2013

Segurança de redes Informáticas

Rui Jorge de Tristão e Castro

LICENCIATURA EM INFORMÁTICA
LISBOA

Coordenador: Dr. Pedro Ramos Brandão

"Concentre-se nos pontos fortes, reconheça as fraquezas,

agarre as oportunidades e proteja-se contra as ameaças"

Sun Tzu

RESUMO

Este trabalho faz uma abordagem aos sistemas de segurança utilizados pelas redes informáticas, suas vulnerabilidades, os ataques utilizados e questões éticas relacionadas com a proteção da mesma.

São explicados métodos de criptografia de substituição e transposição, modelos algoritmos de criptografia simétrica e assimétrica. São apresentados ainda conceitos de chaves públicas e privadas e a utilização destas pelos algoritmos de criptografia no processo de cifragem e decifragem de mensagens.

São igualmente analisadas em as redes sem fios e as VPN's

É também apresentada a arquitectura de rede TCP/IP para uma melhor compreensão da temática em questão.

Palavras-chave: segurança da informação, redes *wireless*

Índice

LISTA DE ABREVIATURAS

AES - Advanced Encription Standard

AP - Access Pointer (Ponto de acesso)

ARP - Address Resolution Protocol

CA – Certificate Authority (Autoridade Certidicadora)

CCTV – Closed-Circuit Television (Circuito interno de televisão)

DES - Data Encryption Standard (Algoritmo de Encriptação de Dados)

DNS – Domain Name System (Sistema de Nomes de Domínios)

DES - Data Encryption Standard

DMZ - DeMilitarized Zone (zona desmilitarizada)

DoS - Distributed Denial of Service (Negação de serviços distribuído)

EAP - Extensible Authentication Protocol

H-IDS –Host Intrusion Detection System (Sistema de deteção de Intrusos em rede)

ICMP – Internet Control Message Protocol

IBM -International Business Machines

IDS - Intrusion Detection System (Sistema de deteção de Intrusões)

IEC – International Electrotechnical Commission

IP – Internet Protocolo

IPSEC - Internet Protocol Security

ISO - International Organization for Standardization

LAN - Local Área Network (Rede de área local)

MAC - Address Resolution Protocol

MD-5 - Message-Digest algorithm 5

N-IDS – Network Intrusion Detection System (Sistema de deteção de Intrusões em rede)

OSI - Open Systems Interconnection

PPTP – Point-to-Point Tunneling Protocol (Protocolo Ponto a Ponto)

QoS – Quality of service (Garantia de qualidade de serviço)

RSA- Ronald, Shamir, Adleman, algorithm

SHA-2 - Secure Hash Algorithm

SSID – *Service Set ID*

SQL - Structured Query Language (Linguagem de Consulta Estruturada)

TCP – Transmission Control Protocol

TLS - Transport Layer Security (Segurança da Camada de Transporte)

UDP - User Datagram Protocol

VPN - Virtual Private Network

WAN - Wide Área Network

WEP - Wired Equivalent Privacy Wep

WPA - Wi-fi Protected Access

WPA-Personal - Wi-Fi Protected Access Personal

GLOSSÁRIO

Application Proxy – Serviço que recebe pedidos destinados a outro servidor e age em nome do cliente (como procurador do cliente) para obter o serviço solicitado

Boot sector – É uma região do disco que contem "código maquina" para ser carregado em memória (RAM), permitindo que o sistema operativo inicie

Broadcast – É uma transmissão de informação em que esta é enviada para uma multiplicidade de nodos simultaneamente

Buffer Overflow - Acontece quando um programa escreve mais dados para um buffer localizado na pilha que ali foi efetivamente reservada

BUS – Topologia de rede BUS é uma arquitetura de rede em que os clientes estão conectados

DNS - Sistema de gerenciamento de nomes, hierárquico e distribuído que resolve nomes em IP's

Event Logs – Registo dos eventos ocorridos no equipamento

Firewall - Dispositivo de uma rede de computadores que tem por objectivo aplicar uma política de segurança com regras que controlam o fluxo de entrada e saída

FRAGGLE – Ataque de negação de serviço com ferramenta com o mesmo nome

Gateway - Um *gateway* é um nó (roteador) em uma rede TCP / IP, que serve como um ponto de acesso para outra rede

Hacker - Indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores.

Honey Pot - Ferramenta que tem a função de, propositalmente, simular falhas de segurança de um sistema, atrair o invasor e colher informações sobre o mesmo

Handshake - Processo pelo qual duas máquinas afirmam uma à outra que a reconheceu e está pronta para iniciar a comunicação. O handshake é utilizado em protocolos de comunicação, tais como: FTP, TCP, HTTP, SMB,SMTP,POP3

Mail Bomb – Forma de ataque de negação de serviço que consiste em enviar grandes volumes de e-mail para um endereço na tentativa sobrecarregar o servidor até que este fique sem recurso

Malware - *Software* malicioso que tem por objectivo infiltrar-se nos sistemas, fazendo com que o sistema se comporte conforme as intenções dos atacantes

Man-in-the-Middle - Forma de ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registados e possivelmente alterados pelo atacante sem que as vitimas se apercebam.

Packet Filtering - Sistema de segurança que controla o tráfego de rede, de entrada e saída através da análise dos pacotes de dados e determina se devem ser permitidos ou não, com base num conjunto de regras.

Phishing - Forma de fraude eletrónica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais

Ping-of-Death - O *ping* da morte é uma forma de ataque a um computador que consiste em enviar um *ping* malformado e malicioso.

RAID - Conjunto Redundante de Discos Independentes

Rougware – Falso software de antivírus

SMURF – Nome de ataque de Negação de Serviço com nome da aplicação usada

Sniffing – Software capaz de intercepta e registrar o tráfego de dados em uma rede de computadores

Software - Sequência de instruções a serem seguidas e/ou executadas, na manipulação, redireccionamento ou modificação de uma dada informação ou acontecimento

Spoofing - Ataque que consiste em mascarar (spoof) pacotes IP utilizando endereços de remetentes falsificados.

SQL Injection – Ataque em que o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação das entradas de dados de uma aplicação.

Stealth - Tecnologia utilizada para ocultar

Trojans - É um malware que parece ser útil e legítimo, mas pode comprometer a segurança do computador.

Worms - É um programa autorreplicante, semelhante a um vírus

Indice de figuras

1.Introdução

1.1 Enquadramento

Este Projecto Global tem como tema principal a problemática da segurança informática.

Actualmente, as organizações encontram-se dependentes dos sistemas de informação sofrendo, no entretanto, em muitos casos, de uma profunda falta de cultura de segurança,

A grande dificuldade de se implementar qualquer sistema que vise a mudança cultural deve-se ao facto de o trabalho ter de ser cíclico, contínuo e persistente.

É pois necessário que cada organização identifique as suas falhas de segurança, adopte as medidas necessárias, monitorize a sua aplicação e eficácia.

A problemática da segurança não passa só pela empresa enquanto entidade abstrata, mas também por uma cultura individual quer dentro das empresas quer a título particular.

Sendo um tema vasto, pretende-se analisar os pressupostos necessários para a implementação de políticas de segurança.

È pois uma abordagem a esta problemática, um olhar atento às várias vertentes que a compõem: as pessoas, os precessos envolvidos, as empresas e a tecnologia.

1.2 Estrutura

Os aspectos principais da segurança da informação que se colocam no contexto actual, são abordados no capitulo 2.

No capitulo 3 são abordados os temas especificos da segurança: as ameaças, os tipos de ataques, sistemas de protecção e a criptografia enquanto peça fundamental da arquitectura de segurança.

O capitulo 4 enquadra a segurança nas redes TCP, que têm por missão proteger.

Nos capitulos seguintes é feita a analise das VPN's e das redes sem fios.

1.3 Objectivo

O presente estudo tem como objectivo apresentar e explorar diferentes aspectos da segurança informática que se colocam na actualidade. Que tipos de perigos existem , que

técnicas são usadas para lançar ataques, que sistemas de defesa podem ser implementados, são temas abordados neste trabalho de forma a dar essa perspectiva ao leitor.

São igualmente abordadas algumas questões sobre a responsabilização que compete a cada um dos intervenientes, bem como questões de ética na vertente do binómio segurança *versus* privacidade.

2 Estado da arte

Introdução

A questão central nesta temática é a informação como activo para pessoas e organizações e consequentemente a necessidade de ser protegida de forma adequada.

Quais as formas de proteger essa informação, que medidas tomar, que medidas implementar, são questões colocadas e abordadas neste capítulo numa perspectiva da problemática em si.

Questões sobre o valor da informação, a responsabilidade das organizações no combate ao crime informático, a proteção dos sistemas ou o direito à privacidade, são aqui revistas[1].

A problemática da segurança

O cibercrime é o exemplo do crime perfeito. As empresas são diariamente atacadas diariamente muitas vezes sem sequer terem conhecimento que informações valiosas lhes estão a ser roubadas. Os cibecriminosos, operam de forma silenciosa e anonima, vasculhando contas à procura de informação que possa ser vendida posteriormente.

Este esforço criminal é facilitado por vulnerabilidades dos sistemas operativos, browsers e aplicações que são exploradas por parte dos atacantes.

Os cibercriminosos, descobriram que comprometer terminais dos colaboradores, é um caminho mais simples para chegar às redes das empresas do que atacando-as directamente. Vulnerabilidades não corrigidas, permitem que os atacantes instalem malware nos equipamentos desses colaboradores, ganhando acesso à rede com o mesmo nível de permissões que estes possuem[2].

Casos de roubos cibernéticos abundam, por exemplo em Setembro de 2012 o FBI lançou um alerta aos bancos americanos relativo a ataques que estavam a ser perpetrados

---

[1] Trustee.(2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods.http://www.trusteer.com/resources/white-papers

[2] (2012). Assessing Security Vulnerabilities and Patches. Autralian Government -Departament of Defence Intelligence and Security.
http://www.dsd.gov.au/publications/csocprotect/assessing_security_vulnerabilities_and_patches.htm

por cibercriminosos, os quais estavam a instalar malware e keyloggers, com vista a obtenção de credenciais[1].

As agências têm reportado espionagem generalizada, patrocinada por países estrangeiros, às indústrias de alta-tecnologia, financeiras, farmacêuticas, comunicações e de defesa. E entre estas empresas encontram-se gigantes como a Google, Intel, Pfizer, etc.

Nestes ataques, devido ao seu carácter anónimo é difícil distinguir quais são patrocinados por estados ou privados.

O MI5 inglês em 2012 revelou uma lista de empresas que tinham perdido receitas, num valor de cerca de 800 milhões de libras. A McAfee afirma que um quarto das empresas viu o lançamento dos seus produtos atrasados, devido a ataques patrocinados por estados, com implicações legais, económicas, perda de confidencialidade dos dados e perdas de confiança. A lista de relatórios deste tipo é enorme.

As investidas aumentam em busca de falhas de segurança[3], podendo os responsáveis das empresas virem a ser responsabilizados por não colocarem em prática as medidas para colmatarem essas mesmas falhas.

Ataques a instituições bancárias, comprometendo os depósitos e informação de clientes, já ocorrem á mais de uma década. Quando o dinheiro dos clientes é roubado, são em geral descobertos, mas quando é informação que é furtada, não é tão óbvio e como tal não o são muitas vezes[4].

Isto leva-nos a refletir sobre o valor da informação. A informação numa organização tem que ser identificada, catalogada, identificado o local de armazenamento e a forma como vai ser disponibilizada aos colaboradores e clientes, para que se lhe possa atribuir um valor.

Para conseguir manter informação, cujo valor é superior ao seu custo e ao potencial risco que representa a sua perda, é necessário começar por a identificar. A dificuldade desta tarefa depende de vários factores, como o tipo de informação, que partes estão interessadas nela, tipo de empresa, localização ou duração do ciclo de vida da informação. Por exemplo, um *email* tem um ciclo de vida útil curto mas por motivos legais tem que ser guardado por vários anos.

---

3 Ackerman,Elise. (2013). New Verizon Security Report Finds A Growing Number Of Attacks By China's Hacker Army. Forbes. http://www.forbes.com/sites/eliseackerman/2013/04/23/new-verizon-security-report-finds-a-growing-number-of-attacks-by-chinas-hacker-army/

4 Trustee. (2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods.http://www.trusteer.com/resources/white-papers

Por outro lado, guardar informação, mesmo considerada valiosa, pode ser arriscad, é o caso de quando se guarda informação relativa a clientes, podendo entrar em conflito com os requisitos de privacidade.

A incapacidade de identificar o valor da informação e por quanto tempo, força normalmente a que seja retida por mais tempo que o necessário. Este facto faz com que 69% da informação guardada pelas empresas seja desnecessária.

Temos que ter em conta que a gestão da informação desnecessária tem custos para as empresas [5]. Consomem recursos na manutenção das aplicações, cópias de segurança, espaço de armazenamento, etc. Outro factor a ter em conta, é o facto de que a informação desnecessária torna a pesquisa da informação importante mais complexa.

Todas as partes envolvidas no processo relativo à manutenção da informação devem estar sensibilizadas para o custo e risco da sua manutenção [6].

Os serviços de TI têm que gerir os requisitos absolutos de segurança com a pressão de facilidade de acesso à informação. Esta tarefa é bastante complicada em ambientes cada vez mais distribuídos, com os colaboradores a usarem os seus próprios dispositivos móveis, os quais escapam completamente ao controlo dos serviços.

O conceito do DLP (*Data Loss Prevention*) consiste em identificar a informação mais crítica e valiosa da empresa e trabalhar na eliminação de falhas que podem expô-la a ameaças internas e externas.

O DLP oferece meios de minimizar perdas e fugas sem limitar a produtividade. Apesar de não eliminar totalmente perdas, o seu objectivo é realista: diminuir a perda e exposição de dados sem interferir na produtividade. O processo passa por várias fases: identificação de locais de armazenamento, classificação de informação baseado no valor, consolidação de dados para facilitar o seu manuseamento, criação de políticas de segurança e a aplicação dessas mesmas políticas [7].

Muitas empresas são alheias ao facto de terem sido atacadas até ao momento que são avisadas por uma terceira parte. O tempo médio, até um ciberataque ser detectado, ronda os 400 dias, o que leva a que grande parte deles acabe por não ser

---

5 Service Alberta and the Office of the Information and Privacy Commissioner.(2008).A Guide for Businesses and Organizations.

[6] Paknad, Deidre . (2013). Sure, information has value, but don't forget the risks. Computerworld

[7] Jach, Matt. (2012). Data Loss Prevention. CDW

detectado. Segundo a McAfee, apenas três em cada dez empresas denuncia as violações e perdas de dados que sofrem [8].

A maior preocupação encontrada pela *PriceWaterHouseCoopers* num estudo realizado em 78 países relativamente à problemática da segurança, é a reputação. Assim, entende-se a relutância que as empresas têm em divulgar informação relativamente aos ataques que são sujeitas, o que não ajuda no entanto ao conhecimento geral do problema.

2.1 Métodos de ataques a empresas

Os cibercriminosos usam uma variedade de técnicas para se poderem infiltrar nas redes empresariais. A abordagem mais vulgar é a de infectar um computador de um colaborador, roubar-lhe as credenciais e usar os seus privilégios para roubar informação ou iniciar transacções fraudulentas. Cerca de 35% desses ataques, são ataques de oportunidade mas os restantes têm objectivos bem definidos. Estudos indicam que 1% de todos os computadores pessoais estão infectados com *malware* [9].

2.1.1 Phishing

Continua a ser um método eficaz de atrair utilizadores para *sites* comprometidos e levá-los a descarregar ficheiros infectados. Apesar dos muitos avisos, os utilizadores continuam a ser enganados por criminosos que se servem de informações retiradas de redes sociais e a pessoas próximas das vítimas, para criar mensagens credíveis. Ataques baseados em *email*, aumentaram 56% em 2012 [10].

[8] Trustee.(2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods.http://www.trusteer.com/resources/white-papers
[9] Trustee.(2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods.http://www.trusteer.com/resources/white-papers
[10] Jach, Matt. (2012). Data Loss Prevention. CDW

2.1.2 Ameaças da Web

Este tipo de ataques é bastante eficaz a comprometer os computadores dos colaboradores das empresas. Os cibercriminosos, constroem *sites* e comprometem *sites* legítimos, para lá colocarem *malware*.

Uma nova técnica chamada "*Watering Hole*" visa infectar as vítima associadas a uma determinada empresa, industria ou região. *Sites* legítimos que se sabe serem do interesse de um determinado alvo, são comprometidos. Assim, é provável que a vítima ou vítimas acabem por aceder a um desses *sites* e serem infectados.

A *sophos*, calcula que 30000 *websites* sejam infectados todos os dias, a *Mcafee*, reportou ter encontrado 10000 sites infectados por dia, em Junho de 2012.
A probabilidade de um dispositivo ser infectado quando acede a um *site*, é maior que nunca [11].

2.1.3 Exploração de vulnerabilidade de sistema

Depois de enganar os utilizadores levando-os a abrir um *email* infectado, o passo seguinte é infectar o dispositivo com *malware*.

Os cibercriminoso, tornaram-se muito eficientes a explorar vulnerabilidades e ultrapassar os sistemas de segurança. Não surpreende pois que um estudo indique que 74% dos profissionais considere que a segurança dos seus computadores pessoais seja ineficiente [7].

2.1.4 Vulnerabilidades de *software*

As vulnerabilidades são referentes a falhas de código do *software*, devido a falhas de projecto ou erros de codificação, que permite que um atacante, comprometa o sistema.

[11] Trustee.(2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods.http://www.trusteer.com/resources/white-papers

A *Symantec*, reportou cerca de 5000 novas vulnerabilidades em 2011, apesar de ter diminuído 19% em relação ao ano anterior, o número de vulnerabilidade críticas aumentou.

Vulnerabilidades de *software* permitem que sejam ultrapassados os sistemas de controlo existentes nos sistemas operativos ou criados por outras entidades [7].

Foi reportado pela Microsoft que vulnerabilidades em aplicações representam 70% das vulnerabilidades encontradas no primeiro semestre de 2012. As restantes repartem-se entre sistemas operativos e *browsers*.

A Microsoft implementou um processo denominado SLD (*Security Development Lifecycle),* com o objectivo de tornar o *software* mais seguro. Este processo encontra-se aberto aos fabricantes, para ser usado livremente pois não há *software* livre de riscos.

A técnica anteriormente passava por correcções após as vulnerabilidades serem detectadas. O SLD foi lançado em 2004 para produtos ligados à Internet, empresariais e domesticas com o objectivo de reduzir as vulnerabilidades.

Este processo não foi bem recebido por alguns fabricantes que viram o lançamento dos seus produtos atrasados pelos novos requisitos da Microsoft.

Apesar do SLD ter reduzido as vulnerabilidades e os problemas dos consumidores dramaticamente, a *Microsoft* sabe que nunca chegarão ao nível de "vulnerabilidade zero" [12].

2.1.5 Exploits

Exploits são pedaços de código desenhado para tirar partido das vulnerabilidades do sistema para entregar *malware*, que de outra forma seria impedido pelas restrições do sistema.

Para combater estas ameaças, os fabricantes de *software* trabalham arduamente para reparar estas vulnerabilidades. Cerca de 91% destas são corrigidas no mesmo dia que são conhecidas.

A IBM declarou que em 2011, havia *exploits* conhecidos para 11% das vulnerabilidades existentes.

[12] InfoWorld Tech Watch.(2013). Microsoft: Invulnerable software is not possible

Apesar das correcções se encontrarem disponíveis, cerca de 2,7% das aplicações da *Microsoft* e 6,7% de outros fabricantes, continuam sem serem aplicadas, deixando assim grande parte dos utilizadores expostos. Assim, é necessário que administradores e utilizadores em geral estejam constantemente a par das correções de *software* que vão sendo lançadas pelos fabricantes.

Apesar das estatísticas de *software* não actualizado não parecem alarmantes, não refletem a realidade do ciclo de vida das vulnerabilidades e dos *exploits* [13]

A descoberta de vulnerabilidades e o desenvolvimento de e*xploits*, é um negócio muito lucrativo para os atacantes [14].

Apenas uma semana após a saída dos *Windows* 8, e segundo a revista *Vupen,* já existia um *Hack* [15] disponível.

Um dos desafios de segurança que os departamentos de TI têm é a de identificar protecção adequada para a informação versus a segurança da própria empresa [16].

Educação e consciencialização de utilizadores[17], medidas preventivas e uma solução moderna, são componentes integrantes de uma defesa contra as ameaças da web [18] .

Algumas medidas preventivas devem ser implementadas para reduzir o risco e manter-se à frente das ameaças tanto quanto possível. Em particular é importante:

- Manter os sistemas actualizados - Ter os sistemas actualizados com as ultimas actualizações lançadas pelo fabricantes, incluido sistema operativo, *browser*, media players, leitores de PDF, e todo as outras aplicações
- Standardizar o software de web - A standardização dos browsers facilita a criação e manutenção de políticas de segurança

---

[13] (2013).Targeted Attack Exploits Ichitaro Vulnerability. Symantec. http://www.symantec.com/connect/blogs/targeted-attack-exploits-ichitaro-vulnerability-0

[14] Constantin, Lucian. (2012). Cybercriminals increasingly use online banking fraud automation techniques. computerworld. http://www.computerworld.com/s/article/9228527/Cybercriminals_increasingly_use_online_banking_fraud_automation_techniques

[15] Modificação de um programa ou dispositivo para dar ao usuário o acesso a recursos que não estariam disponíveis, como adaptações de acessibilidade

[16] Trustee. (2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods. http://www.trusteer.com/resources/white-papers

[17] Kennedy, David.(2013)The Debate on Security Education and Awareness. TrustedSec.https://www.trustedsec.com/march-2013/the-debate-on-security-education-and-awareness/

[18] Evers, Joris. (2006). Security expert: User education is pointless. CNET News. http://news.cnet.com/2100-7350_3-6125213.html

- Implementar medidas de segurança nos browsers - a implementação destas medidas poderão levar ao aparecimento de caixas de diálogo aos utilizadores facto que irá criar alguma oposição por parte destes a estas medidas, são no entanto fundamentais
- Assegurar o uso de palavras-passe seguras - esta é uma das medidas básicas que deve ser implementada, evitando que sejam usadas palavras-passe como nome ou data de nascimento, as quais são facilmente descobertas
- Usar um sistema de segurança de acesso à Internet eficaz - é vital o uso de um sistema robusto como estrategia de segurança. Irá reduzir a exposição a ameaças enquanto limtará o acesso a sites que são terreno fértil para malware como são sites para adultos, jogo, etc.[19].

Se há questão que preocupe os responsáveis pela segurança do TI são os dispositivos móveis e em particular os "*bring-your-own-device*" (BYOD)[20], com implicações ao nível da privacidade, com potencial perda de dados e fuga de informação.

A tendência é de uso cada vez maior de "*smart-devices*"[21], com capacidades de acesso a serviços de *cloud* e integração com os serviços empresariais. Relatórios apontam para que 70% das empresas possuam algum tipo de programa de BYOD, que 62% dos colaboradores usa esse tipo de dispositivo para trabalhar e que 56% dos *tablets* usados pelos colaboradores foram adquiridos pelos próprios. A utilização de dispositivos pessoais nas empresas, escapando ao controlo das TI, representa um grave risco de segurança [22].

O número de dispositivos e sensores à nossa volta pode em breve levar a monitorização das actividades dos utilizadores ao estilo do mundo de Orwell. Esta situação tem levado os defensores da privacidade a questionar a falta de regulamentação clara, sobre os dados moveis dos utilizadores.

A pressão para a recolha de dados móveis por parte das empresas continua a aumentar, aliada à falta de regulamentação, faz aumentar o risco de abusos. Ignoramos as

---

[19] McCormack, Chris. & Chester, Wisniewski. (2010), Five tips to reduce risk from modern web threats, Sophos
[20] Significa que os colaboradores usam *tablets* e *smartphones* no seu dia-a-dia e querem trazê-los para seus ambientes de trabalho
[21] Dispositivo móvel sem fios com capacidades de voz, vídeo, acesso à Internet, geolocalização
[22] Eschelbeck, Gerhard & Schwartzberg, David. (2012). BYOD Risks and Rewards. Sophos. http://www.sophos.com/en-us/security-news-trends/security-trends/byod-risks-rewards.aspx

consequências e implicações desta perda de privacidade e não temos sequer noção do que está para vir neste admirável mundo novo dos ambientes móveis [23].

Os mecanismos de segurança serão instalados em sistemas de suspensão e aquisição de dados (SCADA) e em sistemas lógicos de controlo. A ideia é ser possível que os mecanismos detectem o problema e isolem o equipamento comprometido da rede, antes que ele crie algum dano.

Estes sistemas são usados em infraestruturas críticas, como as de gás, petróleo, electricidade ou de defesa. Cada dispositivo vigia a vizinhança para ver se este se comporta de forma indevida.

Os equipamentos destas indústrias estão sob constantes ataques e de forma crescente com origem na China e em países do médio Oriente.

Devido ao facto de muitos equipamentos não suportarem os protocolos necessários, foi desenvolvido um algoritmo para ser implementado em qualquer dispositivo susceptível de ser ligado à rede, seja como *software* seja como *firmware.*

O algoritmo vai estabelecer parâmetros operacionais tais como a temperatura ou a velocidade para os dispositivos de rede. No caso de alterações nestes parâmetros, os outros dispositivos param as comunicações com o equipamento, para que este não possa operar mais.

A tecnologia irá aumentar a segurança dos sistemas tradicionais de comunicações e de controlo de acessos [24].

2.2 Segurança Cibernética

O crescimento da *Internet* tem impacto profundo no dia-a-dia da economia global. Permitindo a troca de ideias à volta do mundo, a I*nternet* tem contribuindo para uma sociedade mais aberta, maior liberdade de expressão, através dela iniciaram-se revoluções, depuseram-se ditadores [25].

---

[23] Olavsrud, Thor. (2013). 4 Mobile Security Predictions to Help CIOs Plan for the Future. CSO

[24] Gonsalves, Antone (2013). Researchers develop industrial systems that watch for breaches. CSOonline

[25] Manyika,James & Roxburgh, Charles. (2011). The great transformer: The impact of the Internet on economic growth and prosperity. insey Global Institute

A *Internet* evoluiu de um estágio em que servia apenas para ligar alguns polos universitários nos anos 60 para uma rede intercontinental de sistemas e informação. Ninguém a controla centralmente ou globalmente ou é seu dono.

Calcula-se que em 2016, cerca de 3 biliões de pessoas usarão a Internet, no entanto esta não foi desenhada a pensar na questão da segurança.

Apesar de permitir muitas oportunidades, também proporciona um aumento crescente das ameaças. Como não tem fronteiras ou policiamento, os utilizadores legítimos estão vulneráveis a ataques.

Os governos reconhecem a existência de ataques por parte de organizações criminosas com o objectivo de roubar informação empresarial e particular, ataques de cariz político, espionagem por parte de outros estados e ataques às infraestruturas nacionais[26].

Novas estratégias de seguranças nacionais estão a ser implementadas no combate ao crime informático. Essa abordagem passa por dar grande enfase à responsabilização do público e industria em ajudar as autoridades nesta luta, reforçar a lei no que respeita a este tipo de crime, agilizar a actividade governamental nesta área. Esta responsabilização das empresas advém do facto de que grande parte das infraestruturas nacionais que estão em risco tais como: telecomunicações, energia, financeiras, transportes e alimentares, indústrias vitais para o país, se encontrarem no sector privado [27].

A conjuntura económica mundial desfavorável leva a que este combate tenha novas abordagens. A DARPA (*Defense Advanced Research Projects Agency*) do departamento de defesa dos Estados Unidos está a ajustar a sua abordagem para o desenvolvimento de novas tecnologias de defesa neste contexto económico difícil. O objectivo no entanto continua a ser o mesmo, prevenir e criar surpresa tecnológica. Três factores têm orientado este objectivo. O primeiro é o surgimento de novas ameaças. Em vez de se focarem só nas ameaças de outros países, devem estar preparados para lidar com crime organizado, terrorismo organizado e individual. O segundo é a evolução tecnológica rápida em áreas como a dos componentes militares. O terceiro factor advém das restrições orçamentais, com as consequentes reduções de recursos humanos.

Esta pressão leva a DARPA a desenvolver sistemas que continuem a dar-lhe vantagem nesta complexa guerra. Esta estratégia passa também por usar tecnologia comercial

[26] Bumiller,Elisabeth. (2013). Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks. The New York Times

[27] TSO.(2012).The UK cyber security strategy: Landscape review.www.tsoshop.co.uk

existente e encorajar novos desenvolvimentos ao nível universitário, laboratórios governamentais e empresas privadas de desenvolvimento.

A DARPA está apostada em desenvolver capacidades tecnológicas que lhe permitam vantagem nesta ciberguerra, mas sabe que não há uma arma que, isoladamente, seja capaz de a vencer [28].

2.2.1 Segurança da informação em ambientes de *Cloud*

Actualmente usam-se sistemas escaláveis distribuídos espalhados pelos confins da *Internet* conhecidos como *Cloud Computing* [29].

Cloud computing refere-se a uma infraestrutura subjacente para um modelo de prestação de serviços que tem a vantagem de reduzir custos através da partilha de recursos de computação e armazenamento, combinados com um mecanismo de provisionamento, baseando-se num modelo de negócio de *pay-per-use*. Estes novos recursos têm um impacto direto no orçamento de TI, mas também afectam os mecanismos tradicionais de segurança, confiança e privacidade[30].

Neste mundo de computação, os utilizadores são obrigados a aceitar as premissas de segurança que lhes são impostas. Tipicamente os utilizadores não sabem a localização exacta dos seus dados, nem a fonte dos dados que estão armazenados junto com os seus. Os dados que se encontram nas *Clouds*, vão desde dados públicos, com preocupações mínimas de segurança, até informação altamente sensível como números de segurança social, registos médicos, manifestos de carga, etc [31].

As vantagens da Cloud, ou seja a sua capacidade de expansão rápida, armazenamento remoto e partilha de serviços num ambiente dinâmico, torna-se uma desvantagem no que respeita à questão de exitir uma fiabilidade suficiente que sustente a confiança dos clientes [32]. Alguns mecanismos tradicionais para garantia de

---

[28] Wait, Patience. (2013). DRAPA: New Threats Demand New Technologies. InformationWeek

[29] Trustee.(2012).The Rising Threat of Corporate Cybercrime. Cybercriminal motives and methods.http://www.trusteer.com/resources/white-papers

[30] Blandford, Richard. (2011). Information security in the cloud. *Network Security*, Vol. 2011

[31] Security & Privacy, IEEE (Volume:7 , Issue: 4)(2009). http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=5189563

[32] Huizenga, Gerrit & .(2012). Taking Advantage of Cloud Computing to Meet Today's Business Needs. IBM® Redbooks

privacidade como contractos, não sao suficientemente flexives ou dinamicos para atender a este novo paradigma [33].

Levantam-se pois questões, como a referente ao facto de a utilização de ambientes de *Cloud* alivia ou não as entidades proprietárias dos mesmos no que respeita à aplicação de medidas de segurança apropriadas para protecção de dados e aplicações. Ou se devem ser partilhados com as empresas que providenciam os serviços de acesso à *Internet*, entre outras.

A resposta a estas questões ainda se encontra num limbo legal. Como em todas as questões tecnológicas, o regulador n acontecimentos. A não consegue acompanhar os acontecimentos. A problemática da *Cloud Computing* é uma extensão do que se tem experimentado com a Internet.

Para assegurar que tais regras são criadas e apropriadas para os ambientes de *Cloud*, a indústria deveria estabelecer políticas efectivas e coerentes para a aplicação de métodos apropriados de segurança[34]

A segurança da informação tem a longa tradição de se basear na capacidade dos colaboradores em tomar boas decisões. Modificar o comportamento através de treino é difícil, alguns responsáveis consideram-no mesmo uma batalha perdida. Apesar dos sistemas de controle básicos tais como dados de antivírus, protecção de fugas de informação e firewalls serem importantes, eles estão longe de ser suficientes.

O custo de lançar ataques personalizados diminui à medida que os custos para criar tecnologia de defesa personalizada aumenta. O aumento do número de atacantes com capacidades para levar a cabo acções bem definidas e personalizadas, levanta uma importante questão para a indústria da segurança: o que irá acontecer quando os custos marginais de lançar um ataque se aproximar de zero? [35]

---

[33] Blandford, Richard.(2011). Information security in the cloud.Network Security, Vol. 2011, No. 4

[34] Kaufman, L.M. (2009). Data Security in the World of Cloud Computing. Security & Privacy, IEEE (Volume:7 , Issue: 4) http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5189563.

[35] Thompson, H.(2013). The Human Element of Information Security. Security & Privacy, IEEE (Volume:11 , Issue: 1). http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6376054&punumber%3D8013

3 Segurança da Informação

As empresas têm aberto os seus sistemas aos seus clientes e fornecedores com o desenvolvimento da Internet. Esta exposição dos sistemas tem o inconveniente de os tornar susceptíveis a ataques [36].

Existem três principais razões, entre outras, para as empresas justificarem preocupação relativamente à segurança da informação:

- Dependência dos Sistemas de Informação - Sem os seus sistemas informáticos a empresa pára.
- Vulnerabilidades dos Sistemas de Informação – Os sistemas têm que estar protegidos quer de acidentes naturais quer de ataques
- Investimento dos sistemas de informação – O investimento é elevado e a informação que eles possuem é valiosa como tal os sistemas devem ser protegidos.

Um factor importante a ter em conta na questão da segurança é a protecção física dos mesmos:

> "No domínio da informática, a segurança física dos sistemas refere-se principalmente à protecção de equipamentos e instalações contra riscos por perdas, extravios ou por danos físicos. Inclui componentes como controlos de acesso, serviços contra incêndios e dispositivos para a detecção de infiltrações de água que ponha em perigo o funcionamento do S.I. "[37]

Neste âmbito terão que ser defendidos contra catástrofes, ataques terroristas, roubos ou degradação dos equipamentos, utilizando-se aqui sistemas de redundância de equipamentos e de informação. Redundância descreve a capacidade do sistema superar a falha de um

[36] Clapper, James R. (2013). Statement for the Record Worldwide Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence USA

[37] Carneiro, A. (2002). *Introdução à Segurança dos Sistemas de Informação.* FCA.

dispositivo ou serviço utilizado por um recurso redundante, isto é existe um dispositivo que está disponível para ser usado em caso de falha do sistema primário. Nestes casos são usados sistemas de *raid, hardware* redundante, etc., para redundância física e para replicação da informação, utilizam-se formas de ter uma cópia exacta da mesma para outros dispositivos que se podem encontrar geograficamente distantes, para que a informação se encontre disponível em caso do sistema primário falhar.

Neste capítulo também se devem ter em conta as falhas previsíveis, tais como as possíveis falhas de energia que podem levar à perda de informação e à degradação dos sistemas.

A segurança da informação é constituída por seis princípios básicos:

- Confidencialidade: Permitir o acesso à informação ou ao recurso só a quem tem que ter esse direito, ou seja, apenas utilizadores com os privilégios correctos podem ter acesso à informação. De forma a atingir esse objetivo são usados métodos de autenticação de utilizadores como ID's de utilizador, *passwords*, etc. que os identificam no sistema. A confidencialidade também é alcançada encriptando a informação, recorrendo à criptografia.
- Integridade: Garantir que os dados armazenados não sofram alterações quer por motivo de intrusões quer por questões físicas. A integridade tem como objectivo assegurar a confiança que existe na informação existente nos sistemas. Quando a informação é adulterada, a integridade é quebrada. Isto pode ser alcançado com a alteração dos conteúdos ou dos sistemas que os suportam. No caso de perda da integridade também a confidencialidade é posta em causa.
- Disponibilidade: Assegurar que a informação está disponível quando necessária. O sistema para armazenar essa informação e os sistemas de controlo da segurança têm que estar a funcionar correctamente e os sistemas de redundância têm um grau elevado de disponibilidade.
- Autenticidade: Ter a certeza que o utilizador é quem diz que é cada vez que as suas credenciais são apresentadas. É a propriedade de se poder verificar as credenciais apresentadas, de ter confiança na validade da transmissão de uma mensagem

- Não repúdio: "Não Repúdio é a capacidade de garantir que um usuário ou sistema realmente realizou uma operação em um sistema da informação, não permitindo a existência de dúvidas ou questionamentos sobre a sua realização"[38].
- Auditoria: As auditorias internas e externas como medida de detecção, permitem avaliar a eficácia das medidas implementadas e introduzir as correções necessárias. A realização das auditorias dos sistemas de informação têm que acompanhar a evolução das diversas técnologias envolvidas neste domínio. É necessária uma avaliação dos modelos de segurança utilizados de forma a verificar a sua consonância com as novas arquitecturas, plataformas e formas de comunicação, pois auditorias a sistemas obsoletos são irrelevantes.

A segurança da informação é o conjunto de medidas de controlo e de políticas que visam proteger a mesma, evitando o acesso quer esteja residente nos sistemas ou em transito em redes privadas ou públicas, pois pelo facto de esta transitar em redes publicas, não a torna pública.

A segurança é um processo aplicável aos sistemas bem como às organizações sendo necessário um esforço constante de melhoria dos mesmos de forma a prevenir novas ameaças.

Os sistemas informáticos em rede com ligação à Internet, utilizando *software* com um grau de segurança baixa, favorecendo a facilidade de utilização em detrimento da segurança, são um grande entrave à mesma segurança.

A *Internet* em si pela possibilidade de anonimato é um meio propício ao desenvolvimento de ataques difíceis de detectar, feitos a partir de sistemas previamente comprometidos, que servem de plataforma de lançamento para esses ataques.

Na medida em que não há sistemas invioláveis, é necessário uma aposta séria nas políticas e nos mecanismos de defesa que mitigam esses riscos[39]. Esta segurança tem custos elevados em equipamentos, *software*, consultoria, auditoria, que têm de ser ponderados face aos riscos envolvidos, principalmente em certos negócios em que a reputação da segurança é vital para o próprio negócio como é o caso da banca.

---

[38] Ress, W. (2011). *Começando em segurança*. Obtido de MSDN: http://msdn.microsoft.com/pt-br/library/ff716605.aspx#naorepudio

[39] (Rodrigues, 2010)

Os princípios básicos para a implementação da segurança são (Silva, 2003):

- Relação Custo/Benefício: que se traduz na necessidade de que esta relação seja favorável à proteção proporcionada pelo investimento
- Concentração: deve ser analisada a criticidade da informação e agrupada, aplicando medidas idênticas em função dos níveis definidos.
- Protecção em profundidade: com a utilização de medidas se segurança (física e lógica) como CCTV, biometria, sistemas de reconhecimento de voz, que proporcionem uma segurança efectiva e não um somatório de medidas complexas e ineficientes.
- Consistência: que determina que medidas de proteção dos sistemas com um grau de sensibilidade equivalente, seja homogenia seja ao nível físico seja lógico, não possibilitando, por exemplo, o acesso de pessoas não autorizas aos sistemas ou a possibilidade de instalação de *software* sem autorização prévia.
- Redundância: que define a existência de sistemas redundantes de forma a evitar que toda a protecção fique em causa por uma falha de um dos componentes desse mesmo sistema.

As principais falhas dos sistemas têm origem principalmente em quatro causas (Rodrigues, 2010):

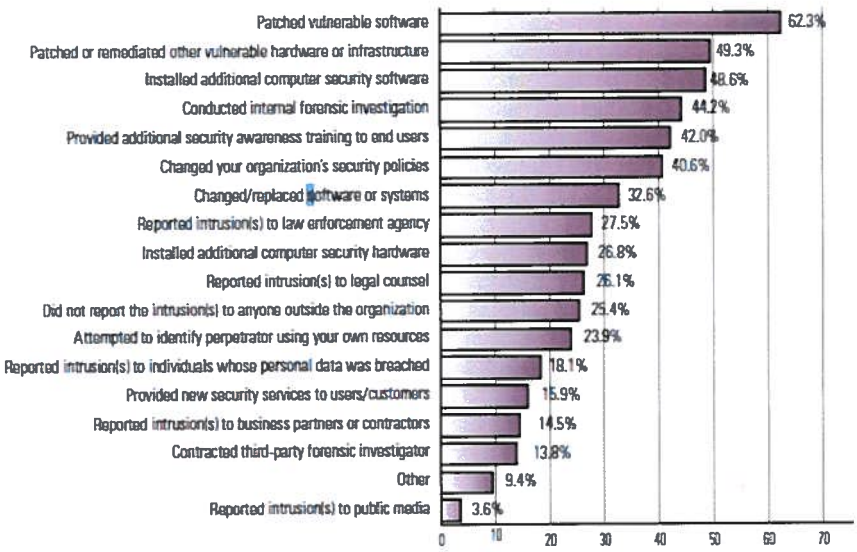
- Erros de programas – Erros em certos programas que podem provocar falhas de segurança, como é o caso dos "*browser*". Essas falhas apesar de parecerem insignificantes podem comprometer a segurança de uma rede.
- Vulnerabilidades – Que são falhas de aplicações que podem provocar, por sua vez, falhas de segurança no sistema, tais com falhas nos "*browsers*", que com a existência de ligação à *Internet* pode comprometer todo o sistemas ou mesmo a rede.
- Configurações incorretas: Implementações dos sistemas sem atender às regras de segurança que deviam ser implementadas, colocando todo o sistema em risco.
- Incumprimento de regras básicas: Alguma incúria por parte de quem gere os sistemas e que leva a que as regras básicas de segurança não sejam cumpridas tal como a manutenção de antivírus actualizados, acesso de utilizadores não autorizados, complexidade de *passwords* demasiado simples, etc.

Type of Attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots / zombies within the organization	added in 2007		21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%	39%
Password sniffing	added in 2007		10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site	option altered in 2009				6%	7%
Exploit of wireless network	15%	14%	17%	14%	8%	7%
Exploit of DNS server	added in 2007		6%	8%	7%	2%
Exploit of client Web browser	option added in 2009				11%	10%
Exploit of user's social network profile	option added in 2009				7%	5%
Instant messaging abuse	added in 2007		25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%	12%
System penetration by outsider	option altered in 2009				14%	11%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%	5%
2010 CSI Computer Crime and Security Survey						2010: 149 Respondents

Fonte : Institute, C. S. (2011). *2010 / 2011 CSI Computer Crime and Security Survey.* CSI.

Figura 3. 1 – Ataques efetuados (2005-2010)

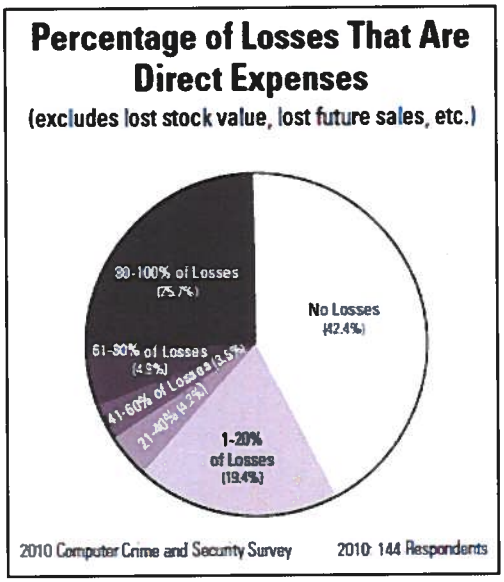
Se verificarmos o relatório (Institute, 2011) poderemos observar a evolução dos ataques efetuados ao longo de cinco anos. A diminuição dos ataques é evidente e pode considerar-se duas razões para essa diminuição. Em primeiro lugar, *software* implementado mais robusto, com menos vulnerabilidades e, em segundo lugar, a utilização mais sistematizada por parte das empresas de softwares de protecção, nas suas redes (Figura 2.1).



Fonte : Institute, C. S. (2011). *2010 / 2011 CSI Computer Crime and Security Survey.* CSI

Figura 3. 2 – Acções correctivas

Assim, com base no mesmo relatório podemos verificar as acções correctivas tomadas após os incidentes. Podemos observar que a aplicação de correcções se situa na ordem dos 63% quando nos anos anteriores se tinha situado nos 50%. Isto demonstra bem a preocupação crescente que sentem, neste âmbito, os responsáveis pela gestão dos sistemas. (Institute, 2011)(Figura 2.2).



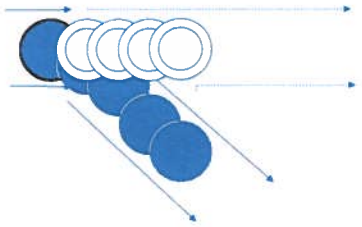
Fonte : Institute, C. S. (2011). *2010 / 2011 CSI Computer Crime and Security Survey.* CSI

Figura 3. 3- Custos dos ataques

Da análise às respostas das empresas questionadas no relatório (Institute, 2011), podemos observar que 25.7% das empresas apresenta percas directas provocadas por ataques. Estas percas representam custos de investigação e correcção das vulnerabilidades. (Figura 2.3) Os custos indiretos, como a perda de clientes ou roubo de dados de cartões de crédito representam 42%.

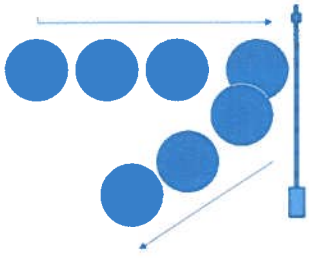
3.1 Ameaças

Para se entender melhor as ameaças elas podem ser divididas em quatro, cada uma explorando diferentes tipos de vulnerabilidades. (Pfleeger, 2006)



Fonte: Pfleeger, C. P. (2006). *Security in Computing.* Prentice Hall.
Figura 3. 4 – Interceção

Intercepção: Ocorre quando uma terceira parte ganha acesso ao recurso, podendo ser efectuado por uma pessoa ou um programa. (Pfleeger, 2006)



Fonte: Pfleeger, C. P. (2006). *Security in Computing.* Prentice Hall.
Figura 3. 5 – Interrupção

Interrupção: Perda de acesso a um recurso por perda ou destruição quer de ficheiros quer de *hardware.* (Pfleeger, 2006)

Fonte: Pfleeger, C. P. (2006). *Security in Computing.* Prentice Hall.
Figura 3. 6 - Modificação

Modificação: Uma parte não autorizada ganha acesso a um recurso e modifica-o. Essa alteração constitui uma ameaça à integridade da informação, podendo acontecer por subtracção de informação ou por adição, (Pfleeger, 2006)

Fonte: Adaptado Pfleeger, C. P. (2006). *Security in Computing.* Prentice Hall.
Figura 3. 7 – Fabricação

Fabricação: Acontece quando dados adulterados são introduzidos na rede por uma fonte não autorizada. (Pfleeger, 2006)

As melhores práticas da implementação, manutenção e gestão da informação estão definidas na ISO/IEC 27002 (Standardization, 2013).

Pretende-se com este padrão a implementação de Sistemas de Gestão de Segurança da Informação (SGSI), estabelecer uma política de segurança, de controlo adequado e gestão de risco. Serve como apoio às organizações para possibilitar uma melhor gestão dos sistemas de informação. Alguns dos princípios para uma boa implementação de um SGSI são: a consciência da necessidade de segurança da informação, atribuição da responsabilidade por

essa segurança, avaliação dos riscos que determinam o controlo adequado para se alcançar os níveis aceitáveis de risco, prevenção activa, auditoria contínua da segurança (Cruz, 2012).

3.2 Tipo de ataques

Os ataques também podem ser divididos em duas categorias (Estrela, 1998):

- Passivos: que se encaixam na área da monitorização. Os autores têm como objectivo a obtenção de informação, capturando-a em trânsito
- Activos: quando existe uma alteração do circuito de dados ou a criação de dados falsos

Para que os ataques aconteçam tem que existir:

- Método: são necessários conhecimentos, ferramentas para ser possível efetuar um ataque.
- Oportunidade: é necessário que haja uma janela de oportunidade para ser possível.
- Motivação: tem que haver uma razão para que seja efetuado o ataque. A motivação é variada, ou por serem atractivas, por serem governamentais, por vingança ou por simplesmente serem fáceis.

23.1

As ameaças podem ser classificadas com base no sistema usado nos USA (Army, 2003):

- Primeiro nível – amadores individuais ou em pequenos grupos, com ferramentas simples e sem grande estrutura de apoio.
- Segundo nível - indivíduos ou pequenos grupo com apoio de empresas, criminosos ou terroristas, utilizando ferramentas comuns mas já de uma forma sofisticada. A este nível são desenvolvidas atividades de espionagem e roubo de informação.
- Terceiro nível - indivíduos ou pequenos grupos com apoio de instituições governamentais com recurso a ferramentas sofisticadas também com objectivos de espionagem e roubo de informação.

- Quarto nível - Operações de Informação definidas por Estados, através de *"Computer Network Attacks (*CNA*)"*, usando as ferramentas realizadas em coordenação com operações militares.

3.3 Fontes de ataques

Os ataques podem ser divididos em algumas categorias, no entanto englobar os ataques nestas categorias pode ser difícil pois, muitas vezes, é difícil de distinguir a sua origem (Army, 2003):

- *Hackers* – Utilizadores não autorizados que tentam ganhar acesso a sistemas ou tentam impedir que utilizadores legítimos o consigam.
- Internos – Utilizadores com acesso legítimo aos sistemas. Estes constituem uma das maiores ameaças. Podem ser auto motivado ou recrutados.
- Activistas não-governamentais – Indivíduos que podem ir de associações criminosas a activistas sociais, utilizando muitas vezes os "media" para influenciar a opinião pública.
- Terroristas – Desenvolvem técnicas que vão do ganhar acessos não autorizados aos ataques físicos, passando informação para outros países.
- Serviços de Informação estrangeiros – Acções desenvolvidas com apoio de serviços de informação de países estrangeiros com o objectivo de roubo informação comercial e científica.
- Informação fratricida – Constituem acções de contrainformação.

3.4 Métodos de ataque

Os métodos de ataque concretizam-se por meio de acções desenvolvidas com o objectivo de explorar as vulnerabilidades dos sistemas (Foundation, 2007)

São analisadas seguidamente as tipologias dos métodos com base no MF 3-13 (Army, 2003)

- Acesso não autorizado – Forçar o acesso não autorizado com objetivo de obter informação, apagá-la ou modificá-la. Pode ser efetuado do exterior pela Internet ultrapassando *firewalls* ou, ser internamente por indivíduos que ganham acesso físico a terminais.
- *Software* malicioso – Com o nome genérico de "*Malware*" tem por objectivo infiltrar-se, fazendo com que o sistema se comporte conforme as intenções dos atacantes. Aqui podemos subdividir em diversas categorias:

    - Vírus – Pedaço de código, enviado normalmente anexado, desenvolvido com a capacidade de se multiplicar, passando de sistema em sistema, espalhando-se como uma infecção. Tem capacidades de atacar sistemas, destruir ou modificar ficheiros dependendo, no entanto, de alguma intervenção humana como por exemplo o abrir de um *email* infectado.
        - O "Anexo A" mostra uma lista dos vírus mais perigosos dos últimos 10 anos
    - *Wormes* – São da classe dos vírus mas com a capacidade de se espalharem sem intervenção, utilizando os recursos de transporte dos sistemas. Depois de infectar o sistema multiplica-se consumindo recursos de memória e de largura de banda, provocando o bloqueio do mesmo
        - O "Anexo A" mostra uma lista dos 10 *worms* mais perigosos
    - *Trojans* – Programas embebidos em outros programas como jogos ou aplicações com o objectivo de comprometer a segurança do sistema. Normalmente abrem uma porta *TCP* de forma a permitir a violação do sistema
    - *Spyware* – Programas que monitorizam a actividade dos sistemas comprometidos enviando essa informação. São muito utilizados como forma de publicidade e de spam.
    - *Rougeware* – São falsos antivírus. Dão a falsa informação da presença de vírus levando os utilizadores a comprar uma suposta versão que irá limpar o sistema.
- Manipulação electrónica- É a emissão de energia eletromagnética com objectivo de manipular, simular procedimentos que enganem o adversário.

- Ataque electrónico – trata-se do uso de energia eletromagnética para degradar, destruir a capacidade de combate do inimigo

- Destruição física – É a destruição física, quer por meios físicos como eletrónicos do alvo
- Gestão de percepção – Tém por objectivo influenciar grupos específicos (guerra psicológica)

3.5 Classificação de Vírus

A guerra entre os criadores dos vírus e os criados dos antivírus é grande desde o surgimento dos primeiros vírus. Apesar de uma classificação dos mesmos não ser consensual irá ser apresentada uma, segundo duas vertentes: o tipo de "*alvo*" dos vírus, e o método de infecção usado (Starllings, 2006).

- Com base no "*alvo*":
  - Infecção do "boot sector" – Infecta o "boot sector" do disco e espalha-se quando o sistema arranca
  - Infecção de ficheiros – Infecta os ficheiros de sistema
  - Vírus de macros – Infecta ficheiros com macros

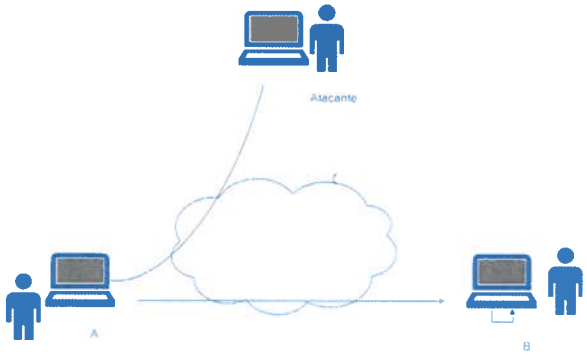
- Com base no método:
  - Encriptado – Uma possibilidade é quando uma porção do vírus cria uma chave aleatória encriptada que encripta o resto do vírus que é guardada no próprio vírus. Quando um programa infectado é invocado, o vírus usa a chave aleatória para desencriptar o vírus. Quando este é replicado uma nova chave é gerada.
  - *Stealth* – Vírus desenhado especialmente para se esconder dos sistemas de detecção
  - Polimórfico – Possui capacidades de mutação alterando-se a cada infecção tornando a deteção "por assinatura" impossível
  - Metamórfico – Para além de capacidade de mutação, consegue reescrever-se completamente a cada infecção, mudando quer o aspeto quer o comportamento

3.6 Ataques à segurança

Os ataques aos sistemas podem ser classificados quando à forma como são perpetrados como em passivos ou activos. Os passivos tendem a recolher informação sem alterar os sistemas. Já os ataques activos provocam danos nos recursos dos sistemas. (Starllings, 2006)

3.6.1 Ataques passivos

Os ataques passivos são do tipo "escuta" ou monitorização. O objetivo do atacante é ter acesso à informação. Podemos distinguir dois tipos: captura de mensagens e análise de tráfego. O primeiro tem como objetivo ler os conteúdos das mensagens em trânsito. O segundo é um ataque mais súbtil na medida em que é feita uma análise do tráfego. Mesmo que as mensagens sejam encriptadas é sempre possível detectar a origem, o destino, o tamanho e a frequência das mesmas podendo, assim, tentar advinha o conteúdo das mesmas (Starllings, 2006).

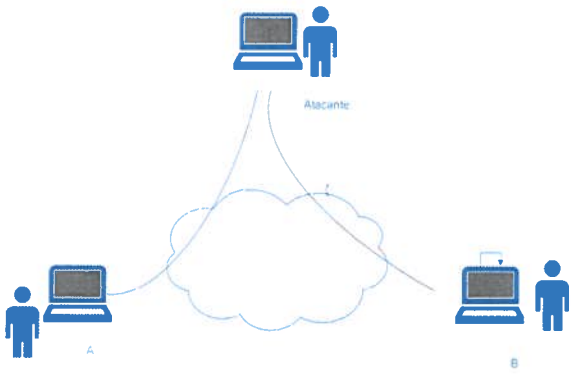


Fonte: Adaptado (Starllings, 2006).
Figura 3. 8– Ataque passivo

3.6.2 Ataques activos

Os *"man-in-the-middle"* é desta categoria de ataques. Quando um destes ataques acontece, o executor do ataque introduz o seu computador entre as comunicações dos outros dois sistemas vítimas do ataque, permitindo assim o

"*sniffing*". O computador atacante vai encaminhar os pacotes entre os computadores das vítimas para que as comunicações não sejam interrompidas (Starllings, 2006).

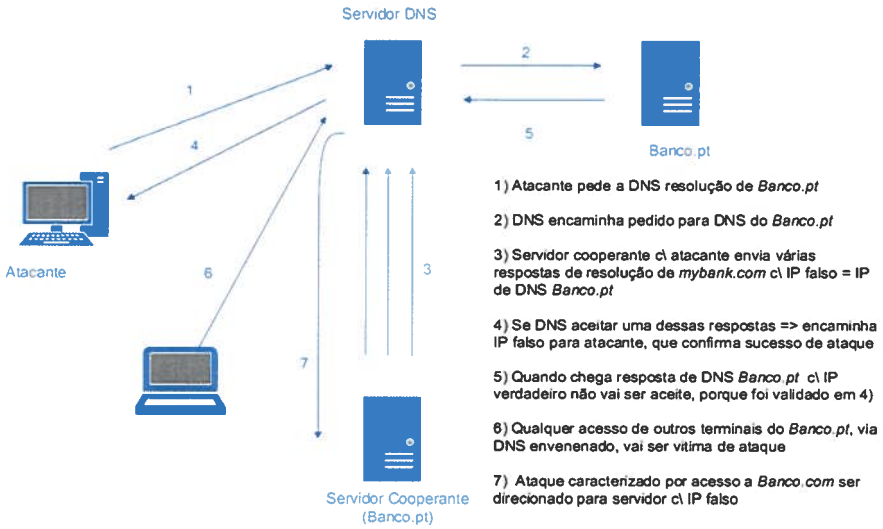


Fonte: Adaptado Starllings, W. (2006). *Cryptography and Network Security.* Prentice Hall.

Figura 3. 9 - Ataque do homem no meio

3.6.2.1 Resolução errada de nomes (DNS *Spoofing)*

É um ataque do tipo "*man-in-the-middle*", em que as vítimas são forçadas a navegar para um falso *website* sem que tenham noção disso. *DNS spoofing* é baseado na apresentação de uma falsa informação em resposta a um pedido de *DNS* e com o objectivo de forçar a uma visita a um *site* que não é real



Fonte: Adaptado, Niranjan. (2007). *DNS Amplification Attack.* Obtido de Security Tools News & Tips: http://securitytnt.com/dns-amplification-attack/

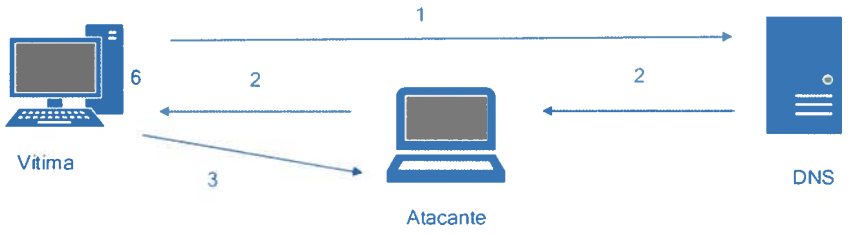
Figura 3. 10 - Acesso por imitação (Spoofing)

3.6.2.2 Alteração da tabela de endereços MAC/IP *(ARP Spoofing)*

É outro ataque do tipo "*man-in-the-middle*". O "ARP *spoofing* é um método de exploração da interacção dos protocolos TCP/IP.

O MAC (endereço físico da placa de rede) sendo teoricamente um endereço único guardado na placa de rede, é necessário para que os pacotes possam ser enviados e recebidos, mas tem que haver uma forma do protocolo, descobrir o endereço MAC da máquina destino e, é ai, que é usado o ARP *(Address Resolution Protocol)*. Como os pedidos de MAC feitos pelo ARP são do tipo "*broadcast*" feitos para a rede, a forma de minimizar esse efeito é através de uma tabela que guarde a informação da relação IP/MAC

Muitos sistemas fazem a actualização das tabelas quando um "*replay*" é recebido mesmo que não o tenha pedido, enviando assim falsas respostas de ARP ficando o sistema de destino convencido a enviar as respostas para o destino pretendido pelo atacante, em vez do correcto, sem que a vítima tenha conhecimento (Zuquete, 2008).



Fonte: Sahlan, A. W. (2008). *Proses Spoofing.* Retrieved from http://hadianto.blog.ugm.ac.id/2008/10/20/proses-spoofing/

Figura 3. 11 - Alteração da tabela de ARP

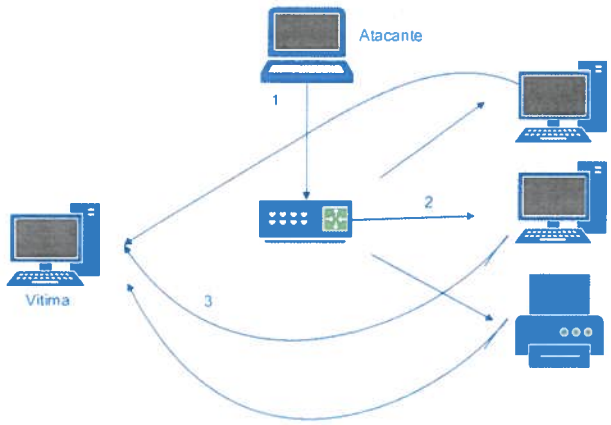
1. Terminal envia pedido ARP para obter endereço MAC de servidor DNS
2. Atacante intercepta pedido e responde (ARP *response*) com o *IP* falso
3. A partir daí, todos os pedidos ARP do terminal para o DNS serão redireccionados para o terminal do atacante, que poderá redireccionar os nomes a resolver para endereços *IP* falsos

3.6.2.3 Negação de Serviço Distribuído (DDoS)

Este tipo de ataque que se encontra em expansão é uma grande preocupação para as empresas. Os ataques por DDoS tornam os sistemas inacessíveis inundando, redes e computadores com trafego desnecessário impossibilitando os utilizadores legítimos de acederem a esses recursos. Os ataques típicos consistem em bombardear os sistemas com pacotes levando a que o sistema fique sem capacidade de resposta tornando-o inacessível.

Reflexão *(Smurf)* – "Quando a ferramenta de *ping* é executada, um pacote de solicitação de eco do ICMP é enviado ao computador de destino. Se o computador de destino receber o pacote do TCP, ele responderá para confirmar a solicitação de *ping*. No caso de um ataque de negação de serviços *Smurf*, o endereço IP de retorno do pacote do *ping* é forjado com o *IP* do computador de destino. O *ping* é emitido ao endereço *IP* de *broadcast*. Esta técnica faz com que cada computador responda aos falsos pacotes de *ping* e envie uma resposta ao computador de destino, inundando-o. Esta técnica é chamada de ataque *Smurf* porque a ferramenta de DoS que é usada para executar o ataque tem este nome. Uma maneira de reduzir o risco deste ataque é a desactivação do *broadcast* dirigido ao IP, que, normalmente, não é usado ou necessário. Alguns sistemas operacionais são configurados para impedir que o computador responda aos pacotes de ICMP"[40].

[40]Corporation, S. (2013). Obtido de Smurf DoS attack (ataque de DoS Smurf): http://www.symantec.com/pt/pt/security_response/glossary/define.jsp?letter=s&word=smurf-dos-attack



Fonte: Zúquete, André, (2008), Segurança em redes informáticas, FCA

Figura 3. 12 - Reflexão

1. O atacante envia uma mensagem mal formada para o endereço de *broadcaste* da rede, contendo como endereço fonte o endereço IP da vítima
2. O *router* faz o trabalho de difundir a mensagem para todos os equipamentos ligados à rede
3. Todos respondem à vítima, inundando-a

FRAGGLE – "O ataque *Fraggle* é parecido ao *Smurf,* mas usa datagramas UDP. O atacante envia um pacote para o endereço difusão da rede, que é redireccionado pelo *router* ou *switch* para todos os computadores. Caso os equipamentos terminais tenham o serviço a correr, respondem para a vítima; caso contrário, mandam um ICMP *Port Unreachable* também para a vítima"[41]

SYN-FLOOD – É mais um ataque de DoS que consiste em enviar um elevado número de pacotes SYN para o equipamento da vítima, sem nunca abrir efetivamente uma conexão. Como esses pacotes são de dimensão reduzida estes ataques podem ser efectuados a partir de qualquer dispositivo. O ataque é efectuado utilizando particularidades da conexão TCP, o "*three-way handshake*". O emissor envia um pacote SYN, o destinatário responde com SYN/ACK e o emissor

[41] Inácio, P. R. (2010). *Engenharia Informatica Tecnologia e Sistemas de Informação*

confirma enviando um pacote ACK ficando então a conexão aberta. Depois de aberta a conexão, o servidor fica à espera de receber um pacote até que o tempo limite se esgote. Como o número de conexões TCP activas em simultâneo no servidor é limitado faz com que este fique impossibilitado de responder a novos pedidos.

Os sistemas *Linux* possuem formas de evitar este tipo de ataques que são os SYN *Cookies*. Assim, o sistema passa a responder ao SYN inicial com um *cookie* que vai identificar a origem e, alocando espaço para a conexão só depois de receber o pacote. Apesar de não evitar totalmente o ataque, torna-o pouco eficaz (Rodrigues, 2010).

Nos sistemas *Windows* 2000 a protecção era efectuada por meio de chaves do registo. Nas das versões *Windows* V*ista/ Windows* 2008 e superiores, o algoritmo de proteção foi reconfigurado, está activo e não pode ser desactivado. O sistema, com base no número de processadores e da memória que possui, calcula os limites a partir dos quais considera um ataque. Ultrapassado esse limite, o sistema começa a descartar novas conexões evitando assim, ficar sem recursos (Murat, 2010).

E-mail Bomba *(Mail Bomb*)- Técnica que consiste em inundar um computador com *emails*. Normalmente é usado um script de forma a gerar um fluxo contínuo de mensagens e, encher a caixa de correio da vítima. Este procedimento tende a provocar negação de serviço do servidor de correio eletrónico (Rodrigues, 2010).

Ping de Morte (Ping-of-Death)– O seu nome tem origem no facto de os primeiros ataques terem sido efetuados com o comando "*Ping*". Neste caso, enviando um pacote IP com um tamanho superior ao permitido (65535 bytes) para o equipamento da vítima. Este envio é efetuado em fragmentos devidos às limitações das redes ao trafego de pacotes com este tamanho. Quando o equipamento vítima do ataque tenta montar os fragmentos estes têm diversos comportamentos, bloquear,

reiniciar ou abortar enviando mensagens para a consola (Rodrigues, 2010).

Profusão de Tampão *(Buffer Overflow)* – Acontece quando o atacante consegue dominar um programa da vítima com privilégios elevados na máquina da mesma, tentando armazenar em memória mais dados do que ela suporta causando, assim erros (Rodrigues, 2010).

Injecção de SQL *(SQL Injection)* – É uma manipulação de uma instrução SQL através das variáveis que compõem os parametros recebidos por um script, seja PHP, ASP, etc. São passados paramentos a mais pela barra de navegação do *browser*, inserindo instruções não esperadas pela base de dados. Este ataque tem o objectivo de roubar dados ou danificar a própria base de dados provocando DoS. (Rodrigues, 2010).

3.6.2.4 Ataque Força Bruta

Ataques de força bruta usam métodos de tentativa e erro para adivinhar, palavras--passe, utilizadores, números de cartões de crédito ou chaves criptográficas (Brute force attacks, s.d.).

Ataques de dicionário – São usadas ferramentas automáticas para tentar adivinhar palavras-chave de um ficheiro de dicionário. Este ficheiro pode conter palavras que foram recolhidas pelo atacante para entender o utilizador da conta a ser atacada ou construir uma lista de palavras únicas disponíveis num *website.*

Ataques de procura – Cobrem todas as combinações de caracteres e tamanhos de palavras-chave. Este ataque pode demorar muito tempo devido à quantidade de combinações possíveis

Ataques baseados em regras – Usam regras para gerar possíveis variações de palavras-chave de parte do nome do utilizador ou utilizando "mascaras" para configurar palavras.

2.6.2.5 *Phishing*

É a técnica pela qual o atacante usa uma de lista correio eletrónico fraudulento em massa, e solicita informações de diversa natureza, em especial financeira. Estes *emails* contem links para páginas com formulários onde é requerida a informação confidencial ou redireccionam para páginas que contêm programas maliciosos que se auto instalam nos computadores. Este ataque é uma ameaça muito grande, quer para particulares, quer para empresa.

3.7 Sistemas de proteção

3.7.1 *Firewals*

Uma *firewall* é um dispositivo que filtra o trafego entre a rede interna e o meio desprotegido das redes exteriores. Normalmente está implementado num sistema dedicado pois a "*performance*" é importante. Como *software* que é não deve estar susceptível de ser comprometido por outro qualquer por isso, deve correr com um sistema operativo mínimo. Este dispositivo deve estar bem colocado na rede de forma a garantir que todo o tráfego passa por ela. Os principais componentes são:

Filtros – Controlam os pacotes IP que entram e saem da rede interna para o exterior

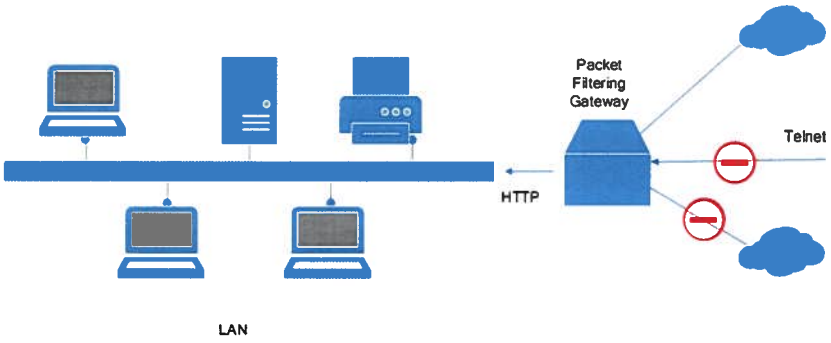
Gateway – composto por uma ou mais máquinas para controlo das interacções ao nível aplicacional de entrada e saída

DMZ *(DeMilitarrized Zone)* – Zona exposta ao exterior no entanto sem acesso à rede interna. São colocados aqui os servidores de *front-end,* como *web servers* ou os de *mail*, que posteriormente comunicam com a rede interna

3.7.2 Topologias

3.7.2.1 *Packet filtering*

Uma *packet filtering gateway* é, muitas vezes, uma simples mas eficiente, proteção. Estas *gateways* controlam o acesso dos pacotes com base "*address*" do pacote, ou seja, o endereço origem e destino ou o protocolo



Fonte: Pfleeger, C. P. (2006). *Security in Computing*. Prentice Hall.
Figura 3.13 Filtros de pacotes

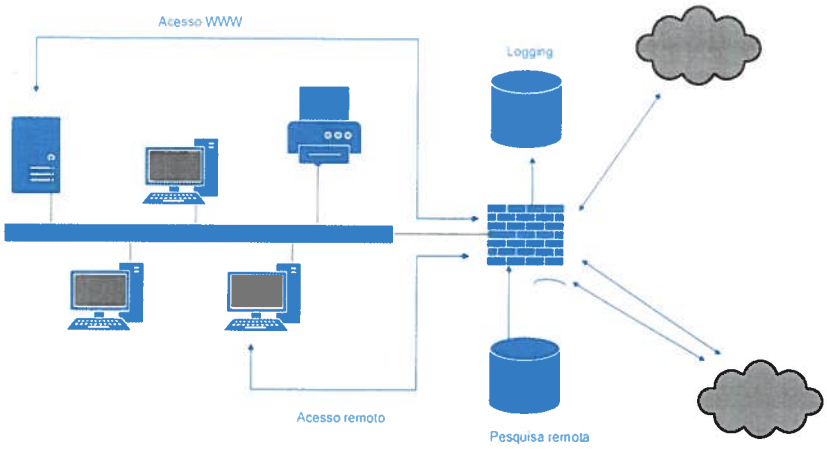
Este tipo de *firewall* não olha para dentro do pacote, não tem capacidade de análise dos seus conteúdos. Devido à sua simplicidade de implementação, como se baseia em permissão/negação de acesso, pode tornar o sistema pesado pois é implantada "caso a caso". Também não suporta sistemas de autenticação (Pfleeger, 2006).

3.7.2.2 *Stateful inspection*

Aqui o trabalho é realizado pacote a pacote, aceitando ou rejeitando cada um deles. O controlo é baseado na identificação do estado da ligação. Depois de estabelecida uma conexão legitima, a *firewall* mantém o registo da sua origem e destino bem como o seu estado. Se um pacote não fizer parte dessa ligação será descartado

3.7.2.3 *Application proxies*

A *firewall* intercepta todo o tráfego dos utilizadores, entrado ou saido da rede. O tráfego é examinado com base numa série de regras com o objectivo de verificar se os dados são "bons" ou "maus". Por exemplo, dados de um utilizador podem ser analisados para verificar se contêm comandos *SQL* que conduzam a um ataque. Quando esses ataques são detectados, pode tomar uma acção correctiva ou evasiva, tomando uma acção mais sofisticada como redireccionar a sessão para um "*honeypot*" em vez de, simplesmente, descart-la. (Lipson & van Wyk, 2005)



Fonte: Pfleeger, C. P. (2006). *Security in Computing.* Prentice Hall.
Figura 3. 14- Procurador aplicacional

Permite regras baseadas na autenticação, análise de conteúdos, nomes de DNS de destino, independentes por protocolo, controlo de largura de banda, QoS *(Quality of Service)* para redes, é um conjunto de normas e mecanismos para a indústria que visam garantir um desempenho de alta qualidade para aplicações críticas.

3.7.2.4 Guardas (*Guards)*

São *firewall* sofisticadas idênticas às das "*application proxies*" que recebem dados de um determinado protocolo, interpreta-os e passa-os usando os mesmos dados ou modificando-os para atingir os mesmos resultados. O *guard* decide que serviços executar em nome do utilizador, como por exemplo, com base no seu conhecimento de interações anteriores, se uma identificação de um utilizador externo é confiável (Pfleeger, 2006).

3.7.2.5 Paredes de Fogo Pessoais (*Personal firewalls)*

Tipicamente são aplicações instaladas em computadores pessoais, normalmente para bloquear tráfego vindo da rede. Pode funcionar como complemento a *firewall* da rede bloqueando um computador específico. Pode ser usada para aplicar configurações particulares como aceitar determinados *sites* como seguros (Pfleeger, 2006).

3.7.3 *Monotorização* –IDS

Como os ataques têm vindo a aumentar ao longo dos anos, os sistemas de detecção de intrusões são de extrema importância na garantia da segurança da informação (Larrieu, 2003).

Apesar das *firewall* providenciarem uma grande protecção não o conseguem fazer na totalidade. Os IDS têm a função de ajudar os computadores a preparar-se e responder a um ataque. São considerados como complementos das firewall de rede, estendendo as capacidades de gestão da segurança incluindo monitorização, auditoria de segurança, reconhecimento de ataques e resposta.

Os IDS recolhem informações de várias fontes em computadores e rede que depois é comparada com padrões pré-definidos de comportamentos anormais para reconhecimento de ataques. Estas técnicas criam uma base de dados do comportamento normal de um utilizador que permitem lançar alertas em caso de desvio a esse comportamento. Estes sistemas são usados para detectar comportamentos desviantes quer do lado de fora da rede quer internamente.

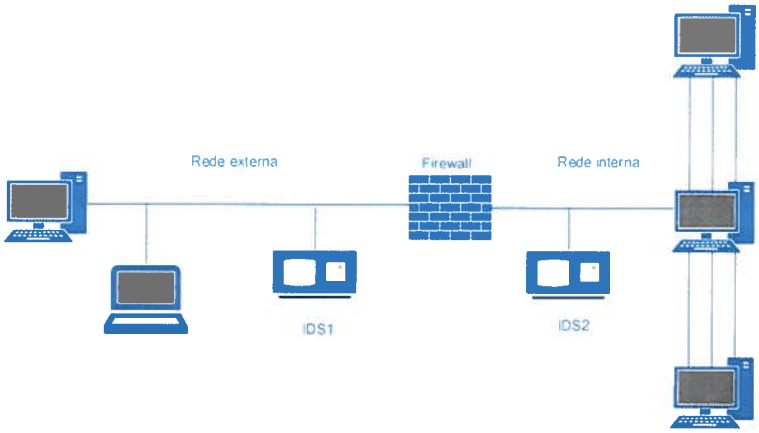
Acontece que a falta de intervenção humana pode levar a respostas imprevisíveis gerando falsos positivos.

Há dois tipos de sistemas de intrusão: **N-IDS** *(Network Based Intrusion Detection System)*, asseguram a segurança a nível da rede e **H-IDS** *(Host Based Intrusion Detection System)*,asseguram a segurança a nível da máquina.

Os N-IDS necessitam de equipamento dedicado. *Promiscuous-mode IDS* (modo que permite a interceção e leitura dos pacotes de rede que chegam) são "*sniffers*" com capacidade de analisar os pacotes que circulam nos vários segmentos da rede.

Os IDS se possuírem um conjunto de sensores em máquinas críticas são chamados de sistemas híbridos. Estes sistemas juntam as características dos sistemas de rede e os de *host*. Eles comparam "*event logs*", trafego de rede para detecção de ameaças, configurações de segurança e integridade de ficheiros.

É frequente encontrar IDS em vários segmentos da rede, em especial do lado de fora da rede, de forma a monitorizar o tráfego proveniente do exterior, estudando tentativas de ataque, mas também são encontrados do lado de dentro da rede..



Fonte: Larrieu, C. (2003). *Sistemas de detecção de intrusão (IDS)*. Retrieved from kioskea.net: http://pt.kioskea.net/contents/detection/ids.php3

Figura 3. 15- *IDS*

Os H-IDS comportam-se como um serviço na máquina que processa dados produzidos pela própria máquina. Usualmente analisa informações específicas dos "*logs*" mas também captura pacote que entram e saem da máquina com o objectivo de detectar tentativas de intrusão. Um dos cenários em que são usados é na detecção de abuso de privilégios. Isto acontece quando um utilizador faz uso dos seus privilégios para fins diferentes daqueles que lhe foram atribuídos (Larrieu, 2003).

Pode-se considerar que existem dois tipos de detecção usados pelos IDS: por detecção de assinatura e por detecção de anomalias. A detecção por anomalias parte do princípio que acções fora do normal podem ser ataques. Baseando-se numa métrica, cria um perfil para o utilizador e quando os dados saem fora desse padrão dispara o alarme. Este método tem o inconveniente de gerar muitos falsos alarmes devido ao comportamento imprevisível dos utilizadores. Os de detecção por assinatura, analisam as actividades dos sistemas e procuram eventos que correspondam a padrões pré-definidos de ataques, conhecidos como assinaturas. Este sistema tem a desvantagem de só detectar ataques conhecidos necessitando de constante manutenção para o manter actualizado (Santos, 2010).

3.7.3.1 Arquitectura

Os *IDS* são usualmente construídos por quatro componentes:

E-Boxes – Possuem sensores de captura de eventos. Funcionam quer ao nível da rede quer do próprio computador. Monitorizam os pacotes em trânsito, as sessões dos utilizadores, níveis de tráfego, alterações em ficheiros. Os resultados são enviados para as *A-Boxes,* para análise. No caso de ser considerado como intrusão, são igualmente enviados para as *D-Boxes*.

A-Boxes – Têm módulos de análise. São responsáveis pela análise dos dados dos eventos recebidos, pela sua correlação. Os dados produzidos podem alimentar-se a si próprias.

D-Boxes – Com módulos de armazenamento de eventos e de resultados das análises efetuadas pelas *A-Boxes*. Armazenam eventos classificados como intrusão, produzem relatórios, alarmes, podem, em alguns casos, reconfigurar sistemas de protecção ou o isolamento dos sistemas (Krulgel, Valeur, & Vigna, 2005).

3.7.4 Pote de Mel *(Honeypots)*

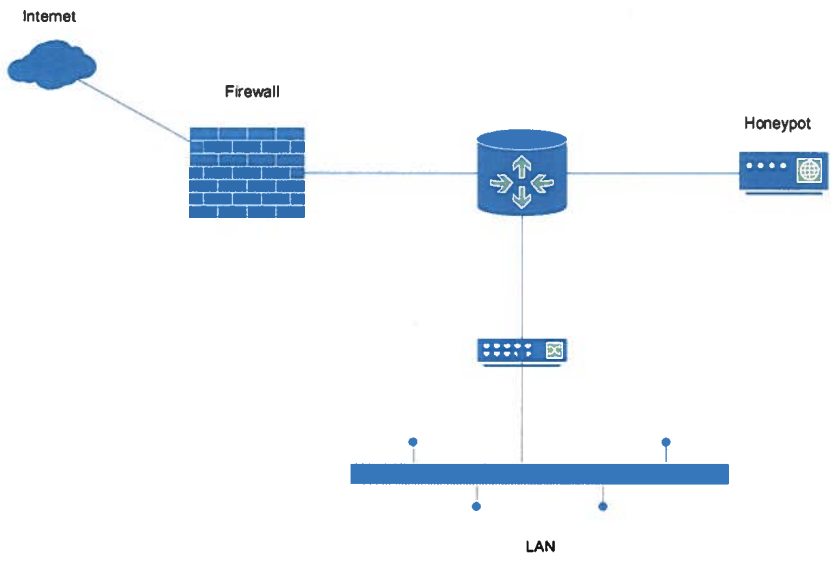
Ao contrário das *firewalls* ou dos *IDS*, os *honeypots* não resolvem um problema específico. Em vez disso, são ferramentas muito flexiveis que têm muitas formas e tamanhos. Eles fazem desde detecção de ataques encriptados até à detecção de uma fraude de um cartão de crédito. É esta flexibilidade que torna os *honeypots* muito poderoso (Hoepers, Steding-Jessen, & Chaves, 2007).

Uma definição pode ser a de um recurso cujo valor depende do uso ilícito que é feito dele.

Num *honeypot* de baixa interactividade são instaladas ferramentas para emular sistemas operativos e serviços com os quais os atacantes irão interagir. Desta forma, o sistema operativo real deste tipo de *honeypot* deve ser instalado e configurado de modo seguro, para minimizar o risco de ser comprometido.

Nos *honeypots* de alta interactividade os atacantes interagem com sistemas operativos, aplicações e serviços reais. Exemplos de *honeypots* de alta interactividade são as *honeynets* e as *honeynets* virtuais.

Uma *Honeynet* é uma ferramenta de pesquisa, que consiste numa rede desenhada especificamente para ser comprometida, e que contém sistemas de controle para prevenir que seja utilizada como base de ataques contra outras redes. É projectada para pesquisar e obter informações dos atacantes. É também conhecida como "*honeypot* de pesquisa". Uma vez comprometida, a *honeynet* é utilizada para observar o comportamento dos atacantes, o que possibilita análises detalhadas das ferramentas utilizadas, das suas motivações e das vulnerabilidades exploradas. Uma *honeynet* normalmente contém um segmento de rede com *honeypots* de diversos sistemas operacionais e que fornecem diversas aplicações e serviços. Também contém mecanismos de contenção robustos, com múltiplos níveis de controle, além de sistemas para captura e recolha de dados, bem como para disparar alertas. (Hoepers, Steding-Jessen, & Chaves, 2007)



Fonte: hdudhade, s. (n.d.). *HoneyBox v0.1 - Honeypots in a box!* Retrieved from Information Security : http://santoshdudhade.blogspot.pt/2012/09/honeybox-v01-honeypots-in-box.html

Figura 3. 16 – Pote de Mel

3.8 Encriptação

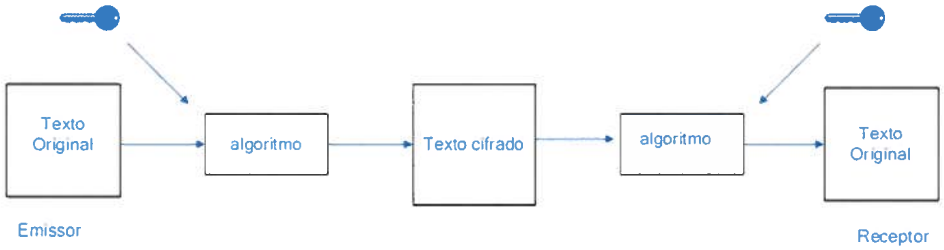
Há muito séculos que a comunicação segura é de vital importancia. Reis tinham necessidade de comunicar com os seus exércitos e para isso era necessário criar técnicas de mascarar as mensagens através de códigos e cifras.

Os primeiros dados relativos a cifras datam do sec.V a.C. Foram utilizadas na antiguidade técnicas diversas desde a utilização de tábuas onde era escrita a mensagem posteriormente coberta de cera de forma a esconde-la ou tiras de cabedal enroladas numa vara onde era escrita a mensagem e depois quando voltava a ser enrolada no destino numa vara igual, permitia descodificar a mensagem. Julio Cesar desenvolveu uma cifra de substituição que ficou conhecida pela "cifra de César" que consistia em avançar três letras no alfabeto e fazer a subtituição das letras da mensagem.

Durante a 2ª guerra mundial foram desenvolvias técnicas sofisticadas de esconder as mensagens como os micro-pontos e tintas invisiveis. Nesta época a "enigma" foi a máquina de cifra mais famosa.

Esta necessidade levou ao desenvolvimento de técnicas, com recurso a algoritmos matemáticos que permitissem a troca de mensagens de forma segura e, assim, nascia a criptografia. A criptografia tem como objectivo a troca de mensagens entre duas entidades sem que terceiros, mesmo tendo acesso à mesma, a consigam descodificar.

Com o desenvolvimento da criptografia surgio a criptoanalise que é a ciência que se dedica a decifrar mensagens sem conhecer a sua chave. A chave é que permite descodificar a cifra (Fincatti C. A., 2010).



Fonte: Fincatti, C. A. (2010). CRIPTOGRAFIA COMO AGENTE MOTIVADOR NA APRENDIZAGEM DA MATEMÁTICA EM SALA DE AULA. São Paulo: UNIVERSIDADE PRESBITERIANA MACKENZIE

Figura 3. 137 – Encriptação

O princípio de *Kerckhoff* afirma que a segurança do "cripto sistema" não deve depender da manutenção do algoritmo em segredo mas sim de manter a chave em segredo (Tanenbaun, 2003).

As cifras de substituição que durante muito tempo foram consideradas indecifráveis, são rapidamente quebradas com uma análise frequencista. Nesta análise, é verificado a frequência com que certos caracteres são utilizados e, em função de cada língua, é possível facilmente descobrir a mensagem (Tanenbaun, 2003).

3.8.1 Cifras

As cifras de substituição podem ser de dois tipos:

Cifras monoalfabéticas, em que um dado caracter é alterado por outro fixo, indicado pelo alfabeto de substituição, em que o caracter de substituição é o que varia

Cifras polialfabéticas, funcionam aplicando sucessivamente, de uma forma cíclica, várias cifras monoalfabéticas. Um exemplo desta cifra é a de *Vigenere*.

As cifras modernas podem ser caracterizadas quanto à operação e segundo o tipo de chave.

Quanto ao modo de operação podem ser divididas em cifras por blocos, que são cifras monoalfabéticas onde, cada caracter original e criptografado é constituído por conjuntos de *bits* vistos sempre como blocos de tamanho constante. As cifras contínuas são polialfabéticas , sendo somado o módulo 2 ao texto original. Aqui cada caracter é traduzido num outro, dependendo do alfabeto a ser usado no momento.

Em relação ao tipo de chave podem ser simétricas ou assimétricas.

3.8.1.1 Cifras simétricas

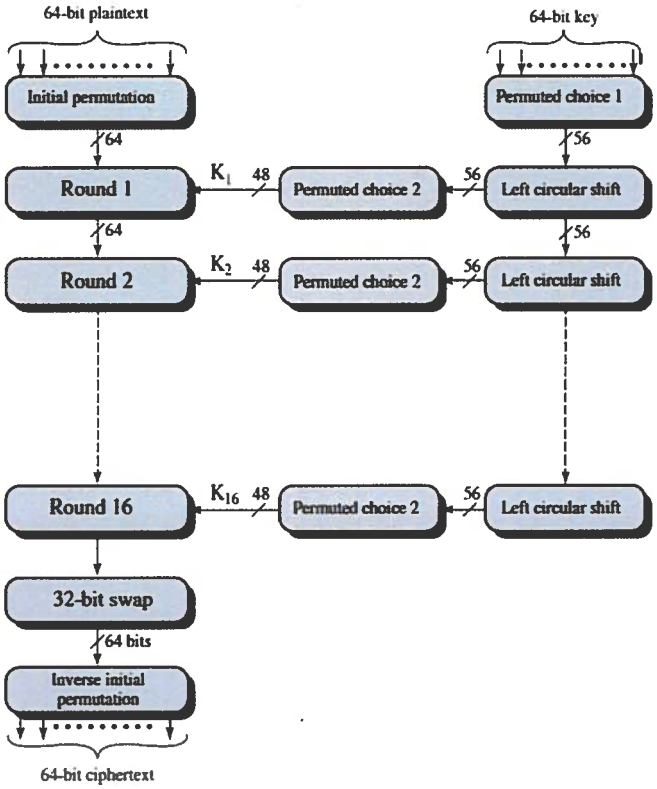
As cifras simétricas utilizam um valor único (chave) para cifrar e decifrar. Assim, a confidencialidade dos dados está garantida pois só quem possuir a chave terá acesso aos mesmos. É mais rápida que a assimétrica no entanto, tem o inconveniente

de o emissor e o receptor terem que partilhar a chave por meio de um canal fiável e da multiplicação de chaves, uma vez que emissor/receptor têm uma chave diferente.

Na década de 60, os computadores começaram a ser cada vez mais poderosos e, a sua utilização, cada vez maior por parte das grandes empresas, para transferência de valores e trocas comerciais, Surgiu então um problema que não existia enquanto o computador esteve restrito ao uso militar. Não havia uma uniformização, um padrão no sistema de cifragem, pois uma empresa podia utilizar um tipo de cifra e outra um diferente, impedindo a troca de mensagens. Em 1974 em resposta a um concurso do *NIST (National Institute of Standards and Technology)* para uma cifra simétrica por blocos para ambientes comercias, a IBM lança o *Lucifer* com uma chave de 128 bits. O *Lucifer* era muito poderoso, oferecendo uma capacidade de cifragem maior que a NSA possuia para o descodificar. Assim, foi encurtado o número de chaves para aproximadamente 100.000.000.000.000.000 (56 bits) e foi lançado oficialmente em 1976 com o nome de DES. Utilizava unidades elementares de permutação, substituição, expansão e compressão de blocos de bits. Basicamente, o DES funcionava através dos seguintes passos:

1. Uma substituição fixa, chamada de permutação inicial, de 64 *bits* em 64 *bits*;
2. Uma transformação, que dependia de uma chave de 48 bits, e que preservava a metade direita
3. Uma troca das duas metades de 32 *bits*
4. Repetição dos passos 2 e 3 durante 16 vezes;
5. Inversão da permutação inicial.

Os blocos que compunham o algoritmo eram permutações, substituições e operações de "ou exclusivo"



Fonte: Starllings, W. (2006). *Cryptography and Network Security.* Prentice Hall.

Figura 3. 18 – *DES*

Apesar do DES ser muito potente, o problema da troca de chaves mantinha-se. Para as empresas a necessidade de confiar numa terceira entidade para a distribuição de chaves, era um problema.

O DES acabou por ser quebrado em 1997 com recurso a técnicas de "*brut force attack*".

Em 1992, com o objectivo de tornar as tentativas de decifragem do algoritmo mais demoradas, passou-se a utilizar a tripla encriptação e foi lançado o 3DES.

Em 1997 foi lançado novo concurso para um algoritmo de 128 bits mais rápido que o DES. Surge então em 2001 *o* AES *: (Advanced Encryption Standard*).

O AES foi projetado para usar somente operações de *bytes* completos. Fornece vários tamanhos de chaves que podem ser de 128, 192 ou 245 *bits.* Com um número variável de "voltas" para além do extra no término da cifragem como passo omitido. O número de voltas são:

9, se o bloco e a chave forem de 128 *bits*

11, se o bloco ou a chave forem de 192 *bits*

13, se o bloco ou a chave forem de 256 *bits*

2.8.1.2 Cifras assimétricas

As cifras assimétricas ou de chaves públicas surgiram em 1977 e o primeiro algoritmo foi o RSA[42], tendo depois surgido outros como *ElGamal, Rabin* e ECC.

A criptografia assimétrica trabalha com duas chaves, uma pública e uma privada

Num cenário assimétrico o utilizador A cria o seu próprio par de chaves sendo uma pública e outra privada. O utilizador A mantém secreta a chave privada divulgando a chave pública. O utilizador B usa a chave pública do utilizador A para enviar uma mensagem que, só com a chave privada do utilizador A é possível decifrar. Este método tem a grande vantagem de não obrigar à de troca de chaves.

As cifras assimétricas usam problemas matemáticos complexos em que a segurança do algoritmo vem da utilização de grandes números. São usados, fundamentalmente três tipos de problemas: factorização, cálculo de logaritmos discretos (usam aritmética modular) e *Knapsacks* (ou problema da mochila, dado um conjunto de itens com o seu valor, é necessário determinar o numero de itens a incluir na mochila de modo a que o custo total seja inferior a um dado limite mas o maior possível). Estes problemas complexos servem para garantir que é impossível efectuar a função inversa.

O RSA utiliza números primos. Dois números primos são multiplicados para se obter um terceiro valor. A chave privada são os números multiplicados e a chave pública é o valor obtido. Num cenário o utilizador A escolhe dois números primos p e q e multiplica-os. O N é a chave pública do utilizador A e o p e q, a chave privada. Quando o utilizador B quer enviar uma mensagem para o A, usa a chave pública de A (o N). Quem conhecer a chave pública pode tentar adivinhar o valor de p e q já que o

[42] Iniciais de Rivest, Shamir e Adleman

N foi calculado a partir deles, mas se esses valores forem suficientemente grandes é impossível em tempo útil (Fincatti C. A., 2010).

3.8.2 Função *Hash*

A partir de uma mensagem original, a função tem como objectivo criar um número (conhecido como resumo) que represente de forma única esta mensagem (criar uma "impressão digital" de um ficheiro, uma mensagem ou blocos de dados) e que seja impossível de forma computacional obter a mensagem original, garantido assim, a integridade da mesma. No caso de algum caracter do conteúdo ser alterado, os algoritmos provocam uma modificação do resumo. 46-1

Dos principais algoritmos, destacam-se o MD-5 *(Message Digest* 5) de 128 *bits* e o SHA-2 *(Secure Hash Algorithm)* com um resumo de 256, 384 ou 512 *bits.*

3.8.3 Assinatura Digital

Uma assinatura digital liga um documento a uma pessoa ou entidade por meio de um código digital, garantindo a autenticidade do documento. A autenticação de documentos garante que a entidade é quem diz ser.

Podem ser utilizados vários métodos para garantir a confidencialidade de documentos, como senhas, cartões magnéticos ou sistemas biométricos. São utilizados cifras assimétricas de par de chaves pública e privada (Tanenbaun, 2003).

3.8.4 Certificado Digital

Os certificados são documentos assinados eletronicamente por uma "Autoridade Certificadora" (CA). Serve para associar uma chave pública a uma dada entidade, divulgando-a. Quem conhecer a chave pública da CA pode verificar o conteúdo e confirmar a autenticidade do certificado emitido pela CA pois esta assina-os com a sua chave privada. No certificado estão incluídos dados como a chave pública, nome da CA, 46-2

número de serie do certificado, etc. Os certificados tem um tempo de validade limitado que pode ser controlado através de um prazo de validade, que não pode ser alterado e, através de certificados de revogação emitido pela CA.

O padrão dos certificados é o x.509. Em 1988 foi definida a versão 1 pelo *International Telecommunication Union –Telecommunication Standardization Sector (*ITU-T*)*. Em 1996 foi revisto e lançada a versão X.509v3 incluído mais informação.

3.8.5 Encriptação Quântica

É um conjunto de técnicas criptográficas baseadas em problemas para os quais não se conhecem soluções eficientes mesmo com computadores quânticos, como é o caso dos grupos não abelianos, dos sistemas quadráticos multivariados, redução de reticulados[43].

O primeiro protocolo de criptografia quântica foi desenvolvido em 1984 por Charles Bennett e Gilles Brassard, e ficou conhecido por BB84. Utiliza a polarização dos fotões de um feixe de raios laser, como unidade básica para a criação um sistema seguro de transmissão de informação (Costa, 2008). Existem outros protocolos como o E91, que faz uso de singletos[44] para gerar sequências de números aleatórios, e o BBM92 e B92 que se poderá dizer que são simplificações dos outros dois.

[43] Regev, O. (2002).Quantum computation and lattice problems. Foundations of ComputerScience. Proceedings. Thee 43rd Annual IEEE Symposium.

[44] Termo espectral em que o número quântico do spin do átomo é igual a zero e cuja multiplicidade é, portanto, igual a um.

4 Redes TCP/IP

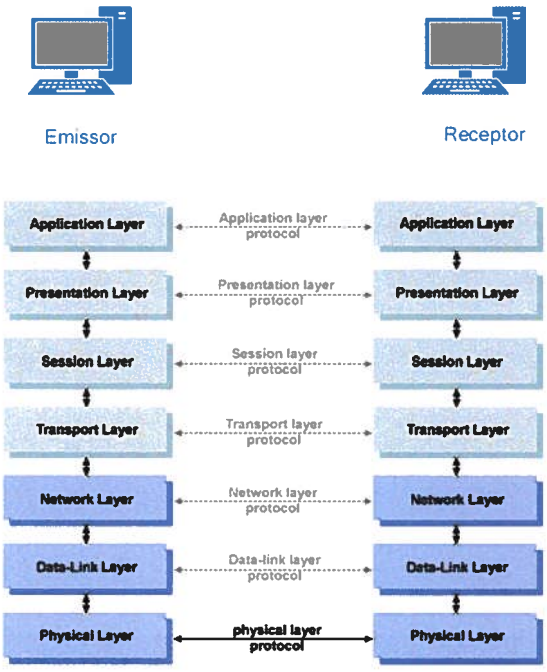
As redes são compostas por dados, *software* e *hardware*, em que cada nó da rede é um sistema sujeito a problemas de segurança, possuindo ainda as vulnerabilidades da comunicação com o exterior. Nas redes, os problemas de segurança de um computador, são aumentados exponencialmente.

Assim, justifica-se um capítulo onde sejam apresentados conceitos sobre redes baseadas nos protocolos (um protocolo é um standard que permite a comunicação entre processos, ou seja, regras e procedimentos para o envio de dados numa rede) *T*CP/IP, as suas classificações, e os principais protocolos usados.

4.1 Conceitos

4.1.1 Arquitectura de Rede

Devido à sua complexidade, as redes são organizadas em camadas formando um pilha onde cada camada tem uma função. Uma camada **n** de uma máquina "comunica" com a camada **n** de outra máquina, através de um protocolo de comunicação.



Fonte: (The OSI Reference Model, 2013)
Figura 4. 1 – Arquitetura de rede (Modelo OSI)

4 Redes TCP/IP

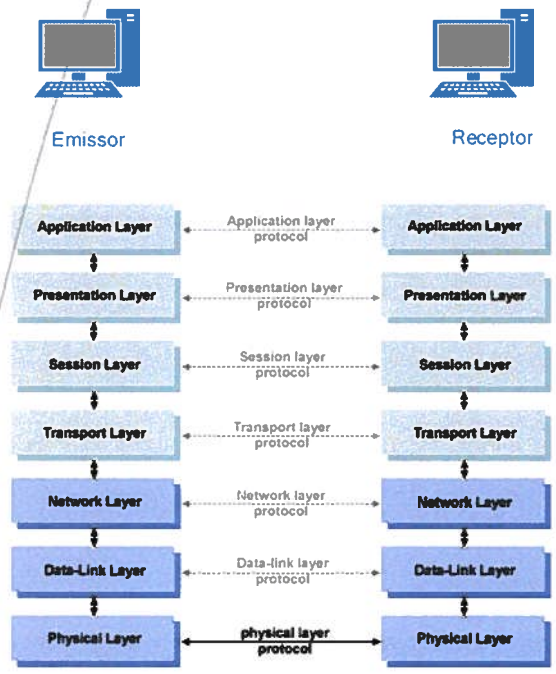
As redes são compostas por dados, *software* e *hardware*, em que cada nó da rede é um sistema sujeito a problemas de segurança, possuindo ainda as vulnerabilidades da comunicação com o exterior. Nas redes, os problemas de segurança de um computador, são aumentados exponencialmente.

Assim, justifica-se um capítulo onde sejam apresentados conceitos sobre redes baseadas nos protocolos (um protocolo é um standard que permite a comunicação entre processos, ou seja, regras e procedimentos para o envio de dados numa rede) *T*CP/IP, as suas classificações, e os principais protocolos usados.

4.1 Conceitos

4.1.1 Arquitectura de Rede

Devido à sua complexidade, as redes são organizadas em camadas formando um pilha onde cada camada tem uma função. Uma camada **n** de uma máquina "comunica" com a camada **n** de outra máquina, através de um protocolo de comunicação.



Fonte: (The OSI Reference Model, 2013)
Figura 4. 1 – Arquitetura de rede (Modelo OSI)

Entre cada par de camadas adjacente existe uma interface que define as operações entre cada camada

A este conjunto de camadas e protocolos é chamado Arquitectura de Rede.

O TCP/IP é um conjunto de protocolos, uma pilha de protocolos. O seu nome já faz referência ao conjunto que o compõe, o *TCP (Transmition Control Protocol)* e o IP (*Internet Protocol*). O IP é responsável por mover os pacotes de um nó para outro, o TCP tem como função verificar a correcta entrega do mesmo.

Conforme afirma Queiroz (2002, p. 34):

> "O protocolo é um conjunto de regras para o envio de informações em uma rede, essas regras regem o conteúdo, formato, duração, sequência e o controle de erro de mensagens trocadas nos dispositivos de rede. Atualmente o TCP/IP (Protocolo de controle de transmissão de Internet) é o protocolo mais usado em redes locais. Isso se deve basicamente a popularização da Internet, a rede mundial de computadores, já que esse protocolo foi criado para ser usado na Internet."

O TCP/IP utiliza uma arquitetura de quatro camadas do modelo OSI:

- Camada aplicação – fornece a interface de utilizador de rede na forma de aplicações e serviços de rede. Alguns dos protocolos desta camada são SMTP, FTP, HTTP, DNS

- Camada de apresentação - A camada de apresentação formata os dados a serem apresentados na camada de aplicação. Pode ser vista como o conversor para a rede. Essa camada pode converter dados de um formato usado pela camada de aplicativo em um formato comum na estação de envio e, em seguida, converter o formato comum em um formato conhecido para a camada de aplicativo na estação de recebimento.

- Camada sessão - A camada de sessão permite o estabelecimento da sessão entre processos em execução em estações diferentes.

Entre cada par de camadas adjacente existe uma interface que define as operações entre cada camada

A este conjunto de camadas e protocolos é chamado Arquitectura de Rede.

O TCP/IP é um conjunto de protocolos, uma pilha de protocolos. O seu nome já faz referência ao conjunto que o compõe, o *TCP (Transmition Control Protocol)* e o IP (*Internet Protocol*). O IP é responsável por mover os pacotes de um nó para outro, o TCP tem como função verificar a correcta entrega do mesmo.

Conforme afirma Queiroz (2002, p. 34):

> "O protocolo é um conjunto de regras para o envio de informações em uma rede, essas regras regem o conteúdo, formato, duração, sequência e o controle de erro de mensagens trocadas nos dispositivos de rede. Atualmente o TCP/IP (Protocolo de controle de transmissão de Internet) é o protocolo mais usado em redes locais. Isso se deve basicamente a popularização da Internet, a rede mundial de computadores, já que esse protocolo foi criado para ser usado na Internet."

O TCP/IP utiliza uma arquitetura de quatro camadas do modelo OSI:

- Camada aplicação – fornece a interface de utilizador de rede na forma de aplicações e serviços de rede. Alguns dos protocolos desta camada são SMTP, FTP, HTTP, DNS

- Camada de apresentação - A camada de apresentação formata os dados a serem apresentados na camada de aplicação. Pode ser vista como o conversor para a rede. Essa camada pode converter dados de um formato usado pela camada de aplicativo em um formato comum na estação de envio e, em seguida, converter o formato comum em um formato conhecido para a camada de aplicativo na estação de recebimento.

- Camada sessão - A camada de sessão permite o estabelecimento da sessão entre processos em execução em estações diferentes.

- Camada Transporte – responsável pela comunicação máquina-a-máquina. Controla também, erros e fluxos, garante que as mensagens são entregues sem erros, em sequência e sem perdas ou duplicações. Protocolos usados: TCP e UDP

- Camada de Rede - responsável pelas conexões entre as redes locais, estabelecendo, assim, a interconexão e a transmissão de dados entre elas, decidindo que caminho físico devem levar os dados com base nas condições de rede, prioridade do serviço e outros factores. Protocolos IP e ICMP

- Camada de vínculo de dados – A camada de link de dados fornece erros de transferência de quadros de dados de um nó para outro, através de camada física, permitindo que camadas acima dela assumam a transmissão virtualmente livre de erros, através do link

- Camada física - camada mais baixa, diz respeito à transmissão e recepção do fluxo de *bits* brutos, não-estruturados através de um meio físico (Microsoft, 2013).

As características principais do TCP são:

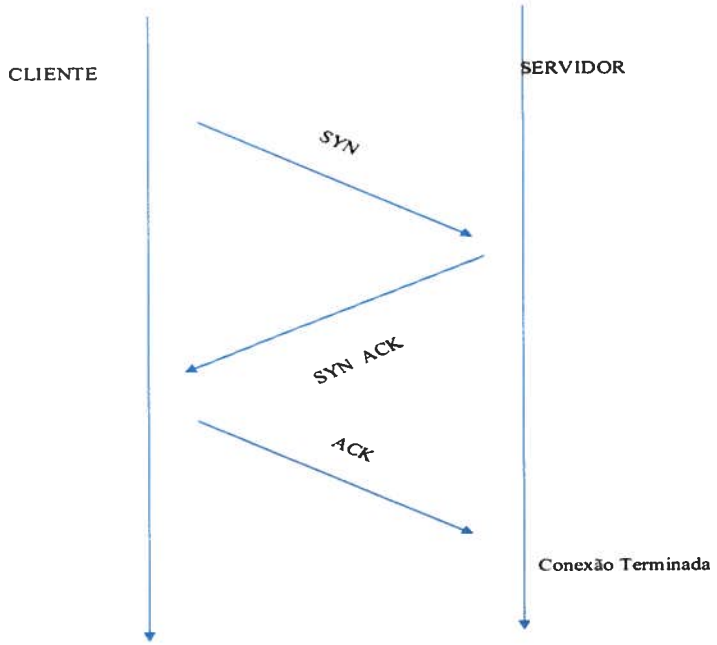
- Orientado à conexão – Realiza um controlo de transmissão dos dados durante a comunicação que é estabelecida entre as máquinas, em que o receptor envia avisos de recepção em forma de fluxo.

- Confiável – Utiliza técnicas que garantem a fiabilidade dos dados enviados, o que não acontece com o UDP. Permite ainda a recuperação de pacotes perdidos, duplicados ou corrompidos e tem capacidade de recuperar ligações perdidas

- *Full-duplex* – Tem capacidade de estabelecer ligações nos dois sentidos.

- *Aperto de mão (Handshake)* – Processo de início e fim de conexão em três tempos que garante a autenticação da sessão, garantindo que todos os pacotes foram recebidos. Para iniciar a conexão TCP, o emissor envia um pacote com o *bit* SYN *on*. Se o receptor estiver pronto para estabelecer a conexão, responde com um

pacote com os bits SYN e ACK a *on.* O emissor completa a troca enviando o pacote com o *bit* ACK a *on* (Pfleeger, 2006).



Fonte: Jr., W. B. (2002). *Advanced Incident Handling and Hacker Exploits* . Retrieved from www.cgisecurity.com : http://www.cgisecurity.com/lib/bill/William_Bellamy_GCIH.html

Figura 4. 2 TCP Aperto de mão

- Entrega ordenada - A entrega é feita em blocos num fluxo de dados que são posteriormente reconstruídos no destinatário

O IP implementa um serviço de datagramas não confiáveis, isto é, não há garantias de entrega dos pacotes. Este pode chegar fora de ordem, duplicado, corrompido ou ser totalmente perdido. É portanto um protocolo não orientado à conexão.

As principais características são:

- Define a estrutura de cada pacote.
- Define as regras de identificação de cada máquina
- Possui técnicas de encaminhamento dos pacotes entre origem e destino através de *routers* e *gateways*

O protocolo possui duas versões, IPV4 e IPV6. O IPV4 tem um endereçamento de 32*bits* enquanto o do IPV6 é de 128*bits*. O IPV4 tem grandes problemas de segurança

bem como escassez de IP's disponíveis, problemas largamente resolvidos pela nova versão.

O problema da escassez de IP's tem sido colmatada com a utilização de técnicas como o NAT que permitem a partilha de um IP no acesso à *Internet*, aumentando também a segurança ao "mascará-lo" ou o *subnetting* (processo de divisão de uma rede em sub-redes mais pequenas que a original).

4.2 Classificação de redes

As redes podem ser classificadas segundo o seu tamanho e topologia dos quais se destacam:

- Dimensão área geográfica

  Redes pessoais (PAM)

  Redes metropolitanas (MAN);

  Redes locais (LAN);

  Redes de área alargada (WAN).

- Capacidade de transferência de informação

  Redes de baixo débito;

  Redes de médio débito;

  Redes de alto débito.

- Topologia ("a forma da rede")

  Redes em estrela;

  Redes em "bus";

  Redes em anel (ring).

  Redes sem fios

- Meio físicos de suporte ao envio de dados

  Redes de cobre;

  Redes de fibra óptica;

  Redes por satélite;

  Redes por rádio.

Desta classificação justifica-se um olhar mais em pormenor sobre a Distribuição Geográfica e pela Topologia:

4.2.1 Distribuição Geográfica

LAN *(Local Area Network)*: são redes de pequena dispersão geográfica, computadores que conectam computadores numa mesma sala, prédio, com objectivo de partilhar recursos.

WAN (*Wide Area Network*): redes que usam linhas de comunicação de operadores de telecomunicações de forma a permitir interligação de computadores localizados em locais afastados fisicamente

MAN (*Metropolitan Area Network*): computadores interligando regiões ou cidades. São usadas para interligação de sistemas dispersos numa área geográfica ampla.

4.2.2 Topologia

Figura 4. 3 - Bus

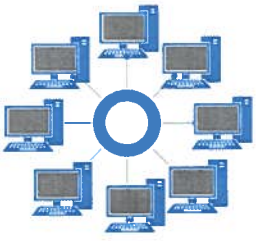


Figura 4. 4 – Anel

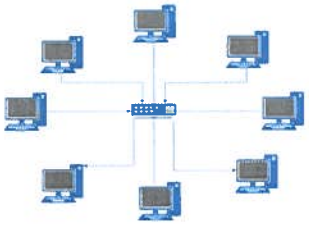


Figura 4. 5 – Estrela

5 VPN

VPN (*Virtual Private Network*): como o nome indica é uma forma virtual de rede física e segura. É uma forma de ligar diferentes redes de uma empresa utilizando um meio publico e inseguro como a internet.

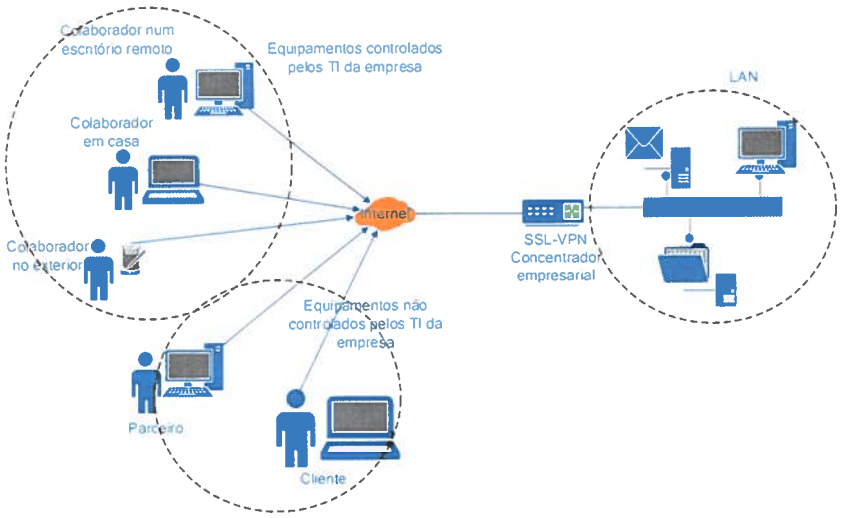
5.1 Funcionalidades

As VPN's, criam túneis virtuais para comunicação entre as redes, permitindo que os dados circulem encriptados aumentado a segurança. Permitem que computadores e outros dispositivos se liguem às empresas a partir do mundo exterior pela Internet de forma segura.

Tem outra vantagem que consiste em aumentar o número de dispositivos que podem ligar a empresa sem ter que realizar avultados investimentos, aumentando a mobilidade dos utilizadores. Possibilita também diferentes redes de escritórios espalhados geograficamente partilhando recursos de forma segura.

Alguns dos dispositivos que implementam VPN's são *routers, firewalls* e software instalados em servidores.

Possuem os seus próprios protocolos de comunicação que funcionam em conjunto com o TCP/IP, permitindo que, depois de estabelecidos os túneis, os pacotes circulem neles. Deles se destacam *Point-to-Point Tunneling Protocol (*PPTP*)*, o *Layer Two Tunneling Protocol (*L2TP*)* e o IPSec.



Fonte: Adaptado *SonicWALL SSL-VPN* . (n.d.). Retrieved from esecurity togo: http://www.esecuritytogo.com/category.aspx?categoryid=236

Figura 5. 1 – VPN

Point-to-Point Tunneling Protocol (PPTP) – Apesar de ser o mais simples de implementar e suportado por quase todos os sistemas operativos, é o menos seguro. Utiliza chaves de encriptação com base numa senha, ficando dependente da complexidade da mesma.

*Layer 2 Tunneling Protocol (*L2TP*)* – Mais seguro que o anterior mas também mais difícil de implementar. A autenticação é feita em dois níveis. No primeiro, é feita a autenticação do utilizador pelo sistema destinatário e só depois é estabelecido o túnel entre as *gateways*. Como não inclui mecanismos de encapsulamento, depende do *ipsec* para garantir segurança.

*Internet Protocol Security (*IPsec*)* – O mais seguro dos três mas também o mais "pesado" e difícil de implementar.

Tem dois modos de funcionamento: modo transporte, em que protege os dados do utilizador e modo túnel em que todo o pacote é protegido.

Não consegue evitar evidentemente ataques do tipo *DoS*.

*Secure Sockets Layer virtual private network (*SSL VPN*)* - É uma forma de VPN que pode ser usada com um "*browser*", não necessitando como o IPsec de qualquer instalação de software no computador cliente. É usado para permitir a utilizadores remotos acesso a aplicações Web e conexões internas à empresa.

Providencia comunicações seguras para a transmissão de dados entre os dois pontos. É composto por um dispositivo de VPN's ao qual o utilizador se liga com o "*browser*". O trafego entre o "*browser*" e o dispositivo é encriptado com SSL ou o seu sucessor *Transport Layer Security (TLS)*.

6 Redes sem fios

As redes sem fios também conhecidas por Wi-Fi, são um conjunto de especificações para (WLAN - *Wireless Local Area Network*) baseada no padrão IEEE 802.11.

As redes sem-fios estão espalhadas por todo o lado por serem económicas, flexíveis e fáceis de instalar, mas têm grandes problemas de segurança em especial as redes baseadas nos padrões 802.11. Os problemas de segurança são essencialmente, a autenticação do STA[45] à rede, o controlo de acesso à rede, a confidencialidade e integridade das mensagens trocadas (Zuquete, 2008).

6.1 Arquitectura

As redes 802.11 operam na frequência de 5 GHz, que é uma faixa mais limpa que a dos 2.4 GHz onde operavam as versões anteriores, pois muito menos dispositivos operam nesta frequência. O padrão 802.11n, oferece velocidades de transmissão na ordem dos 300 Mbps. O novo padrão 802.11ac irá atingir teóricamente1,3 Gbps (Brown, 2012).

As redes 802.11 possuem duas arquitecturas:

- *Ad-hoc* – Nesta arquitecturas todos os STA comunicam entre si num modelo P2P[46]
- Estruturadas – Aqui os STA comunicam com AP[47], que tem a função de ligar as rede cabladas ou outros AP via rádio.

As redes 803.11 podem ser identificadas por meio de um identificador chamado SSID[48], que nas redes estruturadas é definido no AP e nas Ad-hoc é definido em cada STA.

Um STA para se ligar a uma rede tem que saber primeiro qual o SSID da mesma. Para o fazer ou faz uma escuta ao meio, pois os AP anunciam-se periodicamente, ou pode ele interrogar o AP para saber se ele serve a rede com um dado SSID.

---

[45] Station –Dispositivo móvel
[46] Pear to pear - redes
[47] Access Point – Ponto de acesso
[48] Service Set ID – Identificador da rede

A comunicação nas redes sem fios são efectuadas por pacotes chamados tramas.

A associação do STA a uma rede, depois de conhecer o SSID, é feita em duas etapas, autenticação e associação. A autenticação é efectuada por um processo de Desafio/Resposta de Autenticação em que são solicitadas as credenciais. Neste processo o AP força o uso de um protocolo, o qual foi definido na sua configuração, no caso de incompatibilidade por parte do STA, não há lugar a autenticação e consequente recusa de acesso por parte do AP. Após a autenticação dá-se a associação num processo novamente de Pedido de Desafio/Resposta. Um equipamento pode estar autenticado em vários AP mas só associado a um.

6.2 Segurança

Como já foi referido, a segurança é o principal problema das redes sem fios não direcionadas, pois é complexo limitar o acesso físico a utilizadores não autorizados ao sinal emitido. E na medida em que estas redes são cada vez mais comuns, é fundamental garantir os três princípios básicos da segurança: autenticação, confidencialidade e integridade dos dados.

6.2.1 WEP (Wired Equivalent Privacy)

Inicialmente a segurança das redes estruturadas 802.11 era baseada no protocolo WEP. Este protocolo apesar de garantir autenticação dos dispositivos contra o AP, confidencialidade e integridade dos dados transmitidos, possuia no entanto muitas vulnerabilidades.

O WEP define dois modelos de autenticação no acesso ao AP:

- *Open System Authentiction* (OSA) – Neste caso não existe autenticação logo todo os pedidos de associação são autorizados. Este modelo é usado em cenário de redes abertas ao público.
- *Shared Key Authentication* (SKA) – Com esta opção é necessário existir uma chave secreta partilhada entre o equipamento móvel e o AP (*Pre-Shared Key*, PSK). A autenticação realiza-se pelo processo de Desafio/Resposta em que o AP envia o desafio ao equipamento móvel que deverá responder e devolvê-lo cifrado com a PSK. Isto implica que exista uma pré-distribuição das chaves aos dispositivos móveis e ao AP.

A autenticação com WEP é muito insegura, caso sejam capturadas tramas do processo de desafio/resposta de um utilizador legítimo, é possível calcular os valores necessários para uma correcta autenticação.

Um dos problemas do WEP é o facto de não possuir mecanismos geradores de novas chaves de cada vez que um utilizador se associa ao AP. A chave usada é sempre a mesma, a que foi previamente distribuída (PSK).

A chave secreta tem 40 bits é concatenada com um vector de inicialização (IV[49]) de 24 bits formando a chave composta. O algoritmo PNRG[50] baseado no algoritmo RC4[51], é responsável por gerar a trama pseudoaleatória de saída que irá encriptar o texto dando origem ao criptograma. Seguidamente são adicionados quatro bytes resultantes de um processo de ICV (*Integrity check Value*). O algoritmo CRC32 é usado de forma a garantir a integridade do pacote. Este pacote composto por: cabeçalho, dados (IV + criptograma) e ICV, é seguidamente enviado por canal não seguro. Na STA, destino o processo é revertido, usando o IV do pacote, é gerada uma nova trama pelo PRNG com que é desencriptado o texto cifrado. De seguida, usa o CRC32 para gerar um novo IV que vai ser comparado com o que vinha no final do pacote. Se os valores forem diferentes, o pacote é descartado.

Como o IV tem uma dimensão finita, ao fim de algum tempo, as chaves vão se repetir. O uso repetido de chaves contínuas, faz com que os criptogramas gerados a partir das mesmas fiquem vulneráveis (Zuquete, 2008).

Outra fraqueza do WEP é o facto de a garantia de integridade ser dada pelo CRC32, um algoritmo linear. Devido a este facto, é possível fazer modificações nos pacotes sem que sejam detectadas, conhecendo a trama de valores pseudoaleatórios gerados pelo RC4.

6.2.2 WPA (*Wi-fi Protected Access*)

Devido aos problemas e limitações do WEP foi desenvolvido um novo padrão para as redes 802.11, o WPA.

O WPA manteve as funcionalidades que existiam no WEP e acrescentou novas ao nível da gestão das chaves e do controlo de integridade das tramas. Assim, cada trama é cifrada com uma nova chave evitando que se construam dicionários de chaves continuas, apesar de se utilizar a PSK. O controlo de integridade foi melhorado e a autenticação passou a ser mútua entre STA e o AP e passou a existir distribuição de chaves de sessão (Zuquete, 2008).

---

[49] Vector de inicialização
[50] Pseudo-random Number Generator
[51] Algoritmo simétrico de criptografia de fluxo

O 802.11i, também conhecido comercialmente por WPA2, define padrões de segurança para as rede 892.11 e mecanismos de segurança, como o uso do AES[52] e protecção de tramas com AES-CCMP[53], usa igualmente o conceito de redes com segurança robusta, RSN.

O WPA usa o TKIP[54] para lidar com a autenticação e confidencialidade das tramas e o 802.1x para tratar da autenticação entre os comunicantes e da distribuição de chaves de sessão.

O TKIP encapsula o WEP, ou seja usa-o mas de forma a que as suas vulnerabilidades não fiquem expostas. O TKIP usa agora um IV de 48 bits que varia de forma definida, produz chaves WEP para cada trama nos dois sentidos da comunicação, exclui chaves fracas do RC4 resultantes da combinação do IV com as chaves WEP e usa o MIC[55]. O TKIP calcula os valores de integridade (MIC) usando o algoritmo Michael (Zuquete, 2008).

Nas redes 802.1x distinguem-se três tipos de interlocutores: suplicante (STA), o autenticador (AP) e o servidor de autenticação (servidor de RADIUS/Diameter).

As operações, para troca de dados no âmbito 802.1x na sua forma mais complexa, podem dividir-se em três fases. Na primeira, o suplicante liga-se à rede sem fios fazendo o processo de descoberta da rede, autenticação do STA e associação ao AP, mantendo no entanto o estado de "não autorizado". Na fase seguinte é realizada uma autenticação mútua, distribuição de chaves de sessão entre STA e o servidor de autenticação, usando o protocolo *Extensible Authentication Protocol*, EAP, continuando com o estado de "não autorizado". Na terceira fase é realizada a autenticação mutua entre o STA e o autenticador, garantindo assim que está a interagir com o mesmo AP do servidor de autenticação e é feita uma distribuição de chaves de forma a garantir uma chave fresca entre os dois (Zuquete, 2008).

A arquitectura descrita é demasiado complexa para ambientes SOHO[56] e, assim, é possível usar uma solução mais simples dispensando o servidor de autenticação. A solução é normalmente chamada de WPA2-PSK, em que é usada uma PSK para calcular a PMK[57]. Esta solução, com um sistema de autenticação com uma única chave PSK, deve ser usada unicamente em ambientes de redes onde prima a confiança.

---

[52] Advanced Encryption Standard – Algoritmo de chave simétrica de 128 a 256 bits baseado no algoritmo Rijndael

[53] AES-Counter mode with Chipher blick chaining Message authentication code Protocol

[54] (***Temporal Key Integrity Protocol***) é um algoritmo de criptografia baseado em chaves que se alteram a cada novo envio de pacote

[55] Message Integrity Code

[56] Small Office/Home Office

[57] Pairwise Master Key

7 Conclusão

O valor da informação é inquestionável quer para organizações quer para indivíduos e esse valor obriga à necessidade de protecção.

É provável que não haja sistemas invioláveis. Todos os sistemas possuem as suas vulnerabilidades quer por falhas de concepção do *software*, da sua má implementação, de más politicas de segurança ou da sua não aplicação ou da falta de uma cultura de segurança por parte de administradores e utilizadores.

Assim desde que se verifique uma vulnerabilidade, ela é passível de ser explorada expondo toda a informação, colocando em risco organizações ou dados pessoais.

As ameaças podem assumir diversas formas, como a alteração da informação, a violação da confidencialidade, alteração da sua proveniência ou torna-la indisponível.

Os ataques podem ter um caracter passivo, em que a vítima nem se apercebe do mesmo ou um caracter activo onde os ataques acabam por ser descobertos pelo roubo de informação, dinheiro ou pela destruição de conteúdos.

É pois fundamental devido à dependência das organizações dos seus sistemas de informação, a implementação de medidas de protecção cada vez eficazes de forma correctiva, preventiva e dissuasora com o objectivo de proteger a informação e os próprios sistemas. Estas medidas, passam por manter os sistemas actualizados com as últimas correcções disponibilizadas pelos fabricantes, aquisição de equipamento de protecção e de redundância dos sistemas, e a educação dos utilizadores quanto a comportamentos de risco.

Neste âmbito surge um conceito que é o do risco. Esta variável é uma relação entre as ameaças, o nível de proteção e a própria operacionalidade do acesso à informação por parte de quem dela necessita, que tem que ser avaliado. Este risco deve ser analisado periodicamente por meio de um modelo de análise desenvolvido e adaptado à rede informática em causa.

Por fim é necessário também ponderar a problemática entre segurança e privacidade. Até onde estamos dispostos a prescindir da privacidade a troco da segurança.

Bibliografia

Army, D. o. (2003). *FM 3-13 - Information Operations: Doctrine, Tactics, Techniques, and Procedures,*. Washington.

Brown, M. (2012). *Entenda mais sobre o padrão 802.11ac, a 5ª geração do Wi-Fi.* Retrieved from idgnow.com: http://idgnow.uol.com.br/mobilidade/2012/04/11/saiba-mais-sobre-o-padrao-802-11ac-a-5a-geracao-do-wi-fi/

Brute force attacks. (n.d.). Retrieved from IBM Security Network Intrusion Prevention System (IPS) : http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/index.jsp?topic=%2Fcom.ibm.ips.doc%2Fconcepts%2Fwap_brute_force.htm

Business-to-business. (2011). Retrieved from wikipedia.org: http://pt.wikipedia.org/wiki/Business-to-business

Carneiro, A. (2002). *Introdução à Segurança dos Sistemas de Informação.* FCA.

Corporation, S. (2013). Retrieved from Smurf DoS attack (ataque de DoS Smurf): http://www.symantec.com/pt/pt/security_response/glossary/define.jsp?letter=s&word=smurf-dos-attack

Cruz, J. M. (2012). Segurança da informação: a norma ISO/IEC 2700 e ISO/IEC 2701. Porto.

Estrela, J. M. (1998). Segurança em redes de computadores. Master's thesis. Porto.

Fincatti, C. A. (2010). CRIPTOGRAFIA COMO AGENTE MOTIVADOR NA APRENDIZAGEM DA MATEMÁTICA EM SALA DE AULA. São Paulo: UNIVERSIDADE PRESBITERIANA MACKENZIE.

Foundation, O. (2007). *As 10 vulnerabilidades de segurança mais criticas em aplicações web.* Retrieved from OWASP: https://www.owasp.org/images/4/42/OWASP_TOP_10_2007_PT-BR.pdf

Growth of Wireless Broadband and Spectrum Crunch. (n.d.). Retrieved from high tech spectrum coalition: http://static.squarespace.com/static/50d3c930e4b040d796f7a87a/t/51154124e4b0802637f89cdf/1360347428295/PDF_SpectrumCrunch_OnePager_FINAL.pdf

HacK_MiNDeD. (2009). *Top 10 Trojans of All Time*. Retrieved from Hacker's Lane: http://www.hackerslane.com/2009/top-10-trojans-of-all-time/

hdudhade, s. (n.d.). *HoneyBox v0.1 - Honeypots in a box!* Retrieved from Information Security : http://santoshdudhade.blogspot.pt/2012/09/honeybox-v01-honeypots-in-box.html

Hoepers, C., Steding-Jessen, K., & Chaves, M. H. (2007). *Honeypots e Honeynets: Definições e Aplicações*. Retrieved from cert.br: http://www.cert.br/docs/whitepapers/honeypots-honeynets

Inácio, P. R. (2010). *Engenharia Informatica Tecnologia e Sistemas de Informação.*

Institute, C. S. (2011). *2010 / 2011 CSI Computer Crime and Security Survey.* CSI.

Jr., W. B. (2002). *Advanced Incident Handling and Hacker Exploits* . Retrieved from www.cgisecurity.com : http://www.cgisecurity.com/lib/bill/William_Bellamy_GCIH.html

Krulgel, C., Valeur, F., & Vigna, G. (2005). *Intrusion Detection and Correlation: Challenges and Solutions.* Springer.

Larrieu, C. (2003). *Sistemas de detecção de intrusão (IDS)*. Retrieved from kioskea.net: http://pt.kioskea.net/contents/detection/ids.php3

Lipson, H., & van Wyk, K. (2005). *Application Firewalls and Proxies - Introduction and Concept of Operations*. Retrieved from Home Land Security: https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/assembly/30-BSI.html

Loureiro, P. (2004). *TCP/IP em rede Microsoft para profissionais - 5ª Edição.* FCA - Editora de Informática.

Macedo, D. (2012). *Gestão de Riscos*. Retrieved from Diego Macêdo – Analista de T.I.: http://www.diegomacedo.com.br/gestao-de-riscos/

Microsoft. (2013). *Definição das Sete Camadas do Modelo OSI e Explicação de Suas Funções.* Retrieved from Microsof suporte: http://support.microsoft.com/kb/103884/pt-br

Murat. (2010). *nettracer.* Retrieved from Syn attack protection on Windows Vista, Windows 2008, Windows 7 and Windows 2008 R2: http://blogs.technet.com/b/nettracer/archive/2010/06/01/syn-attack-protection-on-windows-vista-windows-2008-windows-7-and-windows-2008-r2.aspx

Niranjan. (2007). *DNS Amplification Attack.* Retrieved from Security Tools News & Tips: http://securitytnt.com/dns-amplification-attack/

Oliveira, D. (2013). *O poder da Internet sobre as empresas*. Retrieved from www.administradores.com.br: http://www.administradores.com.br/artigos/administracao-e-negocios/o-poder-da-internet-sobre-as-empresas/68199/

Pfleeger, C. P. (2006). *Security in Computing.* Prentice Hall.

Ress, W. (2011). *Começando em segurança*. Retrieved from MSDN: http://msdn.microsoft.com/pt-br/library/ff716605.aspx#naorepudio

Roche, R. (2011). *Wireless Data Traffic Grew 110% from 2009-2010*. Retrieved from ctia: http://blog.ctia.org/2011/05/31/wireless-data-traffic-grew-110-from-2009-2010/

Rodrigues, P. E. (2010). *Segurança Informática de Redes e Sistemas.* Retrieved from http://www.di.ubi.pt/~inacio/SI20102011/Aula_8_Lecture_8.pdf

Sahlan, A. W. (2008). *Proses Spoofing.* Retrieved from http://hadianto.blog.ugm.ac.id/2008/10/20/proses-spoofing/

Santos, V. (2010). *Blog SegInfo.* Retrieved from Sistemas de Detecção de Intrusões: http://www.seginfo.com.br/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-softwares-open-source/

Silva, P. T. (2003). *Segurança dos Sistemas de Informação.* Lisboa: Centro Atlântico.

SonicWALL SSL-VPN . (n.d.). Retrieved from esecurity togo: http://www.esecuritytogo.com/category.aspx?categoryid=236

Standardization, I. O. (2013). *ISO/IEC 27002*. Retrieved from http://en.wikipedia.org.

Starllings, W. (2006). *Cryptography and Network Security.* Prentice Hall.

Tanenbaun, A. S. (2003). *Computer Networks.* Pearson Education, Inc.

The OSI Reference Model. (2013). Retrieved from technologyuk: http://www.technologyuk.net/telecommunications/telecom_principles/osi_reference_model.shtml

Top 10 Worst Computer Worms of All Time . (n.d.). Retrieved from TheFreeDictionary : http://encyclopedia2.thefreedictionary.com/Top+10+Worst+Computer+Worms+of+All+Time

Weinberger, S. (2012, Março). *Top Ten Most-Destructive Computer Viruses*. Retrieved from smithsonian.com: http:www.smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html?c=y&page=1

Zuquete, A. (2008). *Segurança em Redes Informáticas.* FCA.

Anexo A

Vírus mais perigosos dos últimos 10 anos (Weinberger, 2012)

1) **Stuxnet (2009-2010)**
2) **Conficker Virus (2009)**
3) **agent.btz (2008)**
4) **Zeus (2007)**
5) **PoisonIvy (2005)**
6) **MyDoom (2004)**
7) **Fizzer (2003)**
8) **Slammer (2003)**
9) **Code Red (2001)**
10) **Love Letter/I LOVE YOU (2000)**

Os 10 worms mais perigosos (Top 10 Worst Computer Worms of All Time , s.d.)

1) Jerusalem (BlackBox)
2) Michelangelo
3) Storm Worm
4) Sobig
5) MSBlast
6) Melissa
7) Code Red
8) Nimda
9) ILOVEYOU
10) Morris Worm (Great Worm)

Os 10 Trojans mais perigosos (HacK_MiNDeD, 2009)

1) **NetBus**
2) **Back Orifice**
3) **Sub7**
4) **Beast**
5) **ProRat**
6) **Zlob Trojan**
7) **SpySheriff**
8) **Vundo**
9) **Turkojan**
10) **Trojan-Downloader.Win32.Kido.a**