoje, importa reforçar que a gestão de risco é um processo imprescindível nas organizações atuais.

No que respeita aos standards internacionais de boas práticas de segurança, e tendo em conta que estes espelham métodos ou técnicas já testados com sucesso, é importante utilizá-los como referência uma vez que podem ajudar as organizações a alcançar os resultados pretendidos de forma mais eficaz e eficiente. Estes documentos oferecem recomendações das melhores práticas a levar a cabo, alertas dos riscos mais prementes e os controlos mais adequados dentro do contexto da segurança e dos Sistemas de Informação.

O exemplo por excelência de referencial de segurança dos Sistemas de Informação é o ISO/IEC 27001 que, com vista à implementação de um Sistema de Gestão da Segurança da Informação (SGSI) nas organizações, encaminha-as no processo de conformidade. Conforme refere GAIVÉO (2008), este SGSI desempenha um papel crucial nas organizações de hoje, possibilitando "processos e controlos apropriados à conceção, implementação, utilização e revisão das políticas de segurança, procurando o cumprimento da legislação em vigor, do normativo aplicado e das estratégias organizacionais". O ISO/IEC 27001, enquanto normativo/referencial de boas práticas de segurança, assume aqui um papel determinante na resiliência das organizações. Este processo de conformidade leva em linha de conta um conjunto de passos, dos quais se evidenciam os seguintes:

- ✓ Identificar os processos críticos para o negócio / definir o âmbito do sistema de gestão da segurança da informação;
- ✓ Identificar o risco a que os ativos e processos críticos de negócio estão expostos;
- ✓ Definir e planear a implementação de controlos de segurança com base na avaliação de risco;
- ✓ Implementar e gerir os controlos de segurança (Pessoas, Processos, Tecnologia);
- ✓ Rever, corrigir, melhorar (voltando ao início).

O ISO/IEC 27001 define as especificações para estabelecer, implementar, manter, monitorizar, auditar e melhorar um sistema de gestão da segurança nas organizações. Segundo este standard, os controlos devem garantir que os riscos identificados serão reduzidos para um nível aceitável, tendo em consideração o seguinte (ISO/IEC 27001, 2005):

- ✓ Os requisitos e restrições legais;
- ✓ Os objetivos da Organização;
- ✓ Os requisitos operacionais e as suas restrições;
- ✓ O custo da sua implementação em relação à criticidade do risco;
- ✓ A necessidade de equilibrar o investimento na implementação e operação dos controlos em relação à probabilidade de problemas derivados das falhas de segurança.

Em suma, todos estes processos inerentes à gestão do risco e à conformidade com os modelos de referência, são fatores que contribuem decisivamente para a melhoria contínua da segurança dos Sistemas de Informação nas organizações em geral e nos organismos públicos em particular.

3.2. CONTROLOS TÉCNICOS PREVENTIVOS

3.2.1. Firewalls

As necessidades incontornáveis de conetividade à rede por parte dos organismos públicos, essencialmente no que concerne aos serviços a disponibilizar ou a aceder na Internet, revelam-se numa oportunidade natural para a melhoria e simplificação dos seus processos mas também constituem riscos muito mais relevantes para os seus ativos e para o seu negócio.

Na constante guerra de mitigação destes riscos, as *firewalls* representam um controlo técnico preventivo crucial para a operação diária dos organismos públicos e das organizações em geral. Compõem a peça fundamental que servirá a base da estratégia de segurança das redes de dados na Administração Pública.

As *firewall's* são assim mecanismos que servem os princípios da comunicação segura entre duas ou mais redes, segregando o tráfego e limitando o seu fluxo consoante as regras que lhes são aplicadas. Funcionam como ponto central de isolamento dos ativos ligados à rede, restringindo acessos ilegítimos e controlando as interações entre ativos de redes distintas.

De uma forma generalista, pode-se então afirmar que as *firewall's* são instrumentos preventivos de filtragem de tráfego, tendo por base critérios como os endereços IP origem ou destino, o protocolo utilizado na comunicação, as portas/serviços de destino ou mesmo o tamanho do pacote recebido. Importa também referir que as suas configurações (regras) devem ser definidas de acordo com os requisitos de negócio das organizações e devem seguir um modelo em que os serviços/acessos só são permitidos quando são efetivamente necessários.

Não devendo ser considerada como a abordagem única e correta em termos de segurança, tipicamente na Administração Pública, as *firewalls* são de forma geral utilizadas como mecanismos para proteção de perímetro, ou seja, promovem o controlo e o limite do tráfego entre as redes inseguras (como a Internet) e as redes privadas de cada organismo; Desta forma, são muitas vezes descoradas necessidades de proteção entre os ativos da mesma rede. Uma outra abordagem, menos prática mas mais segura, é a da existência de mecanismos de proteção em profundidade, onde os recursos não devem depender exclusivamente de equipamentos externos para garantir a sua segurança. Esta visão promove, em acréscimo, também a criação de domínios de segurança na rede (agrupamento dos recursos consoante a sua criticidade), o estabelecimento de diversos níveis de *firewall* e a existência de mecanismos de controlo preventivo nos ativos de rede cliente (tais como *personal firewall's*, *HIPS's*, antivírus, etc).

Só desta forma, se um mecanismo de segurança central for comprometido, será possível conter-se a ameaça, recorrendo-se a formas de isolamento e a outros níveis de proteção existentes.

Apesar da existência de uma consciência generalizada acerca da importância crescente das *firewalls* nas redes da AP, ainda permanecem alguns riscos a este nível que facilmente se conseguem mitigar. Por exemplo, é importante que não se mantenham redes internas desprotegidas de tráfego proveniente de links externos recorrendo-se para isso a *firewalls* ou, no mínimo, utilizando-se software de *packet filtering*/ACL's existentes nativamente nos routers que terminam esses circuitos.

Por outro lado, é ainda de evitar que a gestão e manutenção diárias destes ativos críticos permaneça excessivamente dependente de *know-how* externo, por forma a que os organismos possam atuar de forma rápida e efetiva, preventivamente ou corretivamente, em caso de se verificar essa necessidade.

a. Tipificação

Desde os tempos em que o termo é conhecido (inícios dos anos 90) que as *firewalls* têm sofrido algumas evoluções e que têm proporcionado melhorias significativas na segurança das organizações. Segundo BOYLES (2010), podemos agrupar as implementações de *firewall* em quatro tipos distintos:

- ✓ Packet-filtering Firewall;
- ✓ Circuit-level Firewall;
- ✓ Application-layer Firewall;
- ✓ Stateful Firewall.

As *firewall* do tipo Packet-filtering são as implementações tradicionais que funcionam nos *layers* 3 e 4 do modelo OSI. Este tipo limita-se a examinar os pacotes que chegam, permitindo-os ou negando-os consoante o conjunto de regras definidas nas suas configurações. Os filtros, aplicados nos sentidos "in" ou "out" do interface, podem ser concebidos com base nos endereços de *layer* 3, no protocolo de transporte, nas portas de *layer* 4 ou no tamanho do pacote. É a forma típica de firewall disponível nos routers e nos sistemas operativos mais comuns, representando ainda hoje um tipo de implementação com uma relação custo/benefício interessante.

Contudo, apresenta algumas limitações na proteção, uma vez que não tem a capacidade para comparar um pacote com os antecedentes (sendo suscetível por exemplo a ataques de *ping flood* ou *SYN flood*), nem para disponibilizar autenticação dos utilizadores (não sendo possível controlar acessos por utilizador).

O tipo Circuit-level representa uma segunda geração de *firewall* que, em relação ao tipo anterior, traz a mais valia de conseguir determinar se o tráfego coincide com um novo pedido de conexão ou se pertence a fluxos de sessões já estabelecidas. Representa, por isso, uma melhoria ao nível da proteção.

Em relação às *firewalls* de Application-layer (terceira geração), operam até ao *layer* 7 do modelo OSI, conseguindo assim manter o rasto do estado das conexões, dos números de sequência, dos pedidos de utilizador/password, e de outros atributos do *layer* aplicacional. Estas implementações são também denominadas de *application gateway/proxy* na medida em que, do ponto de vista das máquinas das redes internas, são criadas conexões entre estas e a *firewall* e, só depois da negociação ser bem sucedida, é que esta estabelece a conexão com o destino. Assim, é possível esconder e proteger as máquinas internas das redes potencialmente perigosas. As desvantagens destas implementações são normalmente o consumo excessivo de recursos e o facto de não conseguirem dar resposta a ataques de *ping flood* e *SYN flood* (DoS).

As Stateful firewalls (quarta geração) são equipamentos capazes de manter o rasto da informação de estado a um nível muito mais baixo do que as da geração anterior. Desta forma, estas implementações conseguem inspecionar o header dos pacotes por forma a determinar se este faz parte de uma sessão já estabelecida ou não. Mantêm localmente uma tabela de estado com essa informação para ajudar na decisão de negar ou permitir o pacote. Representam um conceito importante para uma primeira linha de defesa das redes das organizações e demonstram níveis de performance muito superiores aos das *firewall* aplicacionais. Uma das suas grandes vantagens é conseguirem prevenir ataques de *Spoofing* e de DoS, uma vez que lhes é possível identificar tráfego anómalo.

A imagem seguinte exemplifica uma implementação deste tipo (MASON, 2011).

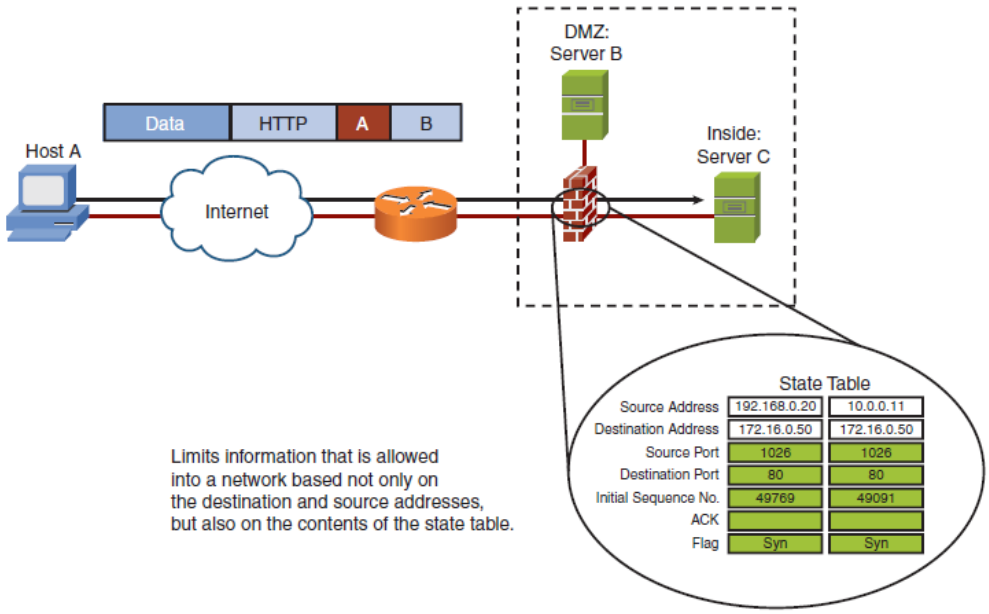


Ilustração 33 - Implementação com Stateful Firewall

Apesar das vantagens que apresentam, e ao contrário das do tipo anterior, estas *firewalls* não são capazes de providenciar autenticação de utilizadores nem de impedir ataques aplicacionais (tais como comandos malignos embebidos em *headers* HTTP*)*, uma vez que não interpretam informação de *layer* 7. Da mesma forma, apenas conseguem dar proteção eficaz a protocolos orientados à conexão como o TCP, apresentando o UDP e o ICMP proteção limitada nestas implementações.

Independentemente das suas desvantagens, este tipo de *firewall* é considerado o mais equilibrado, representando um standard para grande parte das infraestruturas de rede, podendo ser utilizadas em qualquer ambiente e providenciando um nível de inspeção capaz de preservar a integridade das redes que protegem (HENMI et al, 2006).

b. Demilitarized Zones

Um conceito de extrema importância indissociável das *firewalls* e que inevitavelmente se tem de abordar, é o conceito de *Demilitarized Zones* (DMZ's).

As DMZ's representam regiões específicas de rede localizadas entre as redes internas de uma organização (confiáveis) e as redes externas potencialmente inseguras (não confiáveis), como o caso da Internet. As *firewalls* são os equipamentos tipicamente utilizados para segregarem e controlarem o tráfego de rede entre estas zonas distintas.

As DMZ's, sendo redes de perímetro, disponibilizam serviços típicos para as redes externas, tais como acessos de Web Servers, FTP Servers, DNS e E-Mail que, ao serem acedidos a partir do exterior da organização, apresentam maior grau de exposição ao risco do que as suas redes internas. Assim, a ideia inerente às DMZ's (ao serem segregadas das redes seguras), reside essencialmente no facto de se pretender minimizar o potencial impacto em caso de um ataque a algum destes serviços vir a ser bem sucedido. Se a DMZ for comprometida e a *firewall* responsável pelo controlo deste tráfego estiver efetivamente bem configurada, as redes internas permanecerão a salvo.

c. Arquiteturas

Não obstante poderem existir bastantes variantes de implementação, sendo no final cada uma única e específica, tipicamente as arquiteturas de *firewall* são desenhadas a partir de dois modelos predominantes (NOONAN, DUBRAWSKY, 2006):

- ✓ Arquitetura Single-Firewall;
- ✓ Arquitetura Dual-Firewall.

A imagem seguinte esquematiza estas duas arquiteturas:

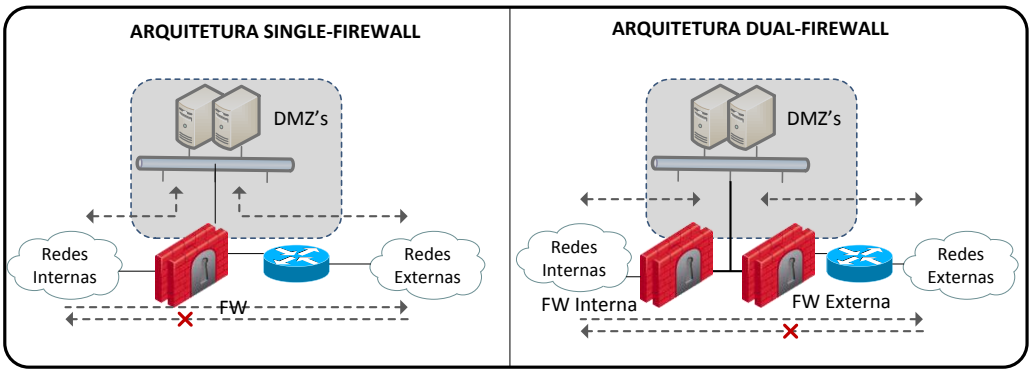


Ilustração 34 - Arquiteturas de Firewall

Conforme o seu propósito, a primeira arquitetura pode ser implementada com recurso a uma DMZ apenas (onde todos os recursos a aceder do exterior partilham o mesmo grau de exposição ao risco), com recurso a várias DMZ's (quando existe necessidade de separar os recursos a disponibilizar consoante requisitos de segurança), ou sem recorrer a nenhuma DMZ (quando não existe necessidade de disponibilizar serviços para o exterior).

Na arquitetura Single-Firewall o fluxo do tráfego é controlado em 3 direções:

- ✓ O tráfego das redes externas é permitido apenas para a DMZ;
- ✓ O tráfego da DMZ é permitido para as redes externas e internas;
- ✓ O tráfego das redes internas é permitido para a DMZ e para as redes externas.

Independentemente das possibilidades anteriores, só passará o tráfego explicitamente permitido nas regras definidas e aplicadas na *firewall*.

Por seu lado, a arquitetura Dual-Firewall, embora seja um pouco mais complexa e dispendiosa, proporciona maior segurança e um nível de controlo de tráfego superior. Nestas implementações, a *firewall* externa é especificamente configurada para controlar os acessos das DMZ's para o exterior e vice-versa, enquanto a *firewall* interna é responsável pelo controlo dos acessos entre as redes internas e as DMZ's, negando todo o fluxo proveniente das redes externas à organização. É a implementação típica para infraestruturas de rede mais críticas, importando referir que, para se tirar maior partido desta arquitetura, se devem utilizar duas *firewalls* de fabricantes distintos, por forma a ser possível minimizar a probabilidade de ambas virem a ser comprometidas.

d. Network Address Translation

Outra das funcionalidades importantes disponíveis nos diversos tipos de *firewall* é a sua capacidade de *Network Address Translation* (NAT). Trata-se de um conjunto de técnicas de modificação dos endereços de *layer 3* aplicadas sempre que se pretende quando os respetivos pacotes atravessam uma *firewall* (ou um router). A necessidade desta modificação pode-se prender com diversos fatores, dos quais se realçam:

- ✓ Por questões relacionadas com a proteção dos ativos, podendo existir vontade de se esconder os endereços IP reais dos mesmos, mascarando-os para determinadas redes através de objetos de NAT para o efeito;
- ✓ Por questões de carácter funcional, uma vez que endereços IP de gamas privadas são inválidos para a Internet, existindo necessidade de haver uma correspondência de um endereço IP capaz de ser comunicável através da rede pública.
- ✓ Por questões relacionadas com a racionalização de endereços, uma vez que com recurso a estas técnicas se potencia a possibilidade de partilha dos limitados endereços IP públicos por vários ativos da organização.

Segundo LAMMLE (2007), existem 3 formas típicas de *Network Address Translation*, a saber:

- ✓ Static NAT - Permite o mapeamento um-para-um entre endereços locais e endereços globais (endereços públicos ou de redes externas);
- ✓ Dynamic NAT - Permite o mapeamento de um endereço IP não registado com um endereço IP registado, dinamicamente a partir de uma *pool/range* de endereços registados; Não é necessário configurar os mapeamentos estaticamente, mas permanece a necessidade do espaço de endereçamento ser o mesmo entre ambos os tipos de endereços;
- ✓ Overloading ou *Port Address Translation* - É o tipo mais comum, permitindo o mapeamento de múltiplos endereços IP não registados a um único endereço registado, através da utilização de diferentes portas; com este mecanismo é, por exemplo, possível aos diversos ativos de uma rede interna acederem à Internet como se de um único IP público se tratasse.

Apesar do NAT representar uma funcionalidade com enormes potencial e utilidade, introduz também algumas desvantagens que convém identificar:

- ✓ Com o NAT perde-se a rastreabilidade na transmissão de pacotes entre a origem e o destino;
- ✓ A modificação dos endereços é um processo que também implica um acréscimo de atraso nas comunicações;
- ✓ Existem aplicações que não funcionam com este mecanismo ativado.

e. Exemplo de Produto de Firewall open-source

As soluções de *firewall* comerciais mais conceituadas do mercado apresentam custos de aquisição e de manutenção/licenciamento que em grande parte dos casos não se coadunam com a situação económico-financeira que os organismos da Administração Pública atravessam.

Não obstante de em casos críticos de proteção de recursos se entenda dever existir produtos comprovadamente mais robustos e seguros, capazes de tranquilizar a operação diária dos organismos públicos, em muitos dos casos a implementação de *firewalls open-source*, devidamente estudadas e testadas, poderá representar uma alternativa bastante interessante.

Neste ponto exemplifica-se uma *stateful firewall open-source* que pode servir os preceitos de muitos dos organismos públicos. Este produto é a plataforma do projeto *pfSense* que, tendo início em 2004, foi desenvolvida com base numa distribuição de FreeBSD.

O *pfSense* disponibiliza uma interface web com as comuns e atuais funcionalidades das *firewalls* comerciais. Entre essas funcionalidades evidenciam-se as seguintes (PFSENSE, 2013):

- ✓ Capacidade de Firewall
  - Filtragem de tráfego por SRC IP e DST IP, protocolo IP, SRC e DST port de tráfego TCP e UDP;
  - Capaz de limitar conexões em simultâneo;
  - Possibilidade de filtrar acessos à Internet por tipo de Sistema Operativo;
  - Capacidade de logging (ou não) por cada regra;
  - Política flexível de *routing* que permite balanceamento de carga, *failover*, etc;
  - Possibilidade de agrupar e atribuir nomes a IPs, redes e portas;
  - Capacidade de filtragem de layer 2;
  - Permite normalização de pacotes ("scrubbing").

- ✓ Tabela de Estado
  - Tamanho da tabela de estado ajustável;
  - Por cada regra permite:
    - Limitar as conexões em simultâneo;
    - Limitar os estados por host;
    - Limitar novas conexões por segundo;
    - Definir o *timeout* do estado;
    - Definir o tipo do estado.
  - Permite a otimização da tabela de estado.
- ✓ Network Address Translation
  - *Port forwards* incluindo ranges e utilização de múltiplos IPs públicos;
  - NAT 1:1 para IPs individuais ou subnets inteiras;
  - *Outbound* NAT;
  - NAT *Reflection* (no caso de ser necessário aceder-se a serviços por IP's Públicos através de redes internas.
- ✓ Redundância, possibilitando a configuração de várias *firewalls* como um grupo de *failover*.
- ✓ Balanceamento de carga

- ✓ VPN
  - IPsec;
  - OpenVPN;
  - PPTP.

As imagens seguintes exemplificam alguns aspetos do interface intuitivo da plataforma *pfSense* (PFSENSE, 2013).

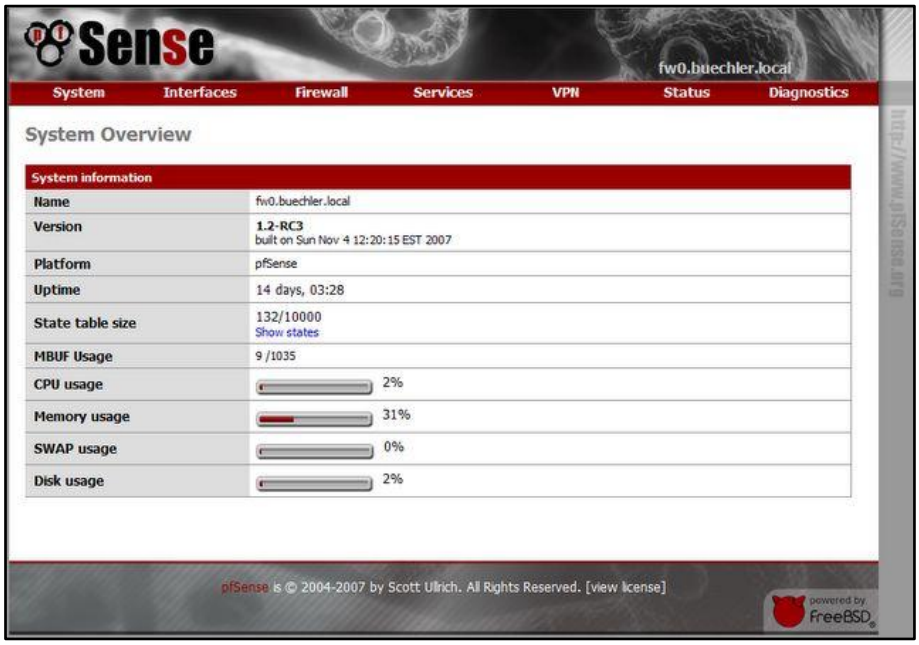


Ilustração 35 - pfSense: System Overview

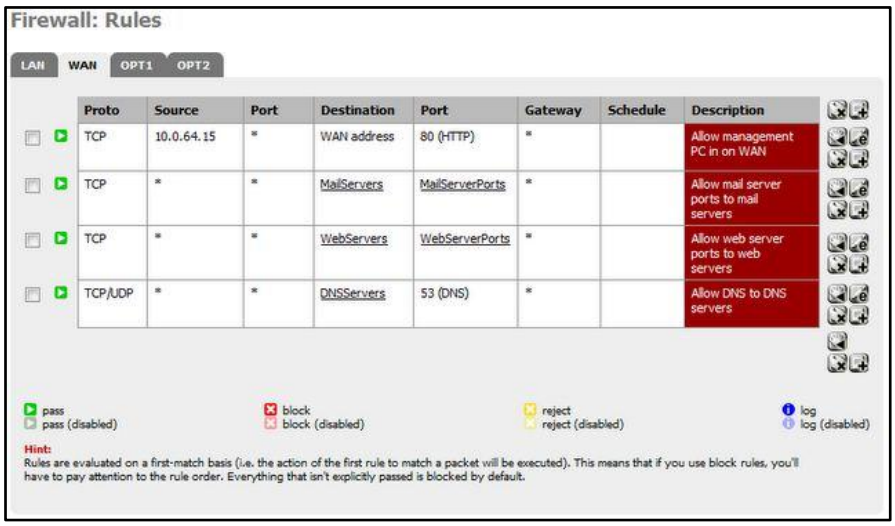


Ilustração 36 - pfSense: Firewall Rules

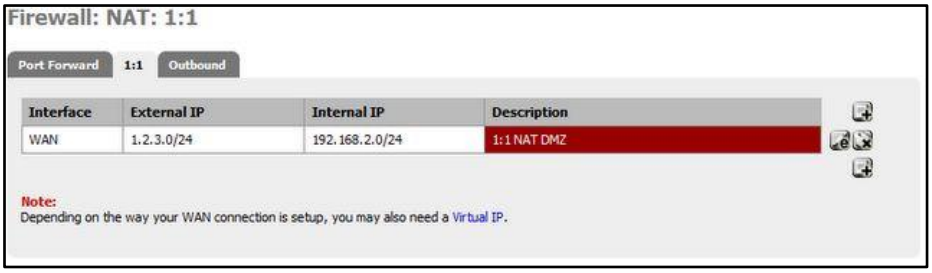


Ilustração 37 - pfSense: NAT

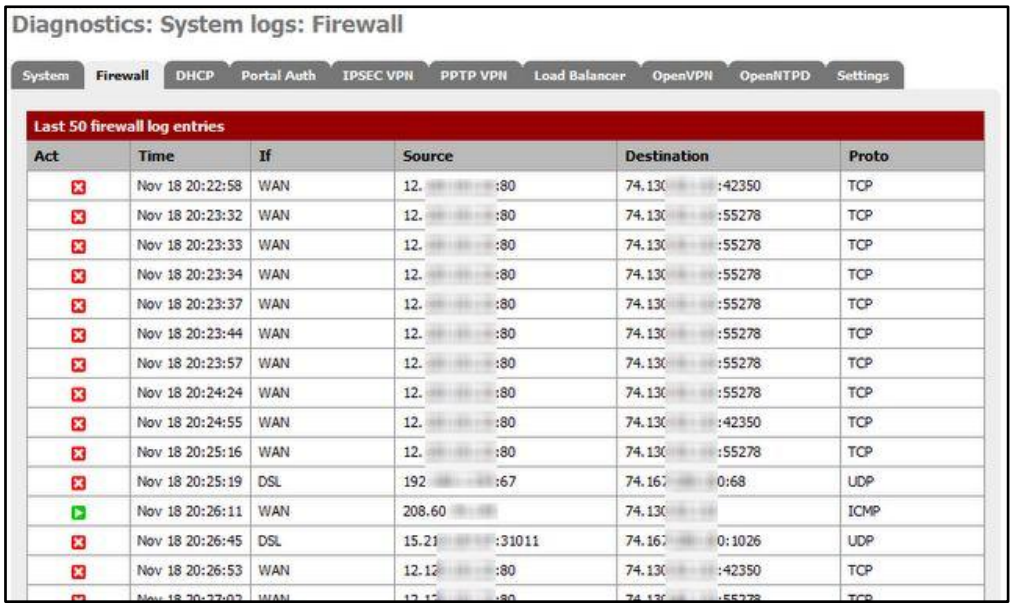


Ilustração 38 - pfSense: Logging

Outro ponto que pode acrescentar níveis de confiança a uma implementação deste tipo é o facto do projeto *pfSense* disponibilizar também, para além de suporte gratuito sobre as formas de fórum, mail e chat, um suporte comercial através da empresa fundada pelos criadores desta iniciativa. Por outro lado, são ainda indicadas no *site* do projeto as listas do *hardware* compatível com o produto bem como algumas empresas recomendadas para o fornecer (PFSENSE, 2013).

3.2.2. Virtual Private Network's

Outro aspeto de extrema importância a envolver na estratégia de segurança das redes de uma organização é a encriptação. Os mecanismos de encriptação permitem salvaguardar a integridade e a confidencialidade da informação sensível em trânsito.

Uma forma de transmitir informação encriptada é utilizando-se *Virtual Private Network's* (VPN's) nas comunicações. Como já abordado em pontos anteriores, as VPN's, que podem ser implementadas em modelos *site-to-site* ou *remote access*, são redes privadas que funcionam em cima de redes públicas como a Internet, através do estabelecimento de conexões virtuais ponto-a-ponto (como se de um túnel se tratasse); os seus extremos, após um processo de autenticação, encarregam-se de transferir os pacotes encriptados.

GREGORY (2010) ilustra na imagem seguinte alguns intuitos e formas para se estabelecerem VPNs:

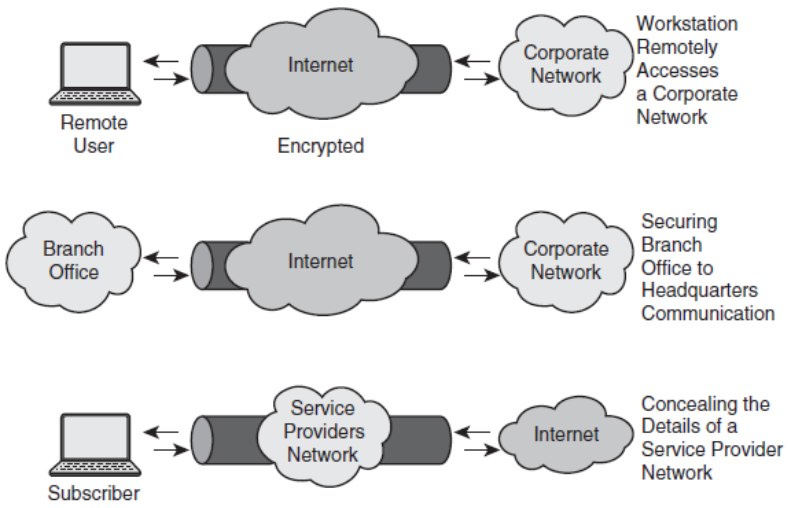


Ilustração 39 - Túneis VPN

As principais vantagens das VPN's residem na independência do meio físico (funcionando por exemplo em acessos à Internet de alto débito), na escalabilidade (sendo possível adicionar *sites* facilmente consoante as necessidades), na segurança (uma vez que permitem simular circuitos dedicados) e, principalmente, na poupança de despesa (quando comparamos com os custos de circuitos dedicados). Todos estes fatores constituem nos dias que correm impulsos importantes para a utilização de VPN's na Administração Pública. De acordo com EASTTOM (2012), as VPN's podem ser implementadas através dos três principais protocolos seguintes:

- ✓ Point-to-Point Tunneling Protocol (PPTP) - Funcionando no Layer 2 do modelo OSI, adiciona funcionalidades de autenticação e de encriptação de pacotes ao antigo Point-to-Point Protocol (PPP).
- ✓ Layer 2 Tunneling Protocol (L2TP) - Explicitamente desenhado como uma melhoria do PPTP, acrescentou métodos de autenticação (para além do CHAP e do EAP, contempla o PAP, SPAP e o MS-CHAP). Para além disso, funciona não só em redes IP como também em redes X.25 e ATM.
- ✓ Internet Protocol Security (IPsec) - O mais recente dos três protocolos identificados e cuja principal diferença é a capacidade de encriptação não só da informação do pacote como também dos headers, apresenta ainda proteção contra retransmissão não autorizada.

Em complemento, no que concerne a este último tipo de VPN's, BOYLES (2010) entende que as características apresentadas de seguida são consideradas as mais típicas e importantes do IPSec.

- ✓ Authentication Header (AH) - protocolo utilizado para providenciar integridade e autenticação aos datagramas IP (nos campos que tipicamente não se alteram);
- ✓ Encapsulation Security Payload (ESP) - pode proporcionar a mesma função que o AH embora consiga proteger o header IP na sua totalidade;
- ✓ Internet Security Association and Key Management Protocol (ISAKMP) - disponibiliza uma estrutura de autenticação e de troca de chaves;
- ✓ Internet Key Exchange (IKE) - baseado no ISAKMP, é utilizado para estabelecer as associações de segurança do IPSec;
- ✓ Hash Message Authentication Code (HMAC) - forma de cálculo do *Message Authentication Code* (código usado para autenticar uma mensagem), envolvendo uma função hash em combinação com uma chave secreta;
- ✓ Message Digest 5 (MD5) - Algoritmo de verificação de integridade que produz um valor *hash* de 128bits;
- ✓ Secure Hash Algorithm (SHA-1) - função de *hash* de 160bits que se assemelha à anterior MD5;
- ✓ Triple Data Encryption Standard (3DES) - algoritmo de encriptação que implementa a cifra do *Data Encryption Standard* (DES) três vezes em cada bloco de dados;
- ✓ Advanced Encryption Standard (AES) - Algoritmo de encriptação que também substitui o DES, aplicando a cifra de *Rijndael* mas com o tamanho do bloco fixo em 128bits (em vez de múltiplos de 32bits).

No entanto, para além das implementações típicas identificadas acima (sendo as mais comuns baseadas em IPSec), também se podem estabelecer VPN's SSL (*Secure Socket Layer*).

Com as VPN's IPSec, o túnel é estabelecido no nível de rede do Modelo OSI com software específico para o efeito, e o tráfego flui sem estar associado a qualquer aplicação, tornando-se os *end-points* virtualmente pertencentes à rede da organização. As VPN's SSL diferem das VPN's IPSec essencialmente nesta medida, uma vez que estabelecem os túneis associando-os diretamente a determinada aplicação e não a toda a rede. Tipicamente estes acessos são feitos por *web browser*, não permitindo que os utilizadores tenham acesso a outros ativos da rede que não a aplicação em causa.

O recurso às VPN's revela-se assim num método preventivo, simples de levar a cabo, que proporciona aos organismos públicos o alinhamento e a conformidade com as boas práticas de segurança referentes à transmissão de informação sensível.

a. Exemplo de Produto VPN open-source

Para o estabelecimento de túneis IPSec *site-to-site*, os organismos públicos podem recorrer à componente de VPN do produto *open-source pfSense*, identificado atrás.

Para a ligação de clientes remotos à rede da instituição existem várias alternativas *open-source* que se podem ter em linha de conta. Para este efeito, dá-se o exemplo da aplicação cliente *Shrew Soft VPN Client*.

Este software está disponível para clientes Windows e Linux e foi desenvolvido para o estabelecimento de comunicações seguras com gateways *open-source* baseadas em standards tais como o IPSec e o ISAKMP, vindo a evoluir as suas funcionalidades até à data. Evidenciam-se abaixo algumas das suas principais funcionalidades disponíveis (SHREW SOFT, 2013):

- ✓ Múltiplas opções de Firewall Traversal (NAT Traversal, NAT Keepalive, IKE Fragmentation);
- ✓ Múltiplos métodos de autenticação (PSK, RSA, etc);
- ✓ Cifras de 1ª fase (AES, Blowfish, 3DES, etc);
- ✓ Algoritmos hash de 1ª fase (MD5, SHA1);
- ✓ Algorítmos HMAC de 2ª fase (HMAC-MD5, HMAC-SHA1);

- ✓ Transformações de 2ª fase (ESP-AES, ESP-Blowfish, ESP-3DES, etc);
- ✓ Múltiplos modos de troca (rápido, essencial, agressivo, etc);
- ✓ Túnel mode;
- ✓ Banner;
- ✓ WINS Server;
- ✓ DNS Server.

Em termos de autenticação, esta aplicação utiliza o IKE do IPSec que define vários métodos para autenticar o cliente à gateway (SHREW SOFT, 2013):

- ✓ Autenticação Preshared Key - O Cliente e a Gateway têm que ter acesso a uma chave partilhada comum e, durante a autenticação, o *peer* a ser validado envia um valor *hash* (utilizando a chave partilhada e dados auxiliares) que é comparado pelo recetor com outro *hash* gerado localmente (utilizando a mesma chave partilhada e dados auxiliares); Só se coincidir é que o *peer* é considerado autêntico.
- ✓ Autenticação RSA - O *peer* a ser validado mantém um certificado digital assinado por uma autoridade certificadora (CA) e a chave privada do mesmo; durante a autenticação IKE, o *peer* a ser validado envia uma cópia do certificado e um *hash* assinado com a chave privada e o recetor verifica se o certificado foi assinado pela CA, bem como se o *hash* foi assinado pela chave privada do certificado. Só se coincidir em ambos os processos é que o *peer* é considerado autentico.
- ✓ Autenticação Estendida - Uma associação de segurança ISAKMP é estabelecida utilizando-se uma autenticação normal Preshared Key ou RSA e, seguidamente, o cliente terá de providenciar um user e uma password que a gateway validará junto de uma base de dados de utilizadores. Só se coincidir em ambos os processos é que o *peer* é considerado autentico.
- ✓ Autenticação Híbrida - Uma associação de segurança ISAKMP é estabelecida utilizando-se uma forma de autenticação modificada de RSA que apenas valida a gateway e, seguidamente, o cliente terá de providenciar um user e uma password que a gateway validará junto de uma base de dados de utilizadores. Só se coincidir em ambos os processos é que o *peer* é considerado autentico.

O software *Shrew Soft VPN Client* apresenta um interface gráfico intuitivo e simples de configurar, cujo aspeto se exemplifica nas imagens abaixo (SHREW SOFT, 2013).

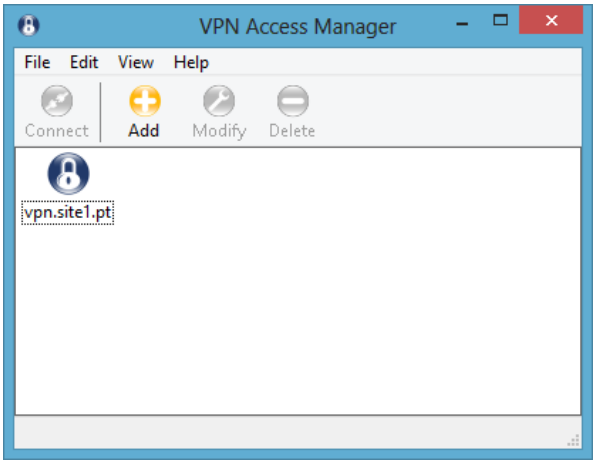


Ilustração 40 - Shrew Soft VPN Client: Access Manager

A janela "VPN Access Manager" é o primeiro interface deste software e permite-nos criar a ligação à gateway (clicando-se no botão "Add"), que neste caso está identificada como "vpn.site1.pt"; este nome terá que estar relacionado com um endereço IP num serviço de DNS que possa ser consultado a partir da Internet.

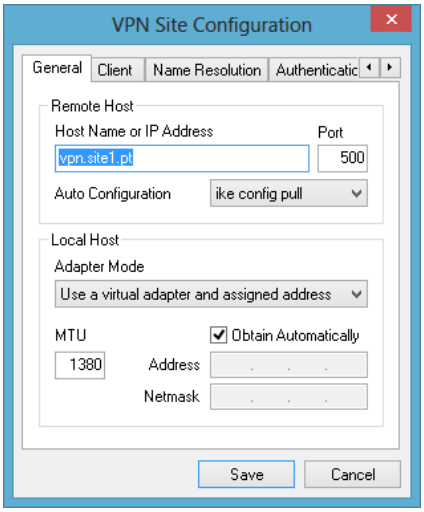


Ilustração 41 - Shrew Soft VPN Client: Definições gerais do site

O separador ilustrado na imagem abaixo permite-nos especificar o método de autenticação escolhido para o processo de ligação deste cliente à gateway; Neste exemplo, foi escolhida a opção de "Mutual RSA", tendo que ser selecionado o certificado "site1.p12" para o devido efeito.

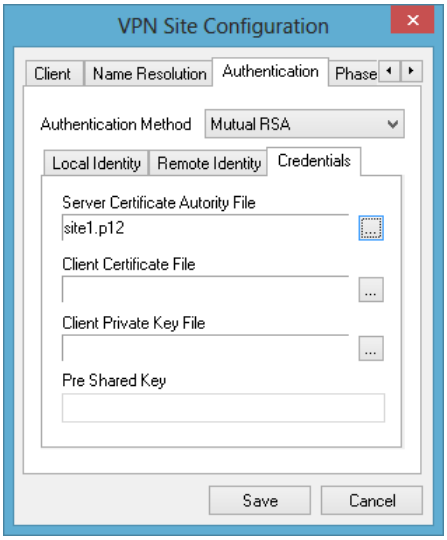


Ilustração 42 - Shrew Soft VPN Client: Método de autenticação

Em termos de suporte, a aplicação *Shrew Soft VPN Client* disponibiliza documentação do produto, guias de configuração, mailing lists, bug reports e uma área destinada a *Frequently Asked Questions* (FAQ's).

3.2.3. Proteções de Layer 2

As proteções de Layer 2 são determinantes para se conseguir mitigar uma fatia considerável dos riscos provenientes do interior da própria organização, devendo ser consideradas uma preocupação de carácter imperativo na operação diária dos organismos públicos.

Os mecanismos preventivos que se identificam neste ponto constituem medidas simples e com custos de implementação residuais, representando assim ainda mais uma razão para se melhorar a segurança nas redes internas da Administração Pública.

Apesar de existirem outras formas mais abrangentes e complexas de proteção no acesso à rede, como os sistemas de *Network Access Control* (NAC) que permitem ou negam o acesso de ativos à rede consoante uma política previamente definida de requisitos que estes têm de cumprir, estas exigem custos de implementação bastante mais elevados. Dada a conjuntura económico-financeira que o país atravessa e da qual os organismos públicos não se podem alhear, e não obstante destes sistemas de NAC melhorarem as componentes de segurança e de facilidade da gestão dos acessos à rede interna, consideram-se apropriados (quando bem implementados) os

mecanismos identificados de seguida, uma vez que mitigam eficazmente os principais riscos de ataques a partir da infraestrutura interna.

a. Proteção básica

Primeiro que tudo, importa salientar que a separação de funções, a sensibilização dos colaboradores e o seu respetivo treino no âmbito da segurança, assumem uma relevância determinante no que respeita à prevenção de incidentes de segurança provenientes do interior das próprias organizações. Análises relativas ao comportamento dos utilizadores finais expressam que problemas que afetam a segurança da informação têm sido minimizados devido à separação de funções, mas que existe ainda muita necessidade de se sensibilizar e de se treinar os utilizadores finais para as questões da segurança (KREICBERGA, 2010).

No que respeita às interações dos colaboradores com a rede em concreto, e para além das proteções físicas necessárias inerentes ao acesso condicionado às áreas onde se encontram ativos sensíveis (como os *switches* e *routers),* a melhor forma de se evitar que um dispositivo não permitido seja ligado é minimizando-se na infraestrutura da organização os pontos de acesso físico à rede. Isto é, as boas práticas e o bom senso indicam-nos que só devem estar estabelecidas as interligações entre os painéis da cablagem e os *switches* de rede nos pontos de conexão que efetivamente necessitam ter um dispositivo autorizado lá ligado. Acresce ainda que todas as portas dos *switches* que não tenham necessidade de estar em uso devem estar propositadamente desligadas, a fim de se minimizar o risco de acessos indevidos.

Por outro lado, a monitorização e o registo permanente dos *logs* de operação e de segurança nos ativos de rede, bem como o despoletar de mensagens para as equipas de gestão, consoante a sua severidade, são processos simples e de extrema importância para haver uma real noção da atividade na rede.

Outra forma de proteção básica muito importante é a existência de encriptação nos acessos de administração aos equipamentos de rede, por forma a se minimizar a probabilidade de ser capturada informação crítica como login’s e password’s. Um exemplo típico são os acessos por *telnet* que enviam esta informação sensível em clear, enquanto os acessos por *ssh* a transmitem de forma cifrada.

b. Port Security

O *Port Security* é um método simples e eficaz para se poder controlar que dispositivos poderão ter de facto acesso à rede da organização. A sua implementação é feita ao nível dos *switches* de rede e promove a mitigação de ameaças de *Layer 2*, tais como os ataques de "CAM table overflow" e de "MAC spoofing" abordados anteriormente. Com esta funcionalidade pode-se indicar na configuração dos *switches* qual o único (ou um conjunto de) *MAC Address* que se pretende ligar em determinada porta/interface e qual a ação a despoletar em caso de violação dessa regra.

Pode-se em alternativa configurar o equipamento para que o primeiro dispositivo a ser conectado em determinada porta seja "agarrado" (*sticky)*, sendo desencadeada uma ação quando for detetada uma tentativa de outro dispositivo tentar aceder à rede por essa via.

As configurações seguintes exemplificam estas opções de *Port Security*:

```
(…)
SW_PISO2(config)# interface fastethernet 0/5
SW_PISO2(config-if)# switchport port-security maximum 2
SW_PISO2(config-if)# switchport port-security violation shutdown
(…)
```

Neste caso, existe necessidade da porta/interface fast ethernet 0/2 poder dar acesso à rede a dois dispositivos ou *MAC Addresses* distintos. Esta necessidade pode-se verificar quando, por exemplo, um posto cliente corre uma máquina virtual em cima do sistema operativo nativo. A ação despoletada em caso de violação (quando um terceiro *MAC Address* se tenta ligar) é desligar a porta, cortando qualquer interação com a rede por essa via, sendo ainda enviada uma mensagem de *Syslog* e uma *trap SNMP* à equipa de gestão da rede.

No exemplo da configuração abaixo, é agarrado para a CAM table o primeiro *MAC Address* a ser ligado na porta fast ethernet 0/6 e, em caso de violação, em vez da porta ser desligada quando um *MAC Address* diferente do que aquele (que se encontra na tabela) se tenta ligar, apenas é incrementado um contador de violações e é enviada uma mensagem de *Syslog* e uma *trap SNMP* à equipa de gestão da rede.

```
(…)
SW_PISO2(config)# interface fastethernet 0/6
SW_PISO2(config-if)# switchport port-security mac-address sticky
SW_PISO2(config-if)# switchport port-security violation restrict
(…)
```

Uma opção mais segura, embora bem mais trabalhosa em termos de implementação e em termos de gestão corrente, é configurar-se explicitamente qual o MAC Address que se pretende permitir em cada uma das portas dos *switches*, desligando-se as mesmas no caso de se detetar uma tentativa de outro dispositivo aceder à rede.

```
(…)
SW_PISO2(config)# interface fastethernet 0/7
SW_PISO2(config-if)# switchport port-security mac-address e0db.55e1.9255
SW_PISO2(config-if)# switchport port-security violation shutdown
(…)
```

c. Proteções contra ataques ao Spanning Tree Protocol

Como explicitado atrás, os ataques ao *Spanning Tree Protocol* dão-se quando é introduzido um falso *switch* na rede, com uma prioridade baixa, para que este possa ser considerado o *root bridge* da nova topologia e o atacante consiga capturar o tráfego desviado para esse equipamento.

Segundo BOYLES (2010), os equipamentos de layer 2 podem mitigar os ataques de STP através de duas funcionalidades existentes:

- ✓ Através do Root Guard - Configuração de segurança a ativar em todas as portas dos *switches* que não sejam *root ports*, protegendo-as de se virem a tornar *root ports* após receberem uma BPDU com essa indicação de alteração topológica. A proteção é refletida abaixo.

```
(…)
SW_PISO2(config)# interface fastethernet 0/8
SW_PISO2(config-if)# spanning-tree guard root
(…)
```

- ✓ Através do BPDU Guard - Configuração de segurança disponível quando se ativa o *portfast* (funcionalidade que coloca as portas em modo *forwarding* rapidamente, em vez de entrarem na operação normal do algoritmo do STP). Como se assume que as portas em *portfast* têm diretamente ligado um dispositivo cliente e não outro *switch*, não existindo portanto a probabilidade de, por aí, existirem loops na rede, em circunstâncias normais, estas portas não têm necessidade de receber BPDU's (sendo suspeito quando recebem). Esta proteção força que a porta seja desligada no caso de receber mensagens BPDU's.

```
(…)
SW_PISO2(config)# interface fastethernet 0/9
SW_PISO2(config-if)# spanning-tree portfast bpduguard
(…)
```

d. Proteções contra ataques a VLAN's

A existência de VLAN's na infraestrutura interna, segregando o tráfego consoante critérios bem definidos e reduzindo os domínios de broadcast na rede representa, só por si, uma melhoria de segurança a generalizar nos organismos públicos.

No entanto, tendo em conta as ameaças identificadas a este nível, existe ainda necessidade de se levar a cabo medidas complementares por forma a serem reduzidos estes riscos de ataques.

No que respeita ao ataque de "Double Tagging", pode facilmente ser mitigado o seu risco de ocorrência ao não ser utilizada a *Native* VLAN1 nos *switches* para transmissão de dados, VLAN por defeito utilizada pelos hackers para este fim (BOYLES, 2010); O exemplo seguinte demonstra uma *Native* VLAN configurada para ser uma VLAN não utilizada:

```
(…)
SW_PISO2(config)# interface gigabitethernet 0/1
SW_PISO2(config-if)# switchport trunk native vlan 333
(…)
```

Por outro lado, para se reduzir os riscos de ataque de "Switch Spoofing", em que o atacante força a conexão a um *switch* legítimo através de uma *trunk port* em "*auto negotiation mode"*, podendo desta forma capturar o tráfego de várias VLAN's, devem também ser tomadas algumas medidas de proteção.

Segundo BOYLES (2010), os dois simples processos seguintes são eficazes na mitigação dessa ameaça:

- ✓ Desligar todas as portas em *trunk* não utilizadas, ou colocá-las em modo *access*, para terem acesso apenas a uma VLAN.

```
(…)
SW_PISO2(config)# interface fastethernet 0/10
SW_PISO2(config-if)# switchport mode access
(…)
```

- ✓ Nas portas *trunk* em uso, desabilitar o *Dynamic Trunk Protocol*.

```
(…)
SW_PISO2(config)# interface gigabitethernet 0/24
SW_PISO2(config-if)# switchport trunk encapsulation 802.1q
SW_PISO2(config-if)# switchport mode trunk
SW_PISO2(config-if)# switchport trunk nonenegotiate
(…)
```

Mais uma vez, reforça-se a ideia de que estas medidas de prevenção resultam da aplicação de configurações simples de efetuar e sem custos relevantes associados, razões pelas quais deverão ser, sempre que possível, levadas em consideração na estratégia de segurança dos organismos públicos.

3.3. CONTROLOS TÉCNICOS DETETIVOS

3.3.1. Antivírus

Os Antivírus são mecanismos tecnológicos de proteção que se enquadram simultaneamente nos conjuntos dos controlos de segurança do tipo preventivo, detetivo e corretivo. Apesar de serem constituídos por peças de software desenvolvidas com o intuito de evitar, detetar ou remover a instalação de *mallware* em sistemas, será dada enfase à sua capacidade de deteção destas ameaças, razão pela qual este tema está embutido no ponto "3.3 Controlos Técnicos Detetivos".

As ferramentas de Antivírus, ao serem capazes de detetar a existência de código (potencialmente) malicioso, bloqueando-o para minimizar o seu impacto, têm um carácter determinante na estratégia de segurança das organizações atuais. Nos dias que correm, torna-se assim imprescindível a existência de Antivírus permanentemente atualizados nos postos-cliente das organizações, minimizando-se a probabilidade dos ativos da rede virem a ser comprometidos e favorecendo-se assim a lógica da proteção em profundidade.

Existem vários tipos de tecnologias de deteção que os fabricantes utilizam com o intuito de tornar os seus produtos de Antivírus o mais eficientes possível, isto é, reduzir ao máximo os falsos positivos, disponibilizando ao mercado uma ferramenta capaz de ser efetivamente segura e de não comprometer de forma significativa a performance do sistema. Estes tipos de métodos de deteção são por vezes pouco claros e as suas nomenclaturas sujeitas a interpretações distintas por parte dos vários quadrantes da comunidade.

a. Métodos de deteção

Em termos de métodos de deteção de vírus em sistemas, os mais comuns e generalizadas nas ferramentas de Antivírus atualmente disponíveis no mercado são os seguintes:

- ✓ Deteção por assinatura - Baseia-se em reconhecimento de padrões; ao examinar o *filesystem,* o Antivírus compara o código fonte dos ficheiros com uma base de dados de assinaturas de mallware que deverá permanecer atualizada.
- ✓ Heurística - Técnica idêntica à anterior mas promovendo a deteção de novo mallware (que não se encontra na base de dados de assinaturas), examinando os ficheiros à procura de um conjunto de características genéricas suspeitas; técnica adequada para identificar novas variantes do mallware já conhecido.
- ✓ Proteção Proactiva - O software de Antivírus examina o sistema tentando identificar em tempo real processos suspeitos, bloqueando-os antes de causarem danos.
- ✓ Emulação - Possibilita o carregamento de programas num ambiente virtual que simula o ambiente do sistema, permitindo ao software de Antivírus observar o comportamento dos programas sem colocar em risco o sistema ou a informação.
- ✓ Sandboxes - Representa uma extensão à emulação e é uma área virtual isolada que interceta todas as interações entre o sistema e o exterior; se houver uma interação exterior a tentar promover uma alteração no sistema, essa alteração é efetuada temporariamente na Sandboxe e sujeita a aprovação do utilizador para ser posteriormente (e com carácter permanente), efetuada no sistema.
- ✓ Deteção por comportamento - Em vez de verificar meramente como um programa é construído, ou de emular a sua execução, esta técnica de deteção observa como um programa é executado; se for detetado comportamento anormal (exemplo de modificação do ficheiro de hosts, ou descompactação de código suspeito), o programa é marcado. A utilização deste tipo de deteção nas ferramentas de Antivírus, aproxima-as ao conceito dos *Host-based Intrusion Prevention Systems* que tradicionalmente representavam produtos de categoria distinta.

Por forma a minimizar as interpretações distintas das nomenclaturas referentes aos métodos de deteção de mallware, a empresa de segurança Kaspersky disponibiliza um modelo de distribuição dos mesmos, agrupando-os tendo em conta a sua componente técnica (técnicas de recolha de informação a utilizar na identificação de código malicioso) e a sua componente analítica (algoritmos de análise da informação recolhida).

No que respeita à componente técnica da visão da Kaspersky, são evidenciadas as seguintes funções de recolha de informação para a posterior análise (SHEVCHENKO, 2008):

- ✓ Examinar ficheiros, extraindo dados dos ficheiros e estruturando esses bytes de forma a serem transmitidos nas condições apropriadas à componente analítica.
- ✓ Capacidade de emulação, separando o código dos programas em comandos e carregando cada comando num ambiente virtual paralelo.
- ✓ Capacidade de virtualização (Sandbox), executando os programas no ambiente real do sistema, mas sob determinadas regras e orientações.
- ✓ Monitorizar eventos do sistema, implicando a observação simultânea de todos os programas para compreender o seu impacto no funcionamento global; A informação é capturada, intercetando as funções do sistema e gerando estatísticas a transferir à componente analítica.
- ✓ Pesquisa de anomalias no sistema, comparando o status momentâneo do sistema integrado com um status de referência (identificado como saudável).

Relativamente à componente analítica, os métodos de deteção podem ser distribuídos em três categorias distintas, tendo em conta a forma utilizada para a análise da informação previamente recolhida (SHEVCHENKO, 2008):

- ✓ Algoritmos de comparação simples - Cujo veredicto resulta da comparação de um único objeto com uma amostra disponível, sendo o seu resultado binário (sim/não). Exemplo: identificar código malicioso localizando determinada sequência de bytes, ou identificar um programa suspeito através de determinada ação que promove no sistema.
- ✓ Algoritmos de comparação complexa - Cujo veredicto resulta da comparação de múltiplos objetos com as amostras correspondentes, sendo o seu resultado baseado em probabilidades. Exemplo: identificar código maliciosos utilizando várias assinaturas não determinantes quando analisadas de forma isolada.
- ✓ Algoritmos de análise detalhada - Cujo veredicto só é emitido após haver uma análise sofisticada dos dados, incluindo elementos de inteligência artificial. Exemplo: identificar código maliciosos recorrendo, não a um rigoroso conjunto de parâmetros, mas sim a uma avaliação multifacetada de todos os parâmetros de uma só vez, tendo em conta a probabilidade individual de cada parâmetro e calculando o resultado global.

Com recurso a estes dois vetores e a esta visão integrada, a imagem seguinte ilustra o modelo referido (SHEVCHENKO, 2008):

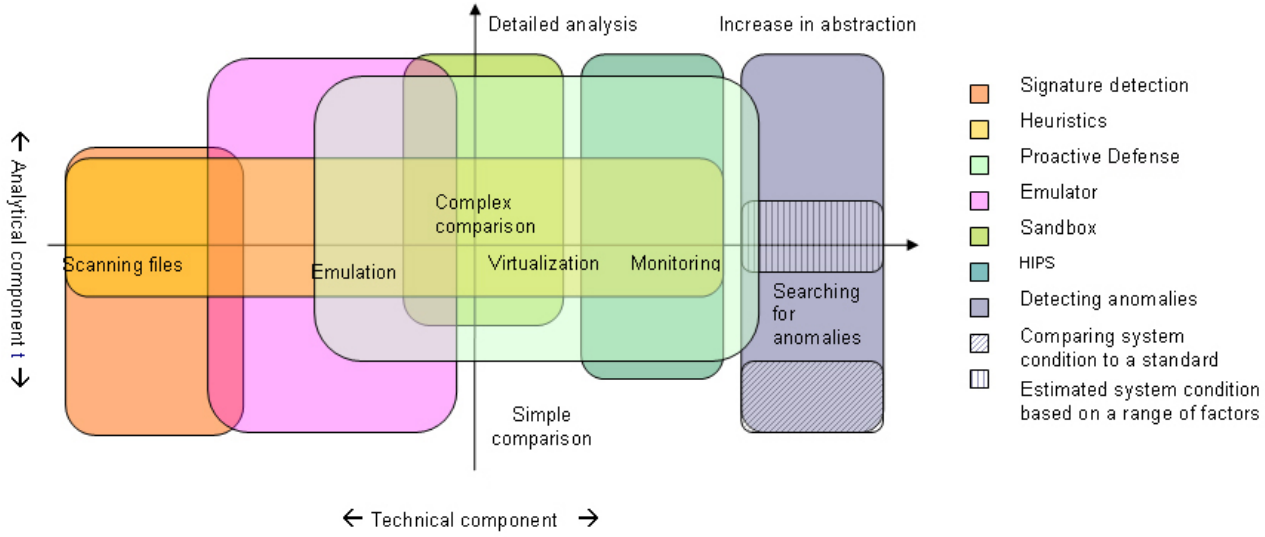


Ilustração 43 - Modelo de avaliação dos métodos de deteção de mallware

Este modelo poderá contribuir não só para facilmente se enquadrar os múltiplos métodos de deteção de código malicioso nas diferentes vertentes de recolha de dados e da posterior análise, como também poderá servir de suporte à avaliação dos próprios métodos de deteção disponíveis nos diversos produtos atuais de Antivírus.

b. Exemplo de Produto de Anti-vírus open-source

Atualmente existe bastante variedade de software de Antivírus no mercado, o que, apesar de dificultar a decisão da escolha, promove a competitividade e a melhoria dos produtos à nossa disposição. Numa altura particularmente difícil em termos de orçamento disponível nos departamentos de IT da Administração Pública e das organizações em geral, as opções por ferramentas gratuitas e *opensource* assumem cada vez mais enfase, representando pelo menos uma hipótese plausível a ponderar. No que respeita aos softwares de Antivírus em concreto, apesar de existirem numerosas opções gratuitas a utilizar na vertente de consumo doméstico, na realidade empresarial esta escolha ainda se encontra de alguma forma limitada, uma vez que muitos fabricantes possibilitam a utilização gratuita dos seus produtos em ambiente doméstico, mas não legitimam a sua utilização no interior das organizações.

Um exemplo de Antivírus que pode claramente jogar a favor da contenção de despesa no meio empresarial é o software *open-source* ClamAV.

O ClamAV, apresentando já alguma maturidade e respeito na comunidade, é uma ferramenta construída para ambientes baseados em sistemas UNIX. Desenhado especialmente com a preocupação de examinar e-mail, apresenta em termos genéricos o seguinte conjunto de funcionalidades (CLAMAV, 2013):

- ✓ Scanner (examinador) de ficheiros na linha de comandos;
- ✓ Interface para o sendmail (servidor de mail em sistemas UNIX);
- ✓ Sistema de update da Base de Dados avançado com suporte para scripting dos updates e assinaturas digitais;
- ✓ Livraria C de examinação de vírus;
- ✓ On-access scanning (apenas para Linux e FreeBSD);
- ✓ Base de Dados de mallware passível de updates várias vezes por dia;
- ✓ Suporte nativo para vários formatos de ficheiros, nomeadamente Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS, entre outros;
- ✓ Suporte nativo para a maioria dos formatos de ficheiros de mail;
- ✓ Suporte nativo para executáveis ELF e executáteis protáteis comprimidos com UPX, FSG, Petite, NsPack, wwpack32, MEW;
- ✓ Suporte nativo para formatos populares de documentos, tais como ficheiros de MS Office, de MacOffice, HTML, RTF e PDF.

Uma opção para sistemas Windows que utiliza o motor de Antivírus do ClamAV, é o produto desenvolvido posteriormente denominado de ClamWin. Este software disponibiliza, também de forma gratuita, as seguintes principais características (CLAMWIN, 2013):

- ✓ Altas taxas de deteção de vírus e *spyware;*
- ✓ Agendamento da examinação do sistema (Scheduling);
- ✓ Downloads automáticos e regulares dos updates da BD de mallware;
- ✓ Vírus Scanner isolado e integrado com o menu do Windows Explorer;
- ✓ Integração com o MS Outlook para remoção de anexos infetados.

Um contra identificado neste produto é o facto de não disponibilizar uma forma automática e em tempo real de examinar o sistema, tendo que ser despoletada manualmente essa função pelo utilizador para que a ferramenta possa averiguar a eventual existência de mallware instalado. No entanto, o utilizador (ou o administrador) do sistema, pode perfeitamente agendar previamente estes scans nos períodos do dia que entender mais apropriados, com recurso à funcionalidade de *Scheduling*.

A ilustração seguinte exprime as principais interfaces do produto, nas suas componentes de entrada, configuração, update e de examinação.

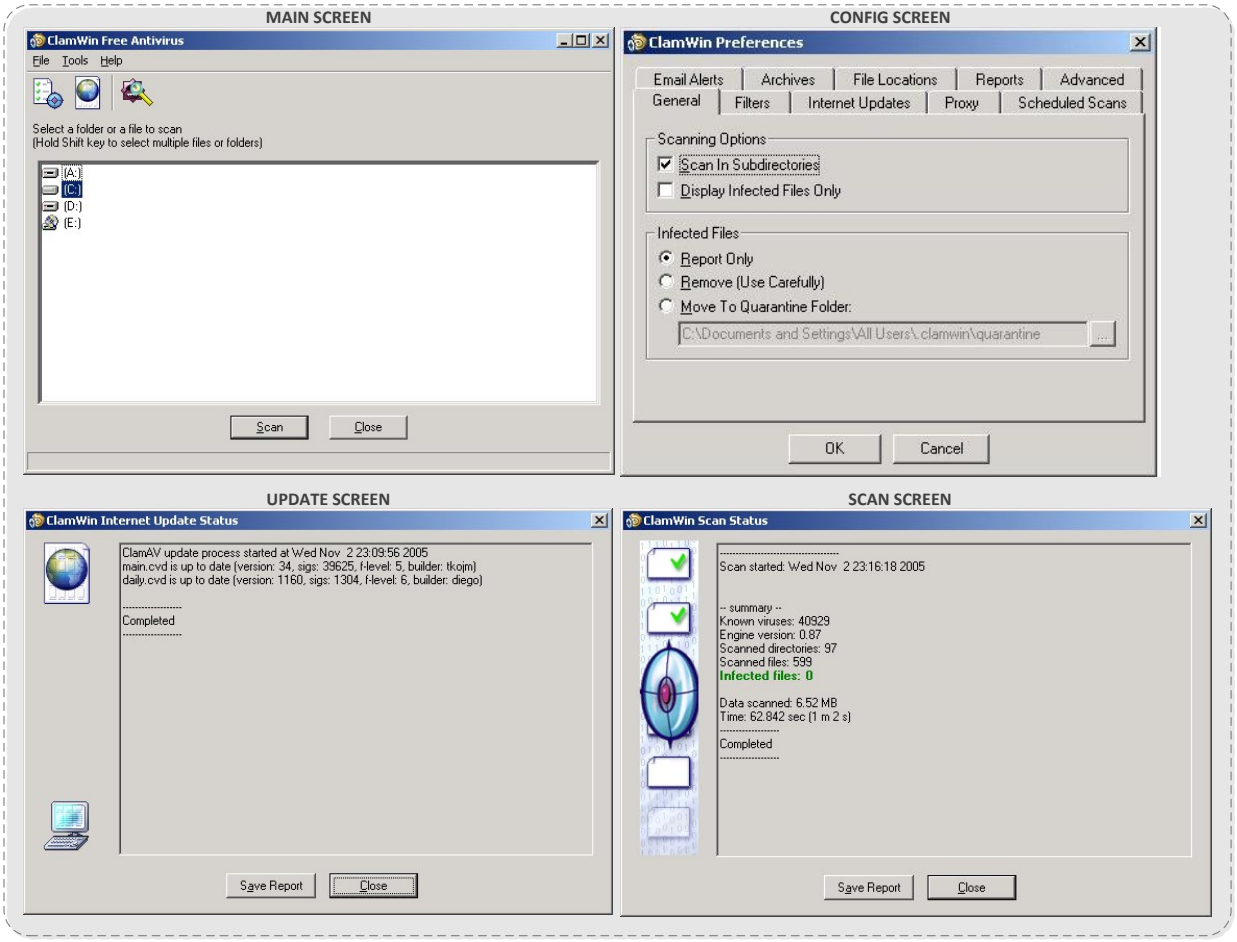


Ilustração 44 - Interfaces do ClamWin

No que respeita ao suporte do software, pode-se apenas contar com a disponibilização gratuita, por parte das equipas responsáveis pelos produtos ClamAV e ClamWin, de documentação, fóruns e mailing list's para o efeito.

3.3.2. Intrusion Detection Systems

Os Sistemas de Deteção de Intrusão (IDS) são utilizados para a monitorização de atividades suspeitas ou maliciosas nas redes das organizações. Um IDS, de uma forma genérica, funciona como um sniffer de rede que analisa o conteúdo/informação dos pacotes que passam no meio físico, comparando-o com uma base de dados referente a anomalias ou potencial atividade maliciosa. Os sistemas de IDS são hoje em dia, por isto mesmo, uma peça fulcral na estratégia de segurança da informação a circular nas redes de dados.

Este tipo de controlo técnico detetivo vai também ao encontro do conceito de proteção em profundidade, uma vez que, se um determinado mecanismo de segurança de perímetro (como uma firewall ou um IPS) não for suficiente para prevenir/evitar determinado ataque, com os sistemas de IDS estrategicamente distribuídos na rede, será em princípio possível identificar essa ação maliciosa, possibilitando assim, ainda atempadamente, que se tomem as devidas medidas de contenção desse ataque.

Numa fase inicial do seu aparecimento, e de forma generalizada, os IDS's não apresentavam capacidade reativa quando deparados com eventos maliciosos, limitando-se a identificá-los e a fazerem o *report* dos mesmos às equipas envolvidas. Esta capacidade reativa que, de forma automática, permite bloquear o ataque antes dele efetivamente se concretizar, é o elemento chave que distingue os sistemas de Deteção de Intrusão dos Sistemas de Prevenção de Intrusão (IPS). Cada vez mais, tem-se notado evolução no sentido destes sistemas aparecerem disponíveis de forma integrada, ou seja, com as componentes de deteção e de reação a funcionarem em harmonia.

a. Necessidade de utilização e objetivos fundamentais

O objetivo primordial dos Sistemas de Deteção de Intrusão é, naturalmente, melhorar a segurança das redes, servindo de complemento aos tradicionais mecanismos de proteção, como é o caso das firewall's. De entre outros objetivos importantes dos IDS que contribuem para melhorar a segurança, destacam-se os seguintes:

- ✓ Detetar a generalidade das anomalias de rede, classificando os ataques, os vírus e outras ameaças através, nomeadamente, da observação dos portos e serviços onde é detetada atividade suspeita;
- ✓ Dar a conhecer quais as principais violações de segurança na rede e as respetivas vulnerabilidades associadas;
- ✓ Implementar políticas de segurança centralizadas;
- ✓ Proporcionar estatísticas de potenciais ataques reais;
- ✓ Disponibilizar inputs para tratamento de incidentes;
- ✓ Antecipar e prevenir potenciais ataques futuros.

Esta necessidade genérica de melhoria contínua da segurança nas redes de dados pode derivar de um conjunto de *inputs* tecnológicos, de negócio ou regulamentares que despoletam o reforço da importância da temática de intrusão em redes. Entre esses *inputs* que intensificam a relevância dos IDS's, BIRDI (2006) dá ênfase aos seguintes:

- ✓ Alterações estratégicas de negócio - As organizações têm que, por vezes, levar a cabo iniciativas para melhorar a sua competitividade no mercado, incrementando constantemente a sua presença na Internet. Estas necessidades revelam-se não só em oportunidades, como também em riscos que devem ser controlados.
- ✓ Requisitos regulamentares - Os requisitos legais e regulamentares no meio eletrônico têm vindo a evoluir ao longo das últimas décadas e é previsível que este progresso continue com a constante modernização tecnológica. Exemplos disso são as decisões judiciais com base em evidências forenses e a legislação da proteção dos dados pessoais e documentos eletrónicos.
- ✓ Gestão de expectativas - Muitas organizações têm sido afetadas por incidentes informáticos que resultam na exposição de informações confidenciais, na indisponibilidade de sistemas ou na quebra da integridade da sua informação. Estes casos, e as correspondentes expectativas e confiança dos *stakeholders* culminam em perdas concorrenciais para as mesmas.
- ✓ Dependência dos Sistemas de Informação - A atual utilização imprescindível dos SI revela-se no aumento abrupto dos custos de interrupção. Uma deteção oportuna com a resposta adequada a uma indisponibilidade pode evitar custos bastante significativos.
- ✓ Evolução do número e sofisticação das ameaças nas redes - As ameaças atuais mudam o cenário de risco das organizações; Os mecanismos de controlo devem ser constantemente reavaliados a fim de se adaptarem a cada ambiente em particular.

b. Métodos de deteção e tipificação de IDS

À semelhança do que acontece com os mecanismos de Antivírus, também os sistemas de Deteção de Intrusão apresentam diversos métodos para detetar a ocorrência de atividades anómalas ou maliciosas.

As tecnologias disponíveis nas soluções de IDS atuais combinam frequentemente as diversa metodologias de deteção existentes, de forma integrada ou separada, com o intuito de proporcionarem uma deteção de intrusões mais abrangente e fidedigna.

De acordo com SPEROTTO (2010), um IDS alcança os seus objetivos de deteção ao distinguir o que é atividade normal daquilo que é atividade intrusiva. Contudo, estas classificações implícitas são passíveis de erro, considerando-se "falsos positivos" as atividades normais observadas como intrusivas e "falsos negativos" as atividades intrusivas não detetadas.

Por sua vez, os inputs corretamente classificados como ataques assumem a nomenclatura de "verdadeiros positivos" enquanto os inputs corretamente classificados como atividade normal, correspondem a "verdadeiros negativos".

Deve haver um equilíbrio natural entre querer-se detetar toda a atividade maliciosa (obtendo-se um nº elevado de falsos positivos) e considerar-se perder alguma dela, obtendo-se muitos falsos negativos mas poucos falsos positivos (SPEROTTO, 2010).

Os principais métodos de deteção de ameaças neste âmbito são os seguintes (SCARFONE, MELL, 2007):

- ✓ Deteção por assinatura - É o processo de comparação dos eventos observados com a base de dados de assinaturas (padrões que correspondem a ameaças conhecidas), de forma a ser possível identificar se estamos perante a ocorrência de um incidente ou não. Este método é muito eficaz na deteção de ameaças conhecidas, mas ineficaz na deteção de ameaças desconhecidas e de ameaças conhecidas disfarçadas, através de técnicas de evasão. É, assim, o método mais simples de deteção, uma vez que se limita a operações de comparação de strings entre uma unidade de atividade (como um pacote ou uma entrada de log) e uma lista de assinaturas conhecidas.

- ✓ Deteção baseada em anomalias - É um processo mais complexo, caracterizado pela comparação entre um conjunto de eventos observados no sistema e um padrão de definições (de users, hosts, acessos, aplicações, etc) que compõem um perfil de atividade considerado normal. Com esta comparação é possível identificar-se, se ocorrerem desvios significativos a esse padrão, se estamos perante atividade considerada anormal ou maliciosa. A principal vantagem deste método é ser muito eficaz na deteção de ameaças anteriormente desconhecidas. No entanto, importa referir que, uma vez que os sistemas e redes estão em constante mutação, o perfil correspondente a um comportamento dito normal, também deverá ser permanentemente ajustado, sob pena de poder vir a tornar a deteção imprecisa. Um outro problema deste método é o facto de, muitas vezes, ser difícil validar se na base de um alerta está verdadeiramente atividade maliciosa ou se trata apenas de um falso positivo, devido à complexidade e número de eventos que podem ter causado esse alerta.
- ✓ Deteção pela análise de estado dos protocolos - É o processo de comparação de um conjunto de eventos observados no sistema com perfis de definições referentes a atividade benigna em cada estado dos protocolos. Com este método, o IDS é capaz de compreender e acompanhar o estado dos protocolos das camadas de rede, transporte e aplicação. Pode identificar sequências inesperadas de comandos, tais como a emissão do mesmo comando várias vezes (como em ataques DoS), ou detetar a emissão de um comando sem anteriormente ser detetado outro seu precedente/dependente. Geralmente, inclui verificações de razoabilidade em comandos individuais, tais como comprimentos mínimos e máximos para os seus argumentos. As principais desvantagens deste método são o consumo elevado de recursos, o facto de não detetar ataques que não violem o comportamento aceitável dos protocolos, e de poder entrar em conflito com a forma como os protocolos são implementados em determinadas versões.

Paralelamente à questão dos métodos de deteção, os IDS's podem também ser categorizados com base na localização dos seus sensores (LUAN, 2010):

- ✓ IDS de host (*Host-based IDS*, HIDS) - Sistema de deteção de intrusão instalado em determinado host (um servidor ou um posto cliente) com o intuito de monitorizar apenas os seus recursos em busca de atividade maliciosa. Os sensores locais são os primeiros a inspecionar o sistema, tendo acesso a logs, memória, *registry*, tráfego, etc. Apresentam de forma integrada as componentes de sensores, mecanismo de análise e consola de gestão. A sua principal vantagem é conseguir obter dados de elevada qualidade a partir de inspeção local, uma vez que opera junto do kernel;

A principal desvantagem deriva do facto da sua operação ser local e individual, não apresentando por isso capacidade de deteção de ataques destinados a outros ativos que não ele próprio.

- ✓ IDS de rede (*Network-based IDS*, NIDS) - Sistema de deteção de intrusões que, instalado em equipamento dedicado para o efeito, captura e analisa o tráfego de rede em determinadas localizações da mesma, com o intuito de proteger de atividade maliciosa um conjunto de ativos pertencentes a essa rede. Por forma a ser possível examinar todo o tráfego e a deteção de ameaças em (quase) tempo real, estes sistemas são tipicamente colocados nos perímetros de cada segmento de rede. A sua principal vantagem é o facto de conseguir proteger um conjunto de ativos ligados à rede, sem estes que tenham de ter qualquer software adicional instalado; As principais desvantagens são os problemas de performance quando o tráfego for demasiado elevado (levando a perda de pacotes) e a impossibilidade de examinar o tráfego encriptado (embora continue a ser possível analisar o volume de tráfego e os protocolos e endereços de origem e de destino).
- ✓ IDS Híbrido - Sistema de deteção de intrusões que tem vários agentes/sensores instalados num conjunto de hosts da rede (ou em todos), em que cada agente capta informação potencialmente pertinente (como atividade local ou tráfego de rede) e envia-a para uma consola central responsável pela sua análise. Esta consola central disponibiliza ainda um interface de gestão e controlo que permite, por essa via, a configuração da totalidade do sistema. A sua principal vantagem reside no facto de conseguir obter uma grande abrangência quer ao nível da rede, quer ao nível dos recursos locais de cada host, o que proporciona uma quase certa deteção no caso de uma intrusão se verificar; Contudo, este facto pode-se refletir também na sua principal desvantagem, uma vez que os pesados e heterogéneos processamentos e tráfego de rede que lhe estão inerentes têm impacto significativo na performance dos hosts que têm os agentes de IDS instalados.

c. Arquitetura genérica

Independentemente de existirem arquiteturas específicas a cada tipo de solução disponível no mercado, e de ser possível adotar-se com cada uma dessas soluções esquemas de implementação diversos, existem algumas componentes funcionais comuns que compõem a arquitetura base dos sistemas de IDS. Essas componentes já têm sido abordadas em pontos anteriores e assumem em termos arquiteturais papéis bastante distintos.

Segundo LUAN (2010), cada IDS apresenta três componentes funcionais primordiais:

- ✓ Sensores - É a componente responsável por coletar a informação pertinente na rede e/ou sistema e encaminhá-la para o "Mecanismo de análise" para ser examinada.
- ✓ Mecanismo de análise - É a componente que recebe os inputs dos sensores, analisando-os e determinando se correspondem ou não à ocorrência de uma intrusão. É nesta componente que entram os diferentes métodos de deteção abordados atrás. No caso do mecanismo de análise entender que um tipo de atividade verdadeiramente legítima é considerada anómala, estamos perante um "falso-positivo" na deteção; se por contrário, entender que atividade verdadeiramente maliciosa é considerada normal, estamos então perante um "falso-negativo".
- ✓ Consola de gestão - É a componente que disponibiliza à equipa de gestão um interface para poder configurar o IDS, controlar os sensores e avaliar o output do mecanismo de análise.

Acrescentam-se ainda a estas três componentes duas outras que se entende serem também de extrema importância para a arquitetura base e que são comuns aos diversos tipos de implementações:

- ✓ Base de Dados de Regras - É a componente que dá apoio à decisão por parte do mecanismo de análise se se está ou não perante uma intrusão; é neste repositório que estão, por exemplo, identificados os padrões de ameaças conhecidas.
- ✓ Geração de alertas e logging - É a componente que despoleta os alertas e armazena a informação dos eventos registada pelas diversas componentes; a informação registada nos logs pode, por exemplo, servir para se validar posteriormente atividade maliciosa ou mesmo para correlacionar esses eventos com outras fontes disponíveis.

Para o sucesso na deteção de intrusões, e para que o valor acrescentado dos IDS não se transforme num problema de desempenho e de gestão, todas estas componentes necessitam funcionar de forma articulada, seja em implementações centralizadas ou em implementações distribuídas pela rede.

O esquema seguinte sintetiza esta articulação e demonstra a interdependência existente entre as componentes referidas da arquitetura genérica.

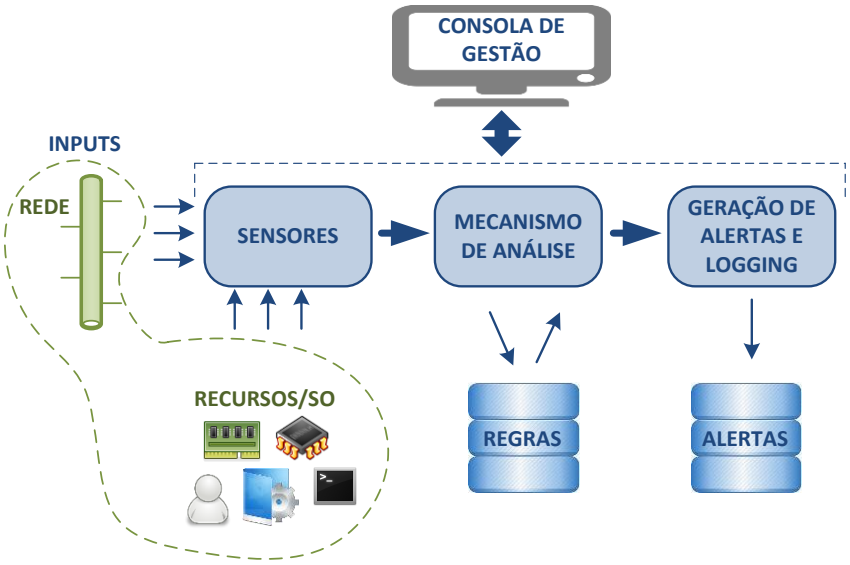


Ilustração 45 - Arquitetura genérica dos IDS's

Como visto anteriormente, para que seja possível haver uma tomada de conhecimento de potencial atividade maliciosa extensível a toda a rede e que, portanto, afete vários ou mesmo todos os ativos, é necessário haver sensores estrategicamente distribuídos na infraestrutura. Por forma a facilitar a gestão e mesmo a racionalizar alguns custos inerentes, é importante que seja possível, com uma arquitetura distribuída destas, centralizar toda a informação de eventos e disponibilizá-la de forma integrada e percetível às equipas responsáveis pela administração da solução. Assim, uma implementação distribuída simples e típica de um sistema integrado de deteção de intrusões, pode ser a refletida no diagrama seguinte:

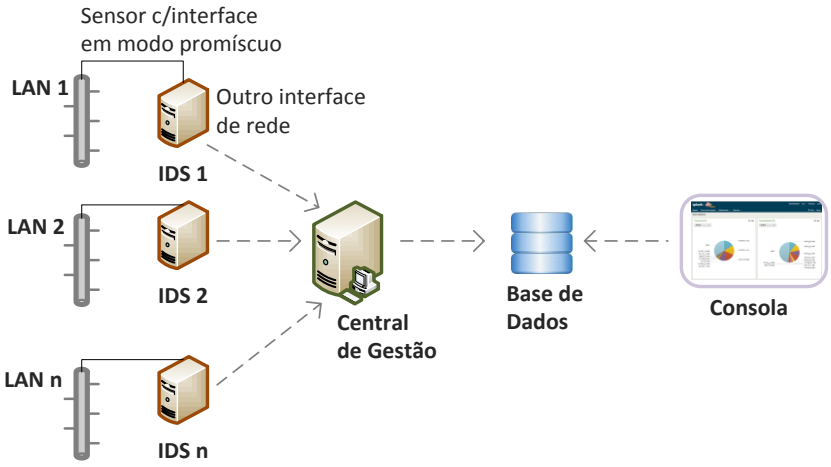


Ilustração 46 - Implementação distribuída de IDS's

Os IDS's, na sua componente de "sensores de rede" capturam o tráfego através de um interface colocado em modo promíscuo, ou seja, sem endereço IP associado e a capturar todos os pacotes que circulam nesse segmento de rede. Se detetarem intrusão, através da sua componente de "mecanismo de análise", reportam de forma cifrada os eventos de alertas desencadeados a um servidor remoto denominado no diagrama de Central de Gestão. Os IDS's, independentemente do seu fabricante, utilizam tipicamente para esta tarefa de reporte o standard IDMEF (Intrusion Detection Message Exchange Format), para que os eventos sejam interpretados através de uma linguagem única.

Este servidor Central de Gestão processa os eventos recebidos, correlaciona-os e armazena-os numa base de dados. Por fim, disponibiliza essa informação devidamente organizada numa consola Web, para que a equipa responsável pela gestão da segurança possa analisar os eventos gerados a partir dos vários IDS's distribuídos, de forma fácil, intuitiva e eficaz.

d. O uso de SPAN/ RSPAN

O Switched Port Analyzer (SPAN) e o Remote Switched Port Analyzer (RSPAN) são funcionalidades dos equipamentos de switching que permitem que seja analisado o tráfego em determinada porta ou VLAN, com o intuito de se poder determinar se existem problemas ou intrusões na rede. Representam, por isto, funcionalidades muito importantes quando se pretende implementar um sistema de deteção de intrusão.

A configuração do SPAN envolve a seleção de uma "porta origem" do switch, referente ao tráfego que se pretende analisar, e de uma "porta destino" do switch, relativa à interligação com o analisador de tráfego (tipicamente um IDS ou um sniffer de rede). A funcionalidade de SPAN é simples e fácil de implementar e permite replicar todo o tráfego que passa em determinado interface, noutro que estejamos a monitorizar. Por exemplo, se tivermos uma firewall no interface gigabitethernet 0/24 de determinado switch e pretendermos averiguar se existe atividade anómala dela proveniente, podemos instalar um IDS por exemplo na porta gigabitethernet 0/2 e, efetuando os seguintes dois comandos, conseguimos ativar a capacidade de monitorização de todo esse tráfego (BOYLES, 2010):

```
Switch1(config)# monitor session 1 source interface giga 0/24
Switch1(config)# monitor session 1 destin interface giga 0/2
```

Contudo, o SPAN só pode ser configurado e aplicado a um único switch, o que implica que tenha de haver um IDS por cada switch da infraestrutura, se pretendermos atingir esse nível de abrangência. Daí resulta a importância do RSPAN que permite a poupança de custos em IDS's, proporcionando que um único IDS monitorize vários segmentos da rede.

Se pretendermos, por exemplo, que um IDS analise o tráfego proveniente da Internet e o tráfego do piso de um departamento crítico (por exemplo do departamento Financeiro), podemos recorrer ao uso do RSPAN.

A figura e as configurações seguintes exemplificam um caso destes em que facilmente se pode colocar um sensor IDS a monitorizar várias zonas sensíveis da rede da organização (BOYLES, 2010):

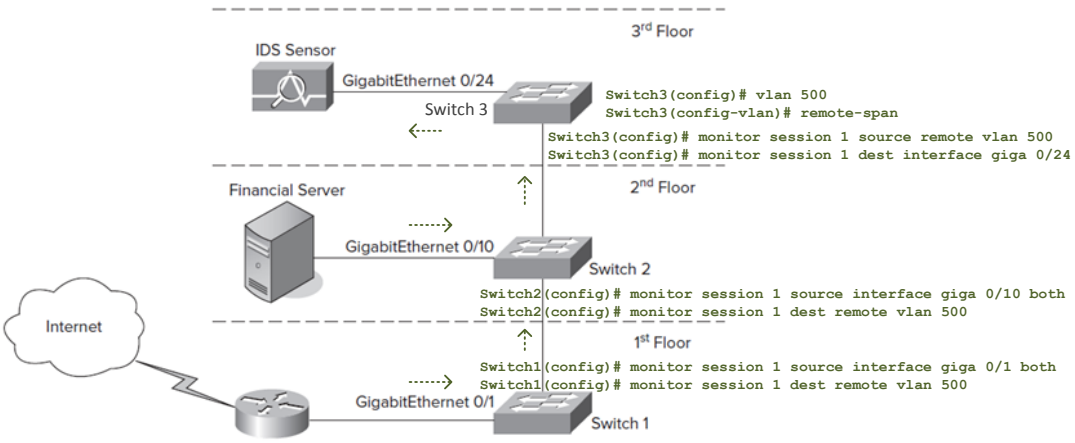


Ilustração 47 - Exemplo de configuração de RSPAN para uso de um IDS

e. Exemplo de Produto de IDS open-source

Devido à sua excelência e aceitabilidade tecnológica, selecionou-se como exemplo de IDS o produto *open-source* Snort.

O Snort é um IDS de rede (NIDS) desenvolvido pela Sourcefire (atualmente uma empresa Cisco) que combina os métodos de deteção por assinatura, deteção baseada em anomalias e deteção pela análise de estado dos protocolos. Foi criado no final da década de 90 e desde então que tem evoluído e crescido enquanto produto, apresentando atualmente também capacidades preventivas e sendo aceite mundialmente como o NIDS de eleição.

O Snort encontra-se estabilizado na versão 2.9.5.5 e existem binários disponíveis para sistemas operativos Windows e Linux. Pode ser executado em três modos distintos (PROJETO SNORT, 2012]):

- ✓ Modo de Sniffer - Simplesmente disponibiliza no ecrã, continuamente, o conteúdo dos pacotes que são lidos a partir da rede;
- ✓ Modo de Logger de pacotes - Regista no disco o conteúdo dos pacotes lidos a partir da rede, para posterior análise;
- ✓ Modo NIDS - Modo mais complexo que permite ao Snort analisar o tráfego de rede, comparando-o com o conjunto de regras definidas, e desencadear ações com base nessa análise.

O Snort é constituído por vários elementos que caracterizam a sua arquitetura e que funcionam em conjunto para o sucesso da deteção de ataques. A interdependência destes elementos é ilustrada no fluxograma abaixo:

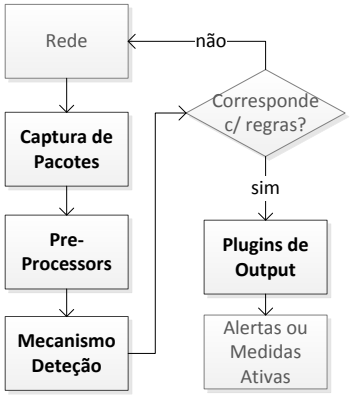


Ilustração 48 - Elementos constituintes do Snort e suas interdependências

Cada um destes elementos é resumidamente explicado de seguida:

- ✓ Captura de pacotes - Captura e prepara os pacotes provenientes de diferentes tipos de interfaces de rede para serem pré-processados e enviados para o mecanismo de deteção.
- ✓ Pre-processors - Utilizados para normalizar os cabeçalhos dos protocolos e detetar anomalias na construção dos pacotes; São elementos/plug-ins que podem ser usados para reconstruir ou modificar dados dos pacotes antes do mecanismo de deteção realizar qualquer operação. Muitos atacantes utilizam fragmentação de pacotes para poderem enganar os IDS's; Para estes casos, os pré-processadores do Snort fazem desfragmentação de pacotes, integram streams TCP, etc.

- ✓ Mecanismo de deteção - O motor de deteção do Snort é um dos seus elementos mais importantes, sendo responsável por detetar atividades de intrusão refletidas nos pacotes de rede. Para este efeito, são lidas regras em bases de dados internas, onde é verificada a correspondência com os pacotes. Caso um pacote corresponda a alguma regra, serão desencadeadas as ações apropriadas/definidas; Caso contrário, o pacote é descartado da análise e flui normalmente.
- ✓ Plugins de Output - Dependendo do que o mecanismo de deteção encontra no pacote, este elemento despoleta as ações de logging, de geração de alertas e, a partir da versão 2.9 do Snort, de tomada de medias ativas de prevenção de intrusão. Esta última capacidade de reação exige que o IDS esteja colocado na rede em modo Inline (todo o tráfego passa por ele, entrando num interface e saindo por outro) para que, em tempo real, seja possível bloquear os pacotes anómalos. A desvantagem é que possíveis falsos-positivos inibem o tráfego legítimo.

O Snort é uma ferramenta extremamente apreciada na esfera tecnológica e apresenta custos de implementação bastante reduzidos, trazendo grande benefício para as organizações, no contexto da deteção e prevenção de intrusões em redes.

3.3.3. Auditorias à rede para deteção de vulnerabilidades

De acordo com MOELLER (2010), a influência global da Web, juntamente com as necessidades crescentes de segurança, de controlo interno e de auditoria, foram tornando os controlos técnicos muito mais importantes nos dias que correm. Daí advém a relevância das auditorias periódicas à rede para a deteção de vulnerabilidades nas tecnologias de informação das organizações atuais. Estas auditorias assumem a forma de controlo técnico que serve simultaneamente de validação a outros controlos técnicos já implementados. Apesar de representarem um conjunto de ações propositadamente despoletadas na rede para a deteção de vulnerabilidades, podendo por isso serem detetadas ameaças concretas em exploração dessas mesmas vulnerabilidades, estas auditorias podem-se também exprimir como medidas de carácter preventivo, uma vez que visam a redução do risco *a priori*, por intenção de diminuição da quantidade de vulnerabilidades ou da criticidade das mesmas. As vulnerabilidades, em maior ou menor quantidade, com maior ou menor criticidade, existem permanentemente e podem sempre ser exploradas. As auditorias de vulnerabilidades devem, assim, ser encaradas como procedimentos periódicos, com vista à melhoria contínua no âmbito da segurança em redes.

São caracterizadas pelo processo de identificação, quantificação e classificação de vulnerabilidades da rede ou de sistemas que nela estão interligados, culminando em recomendações de mitigação do risco de exploração das mesmas. A classificação destas vulnerabilidades leva em linha de conta a sua criticidade, no que respeita à probabilidade de serem exploradas e ao potencial impacto que haverá para a organização se isso acontecer. Este processo de levantamento de vulnerabilidades nos ativos da rede consiste essencialmente em três etapas fundamentais que devem ser levadas a cabo por uma ordem específica (MANZUIK, PFEIL, GOLD, 2007):

1º. Recolha de Informação/ descoberta;
2º. Enumeração;
3º. Deteção.

a. A recolha de Informação/ Descoberta

Esta etapa resume-se à averiguação de qual o âmbito da avaliação. Consiste em identificar e determinar o total de sistemas e aplicações que serão alvo de avaliação, recolhendo-se informação de hostnames, de endereços IP, de portos disponíveis e de outras especificidades de contacto com os alvos. Pode ser composta por dois tipos de ações (MANZUIK, PFEIL, GOLD, 2007):

- ✓ Ações de carácter não-intrusivo - Quando se recolhe informação considerada pública acerca dos alvos envolvidos;
- ✓ Ações de carácter semi-intrusivo - Sempre que se recolhe informação complementar à pública, embora de forma não disruptiva.

Um exemplo deste passo com ações não-intrusivas é o uso de consultas de *whois* para os nomes de domínio dos alvos, obtendo-se diversa informação, nomeadamente os respetivos endereços IP.

A imagem seguinte reflete um exemplo destes, recorrendo-se a uma ferramenta de *whois* disponível via web no *site* http://who.is, e através da qual se consegue obter um conjunto de informação referente a um qualquer host disponível na Internet.

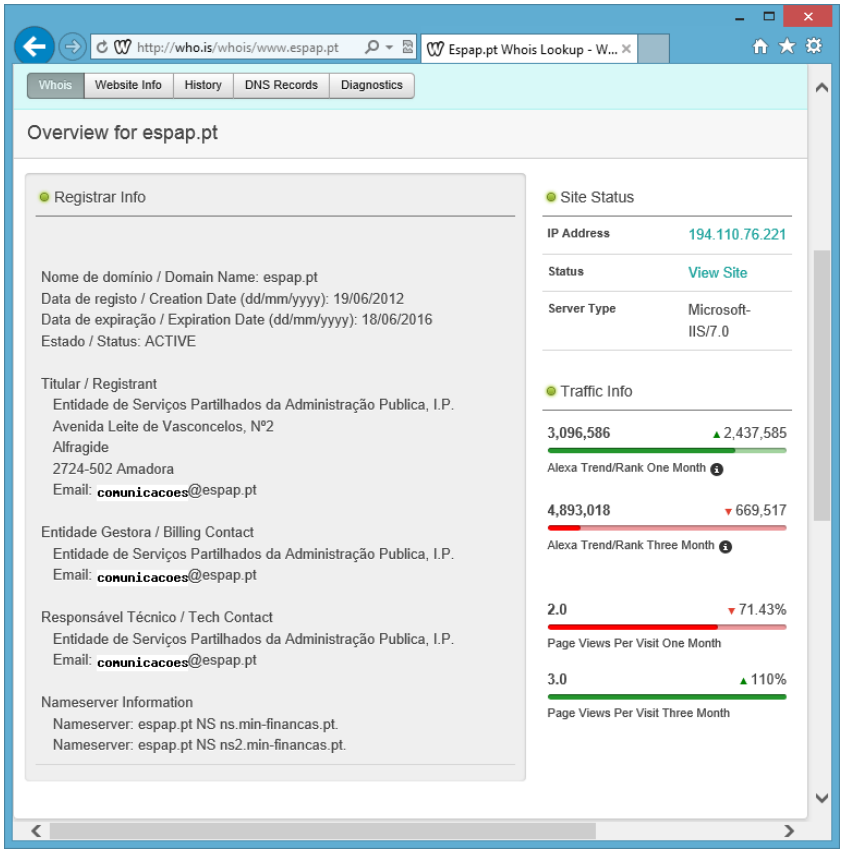


Ilustração 49 - Ferramenta de Whois

Se de seguida colocássemos na query o endereço IP que obtivemos anteriormente, conseguiríamos recolher informação adicional, tal como a range de IP's públicos disponíveis.

Um exemplo desta etapa com ações semi-intrusivas é o uso de varrimentos de ping na rede (ping sweep), com recurso a ferramentas existentes para o efeito. Tipicamente, utiliza-se o comando nmap para se obter esta informação (excerto de exemplo com informação descaracterizada a cinzento):

```
[username@hostname ~]# nmap -v -sP 10.1.1.0/24
Host hostnamexx.dominio (10.1.1.xx) appears to be up.
MAC Address: xx:xx:xx:xx:xx:xx (Unknown)
Host 10.1.1.xy appears to be down.
Host hostnameyy.dominio (10.1.1.yy) appears to be up.
(…)
The ARP Ping Scan took 0.64s to scan 209 total hosts.
DNS resolution of 94 IPs took 4.50s.
```

b. A enumeração

A enumeração é o processo seguinte para determinação do sistema operativo e aplicações/portos a correr no sistema alvo (MANZUIK, PFEIL, GOLD, 2007). Mais uma vez, a utilização do nmap, com outras opções no comando, permite a identificação de quais os portos abertos a correr no sistema alvo:

```
[username@hostname ~]# nmap -sV -A 10.1.1.xx

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-11-03 14:34 WET
Interesting ports on hostnamexx.dominio (10.1.1.xx):
Not shown: 1669 closed ports
PORT                STATE SERVICE           VERSION
21/tcp              open  ftp               vsftpd 2.0.5
135/tcp             open  msrpc             Microsoft Windows RPC
139/tcp             open  netbios-ssn
445/tcp             open     microsoft-ds   microsoft-ds
3389/tcp            open     microsoft-rdp  Microsoft Terminal Service
8080/tcp            open     http           Apache Tomcat/Coyote JSP
13722/tcp           open  netbackup         Veritas Netbackup

(…)

MAC Address: xx:xx:xx:xx:xx:xx (Unknown)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP|2003/.NET
OS details: Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2

Service Info: OS: Windows
Nmap finished: 1 IP address (1 host up) scanned in 115.653 seconds
```

A opção –sV do nmap devolve os serviços/aplicações/portos abertos e a opção –A devolve o sistema operativo e a sua versão. Neste exemplo, é possível identificar a utilização de um porto potencialmente perigoso (21), uma vez que é utilizado para a transferência de dados em clear, através do serviço FTP.

Esta etapa deve ser levada a cabo para todos os ativos identificados na etapa anterior. Com o esforço árduo inerente a estas etapas de recolha de informação e de enumeração concluído, passa-se então à fase da deteção de vulnerabilidades propriamente dita.

c. A deteção

A deteção é a etapa em que se pretende determinar se um sistema ou aplicação está suscetível à concretização de uma ameaça, isto é, se possivelmente detém alguma vulnerabilidade.

Este processo não confirma na íntegra a existência de vulnerabilidades, apenas reporta a probabilidade de estarem presentes. Para se obter posteriormente a confirmação dessa presença, recorre-se a testes de penetração (MANZUIK, PFEIL, GOLD, 2007).

Para detetar vulnerabilidades será necessário recorrer-se a ferramentas existentes para o efeito, tais como o software Nessus ou o software Retina. Com uma aplicação deste tipo disponível, é possível facilmente avaliar os ativos identificados nas fases anteriores, detetando-lhes a existência de potenciais vulnerabilidades.

Isto é possível sondando-se com estas ferramentas os sistemas em causa e comparando as suas respostas com um conjunto respostas tipo. Se as respostas forem boas/ as esperadas, é porque não estamos perante vulnerabilidades, se forem consideradas más, a ferramenta assume que o ativo está vulnerável.

Depois de serem identificadas as diversas vulnerabilidades nos ativos em causa, e não havendo dúvidas em relação à confirmação das mesmas, importa então tomar as medidas necessárias para a mitigação do risco da sua exploração. No entanto, se a relação entre o custo de implementação dessas medidas e a probabilidade/impacto das respetivas ameaças se concretizarem assim o sugerir, esse risco poderá ser assumido pela organização e a vulnerabilidade permanecer.

d. Exemplo de scanner de vulnerabilidades open-source

Um exemplo atual de um scanner/detetor de vulnerabilidades *open-source* é o OpenVAS (Open Vulnerability Assessment System). Esta ferramenta, idêntica em objetivo ao conhecido Nessus, disponibiliza à comunidade um conjunto de serviços e ferramentas que oferecem uma solução poderosa e abrangente de deteção e gestão de vulnerabilidades. Este produto gratuito é atualmente acompanhado por um conjunto de cerca de 30000 testes de vulnerabilidade (Network Vulnerability Tests – NVTs), atualizado diariamente. Em termos de arquitetura, o elemento principal do OpenVAS é o seu eficiente "scanner" que executa estes NVT's.

Depois, existe o elemento "manager", que é o serviço central que consolida o scan de vulnerabilidades numa solução completa de gestão das mesmas; o "manager" controla o "scanner" e uma base de dados SQL onde as configurações e os resultados das avaliações são armazenados. O elemento "administrator" atua como uma ferramenta de linha de comando ou como um daemon que disponibiliza o protocolo "OpenVAS Administration Protocol"(OPENVAS, 2013).

O esquema seguinte caracteriza em termos genéricos a arquitetura da solução OpenVAS (OPENVAS, 2013).

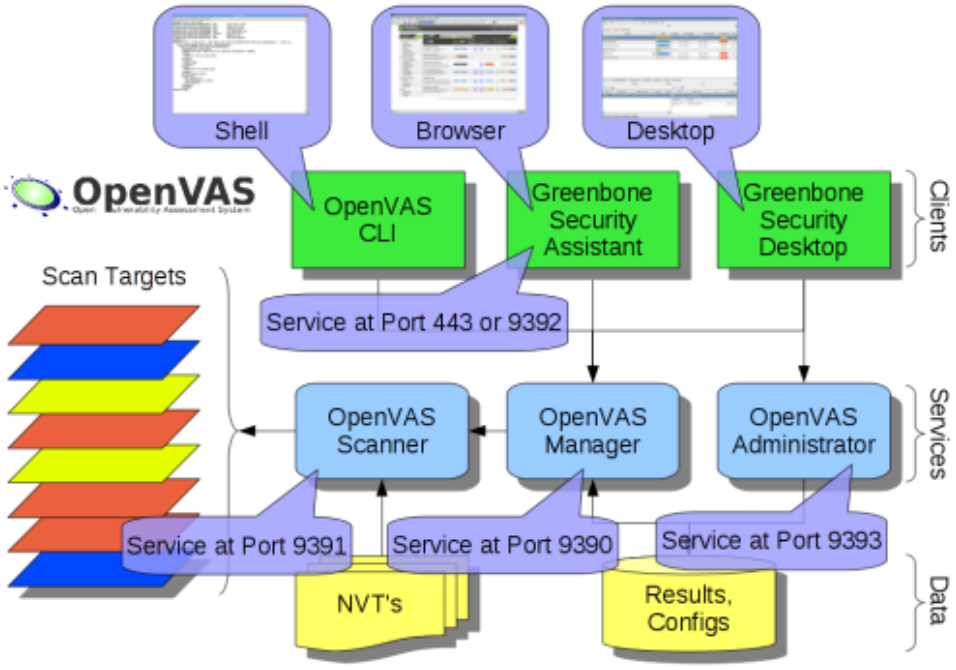


Ilustração 50 - OpenVAS framework

O "manager" controla o "scanner" utilizando o "OpenVAS Transfer Protoco" e disponibiliza para a sua utilização o "OpenVAS Management Protocol". Em termos de clientes de gestão que interagem com o "manager", a solução disponibiliza (OPENVAS, 2013):

- ✓ Greenbone Security Assistant - Um interface web para acesso browser;
- ✓ Greenbone Security Desktop - Um cliente Desktop para plataformas Windows e Linux;
- ✓ OpenVAS CLI - Um interface de linha de comandos, essencialmente para criação de processos batch.

No que respeita às principais funcionalidades do OpenVAS, destacam-se as seguintes (OPENVAS, 2013):

- ✓ OpenVAS Scanner - Scan de múltiplos hosts concorrencialmente, suporte SSL e suporte WMI;
- ✓ OpenVAS Manager - Suporte de SSL, múltiplas tarefas concorrentes, gestão de notas, gestão de falsos-positivos, agendamentos, etc;
- ✓ OpenVAS Administrator - Suporte SSL, gestão de utilizador, vista de "feed status", sincronização de feed;
- ✓ Greenbone Security Assistant - Cliente para OpenVAS Management Protocol e para OpenVAS Administration Protocol, suporta HTTP e HTTPS e não necessita de servidor web externo;
- ✓ Greenbone Security Desktop - Cliente OpenVAS Management Protocol, suporta plataformas Windows e Linux e o interface está disponível em diversas línguas;
- ✓ OpenVAS CLI - Cliente OpenVAS Management Protocol, suporta plataformas Windows e Linux.

4. MODELO DE SEGURANÇA PARA AS REDES DE DADOS DA AP

Em traços gerais, este ponto pretende sugerir um modelo com mecanismos preventivos e detetivos de segurança, a aplicar às redes de dados dos organismos públicos, tendo em conta uma prévia reorganização das infraestruturas do Estado que lhe deve estar inerente.

Apesar de todo o esforço que tem sido levado a cabo no sentido de se restruturar e de se melhorar as componentes TIC na Administração Pública, não existe a definição de um modelo operacional que explicite a melhor forma de interligação das infraestruturas de rede dos ministérios e que identifique claramente os mecanismos tecnológicos básicos de segurança e o seu posicionamento estratégico nessas redes. É este o contributo que se pretende sugerir com a definição deste modelo de segurança, realçando-se a importância de alguns controlos preventivos e detetivos.

O modelo a definir faz uso dos principais controlos preventivos e detetivos identificados e caracterizados nos pontos anteriores, sem prejuízo de também poder fazer referência a outros controlos complementares importantes, como são caso disso os mecanismos de *Anti-Spam* e de *URL filtering*.

Como já referido, e aproveitando os tempos de mudanças significativas na esfera da Administração Pública em Portugal, entende-se importante ficar espelhado neste modelo a racionalização dos recursos de rede, fazendo-se assim prevalecer a prática da contenção da despesa. É igualmente importante proceder-se à normalização/estandardização dos locais a interligar, agrupando-os consoante um conjunto de fatores, nomeadamente o papel que assumem no Estado, a sua capacidade de disponibilização de serviços e o seu grau de exposição ao risco. É neste contexto que o modelo faz sobressair a relevância dos organismos responsáveis pela operacionalização e gestão das TIC de cada ministério (“organismos TIC”). Estas competências/atribuições não estão atualmente centralizadas num organismo por ministério. Tendo em conta os limites inerentes à contenção de custos, pretende-se então apresentar um modelo cujo principal objetivo será permitir aumentar a segurança das infraestruturas de rede do Estado, racionalizando simultaneamente os recursos envolvidos. Com base nesta relação estreita entre os custos e os benefícios da segurança preventiva e detetiva nas redes do Estado, reforça-se que o *open-source* pode representar uma oportunidade e um meio para se atingir um fim, que é poder melhorar a segurança nas redes e sistemas da Administração Pública.

4.1. PROPOSTA DE MODELO

4.1.1. Pressupostos e governança

Tendo sempre presente o trabalho já efetuado neste âmbito pela AMA e pelo GPTIC, bem como as medidas de racionalização das TIC resultantes da RCM 12/2012, entende-se haver um conjunto pressupostos condicionantes deste modelo de segurança para as redes do Estado que devem, precedentemente, ser assumidos. Apesar de no referido regulamento não ser claro haver prioridades ou precedências nas implementações das medidas, para que este modelo possa ser seguido e para que seja possível atingir-se os objetivos com eficácia e de forma eficiente, entende-se que os seguintes processos deverão ser previamente implementados.

1º. Unificação da função TIC por ministério - As competências de aquisição, operacionalização e gestão das tecnologias de informação e comunicação devem estar centralizadas num único organismo por cada ministério; Em vários casos (ex.: MJ, MSESS) estas funções já se encontram tradicionalmente centralizadas, sendo importante que o fiquem em todos os ministérios, obtendo-se assim maior controlo e racionalização nas TIC da Administração Pública.
2º. Unificação das Redes de dados por ministério - Deve haver uma rede única por cada ministério que abranja todos os locais com necessidades de acesso às TIC; Esta infraestrutura deverá também unificar e centralizar as ligações à Internet e a entidades externas ao ministério.
3º. Unificação dos CPD's por ministério - Por outro lado, e havendo já a responsabilidade única da função TIC bem como uma única infraestrutura de rede por ministério, os serviços a disponibilizar deverão ser naturalmente centralizados num único Centro de Processamento de Dados por cada ministério; Apenas alguns dos serviços de pequena dimensão, necessários às redes locais de cada *site*, deverão permanecer distribuídos, mas sempre sobre o controlo e a gestão do "organismo TIC" respetivo.

À semelhança do referido a respeito da função TIC, no que concerne à função de gestão da segurança, o racional deverá ser idêntico. O mesmo organismo por cada ministério que tem a seu cargo a responsabilidade das TIC, deverá também ter estrutura e capacidade para assumir a gestão da segurança no seu âmbito de atuação.

Os organismos com estas competências deverão interagir de perto com o Centro Nacional de Cibersegurança (CNCSeg, a criar por força do "Plano Global Estratégico TIC" e da "Estratégia Nacional de Segurança da Informação"), trocando sinergias e esforços na prevenção, deteção e eliminação das ameaças TIC e dos respetivos riscos nos sistemas de informação públicos. De entre as principais ações que devem ser implementadas e mantidas por estes "organismos TIC" no âmbito de cada ministério, destacam-se as seguintes:

- ✓ Inventário de Ativos TIC - Deverá ser criado e mantido um inventário de ativos TIC por cada ministério, que seja permanentemente atualizado e que identifique, nomeadamente, o grau de criticidade de cada ativo (nas componentes da confidencialidade, integridade e disponibilidade), bem como o responsável de cada ativo.
- ✓ Classificação da informação - Estes organismos devem conduzir e manter um processo de classificação de toda a informação do seu ministério, tendo em conta as referidas propriedades da segurança da informação (confidencialidade, integridade e disponibilidade); A informação mais crítica deverá, naturalmente, deter mecanismos de proteção mais exigentes.
- ✓ Levantamento e documentação dos processos TIC - Todos os processos de gestão das TIC devem ser levantados, otimizados e documentados tendo em conta critérios de segurança; Devem ser criados normativos com os respetivos fluxogramas dos processos, revistos periodicamente, e deverão ser utilizados modelos de referência como a ISO 27001 ou a ISO 27002.
- ✓ Monitorização da rede, dos sistemas e da segurança - Os "organismos TIC" deverão ter capacidade de monitorizar permanentemente, aos níveis da performance e da segurança, todos os ativos TIC ligados à rede do seu ministério.
- ✓ Gestão de Problemas TIC - Todos os problemas TIC do ministério em causa devem ser registados e resolvidos pelo "organismo TIC"; A ferramenta utilizada para o registo desses problemas deve permitir a associação com os ativos TIC, a tipificação dos problemas, a identificação de possíveis reincidências, bem como retirar estatísticas por área de atuação.
- ✓ Gestão de Incidentes de Segurança nas TIC - Todos os incidentes de segurança nas TIC do ministério em causa devem ser registados e resolvidos pelo "organismo TIC"; A ferramenta utilizada para o registo desses problemas deve permitir a associação com os ativos TIC, a tipificação dos incidentes, a identificação de possíveis reincidências, a identificação das vulnerabilidades exploradas, bem como retirar estatísticas por área de atuação.

- ✓ Gestão das Vulnerabilidades Técnicas - Com base em Auditorias periódicas de deteção de vulnerabilidades, bem como no historial de incidentes identificados, deve ser conduzido e mantido permanentemente pelo "organismo TIC" de cada ministério, um plano de revisão e mitigação de vulnerabilidades técnicas; Este plano servirá de suporte à gestão do risco.
- ✓ Estabelecimento do plano de Continuidade do Negócio - Os "organismos TIC" de cada ministério deverão definir e manter permanentemente um Plano de Continuidade do Negócio do seu ministério, contemplando nomeadamente as ações de todos os intervenientes bem como a respetiva estratégia de *Disaster Recovery*.

Entende-se pertinente que cada um destes "organismos TIC", juntamente com o CNCSeg, o CEGER, o GNS e a AMA, integre a rede nacional de resposta a incidentes de segurança - CSIRT's, coordenada pelo CeRT.PT (FCCN). A integração nesta rede comum de intervenientes da segurança na esfera nacional vai permitir, não só uma maior pró-atividade e prevenção de incidentes de segurança nas redes de dados da Administração Pública, como também promoverá a maior eficácia na resolução dos mesmos, uma vez que tira partido da rápida entreajuda e experiência das diferentes entidades públicas e privadas.

O CEGER, sendo já o órgão responsável pela gestão da rede dos membros do governo, deve também ser o organismo responsável pela gestão da rede de *core* que interligará todos os "organismos TIC" de cada ministério, garantindo o controlo de todo o tráfego interministerial e disponibilizando ainda um acesso à Internet alternativo para os ministérios.

O GNS, por sua vez, deve ser o organismo responsável por promover e coordenar, periodicamente, auditorias de vulnerabilidades e testes de Intrusão aos "organismos TIC" de cada ministério. Destas auditorias devem resultar recomendações de melhoramentos/ mitigações, com tempos bem definidos de implementação, que contribuirão de forma determinante para a melhoria contínua da segurança nas TIC do setor público. O GNS deve ainda colaborar com os "organismos TIC", enquanto órgão consultor, nos processos de classificação da informação dos ministérios.

Como já referido, os "organismos TIC" assumem um papel determinante neste modelo, uma vez que são os responsáveis pela coordenação e gestão das TIC e da segurança no seu ministério. Poder-se-á pensar por que razão não é um único organismo a assumir estas funções em toda a Administração Pública, embora as razões sejam simples e fáceis de expor:

- ✓ Por um lado, seria uma mudança bastante ambiciosa e com riscos muito consideráveis, uma vez que as competências TIC estão atualmente bastante descentralizadas, havendo na grande maioria dos organismos uma área de informática com o *know-how* específico das suas infraestruturas e dos seus Sistemas de Informação.
- ✓ Por outro lado, embora se trate do âmbito global da Administração Pública, o negócio de cada ministério tem as suas especificidades e os seus fatores distintivos, sendo conveniente que as tecnologias de informação e a sua segurança estejam, tanto quanto possível, alinhadas com esse negócio.

Entende-se portanto que, nesta fase, quando há muito pouca agregação das TIC no setor público, será prudente efetuar-se essa consolidação no seio de cada ministério, obtendo-se os ganhos respetivos de racionalização e de controlo a este nível, sem comprometer o desempenho e a qualidade dos seus processos de negócio. Isto, claro, sem prejuízo de futuramente, após este esforço de unificação das TIC por ministério ser feito e de estar devidamente testado e consolidado, se analisar a hipótese e as eventuais vantagens em se centralizar estas competências num único organismo do Estado.

Também na ótica da melhoria contínua no seio da Administração Pública, toda esta estratégia da governança das TIC e da sua segurança deve ser liderada pela AMA e revista periodicamente com os contributos de todos os intervenientes, com o intuito de se conseguir trazer, de forma permanente, melhoramentos neste âmbito.

4.1.2. Organização hierárquica da rede e tipificação dos sites

Para se poder associar os controlos técnicos preventivos e detetivos aos *sites* dos organismos, consoante as suas necessidades e da forma mais racionalizada possível, importa tipificar os locais que farão parte das redes únicas de cada ministério.

Como já referido, estas redes únicas serão da gestão do "organismo TIC" desse ministério, propondo-se ainda que a rede de *core* que interligará todos os organismos TIC dos ministérios (Rede Interministérios) seja da gestão do CEGER.

Desta forma, e para além dos mecanismos de segurança que naturalmente é necessário existir na infraestrutura *core*, o modelo sugere a existência de três tipos de *sites* que deverão fazer parte integrante das redes da Administração Pública, a saber:

- ✓ SITES NÍVEL 1 – *Site* TIC do organismo TIC do ministério - É o local do "organismo TIC" onde será centralizada a disponibilização de serviços para a rede e onde é primeiramente garantida a gestão e o controlo de todo o tráfego do ministério. Tipicamente, será o *site* da localização do Centro de Processamento de dados do ministério e o ponto de comunicação com os outros ministérios, com entidades externas e com a Internet.
- ✓ SITES NÍVEL 2 – *Sites* TIC dos restantes organismos - São os locais dos restantes organismos do ministério (que não o "organismo TIC") responsáveis pela interligação da *WAN* de cada organismo com o *site* do organismo TIC do ministério; realça-se que a gestão da infraestrutura destes locais é da responsabilidade dos "organismos TIC".
- ✓ SITES NÍVEL 3 – *Sites* consumidores de recursos - São todos os locais da *WAN* privada de cada organismo que não disponibilizam serviços para a rede e que apenas necessitam aceder aos sistemas centralizados, a entidades externas e à Internet para suportar os seus processos de negócio.

O diagrama hierárquico seguinte ilustra as interdependências destes tipos de locais, representando ainda uma quantificação subjetiva de cada tipo de local.

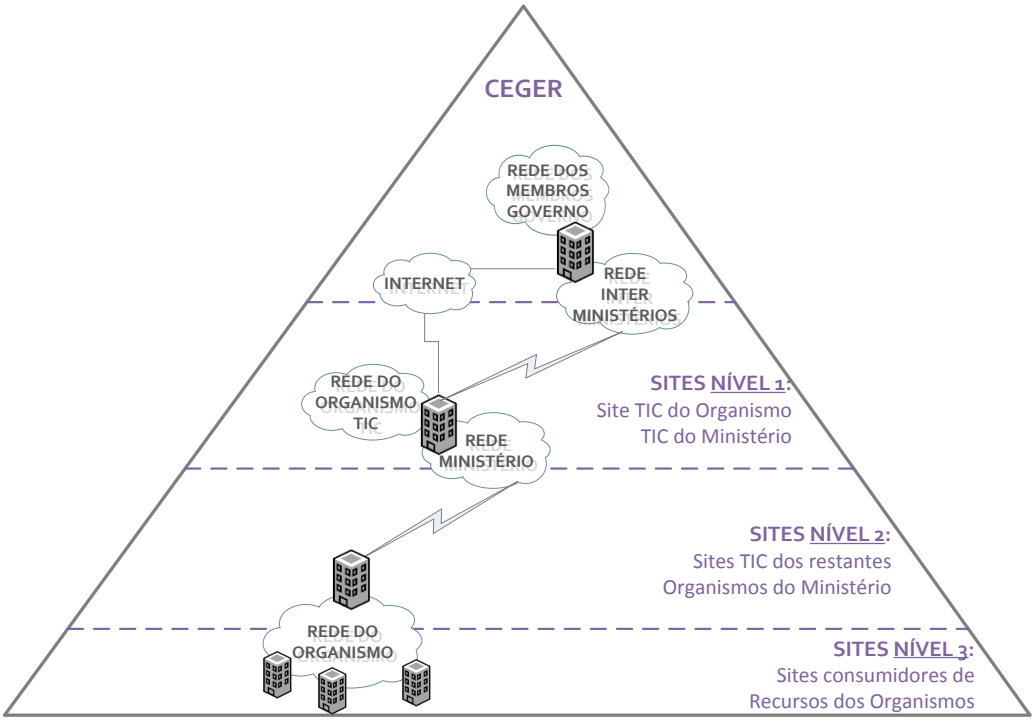


Ilustração 51 - Diagrama hierárquico de alto nível da rede da AP

Os “SITES NÍVEL 3” são em número muito superiores aos “SITES NÍVEL 2” que, por sua vez, representam quantidades muito superiores que as dos “SITES NÍVEL 1”. No topo da pirâmide é representado um único organismo, o CEGER, que se sugere ser o organismo responsável pela gestão da rede Interministérios, o *core* da rede da Administração Pública.

Por forma a haver uma noção mais concreta do peso de cada tipo de *site* num ministério, exemplifica-se o caso do Ministério da Agricultura e do Mar, que formalmente ainda não dispõe de um “organismo TIC”. Neste caso concreto, o ministério é composto por 18 organismos, abrangendo 565 locais (*sites*). A distribuição dos mesmos pelos 3 tipos de *site* contemplados neste modelo, e seguindo o racional envolvido, é expressa da seguinte forma:

- ✓ 1 “SITE NÍVEL 1” - Representa **0,18%** dos locais do ministério;
- ✓ 17 “SITES NÍVEL 2” - Representam **3,01%** dos locais do ministério;
- ✓ 547 “SITES NÍVEL 3” - Representam **96,81%** dos locais do ministério.

Extrapolando-se para os outros ministérios, as percentagens de cada tipo de *site* não sofrem alterações muito significativas. Cada ministério terá 1 “SITE NÍVEL 1” e o número de “SITES NÍVEL 2” será equivalente ao nº de organismos do ministério menos 1.

No que respeita ao número de “SITES NÍVEL 3”, será correspondente o total de locais menos o somatório das quantidades dos tipos de *sites* anteriores.

O diagrama seguinte representa esta rede Interministérios (que interliga os “organismos TIC”) e a forma como nela deverão ser utilizados os mecanismos de proteção abordados nesta dissertação, sem prejuízo de poderem existir controlos técnicos preventivos e detetivos adicionais:

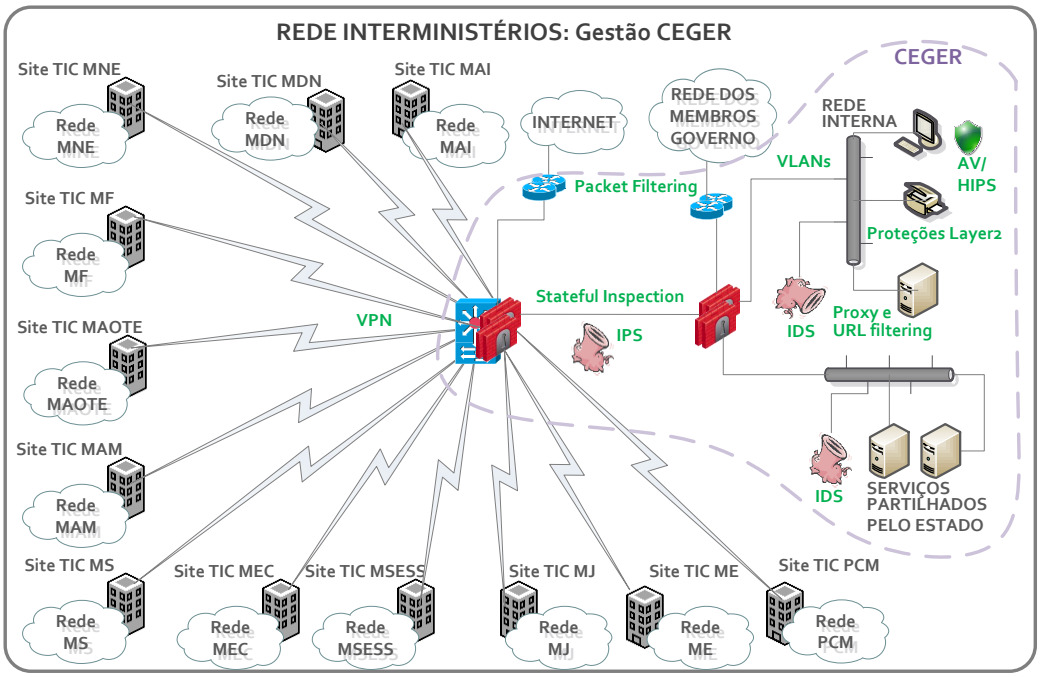


Ilustração 52 – Diagrama da Rede Interministérios

Os controlos técnicos preventivos e detetivos ilustrados a verde na imagem anterior representam a proteção básica que deverá haver num organismo responsável pela gestão da componente central da rede do Estado.

Realça-se a necessidade de existência de encriptação na rede Interministérios, a devida redundância de circuitos, o *packet filtering* nos routers, os dois níveis de firewall *statefull inspection*, o sistema de prevenção de intrusão a proteger as VLANs internas, e os sistemas de deteção de intrusão inerentes a cada uma delas. Sugere-se ainda, essencialmente no que respeita às redes de postos-cliente, a necessidade de haver mecanismos de proteção de *layer* 2, a existência de *proxys* e de URL *filtering* para os acessos à Internet, bem como a instalação e atualização permanente de software de antivírus e HIPS.

Nos pontos seguintes serão abordados os detalhes referentes a cada um das três tipificações de *sites* enunciadas.

4.1.3. SITE Nível 1 – Site TIC do Organismo TIC do Ministério

Este tipo de *site* é o que apresenta maior relevância no modelo de segurança, na medida em que é o ponto central de interligação entre os diversos locais dos organismos de determinado ministério e os organismos dos outros ministérios, a Internet e entidades externas à Administração Pública.

É este o *site* que, fundamentalmente, disponibilizará em cada ministério serviços para a rede e que por isso apresenta maior grau de exposição ao risco, sendo necessário dispor de controlos preventivos e detetivos eficazes e que consigam transmitir um grau de segurança e um grau de confiança aceitáveis a todos os organismos de cada ministério. O diagrama seguinte evidencia a forma como se pretende, neste modelo, organizar os controlos de segurança inerentes a este tipo de *sites*:

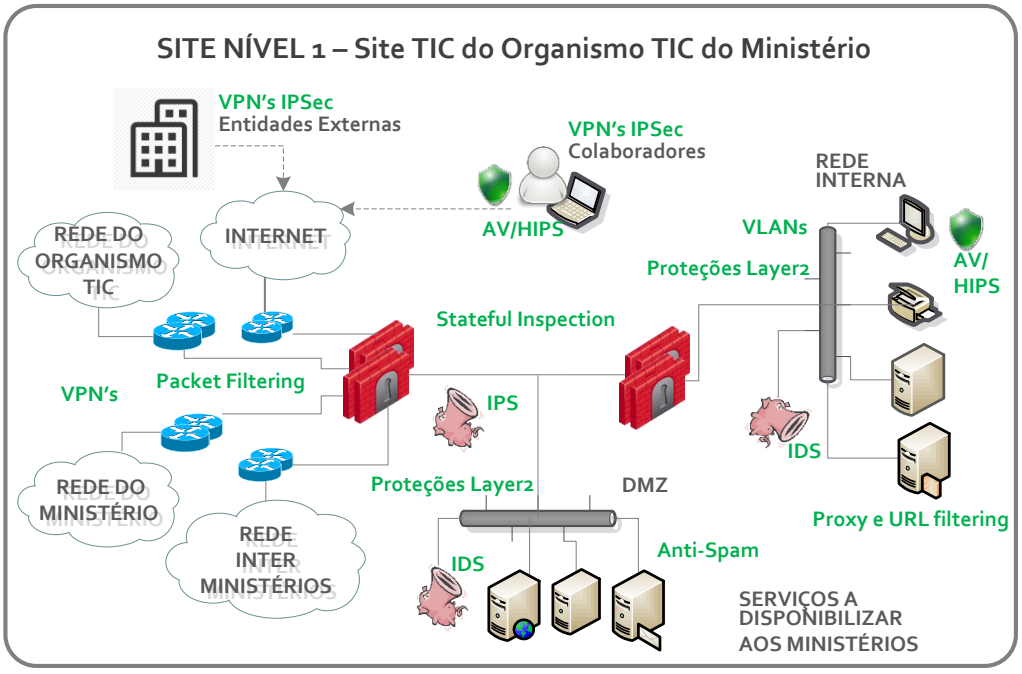


Ilustração 53 - SITE Nível 1: Site TIC do Organismo TIC do Ministério

Entende-se que, para se poder privilegiar a confidencialidade e a integridade da informação dos organismos, sem que para isso se tenha que fazer crescer demasiado os custos da rede, é importante estabelecer VPNs IPSec nas *WANs* de cada ministério, nos acessos móveis/remotos dos colaboradores, bem como nas ligações a/de entidades externas.

Como os "*sites* TIC do organismo TIC do ministério*"* disponibilizam serviços para o seu e para outros ministérios, considera-se também necessário haver a devida redundância, a vários níveis, por forma a salvaguardar a disponibilidade da informação, assim como uma filtragem robusta nos acessos a esses sistemas de maneira a prevenir a concretização de ataques aos mesmos.

Tipicamente, estes locais apresentam quatro origens de pedidos às suas aplicações e sistemas:

- ✓ Da Internet;
- ✓ Da *WAN* do próprio organismo;
- ✓ Da *WAN* do ministério;
- ✓ Da rede Interministérios.

Os routers destas ligações devem dispor de um primeiro nível de filtragem, disponibilizando para o efeito mecanismos de *packet filtering* nos sentidos *inbound e outbound*.

Os acessos externos às DMZs devem depois passar por um nível de *firewall stateful inspection* e por um sistema de prevenção de intrusões que poderá ou não ser integrado nesse nível de firewall. Todas as aplicações acessíveis a partir das redes externas, nomeadamente da Internet, devem ser disponibilizadas com recurso ao uso de SSL.

As redes internas devem ser segregadas em VLANs distintas e os seus acessos a partir das DMZs (nomeadamente à VLAN específica das Bases de Dados de negócio) devem passar por outro nível de firewall *stateful inspection*. Este último nível só deve permitir a passagem de tráfego proveniente das DMZs para as redes internas, e não do tráfego proveniente das redes externas.

Tanto as DMZs como as redes internas devem dispor de sondas inerentes a sistemas de deteção de intrusão de rede (NIDS) que assumem o papel importante de mecanismos complementares de segurança, e todos os equipamentos de *switching* destas redes devem ter ativados os mecanismos de *port-security* e as outras proteções de *layer* 2 já referidas.

Por outro lado, estes *sites* TIC dos organismos TIC de cada ministério devem ainda estar dotados de controlos de *Anti-Spam* associados aos seus sistemas de correio eletrónico, e também de proxy servers e de ferramentas de *URL filtering*, capazes de controlar e monitorizar os acessos à Internet a partir dos postos-cliente internos. Todos estes postos-cliente internos (assim como os postos-cliente utilizados para os acessos remotos dos colaboradores) devem ainda estar

protegidos com *personal firewalls*, *software* de antivírus e *software* de HIPS permanentemente atualizado.

O esquema de blocos seguinte demonstra, numa perspetiva diferente, como poderão ser implementadas as interdependências entre os mecanismos de segurança identificados e todas as entidades e recursos envolvidos nas redes de dados da Administração Pública:

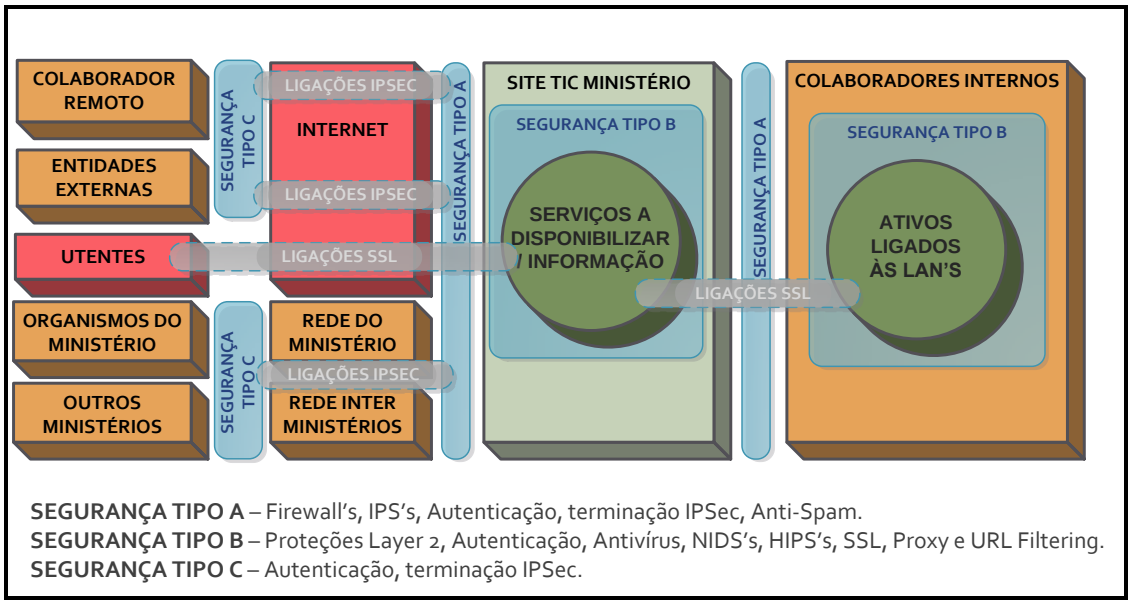


Ilustração 54 - Esquema de blocos de segurança: Site TIC do Ministério

4.1.4. SITE Nível 2 – Sites TIC dos restantes Organismos

Os "*sites* TIC dos restantes organismos" são os locais de interligação entre as suas *WANs* privadas e a rede do ministério. É através deste ponto central de cada organismo que é estabelecida a comunicação com os outros organismos desse ministério. Não é pretendido neste modelo que locais deste tipo disponibilizem aplicações de negócio ou outros serviços para a rede, sendo exceção a isso alguns serviços de pequena escala que, por questões de proximidade e diminuição da complexidade, sirvam os preceitos da *WAN* desse organismo.

Salienta-se novamente que toda a gestão desta infraestrutura deverá também ser a cargo do "organismo TIC" do ministério respetivo, nomeadamente a gestão remota de todas componentes de rede e de segurança.

Estes *sites* devem assim ser dotados de mecanismos de *packet filtering* nos *routers* de acesso à *WAN* do próprio organismo e de acesso à rede do ministério, que também deverá ser constituída com recurso ao estabelecimento de VPNs IPSec, a fim de poder ser garantida a integridade e a confidencialidade da informação em trânsito, preservando-se igualmente a contenção de custos. Os ativos das VLANs internas destes *sites* devem ainda ser protegidos com um nível de firewall *statefull inspection* e com sistemas de deteção de intrusão de rede, não devendo também ser descorada a implementação do *port-security* nos *switches* e as restantes proteções de *layer* 2, nem tão pouco a *personal firewall*, o antivírus e o *software* HIPS a instalar e a atualizar permanentemente nos postos-cliente.

A imagem seguinte esquematiza, de uma forma mais visual, as necessidades básicas de segurança tecnológica preventiva e detetiva nos *sites* deste tipo:

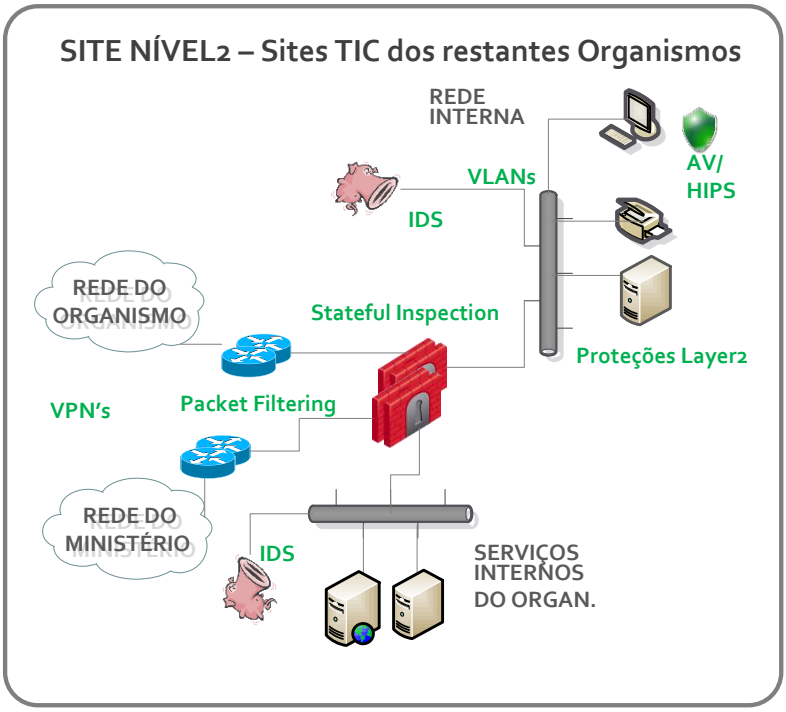


Ilustração 55 - SITE Nível 2: Sites TIC dos restantes Organismos (não TIC)

4.1.5. SITE Nível 3 – Sites consumidores de recursos

Por último, este tipo de *sites* representa todos os locais que apenas têm necessidade de consumir recursos e serviços disponibilizados na rede. Os "*sites* consumidores de recursos" não partilham serviços para a rede.

Apesar disso, a segurança dos seus ativos não deve ser negligenciada uma vez que, se algum deles vier a ser comprometido, poderá também vir a comprometer outros ativos mais críticos e com maior valor para o negócio. De qualquer forma, e mantendo o racional de contenção de despesa na Administração Pública, é de referir que as suas exigências de proteção e os custos que lhes estão associados são em muito inferiores às dos tipos anteriores.

A única ligação à rede que estes locais terão será o acesso à VPN do seu próprio organismo e, por isso, apenas haverá necessidade de terem um router com a respetiva redundância. Estes equipamentos deverão ter ativados os controlos de *packet filtering* tão restritamente afinados, quanto possível. O acesso à rede interna deve ainda estar filtrado com mecanismos de proteção de *layer* 2 e os postos-cliente devem também estar preparados com *personal firewalls*, com software de antivírus e com HIPS permanentemente atualizados.

A figura seguinte sintetiza os mecanismos de proteção deste tipo de *sites*, bem como o seu posicionamento estratégico na rede destes locais:

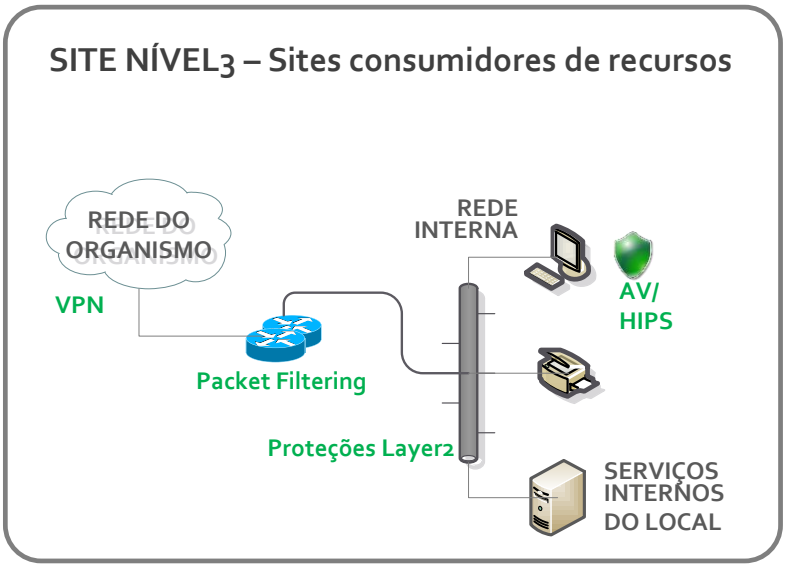


Ilustração 56 - SITE Nível 3: Sites consumidores de recursos

Importa novamente realçar que, neste modelo, a gestão dos ativos TIC destes locais, incluindo as suas componentes de segurança, fica também sob a responsabilidade do organismo TIC do respetivo ministério.

4.2. VANTAGENS DA IMPLEMENTAÇÃO DO MODELO PROPOSTO E ANÁLISE DAS DIFERENÇAS

Atualmente, os mecanismos técnicos de segurança que são implementados nas redes da Administração Pública, são na sua generalidade pensados a avulso e levados a cabo de forma *ad hoc*, sem que hajam preocupações de se integrarem com outros já implementados ou tão pouco de se corelacionarem com modelos de implementação previamente definidos para o efeito.

É importante que existam definidas estas regras, tipificações e planeamentos de implementação para que, não só seja possível haver maior eficiência e controlo nas redes e nos ativos dos organismos, como também se consiga obter uma visão concertada e hierárquica do Estado a este nível. Através destas normalizações e desta visão integrada da Administração Pública, é possível reduzir o risco e o desperdício de recursos.

Assim, e de uma forma geral, pode-se afirmar que a grande vantagem que se consegue obter com a implementação deste modelo é, simultaneamente, melhorar-se a segurança e reduzirem-se os custos nas infraestruturas de rede do Estado. Aproveitando-se o momento de grande mudança e de forte racionalização que a Administração Pública está a sofrer, e após se conseguir claramente identificar todos os locais que efetivamente precisam de ser conectados às redes do Estado, é importante inseri-los nas categorias especificadas consoante as suas características e necessidades. Assim, é mais fácil conseguir-se encontrar o melhor equilíbrio entre a redução do risco de concretização de ataques às infraestruturas e à informação, e a contenção de despesa nos orçamentos dos ministérios.

Se por um lado não se pretende que ataques básicos, como os já experienciados, sejam bem sucedidos nos ativos do Estado, por outro também não é benéfico gastarem-se verbas altas e desnecessárias para mitigar riscos com baixa probabilidade e baixo impacto. A centralização de competências de gestão da rede, do risco e dos mecanismos de segurança por ministério favorece a procura deste equilíbrio, trazendo uma visão única em cada sector mas com regras transversais à Administração Pública.

A interoperabilidade entre os diversos tipos de locais das redes do Estado passa a ser *standard*, seguindo uma ordem e um racional, sendo assim possível reduzir-se as brechas de segurança e favorecendo-se os relacionamentos e as trocas de experiência a este respeito entre os organismos públicos. Também a interação com entidades externas sai favorecida, uma vez que o

Estado passará a comunicar com os privados de forma mais objetiva, normalizada e centralizada. Os "organismos TIC" dos ministérios têm um enorme relevo na implementação deste modelo, sendo os principais responsáveis pela obtenção destas vantagens. O seu desempenho é o principal fator de sucesso do modelo. Os poucos organismos que atualmente já têm competências de gestão das TIC de todo o ministério a seu cargo, têm ainda uma preponderância superior, uma vez que lhes é exigida, implicitamente, uma responsabilidade maior proveniente da experiência e uma vez que as expectativas lhes apontam a incumbência da passagem de conhecimento e o apoio necessário aos restantes "organismos TIC".

O esquema SWOT seguinte pretende evidenciar algumas das principais forças, oportunidades, fraquezas e ameaças inerentes à implementação do modelo, sem prejuízo de puderem existir outras não identificadas:

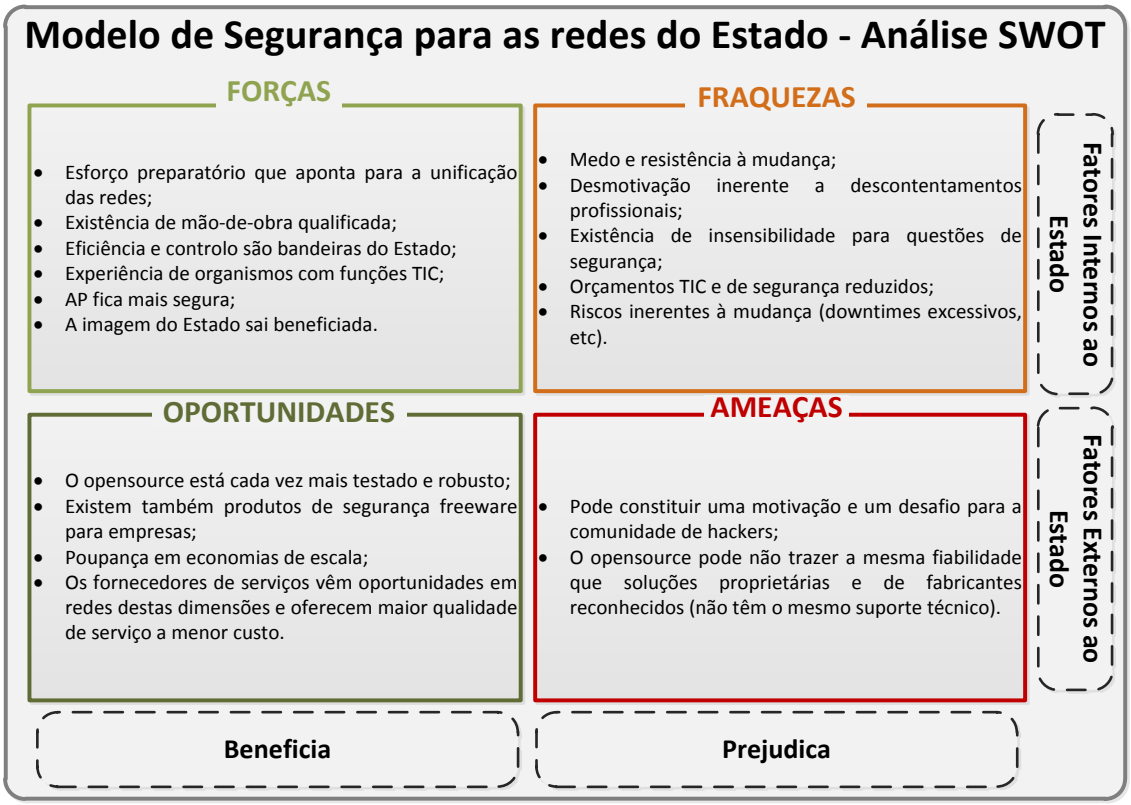


Ilustração 57 - Modelo SWOT da implementação do modelo

A possibilidade de implementação deste modelo vai então permitir, no mínimo, uma reflexão profunda acerca do papel que as tecnologias de informação e a sua segurança deverão assumir

nos organismos públicos, bem como uma clarificação da importância da visão do Estado como um todo e das suas respetivas vantagens.

5. CONCLUSÕES

5.1. DISCUSSÃO

É possível então concluir que os controlos técnicos preventivos e detetivos identificados nesta dissertação revestem-se de uma importância primordial para a segurança das redes de dados da AP. Como foi referido, a grande maioria dos ataques recentemente concretizados com sucesso a infraestruturas da Administração Pública, não se baseou em procedimentos de grande complexidade técnica, mas sim em formas básicas de exploração de vulnerabilidades críticas existentes, nomeadamente derivadas da falta de controlos técnicos preventivos e detetivos importantes. Assim, e independentemente do tipo e das motivações dos atacantes, pode-se afirmar que muitos dos ataques levados a cabo foram básicos e fáceis de promover.

É por isso fundamental haver também uma reflexão sobre a reorganização do Estado ao nível das tecnologias de informação, das redes e da segurança e, principalmente, sobre o que se poderá melhorar a baixo custo. Apesar de, nestes tempos de mudança na Administração Pública, terem já havido esforços no que respeita a estratégias de restruturação e de racionalização das TIC, que por si só já favorecem a segurança, não está pensado nenhum modelo operacional que explicite a melhor forma de interligação das redes dos ministérios e que identifique claramente os principais mecanismos tecnológicos de contenção do risco, o seu posicionamento estratégico e os procedimentos para a sua gestão.

Um esquema tipificado e normalizado de controlos técnicos preventivos e detetivos a adotar nos organismos públicos, consoante características como o seu grau de exposição ao risco, contribui de forma determinante para haver maior controlo na segurança das TIC e para se reduzirem as vulnerabilidades e o risco inerente. O modelo proposto nesta dissertação traz esse contributo, mas também o de proporcionar a gestão mais contida dos custos associados à segurança das redes dos organismos públicos.

No entanto, pretende-se que este modelo seja encarado como um ponto de partida, um momento zero, sendo importante haver constantemente mecanismos de avaliação do risco para que se consiga otimizar o equilíbrio entre a necessidade dos controlos preventivos e detetivos e a necessidade da contenção dos custos.

Por outro lado, e sem prejuízo de também deverem existir, é relevante concluir que a implementação de controlos corretivos, decorrentes de ataques já concretizados, expressa-se na maioria das vezes em custos muito superiores aos referentes a controlos preventivos e detetivos. Ou seja, se for possível evitar ou parar os ataques antes de terem efetivamente impacto no organismo, os custos inerentes a essas proteções serão sem dúvida inferiores aos de voltar a normalizar uma situação após a ocorrência de um incidente grave, com todos os gastos diretos e indiretos que isso acarreta.

No que respeita aos objetivos que se pretendia atingir com esta dissertação, é possível aferir que na sua generalidade foram cumpridos.

Em termos de análise da situação atual, ficou claro que na Administração Pública, apesar de naturalmente existir alguma preocupação com a segurança nas redes de dados, existem ainda necessidades de sensibilização e muito a melhorar. Foi feito um resumo histórico das redes do Estado, foram identificadas algumas das principais ameaças com base em eventos ocorridos e previsões de entidades ligadas à segurança, e foi reconhecido um conjunto de vulnerabilidades genéricas das infraestruturas de rede e sistemas atuais. Foram ainda exemplificadas ocorrências recentes de concretização de ameaças, algumas das quais afetando entidades públicas.

Da mesma forma, foi sintetizado algum trabalho já desenvolvido no âmbito das redes e da segurança dos organismos públicos, bem como identificados os principais intervenientes envolvidos. Foram enumeradas medidas que se pretende implementar, relativas à melhoria das redes do Estado, algumas das quais com tempo estimado de implementação já ultrapassado.

Com o intuito de se vir a estabelecer um modelo de segurança para as infraestruturas de rede do Estado, por forma a se mitigar eficazmente e eficientemente os riscos inerentes às ameaças identificadas atrás, caracterizaram-se alguns dos principais controlos técnicos preventivos e detetivos essenciais às redes de dados, explicitando-se a sua importância para a segurança da informação dos organismos públicos. Como a contenção de custos é uma constante na equação da segurança das TIC no setor público, apresentaram-se ainda exemplos de produtos *open-source* capazes de dar resposta às necessidades dos organismos.

Tendo em conta critérios de racionalização das TIC e de otimização dos recursos, bem como a visão articulada do Estado como um todo, definiu-se então um modelo de segurança para as infraestruturas de rede do Estado, recorrendo-se a mecanismos técnicos de prevenção e deteção de ameaças. Este modelo tipifica e agrupa os locais a ligar à rede com base em alguns critérios e

aplica-lhes um conjunto de controlos técnicos preventivos e detetivos essenciais, tendo em conta esses mesmos critérios. Para além disso, define responsabilidades na operação e gestão destes recursos, salientando o papel determinante dos organismos TIC de cada ministério.

Neste aspeto, sugere-se que a aplicação do modelo, e a sua permanente avaliação, permite melhorar a segurança nas redes do Estado e simultaneamente racionalizar os custos.

Com isto, e analisando-se as diferenças entre o que é a realidade atual das redes e respetivos sistemas dos organismos públicos e o que se pretende para o futuro, é possível aferir acerca da importância da segurança dos Sistemas de Informação e da sua Imprescindibilidade no seio da Administração Pública.

É conclusivo que existe a necessidade de se promover a eficiência e a diminuição do risco nas redes e nos Sistemas de Informação do Estado Português, podendo o modelo proposto contribuir para a reflexão de como o fazer.

Por último, entende-se que a presente dissertação contribui com valor para comunidade, principalmente para todos os intervenientes das tecnologias de informação e da segurança na Administração Pública, uma vez que apresenta um panorama dos principais riscos nas redes aos quais os organismos podem estar sujeitos, sugerindo um conjunto de boas práticas e de mecanismos técnicos para a sua prevenção e deteção, expondo ainda uma visão agregada e normalizada do Estado a este nível.

5.2. TRABALHO FUTURO

Dando continuidade ao que já foi feito neste âmbito, e com o intuito de serem prestados todos os contributos necessários para formalmente se definir um modelo operacional de reorganização das redes de dados da Administração Pública e da sua segurança, pretende-se apresentar esta dissertação junto da AMA. Em acréscimo, importa igualmente propor planeamentos e cronogramas de implementação, com o envolvimento de todos os intervenientes transversais e específicos a cada ministério.

A fim de serem comprovadas na prática as vantagens do modelo, é também importante para um trabalho futuro proceder-se a um piloto de implementação, num dos ministérios que atualmente ainda não tenham centralizada a responsabilidade de gestão das tecnologias de informação e da

segurança. No entanto, antes e após esse piloto, e em períodos funcionais, deverão ser efetuados, por diferentes entidades, testes de intrusão e auditorias à rede, por forma a ser possível comparar-se os resultados obtidos e se validarem as vantagens inerentes ao modelo previamente antecipadas.

Uma vez que as ameaças em redes são muito mutáveis, e que as vulnerabilidades existirão sempre, as análises de risco periódicas e globais inerentes às redes e sistemas de cada um dos ministérios, são projetos de extrema importância para a segurança da Administração Pública e que também se entende serem pertinentes para trabalho futuro.

Quando for possível assegurar-se a centralização da gestão das TIC e da segurança num organismo por ministério, assim como a correspondente unificação das redes e dos centros de processamento de dados, é igualmente importante proceder-se a um estudo de nova restruturação. Este estudo deverá incidir sobre a viabilidade de existir um único organismo TIC em toda a Administração Pública, contrapondo os riscos e as dificuldades inerentes com as possíveis poupanças e ganhos de controlo que possam eventualmente existir nesse cenário.

REFERÊNCIAS BIBLIOGRÁFICAS

- ✓ AMA, **Documento de suporte à Rede Interministerial TIC – 1ª Reunião 2010**, Agência para a Modernização Administrativa, 2010;
- ✓ BARRETO, João, **Documentação da disciplina de Riscos e Ameaças incluída no Mestrado em Segurança dos Sistemas de Informação - Hacking de Redes e Sistemas**, Faculdade de Engenharia da Universidade Católica Portuguesa, 2009;
- ✓ BIRDI, Tarlok, **Network Intrusion Detection: Know What You Do (not) Need**, ISACA, 2006;
- ✓ BOWEN, Pauline, HASH, Joan, WILSON, Mark, **Information Security Handbook: A Guide for Managers**, National Institute of Standards and Technology, 2006;
- ✓ BOYLES, Tim, **CCNA Security Study Guide**, Wiley Publishing Inc, 2010;
- ✓ CORREIA, Pedro, **Caracterização Estatística de Botnets**, Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro, 2011;
- ✓ EASTTOM, Chuck, **Computer Security Fundamentals**, Pearson, 2012;
- ✓ ESTRELA, José, **Segurança em Redes de Computadores**, Faculdade de Engenharia da Universidade do Porto, 1998;
- ✓ ENISA, **Threat Landscape - Responding to the Evolving Threat Environment**, ENISA, 2012;
- ✓ ERICKSON, Jon, **Hacking: The Art of Exploitation 2nd Edition**, 2008;
- ✓ FERREIRA, Júlio, **Caracterização Estatística de Ataques Distribuídos em Redes Locais**, Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro, 2010;
- ✓ GAIVÉO, José, **As Pessoas nos Sistemas de Gestão da Segurança da Informação**, Universidade Aberta, 2008;
- ✓ GPTIC, **Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública**, GPTIC, 2011;
- ✓ GREGORY, Peter, **CISSP guide to Security Essentials**, Course Technology - Cengage Learning, 2010;
- ✓ HENMI, Anne, LUCAS, Mark, SINGH, Abhishek, CANTRELL, Chris, **Firewall Policies and VPN Configurations**, Syngress, 2006;
- ✓ **ISO/IEC 27001**, International Organization for Standardization and International Electrotechnical Commision, 2005;
- ✓ KREICBERGA, Liene, **Internal threat to information security – countermeasures and human factor wihin SME**, Lulea University of Technology, 2010;

- ✓ LAMMLE, Todd, **CCNA: Cisco Certified Network Associate Study Guide Sixth Edition**, Wiley Publishing Inc, 2007;
- ✓ LUAN, Hai, **Intrusion Detection and Management over the World Wide Web**, Faculty of Engineering and Computing - Dublin City University, 2010;
- ✓ MACEDO, Filipe, **Models for Assessing Information Security Risk**, Instituto Superior Técnico da Universidade Técnica de Lisboa, 2009;
- ✓ MASON, Andrew, **CCNP Security Firewall 642-617 Quick Reference**, Cisco Press, 2011;
- ✓ MANZUIK, Steve, PFEIL, Ken, GOLD, Andre, **Network Security Assessement From Vulnerability to Patch**, Syngress, 2007;
- ✓ MCAFEE, **Mcafee Threats Report: First Quarter 2012**, McAfee Labs, 2012;
- ✓ MCAFEE, **Mcafee Threats Report: Second Quarter 2012**, McAfee Labs, 2012;
- ✓ MCAFEE, **2013 Threats Predictions**, Mcafee Labs, 2012;
- ✓ MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George, **Hacking Exposed 6 – Network Security Secrets & Solutions**, McGraw-Hill, 2009;
- ✓ MOELLER, Robert, **IT Audit, Control and Security**, Wiley Publishing Inc, 2010.
- ✓ NAKAMURA, Juliana, **Evolução das Redes de Telecomunicação e o Multiprotocol Label Switching (MPLS)**, Escola de Engenharia de São Carlos da Universidade de São Paulo, 2009;
- ✓ NOONAN, Wes, DUBRAWSKY, Ido, **Firewall Fundamentals**, Cisco Press, 2006;
- ✓ OCONNOR, TJ, **Detecting and Responding to Data Link Layer Attacks**, SANS Institute, 2010;
- ✓ PAGET, François, **Hacktivism - Cyberspace has become the new medium for political voices**, McAfee Labs, 2012;
- ✓ **Resolução do Conselho de Ministros nº 109/2009**, Diário da República 1ª Série Nº 192, 2009;
- ✓ **Resolução do Conselho de Ministros nº 12/2012**, Diário da República 1ª Série Nº 27, 2012;
- ✓ **Resolução do Conselho de Ministros nº 42/2012**, Diário da República 1ª Série Nº 74, 2012;
- ✓ **Resolução do Conselho de Ministros nº 46/2011**, Diário da República 1ª Série Nº 218, 2011;
- ✓ RODRIGUES, Pedro, **Segurança Informática de Redes e Sistemas (Abordagem Open-Source)**, Universidade de Trás-os-Montes e Alto Douro, 2010;

- ✓ SAMUEL, Alexandra, **Hacktivism and the Future of Political Participation**, Harvard University, 2004;
- ✓ SANTOS, António, **Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação**, Escola de Engenharia da Universidade do Minho, 2007;
- ✓ SANTOS, José, **Contributos para uma melhor governação da cibersegurança em Portugal**, Faculdade de Direito da Universidade Nova de Lisboa, 2011;
- ✓ SANS Institute, **Critical Controls for Effective Cyber Defense**, SANS Institute, 2013;
- ✓ SCARFONE, Karen, MELL, Peter, **Guide to Intrusion Detection and Prevention Systems (IDPS)**, National Institute of Standards and Technology, 2007;
- ✓ SCHECHTER, Stuart, **Computer Security Strength & Risk: A Quantitative Approach**, Division of Engineering and Applied Sciences of Harvard University, 2004;
- ✓ SHEVCHENKO, Alisa, **Malicious Code Detection Technologies**, Kaspersky Lab, 2008;
- ✓ SOPHOS, Security Threat Report 2012 - Seeing the Threats Through the Hype, Sophos, 2012;
- ✓ SOFTWARE ENGINEERING INSTITUTE, **2011 CyberSecurity Watch Survey – How bad is the Insider Threat?**, CERT - Carnegie Mellon University, 2011;
- ✓ SPEROTTO, Anna, **Flow-Based Intrusion Detection**, University of Twente - Centre for Telematics and Information Technology, 2010;
- ✓ SZOR, Peter, **The Art Of Computer Virus Research And Defense**, Addison Wesley Professional, 2005;
- ✓ TAVARES, João, **O Sistema de Informação das Finanças Públicas: sua evolução e perspectivas de futuro**, Instituto de Informática, 2007;
- ✓ VACHON, Bob, GRAZIANI, Rick, **Accessing the WAN - CCNA Exploration Companion Guide**, Cisco Press, 2008;
- ✓ WEBSENSE, **Security Predictions**, Websense, 2013;
- ✓ ZÚQUETE, André, **Segurança em Redes Informáticas**, FCA, 2008;
- ✓ WEBSITES:
    - o AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA, **http://www.ama.pt/**, consultado em Julho/2012;
    - o ANONYMOUS-PORTUGAL, **https://www.facebook.com/AnonymousPORTUGAL**, consultado em Março/2013;

- BITS, **http://bits.blogs.nytimes.com/2012/10/03/hackers-breach-53-universities-dump-thousands-of-personal-records-online**, consultado em Janeiro/2013;
- CBS NEWS, **http://www.cbsnews.com/8301-501465_162-57470956-501465/yahoo-reportedly-hacked-is-your-account-safe**, consultado em Janeiro/2013;
- CDC, **http://w3.cultdeadcow.com/cms/texXxt.html**, consultado em Outubro/2012;
- CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO, **http://www.ceger.gov.pt/**, consultado em Julho/2012;
- CERT.PT, **http://www.cert.pt/**, consultado em Maio/2013;
- CLAMAV, **http://www.clamav.net**, consultado em Setembro/2013;
- CLAMWIN, **http://www.clamwin.net**, consultado em Setembro/2013;
- DIÁRIO DE NOTÍCIAS, **http://www.dn.pt/inicio/portugal/interior.aspx?content_id=2167383**, consultado em Setembro/2012;
- FIREHOST, **http://www.firehost.com/company/newsroom/web-application-attack-report-fourth-quarter-2012**, consultado em Fevereiro/2013;
- GABINETE NACIONAL DE SEGURANÇA, **http://www.gns.gov.pt/**, consultado em Julho/2012;
- GESTÃO INTEGRADA DA AVALIAÇÃO DE DESEMPENHO DA ADMINISTRAÇÃO PÚBLICA, **https://www.siadap.gov.pt/PaginasPublicas/Siadap.aspx**, consultado em Julho/2012;
- INFORMATION SECURITY HANDBOOK, **http://ishandbook.bsewall.com/risk/Assess/Risk/control_types.html,** consultado em Setembro/2012;
- KASPERSKY, **http://www.kaspersky.com/about/news/virus/2009/Kaspersky_Lab_publishes_an_analytical_article_on_botnet_economics**, consultado em Dezembro/2012;
- LUSÓFONA ONLINE CONTEÚDOS, **http://loc.grupolusofona.pt/index.php/reportagem/reportagem-2012/portugal-desprotegido-contra-ciberataques.html**, consultado em Setembro/2012;

- OPENVAS, **http://openvas.org**, consultado em Setembro/2013;
- PANDA SECURITY, **http://www.pandasecurity.com/angola/homeusers/media/press-releases/viewnews?noticia=10481**, consultado em Outubro/2012;
- PFSENSE, **http://www.pfsense.org/**, consultado em Junho/2013;
- GOVERNO DE PORTUGAL, **http://www.portugal.gov.pt/pt.aspx**, consultado em Julho/2012;
- PPLWARE**, http://pplware.sapo.pt/networking/sites-da-sonae-atacados-depois-de-afirmacoes-polemicas/**, consultado em Fevereiro/2013;
- PROJETO SNORT, **http://www.snort.org**, consultado em Outubro/2013;
- SAPHETY**, http://www.saphety.com/pt-PT/home**, consultado em Julho/2012;
- SECRETARIA-GERAL DA PRESIDÊNCIA DO CONSELHO DE MINISTROS, **http://www.sg.pcm.gov.pt**, consultado em Outubro/2013;
- SHREW SOFT, **https://www.shrew.net/static/help-2.1.x/vpnhelp.htm**, consultado em Julho/2013;
- SISTEMA DE INFORMAÇÃO DA ORGANIZAÇÃO DO ESTADO, **http://www.sioe.dgaep.gov.pt**, consultado em Julho/2012;
- SPAMHAUS, **http://www.spamhaus.org/news/article/685/**, consultado em Janeiro/2013;
- SUCURI, **http://blog.sucuri.net/2011/03/mysql-com-compromised.html**, consultado em Janeiro/2013;
- SYMANTEC, **http://www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec-0**, consultado em Dezembro/2012;
- TIME, **http://www.time.com/time/business/article/0,8599,1933796,00.html**, consultado em Dezembro/2012;
- TUGALEEKS, **http://www.tugaleaks.com/cabovisao-ataque-informatico.html**, consultado em Janeiro/2013;
- WHOIS, **http://who.is**, consultado em Setembro/2013.

SOBRE O AUTOR

Ricardo João Duque Oliveira nasceu em 16 de agosto de 1978 e iniciou a sua atividade profissional em 1997, na Década Informática SA, onde tinha como principais funções a instalação, manutenção e reparação de desktops e servidores em clientes finais.

Em janeiro de 2000 integrou na Administração Pública, ficando com a responsabilidade de gerir o parque informático do Instituto Nacional de Intervenção e Garantia Agrícola (INGA).

Mais tarde, em meados de 2007 e enquanto concluía a licenciatura em Engenharia Informática na Universidade Autónoma de Lisboa, começou a desempenhar funções de gestão de redes, de segurança e de administração de sistemas operativos Linux no Instituto de Financiamento da Agricultura e Pescas (IFAP). Assumiu projetos no domínio das redes, tais como a reengenharia da rede do ministério, e também no âmbito da Segurança dos SI, nomeadamente contribuindo no estabelecimento e manutenção do Sistema de Gestão da Segurança da Informação do IFAP, no Plano de Continuidade do Negócio e *Disaster Recovery* e no Plano de revisão de vulnerabilidades técnicas e resposta a incidentes. Colaborou ainda em auditorias de segurança dos SI promovidas periodicamente às entidades com funções delegadas pelo IFAP.

Em março de 2014, começou a assumir funções de chefia de divisão de informática na Direção-Geral dos Recursos Naturais, Segurança e Serviços Marítimos.