Instituto Superior de Tecnologias Avançadas

Segurança Informática

Licenciatura em Informática

Ano Lectivo 2012/2013

Aluno: Nuno Miguel Lopes Ferreira

N.º 1727 - Turma A

Coordenador: Professor Doutor Pedro Ramos Brandão

Junho 2014

Dedicatória

Aos meus pais que me encaminharam e tornaram na pessoa que sou hoje.

Aos meus filhos pela ausência de muitas horas despendidas na conclusão desta licenciatura.

À minha namorada pelo apoio e força.

Agradecimentos

À minha mãe.

Aos meus sogros Madalena e José Puga.

Aos docentes do Instituto Superior de Tecnologias Avançadas na transmissão do saber, em especial, ao Prof. Pedro Brandão, Prof. António Fidalgo, Prof. Manuel Garimpo e Prof. José Boturão das Neves. Agradeço ainda à Prof.ª Cátia Ferreira a disponibilidade e o apoio prestado na elaboração deste projecto.

Aos meus colegas de curso pelo o apoio e a força dada. A entreajuda entre todos foi determinante para a conclusão deste curso.

Resumo

Com a evolução da Internet e crescente utilização da mesma, vão surgindo cada vez mais falhas de segurança que tornam vulneráveis os sistemas de informação das empresas. Desta forma, o alerta para os perigos inerentes à utilização desta rede global e dos computadores através da divulgação das melhores práticas de protecção torna-se de extrema relevância.

Este projecto pretende elaborar um modelo simplificado de segurança, identificando as principais vulnerabilidades da segurança informática e definir um conjunto de políticas de segurança, não só para proteger os recursos lógicos como também os físicos, no combate às inúmeras ameaças que tentam explorar as vulnerabilidades dos sistemas de informação.

Pretende-se ainda demostrar neste projecto, as potencialidades da utilização das redes sem fios e principais protocolos de segurança associados.

Após a sua leitura os responsáveis de um sistema de informação poderão entender os riscos aos quais estes sistemas estão sujeitos e ter uma visão mais abrangente das necessidades de segurança e implementação de uma política de segurança numa organização.

Palavras-chave: Segurança Informática, Redes Informáticas, Vírus, Ataques Informáticos, Vulnerabilidades, Internet.

Abstract

With the evolution and the increasing use of the Internet, security flaws are emerging increasingly making vulnerable the information systems of many companies. So, the warning of the dangers inherent in the use of this global network and computers through the dissemination of best practices for the protection becomes paramount.

This project intends to develop a simplified security model, identifying key vulnerabilities of computer security and define security policies, not only to protect the logical resources as well as the physical ones, in the combat against numerous threats that attempt to exploit vulnerabilities in information systems.

We also intend to demonstrate in this project, the potential use of wireless networks and major security protocols associated.

After reading this, the manager of an information system will be able to understand the risks to which these systems are exposed and will have more embracing view of security requirements and implementation to a security policy in an organization.

Keywords: Computer Security, Computer Networks, Virus, Computer Attacks, Vulnerabilities, Internet.

Abreviaturas

ACL – *Access Control Lists* (Listas de Controlo de Acesso)

CIDF - *Common Intrusion Detection Framework Architecture* (Arquitectura do Quadro de Detecção de Intrusões Comum)

DAC - *Discretionary Access Control* (Controlo de Acesso Discricionário)

DARPA - *Department of Advanced Research Projects Agency* (Departamento da Agência de Projectos de Pesquisa Avançada)

DNS – *Domain Name Server* (Sistema de Nomes de Domínio)

DoS - *Denial of Service* (Negação de Serviço)

DDoS - *Distributed Denial of Service* (Negação de Serviço Distribuída)

ICMP - *Internet Control Message Protocol*

IDS - *Intrusion Detection System* (Sistema de Detecção de Intrusões)

IEC - *International Electrotechnical Commission* (Comissão Electrotécnica Internacional)

IP - *Internet Protocol* (Protocolo de Internet)

IPS - *Intrusion Prevention System* (Sistema de Prevenção de Intrusões)

ISO - *International Organization for Standardization* (Organização Internacional para Padronização)

MAC - *Mandatory Access Controls* (Controlo de Acesso Mandatório)

NAT - Network Address Translation (Tradução de Endereços de Rede)

RAID - *Redundant Array of Independent Disks* (Conjunto Redundante de Discos Independentes)

RBAC - *Role-based Access Control* (Controlo de Acesso baseado em *roles*).

SI - Sistema de Informação

SPAM - *Sending and Posting Advertisement in Mass* (Envio e Postagem de Publicidade em Massa)

UDP - *User Datagram Protocol*

VPN – Virtual Private Network (Rede Privada Virtual)

WWW - *World Wide Web* (Teia Mundial)

Índice

Índice de Figuras

Introdução

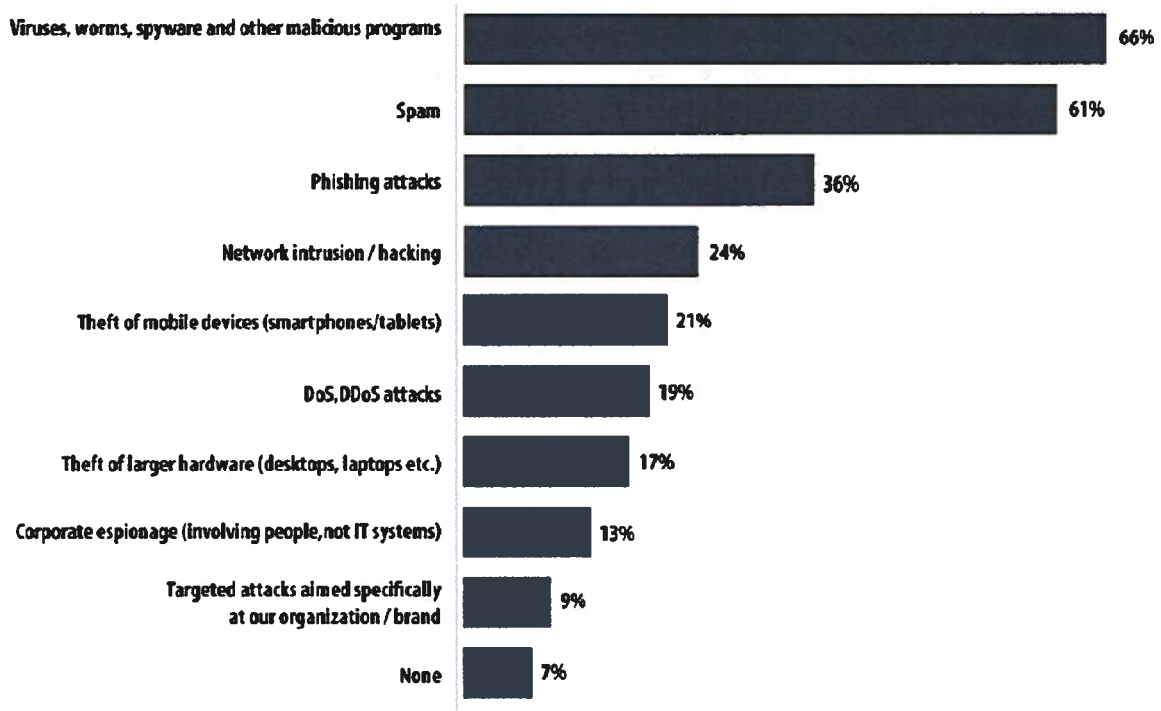
1. Problematização do tema

Com a evolução dos sistemas de informação (SI), não tem sido fácil para as organizações determinarem as ferramentas e metodologias de prevenção e combate aos ataques à segurança desses sistemas.

No meio empresarial, as necessidades assentam cada vez mais na informação, fundamental para as tomadas de decisões e desenvolvimento de novos produtos de forma a obter uma vantagem competitiva face a outras empresas. Com o acesso à informação assente em meios tecnológicos, a globalização das empresas foi extremamente facilitada, mas também com muitas desvantagens com a exposição dos seus sistemas de informação (SI) a diversos tipos de ameaças.

A actualização dos SI para tecnologia de última geração é importante, mas por si só não é tudo. À rápida disseminação do *software* malicioso cada vez mais sofisticado aliado à vulnerabilidade dos sistemas de segurança, existe a vulnerabilidade humana que permite o ataque externo com premissa de um colaborador da organização. Independentemente da escolha das tecnologias utilizadas para protecção dos SI e a informação como activo mais valioso de uma organização, é fundamental garantir a protecção destes sistemas de pessoas mal-intencionadas com o objectivo de furtar e obter informação privilegiada e sigilosa para seu proveito ou de outras organizações.

Segundo Kaspersky Lab e B2B Internacional, 91% das organizações entrevistadas sofreu um ataque cibernético pelo menos uma vez durante um período de 12 meses, enquanto 9% foram vítimas de ataques direcionados. O uso extensivo de computadores e outros dispositivos digitais em todas as áreas de negócio de uma organização criaram as condições ideais para programas de espionagem cibernética e de *software* malicioso capazes de roubar dados destas organizações. Com o seu potencial os programas maliciosos podem substituir em breve completamente membros da companhia como uma forma de colecta de informações (Kamluk & Lozhkin, 2013).



Fonte: http://media.kaspersky.com/pdf/KSB_2013_EN.pdf

Figura 1 - Distribuição das principais ameaças à segurança informática

Segundo Kamluk & Lozhkin(2013), as principais motivações dos atacantes são: os roubos de dados valiosos como, os segredos comerciais, os dados pessoais de funcionários e clientes e a monitorização das actividades de uma organização; a sabotagem da organização através da destruição de informação sensível ou interrupção da actividade desta; roubo de dinheiro por ataques direccionados às actividades de processamento; prejudicar a reputação da organização favorecendo organizações concorrentes que podem originar grandes perdas financeiras levando ao encerramento da organização.

Desde então empresas e organizações, beneficiando da tecnologia disponível criam ferramentas sofisticadas, baseadas em técnicas e mecanismos de segurança no combate ao cibercrime.

Objectivos gerais e específicos

Pretende-se com este projecto elaborar um guia simplificado de segurança para organizações quando ligadas à internet, identificando e prevenindo as principais ameaças à segurança informática e definir um conjunto de políticas de segurança, de forma a proteger e recuperar os SI.

Pretende-se ainda mostrar a potencialidades da utilização das redes sem fios e principais protocolos de segurança associados.

Estrutura do Projecto

Este projecto está organizado em oito capítulos.

No primeiro capítulo é descrito o estado da arte das matérias com relevância para este projecto.

No primeiro segundo é feita a contextualização do tema deste projecto.

No terceiro capítulo são identificadas as principais ameaças à segurança informática.

No quarto capítulo são abordadas às políticas de seguranças a tomar e respectivas áreas de intervenção.

No quinto capítulo são identificadas as principais medidas preventivas de detecção de actividades maliciosas.

No sexto capítulo são abordadas as principais técnicas de recuperação da informação.

No sétimo capítulo é feita uma abordagem às redes sem fio.

I - Estado da Arte

A internet veio revolucionar a forma de comunicação da sociedade moderna através de um conjunto de redes interligadas entre si, com milhões de computadores e dispositivos conectados.

Podemos dizer que a sua origem teve início na década de 50, mais precisamente em 1958, com a criação do departamento ARPA (*Department of Advanced Research Projects Agency*)[1] que consistia numa agência de projectos de pesquisa avançada de defesa, em resposta ao lançamento do primeiro satélite *Sputnik*, em 1957, pelos soviéticos.

A procura pela superioridade tecnológica, a crise dos mísseis de Cuba em plena Guerra Fria e o receio iminente dos Estados Unidos da América serem confrontados com um ataque de mísseis nucleares de larga escala, foram as razões pelas quais foi, em 1969, criado o projecto Arpanet[2], com vista ao desenvolvimento de uma rede de comunicações digital por pacotes. Este projecto, apenas com fins militares, consistia em garantir que se um nó da rede fosse atacado os restantes manter-se-iam operacionais, acabando com a centralização da informação.

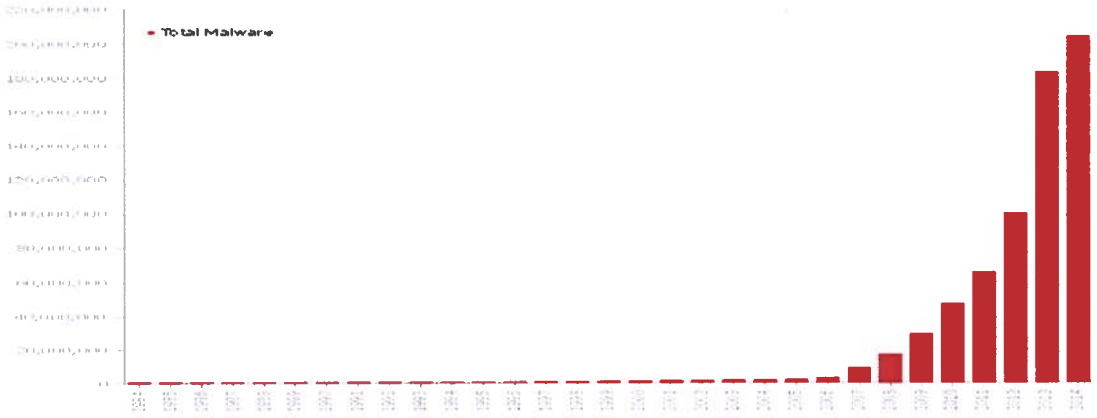
Este paradigma seria mais tarde herdada para a internet, mas apenas no início da década de noventa deixou de ser de uso exclusivo das instituições governamentais, passando também a estar disponível para a população em geral, dando inicio à globalização da informação com a criação do projecto WWW (*World Wide Web*) [3], um sistema de disponibilização universal de documentos no formato *HyperText Markup Language (HTML)*, e com recurso as novas tecnologias de informação e comunicação, que impulsionou a utilização da rede em todo o mundo (Veiga, 2004).

Com o crescimento e massificação do uso da internet, sem limites e fronteiras, pequenas redes domésticas, comerciais e governamentais, transportam a sua informação privada, comercial e sigilosa sobre ela, impulsionando uma nova forma de crime. Designado como cibercrime, após uma reunião de um subgrupo do G-8, no final da década de noventa em França, pretende discutir as melhores práticas de combate a este.

---

[1] http://semanticvoid.com/docs/darpa_directive.pdf acedido em 01 de Dezembro de 2013
[2] http://www.computerhistory.org/internet_history/ acedido em 01 de Dezembro de 2013
[3] http://www.w3.org/Proposal acedido em 01 de Dezembro de 2013

"O cibercrime compreende os crimes em que o alvo são os sistemas informáticos, mas também os crimes convencionais realizados com recurso a dispositivos eletrónicos e ainda aqueles em que, não sendo o computador o instrumento principal da atividade ilícita, o meio de realização de prova assume a forma digital"[4]



Fonte: http://conektinfo.wordpress.com/2013/06/22/virus-de-cumputador-uma-ameaca-invisivel/

Figura 2 - Evolução do número de *software* malicioso por ano

Para combate deste novo tipo de crime é recomendável a consulta da norma internacional ISO/IEC 27002, na qual estabelece um conjunto de orientações e recomendações na criação e gestão de um sistema de informação.

1.1. Princípios da Segurança Informática

Os três princípios fundamentais da segurança também conhecidos como os três pilares da segurança visam garantir a confidencialidade, a integridade e a disponibilidade dos SI na protecção dos activos críticos de uma organização.

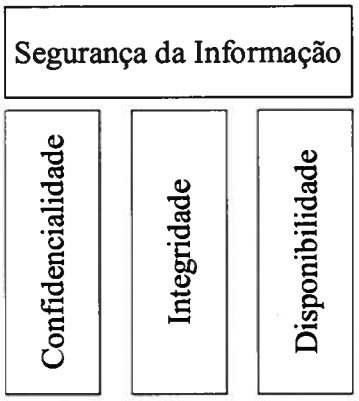


Figura 3 - Os três princípios fundamentais da segurança

[4] http://www.internetsegura.pt/noticias/2013/10/o-que-e-o-cibercrime#.U4IYQfldWSo acedido em 02 de Dezembro de 2013

Cada activo requer diferentes níveis destes princípios. Todos os controlos de segurança, mecanismos e salvaguardas são implementadas para fornecer um ou mais deste tipo de protecções, e todos os riscos, ameaças e vulnerabilidades são medidas pela sua capacidade de comprometer um ou todos dos seguintes principios (Harris, 2013): confidencialidade, integridade e disponibilidade.

A confidencialidade tem como princípio garantir que apenas pessoas autorizadas têm acesso a informação. A quebra de confidencialidade pode assumir diversas formas nomeadamente: permitir que alguém visualize a informação exibida no seu computador quando este trabalha com dados confidenciais, a perda ou roubo de equipamentos informáticos com informação confidencial pode originar uma violação da confidencialidade dessa organização.

A integridade garante a precisão e consistência dos dados durante todo o ciclo de vida em que é utilizada. Isto significa que os dados não podem ser modificados de forma não autorizada ou sem ser detectado. A integridade é violada quando: um utilizador acidentalmente ou com intenção maliciosa elimina ou altera dados importantes; quando um computador é infectado por um vírus; quando um processo automatizado não é escrito e testado correctamente as actualizações em massa para uma base de dados pode alterar os dados desta de uma maneira incorrecta.

A disponibilidade visa garantir que os recursos de qualquer sistema de informação estejam disponíveis sempre que os utilizadores necessitarem. Uns dos tipos de ataques contra a disponibilidade são conhecidos como ataques de negação de serviço.

Outros autores considerem também as propriedades de autenticidade e não repúdio como parte da segurança dos sistemas de informação (Marques, Ferreira, Ribeiro, Veiga, & Rodrigues, 2012).

O não repúdio é a capacidade de um sistema garantir que o remetente de uma mensagem é quem diz ser, não podendo negar o posterior envio da mensagem e que o destinatário desta não pode negar em como a recebeu.

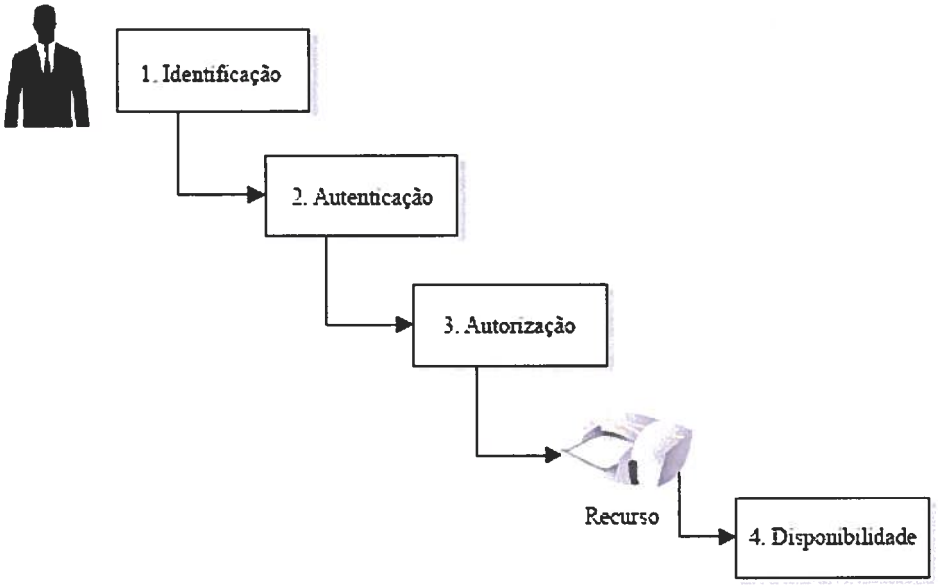
Por sua vez a autenticidade consiste no processo de um sistema de informação garantir a identidade do utilizador que enviou a mensagem ser aquele quem diz ser, garantindo que a mensagem é autêntica. Existem actualmente várias formas de um utilizador proceder à sua autenticação num sistema, a mais comum, a autenticação através de palavras-

chave, mas também por cartões magnéticos e biometria[5] para uma maior protecção de dados sensíveis e confidenciais.

2.2. Políticas de Segurança e Controlo de Acessos

Uma política de segurança é uma declaração formal das regras e procedimentos que os utilizadores devem respeitar quando acedem aos recursos e informação de uma organização. O seu objectivo principal é informar os utilizadores de seus requisitos obrigatórios de forma a proteger os recursos do sistema de informação (Fraser, 1997).

Segundo Harris (2013), existem quatro etapas que devem ocorrer quando um utilizador acede a um objecto: a identificação, a autenticação, a autorização e a responsabilidade.



Fonte adapatada: (Harris, 2013)

Figura 4 - Quatros etapas de acesso a um objecto

A identificação de um utilizador deve ser sempre verificada durante o processo de autenticação. A sua autenticação, geralmente, envolve um processo de dois itens: a inserção de informações públicas como o nome do utilizador, e a inserção de informações privadas como a uma palavra-chave. Estes dois itens comparados em conjunto são validados com a informação armazenada no sistema. Se existir o utilizador é autenticado.

[5] A autenticação biométrica pode ser efectuada com base em características próprias do individuo como a impressão digital, a geometria da mão, o reconhecimento facial, a leitura da retina, entre outras.

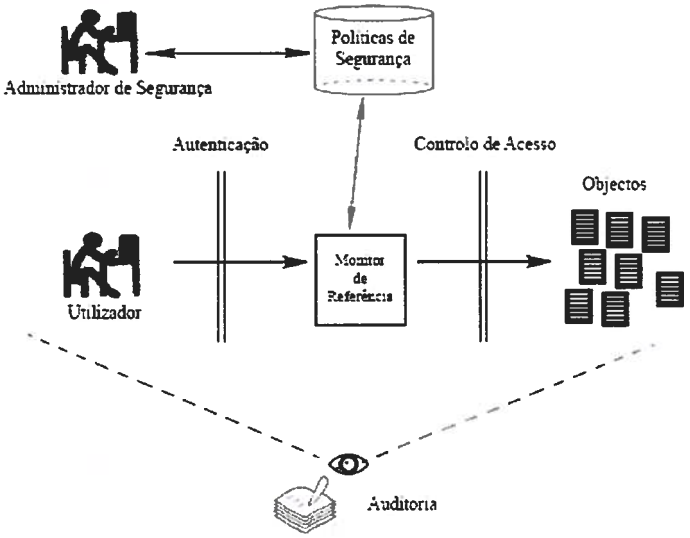
Após o processo de autenticação o sistema vai verificar através de uma matriz de controlo de acesso se o utilizador tem autorização de acesso ao recurso solicitado bem como as acções que pretende efectuar sobre esse recurso.

Todas as acções efectuadas pelo utilizador dentro do sistema de informação deverão ser identificadas e gravadas para uma futura responsabilização deste.

Segundo Harris (2013), uma política de segurança providencia objectivos abstractos e o modelo de segurança providencia o que se pode e o que não se pode fazer para atingir esses objectivos.

A especificação e aplicação de uma ou um conjunto de políticas de segurança representam um modelo de segurança no qual o monitor de acessos tem um papel fundamental no sentido de definir quais os utilizadores tem acesso e quais os recursos que podem ser acedidos (Marques, Ferreira, Ribeiro, Veiga, & Rodrigues, 2012).

O modelo de controlo de acesso é composto por processos de autenticação autorização e auditoria: o processo de autenticação determina se o utilizador tem permissões para aceder ao sistema; a autorização de permitir ou negar o acesso ao objecto solicitado pelo utilizador ocorre após consulta da base de dados das políticas de autorização pelo monitor de acessos. O controlo de acesso deve ser finalizado com um controlo de auditoria, de forma a registar toda a actividade efectuada pelo utilizador efectuada dentro do sistema para posterior análise.



Fonte adaptada: (Sandhu & Samarati, 1994)

Figura 5 - Processos do Controlo de acesso

As três principais técnicas de controlo de acessos são: *Discretionary Access Control* (DAC), *Mandatory Access Controls* (MAC) e *Role-based Access Control* (RBAC) (Sandhu & Samarati, 1994).

O controlo de acesso discricionário (DAC) baseia-se na ideia de que o proprietário do objecto é que deve determinar quem tem acesso a este. Este controlo de acesso permite que os objectos sejam livremente copiados de um objecto para outro, e por isso o acesso ao objecto original é negado, mas o acesso a uma cópia do objecto pode ser obtida. Num controlo de acesso discricionário todos os objectos têm de ter um proprietário.

No controlo de acesso mandatório (MAC), o controlo de acesso é determinado pelo administrador do sistema e não pelo proprietário do objecto como no DAC. Utilizado no acesso a objectos altamente sensíveis e confidenciais é normalmente aplicado em organizações governamentais e militares.

No controlo de acesso baseado em *roles* (RBAC) as permissões de acesso e direito sobre os objectos são atribuídos nas *roles* nas quais os utilizadores estão autorizados. Os utilizadores podem obter permissão sobre uma ou mais *roles*.

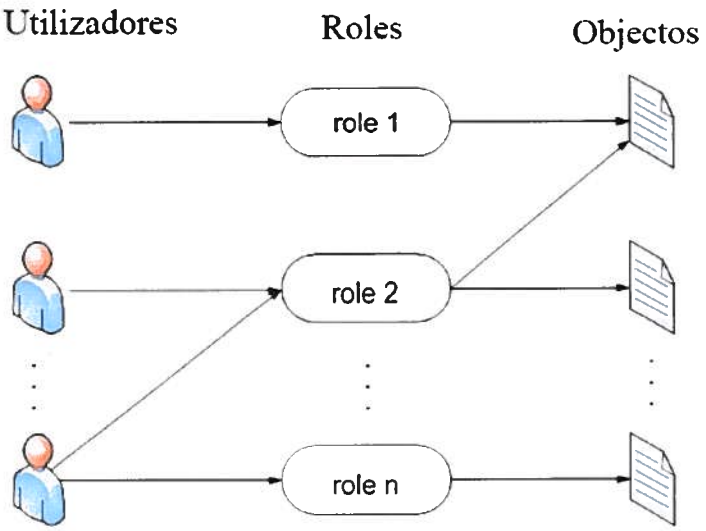


Figura 6 - Controlo de acesso baseado em roles

Um modelo matriz de controlo de acesso proposto por Lampson (1971), é representado por três componentes principais: um conjunto de objectos passivos, um conjunto de sujeitos activos que podem manipular os objectos e um conjunto de regras que rege a manipulação dos objectos pelos sujeitos representados por uma matriz.

	Domain 1	Domain 2	Domain 3	File 1	File 2	Process 1
Domain 1	*owner control	*owner control	*call	*owner *read *write		
Domain 2			call	*read	write	wakeup
Domain 3			owner control	read	*owner	

Fonte adaptada: http://research.microsoft.com/en-us/um/people/blampson/08-Protection/Acrobat.pdf

Figura 7 - Matriz de Controlo de Acesso

Neste modelo proposto por Lampson e reformulado por Harrison, os objectos são tipicamente arquivos, terminais, dispositivos e estações de trabalho, implementados num sistema de informação. Os sujeitos são representados por entidades que podem ou não ter direitos e acesso sobre os objectos. É importante referir que cada sujeito pode ser um objecto e assim também pode ser lido ou manipulado por outro sujeito. A matriz de acesso é representada por uma matriz rectangular com uma linha por sujeito e uma coluna por objecto. O cruzamento de uma linha com uma coluna indica o modo de acesso e correspondente acção entre o sujeito e objecto permitida pelo sistema (Harrison, Ruzzo, & Ullman, 1976).

A sua implementação não é feita directamente através da matriz, pois esta é esparsa, contudo, esta deve ter em consideração duas implementações clássicas do sistema de autorização: listas de controlo de acesso (ACL) e capacidades (Marques, Ferreira, Ribeiro, Veiga, & Rodrigues, 2012).

Uma ACL é uma lista de permissões para um arquivo, pasta ou outro objecto na qual é definido o que os utilizadores ou grupos podem fazer e as operações que podem efectuar quando acedem ao objecto solicitado. Se um determinado utilizador com permissões apenas de leitura pretender modificar um determinado objecto esse pedido ser-lhe-á negado. Uma ACL fornece um método simples de gerenciamento de permissões de arquivos e pastas sendo usados pela maioria dos sistemas operativos.

Numa lista de capacidades (CL) são definidas as actividades que um utilizador pode efectuar num dado objecto. Uma das características principais é a delegação que tem como objectivo permitir que um utilizador proprietário de um objecto possa delegar totalmente ou parcialmente as suas permissões, no entanto a revogação das delegações pode ser um processo complicado sendo difícil determinar se uma capacidade delegada por dois

caminhos distintos deve ser revogada ou não (Marques, Ferreira, Ribeiro, Veiga, & Rodrigues, 2012).

2.3. Modelos clássicos de segurança

Os primeiros modelos de segurança tiveram início na década de setenta e assentavam no fundamento da confidencialidade e integridade da informação.

O modelo Bell-La Padula formulado por David Elliott Bell e Leonard J. Lapadula, em 1976, para controlo de acesso a informação militar é centrado em políticas de confidencialidade. Consistia num modelo matemático formal de transições de estados finitos seguros que pode ser resumido em dois axiomas: nenhum utilizador pode ler as informações classificadas de níveis mais elevados (não ler para cima) e nenhum utilizador pode baixar a classificação das informações (não escrever para baixo) (Landwehr, 1981).

O modelo Biba[6] formulado em 1977, por Kenneth Biba, é um modelo formal de transição de estado para políticas de segurança de computador, no qual são definidas um conjunto de regras de controlo de acesso destinadas a assegurar a integridade da informação. Este modelo utiliza agrupamentos de dados e sujeitos em níveis ordenados de integridade, de modo a que um utilizador não possa corromper objectos de um nível superior ao seu, ou ser corrompido por objectos de um nível inferior.

O modelo de Clark e Wilson, descrito por David D. Clark e David R. Wilson, em 1987, pretendeu modelar os requisitos de integridade das organizações militares para organizações comerciais, em que a integridade da informação devia ser garantida em qualquer nível de classificação (Clark & Wilson, 1987).

O modelo de Brewer-Nash, também conhecido como Muralha da China (*Chinese Wall*), formulado, em 1989, por David Brewer e Michael Nash, foi projectado para gerir o conflito de interesses de organizações comerciais e financeiras e manter a sua confidencialidade das informações dos mesmos. Esta política em conjunto com outras medidas e técnicas, restrige o fluxo de informações impossibilitando que dois utilizadores com o mesmo nível de acesso possam dispor da mesma informação (Festa, 2013).

[6] http://pt.wikipedia.org/wiki/Modelo_Biba acedido em 11 de Maio de 2014

2.4. Normas Padrão

As normas ISO/IEC são publicações efectuadas em conjunto por duas organizações, a Organização Internacional para Padronização (ISO) e pela Comissão Electrotécnica Internacional (IEC), no sentido de publicar normas padrão universalmente aceites nas mais diversas actividades tecnológicas comerciais e científicas.

2.4.1. ISO/IEC 27002:2013

A ISO/IEC 27002:2013, parte da família de normas da ISO 27000 (ISO27k), é a norma padrão da segurança da informação publicada pela ISO/IEC, designada "A tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação".

A ISO27k pretende fornecer as melhores práticas e recomendações sobre gestão de segurança da informação, de riscos e controlos, no contexto de uma estratégia global dos sistemas de gestão de segurança da informação aplicável a todo o tipo de organização independentemente do seu tamanho e fins.

Fonte adaptada: http://www.iso27001security.com/html/timeline.html

Figura 8 - Linha do Tempo da ISO27K

A ISO27k teve início na década de oitenta e desde então tem vindo a reportar as melhores práticas na segurança dos SI, dos quais se destacam as seguintes normas: BS7799, BS7799-2, ISO/IEC 17799, ISO/IEC 27001 e ISO/IEC 27002.

O BS7799 (British Standard 7799) publicado inicialmente em 1995, pelo BSI Group (*British Standards Institute Group*) e escrito pelo Departamento de Industria e Comércio do Governo do Reino Unido, descrevia as melhores práticas[7] a serem utilizadas na gestão da segurança de informação.

Em 1998, foi publicado o BS7799-2 intitulado "*Information Security Management Systems - Specification with guidance for use*" para criar as directivas de como aplicar e implementar a norma BS7799 e manter um sistema de gestão da segurança de informação seguro. Com a publicação da norma BS7799-2, o BS7799 foi renomeado para BS7799-1.

Em 2000, foi publicada a norma ISO/IEC 17799 designada "Tecnologia da Informação - Código de prática para gerenciamento da segurança de informação" que era uma cópia da norma BS7799-1, entretanto actualizada em 1999. Aprovada pela ISO/IEC, esta norma podia ser considerada como um guia prático no desenvolvimento dos procedimentos da segurança de informação a aplicar numa organização.

Em 2005, a norma BS7799-2 foi adaptada pelo ISO como ISO/IEC 27001[8] e posteriormente revista em 2013 vem especificar os requisitos necessários para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação no contexto da organização. Nele constam os requisitos necessários para a avaliação e tratamento de riscos de segurança da informação à medida das necessidades da organização. Os requisitos estabelecidos na ISO/IEC 27001:2013 são genéricos e pretende-se que sejam aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

Em 2007, a norma ISO/IEC 17799 foi renomeada para ISO/IEC 27002 de forma a inclui-la na família de normas ISO27k, mantendo na íntegra o seu conteúdo após a sua revisão, em 2005.

ISO/IEC 27002:2013[9] de tecnologia da informação - Técnicas de segurança - Código de prática para os cento e quarenta e quatro controlos de segurança da informação onde são recomendados controlos com objectivos decorrentes de riscos para a confidencialidade, integridade e disponibilidade da informação.

---

[7] Os princípios gerais de modo a implementar, manter e actualizar a gestão de segurança da informação de uma organização.

[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en acedido em 11 de Maio de 2014

[9] https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en acedido em 11 de Maio de 2014

Dos vinte capítulos que compõem esta norma, catorze são específicos de objectivos de controlo. Nestes catorze capítulos são especificados trinta e cinco objectivos de controlo genéricos no gerenciamento da segurança da informação de uma organização da seguinte forma.

No quinto capítulo é identificado um único objectivo abordando a necessidade de fornecer orientação e suporte para gestão de segurança da informação de acordo com os requisitos de negócio e leis e regulamentos pertinentes.

O sexto capítulo identifica dois objectivos nomeadamente o estabelecimento de uma estrutura de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro de uma organização e garantir a segurança do teletrabalho e a utilização de dispositivos móveis.

O sétimo capítulo repartido por três objectivos, pretende garantir que os funcionários e prestadores de serviços contratados compreendam as suas responsabilidades e se estas são adequadas para as funções para as quais são consideradas, estejam cientes com a sua responsabilidade para com a segurança da informação e que os interesses da organização, como parte do processo de mudança ou cessação de emprego ficam protegidos.

No oitavo capítulo composto por três objectivos, pretende identificar todos os activos da organização e definir responsabilidades de protecção adequadas, garantir que a informação recebe um nível adequado de protecção de acordo com sua importância para o contexto da organização e impedir a divulgação não autorizada de informações armazenadas em mídia em situações em que esta é modificada, removida ou destruída.

No nono capítulo são identificados quatro objectivos fundamentais para o controlo de acesso, uma política de controlo de acesso deve ser estabelecida de modo a garantir o acesso de utilizadores autorizados e prevenir acesso não autorizado a sistemas e serviços, os utilizadores deverão ser responsáveis por salvaguardar a sua informação de autenticação no qual o acesso não autorizado a sistemas e aplicações não deve ser autorizado.

O objectivo descrito no décimo capítulo pretende assegurar uma utilização adequada e eficaz de técnicas criptográficas de modo a manter os princípios fundamentais da informação: confidencialidade, autenticidade e integridade.

O décimo primeiro capítulo identifica dois objectivos. O primeiro para impedir o acesso físico não autorizado, danos e interferências na informação da organização e o segundo, para evitar a perda, dano, roubo ou comprometimento de activos que interrompam as operações de uma organização.

O décimo segundo capítulo composto por sete objectivos pretende garantir operações realizadas nas instalações de processamento de informação sejam correctas e seguras, garantir que as instalações de processamento de informação e a própria informação sejam protegidas contra *software* malicioso, proceder à protecção da organização contra a perda de dados, registo dos eventos ocorridos, garantir a integridade dos sistemas operacionais, impedir a exploração de vulnerabilidades técnicas e minimizar o impacto das actividades de auditoria nos sistemas operacionais.

Os dois objectivos identificados no décimo terceiro capítulo pretendem garantir a protecção das informações na rede e a manutenção da segurança das informações transferidas de uma organização para outra qualquer entidade externa.

No décimo quatro capítulo são descriminados três objectivos relacionados com a necessidade de: garantir que a segurança da informação é projectada e implementada no âmbito do desenvolvimento do ciclo de vida dos SI; garantir a protecção dos dados utilizados para testes e garantir a protecção dos activos da organização quando acessível por fornecedores.

O décimo quinto capítulo composto por dois objectivos pretendem manter um nível de segurança da informação e prestação de serviços em linha com o acordado com o fornecedor e garantir uma abordagem coerente e eficaz para a gestão da segurança do SI informação incluindo a comunicação sobre os eventos e falhas de segurança.

No décimo sexto capítulo é identificado o objectivo de garantir uma abordagem efectiva e consistente da gestão da segurança do SI incluindo comunicação dos eventos e falhas de segurança.

O décimo sétimo capítulo é composto por dois objectivos nos quais identificam a necessidade de manter a continuidade das políticas da segurança do SI e sua disponibilidade na expansão de negócios da organização.

O décimo oitavo capítulo identifica os dois últimos objectivos na prevenção da violação das obrigações legais, estatutárias, regulamentares ou contratuais relativas à informação de segurança e seus requisitos e a garantia de que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos da organização.

2.4.2. ISO/IEC 15408:2009

O *National Computer Security Center* (NCSC), um departamento da defesa do governo dos Estados Unidos da América, publicou em 1983, o *Trusted Computer System Evaluation Criteria* (TCSEC)[10] no qual são definidos os requisitos básicos para avaliar a eficácia dos controlos de segurança de computadores construídos num sistema computacional. O TCSEC foi elaborado para avaliar e classificar os sistemas computacionais que estão sendo considerados para o processamento, armazenamento e recuperação de informações sensíveis ou confidenciais.

O TCSEC é especialmente conhecido e designado por *Orange Book*, inicialmente publicado em 1983, pelo Centro Nacional de Segurança Informática (NCSC) e atualizado em 1985, foi substituído pelo padrão internacional *Common Criteria* (CC) publicado originalmente em 2005.

Os seus objectivos e requisitos básicos eram: uma política de segurança explícita e bem definida que deve ser imposta pelo sistema; os controlos de acesso devem ficar associados aos objectos; utilizadores individuais devem ser identificados; as informações de auditoria devem ser mantidas e protegidas selectivamente para que acções que afectam a segurança possam ser atribuídas aos responsáveis; os sistemas informáticos devem conter mecanismos de *hardware* ou *software* que possam ser avaliados de forma independente de modo a fornecer garantia e funcionalidade suficiente de que o sistema impõe os requisitos e mecanismos de confiança anteriores. Estes requisitos devem ser continuamente avaliados de modo a proteger o sistema contra alterações não autorizadas.

No TCSEC são definidos quatro níveis hierárquicos de segurança: A, B, C e D, onde a divisão A tem a maior segurança e D o mínimo de protecção. As divisões A, B e C são ainda divididas em uma série de subdivisões hierárquicas chamadas classes: C1, C2, B1, B2, B3 e A1. Estes níveis de segurança acabariam por ser usados na classificação de sistemas computacionais de acordo com as exigências especificadas nos mesmos.

[10] http://csrc.nist.gov/publications/history/dod85.pdf acedido em 10 de Maio de 2014

O *Information Technology Security Evaluation Criteria* (ITSEC)[11] publicado em 1990, consiste na uniformização da documentação existente em França, na Alemanha, Holanda e Reino Unido para estruturação dos critérios de avaliação do grau de confiança de um sistema computacional.

Posteriormente revisto em 1991 pela Comissão das Comunidades Europeias e validado por outros países, tornou-se a norma padrão europeia para avaliação e certificação dos sistemas computacionais.

Diverge do TCSEC ao separar funcionalidade de garantia na avaliação dos sistemas computacionais e na classificação atribuída aos níveis de segurança (E0 a E6). Pode ser resumido numa implementação de três níveis: objectivos de segurança (porque é que a funcionalidade é desejada?); funções que garantam a segurança (que funcionalidade é efectivamente prestada?) e mecanismos de segurança (como é que a funcionalidade é fornecida?).

O ITSEC em conjunto com o TCSEC foi substituído pelo CC em 1999.

ITSEC		TSCEC
E0	<-->	D
E1	<-->	C1
E2	<-->	C2
E3	<-->	B1
E4	<-->	B2
E5	<-->	B3
E6	<-->	A1

Fonte adaptada: http://www.sogisportal.eu/documents/itsec/itsec-en.pdf

Figura 9 - Correspondência de níveis de segurança do ITSEC e TCSEC

O padrão internacional ISO/IEC 15408 (Tecnologias de Informação - Técnicas de Segurança - Critérios de avaliação da segurança das TI) conhecido como *Common Criteria* (CC) publicado em 1999 é a norma padrão aplicada para a segurança lógica das aplicações e para o desenvolvimento de aplicações seguras definindo um método para avaliação de sistemas computacionais em ambientes seguros.

[11] http://www.sogisportal.eu/documents/itsec/itsec-en.pdf acedido em 10 de Maio de 2014

A primeira parte (ISO/IEC 15408-1) descreve os conceitos e principios gerais do modelo de avaliação. Nesta parte são definidos os termos e estabelecidos os principais objetivos do alvo de avaliação.

A segunda parte (ISO/IEC 15408-2) define os requerimentos funcionais de segurança que serão verificados durante a avaliação. Contem um catálogo de componentes funcionais de segurança pré-definidos que se enquadra na maioria das necessidades de segurança. Estes requerimentos são organizados numa estrutura hierarquica por classes, famílias e componentes.

Na terceira parte (ISO/IEC 15408-3) são definidos os requisitos de garantia que também são organizados numa hierarquia de classes, famílias e componentes. Esta parte descreve os níveis de garantia de avaliação através de uma escala que mede a garantia do alvo de avaliação e que fornece os critérios de avaliação dos sistemas computacionais e os seus diferentes níveis de confiança: EAL1 a EAL 7.

O EAL1 (funcionalmente testado) é aplicado onde é necessária alguma confidencialidade na operação, no entanto as ameaças à segurança não são tidas em conta.

O EAL2 (estruturalmente testado) requer a colaboração do programador na medida em que fornece os dados a respeito da estrutura do programa e dados de testes dos componentes.

O EAL3 (testado e verificado metodicamente) permite ao programador obter a máxima garantia de segurança na fase de desenvolvimento e gestão da configuração.

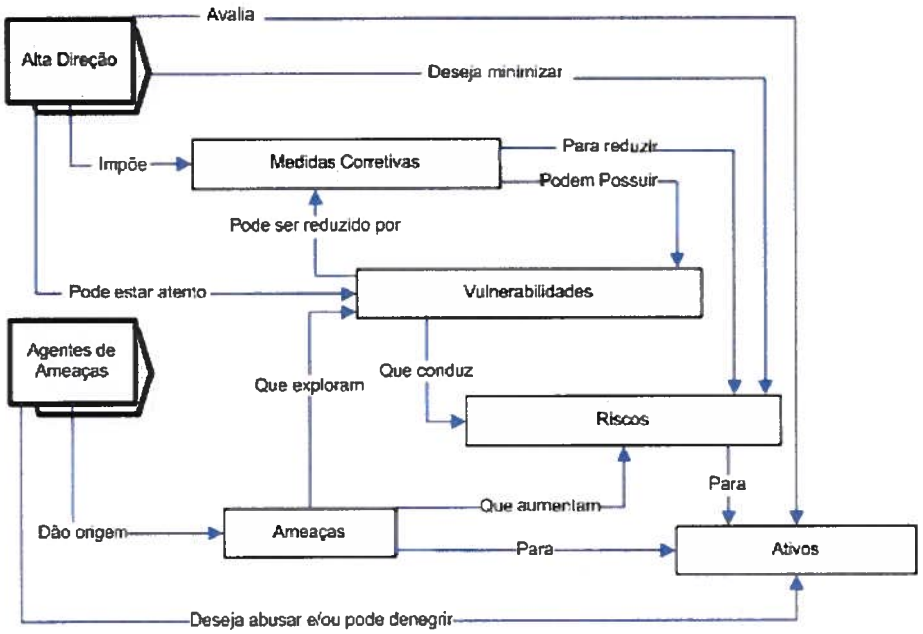
O EAL4 (desenhado, testado e revisto metodicamente) permite ao programador obter a máxima garantia de segurança baseando-se no uso de boas práticas no desenvolvimento do sistema, que apesar de rigorosas, não requerem um conhecimento substancial nem habilidades especiais.

O EAL5 (desenhado e testado semi-formalmente) permite ao programador obter a máxima garantia de segurança baseando-se em rigorosas praticas de desenvolvimento de um sistema suportado por uma aplicação moderada de técnicas de engenharia de segurança especializada. Deve mostrar a correspondência entre os requisitos de segurança e os componentes do programa.

O EAL6 (desenhado e testado de forma verificada e semi-formal) permite ao programador obter elevada garantia nas aplicações das técnicas de engenharia de segurança para um ambiente de desenvolvimento rigoroso de modo a criar um objetivo de avaliação de topo de forma a proteger activos de valor elevado contra riscos significativos.

O EAL7 (desenho e testes formalmente verificados) é aplicável ao desenvolvimento de um objetivo de avaliação para aplicações em situações de extremo alto risco onde o elevado valor dos activos justifica os elevados custos.

Assim, os fornecedores de produtos poderão seguir estes padrões na construção de produtos que vão passar pelo processo de avaliação tal como os avaliadores desses produtos seguem estes padrões ao realizar os mesmos processos de avaliação.



Fonte: http://eciti.wordpress.com/2012/07/02/iso-15-408-e-ciencia-da-informacao

Figura 10 - Conceitos de Avaliação e suas relações na norma ISO/IEC 15408

Diferente da norma ISO/IEC 27002 que pretende abordar a segurança da informação num contexto organizacional a norma ISO/IEC 15408 define e avalia os requisitos de segurança de sistemas computacionais em ambientes seguros.

Neste capítulo deste projecto pretendeu-se identificar os princípios da segurança informática, as suas políticas e a sua aplicação em modelos segurança de modo a combater as principais ameaças da segurança informática.

II - Contextualização

Com o crescente uso de computadores e outros dispositivos digitais nas mais diversas áreas de negócio foram criadas as condições ideais para o desenvolvimento de *software* malicioso capaz de roubar ou destruir dados de uma organização.

Segundo *Kaspersky Security Bulletin 2013*, as principais motivações dos atacantes, na utilização de programas maliciosos para penetrar na rede de uma organização, devem-se ao roubo da informação valiosa, segredos comerciais, dados de funcionários e clientes, e monitorização das actividades desta.

Os atacantes têm interesse em roubar informações de todos os tipos, desde tecnologias de ponta desenvolvida por empresas e institutos de pesquisa, códigos-fonte de produtos de *software*, documentos legais e financeiros, informações pessoais sobre funcionários e clientes, ou qualquer outra informação que possa constituir um segredo comercial. Esta informação é muitas vezes armazenada em texto simples nas redes organizacionais na forma de documentos eletrónicos, documentos de rascunho, relatórios, desenhos, apresentações, imagens, entre outras.

Outro alvo dos atacantes são as organizações bem sucedidas e sites com elevado número de acessos. Neste tipo de ataques os utilizadores legítimos são direccionados para sites maliciosos semelhantes ao original ou através de banners de publicidade maliciosa, que podem causar danos significativos à reputação de uma organização aos olhos de seus clientes.

Um dos métodos mais popular de causar danos directos numa organização é, submetendo-a a um ataque DDoS. Um ataque deste tipo pode resultar num site fora de serviço durante vários dias, impedindo os clientes e potenciais clientes de ter acesso aos serviços disponibilizados pela organização, fazendo-os procurar organizações alternativas.

Actualmente os cibercriminosos têm ao seu dispôr uma grande variedade de ferramentas sofisticadas para ajudá-los a corromper uma rede organizacional. O planeamento de um ataque direccionado a uma empresa pode levar vários meses. Os atacantes estudam meticulosamente o perfil comercial da organização, os recursos públicos, sites, perfis de funcionários em redes sociais, comunicados e os resultados de várias apresentações, exposições, bem como qualquer tipo informação que lhes seja útil. Enquanto

planeiam o ataque, os cibercriminosos podem criar um falso *site* malicioso, que se traduz numa cópia exacta do original, registando-o com um nome de domínio semelhante, que será utilizado para enganar utilizadores que pretendam aceder ao *website* da empresa atacada e desta forma infectar os seus computadores.

Em 2013, uma das técnicas mais populares para a introdução de *software* malicioso numa organização foi o envio de *e-mails* com anexos maliciosos para os funcionários da organização. Na maioria das vezes, os documentos anexos a esses *e-mails* eram em formatos familiares como documentos word, excel ou pdf. Quando o arquivo anexado é aberto, caso haja vulnerabilidade do *software*, o sistema é infectado por um programa mal-intencionado.

Outra técnica usada activamente nos ataques são os *exploits*, baseados na exploração das vulnerabilidades de *software* mais conhecidas. Uma extensa rede de ciberespionagem com o nome de código Outubro Vermelho, utilizou pelo menos três *exploits* diferentes na exploração das vulnerabilidades conhecidas do *Microsoft Office*: CVE-2009-3129 (*MS Excel*), CVE-2010-3333 (*MS Word*) e CVE-2012-0158 (*MS Word*).

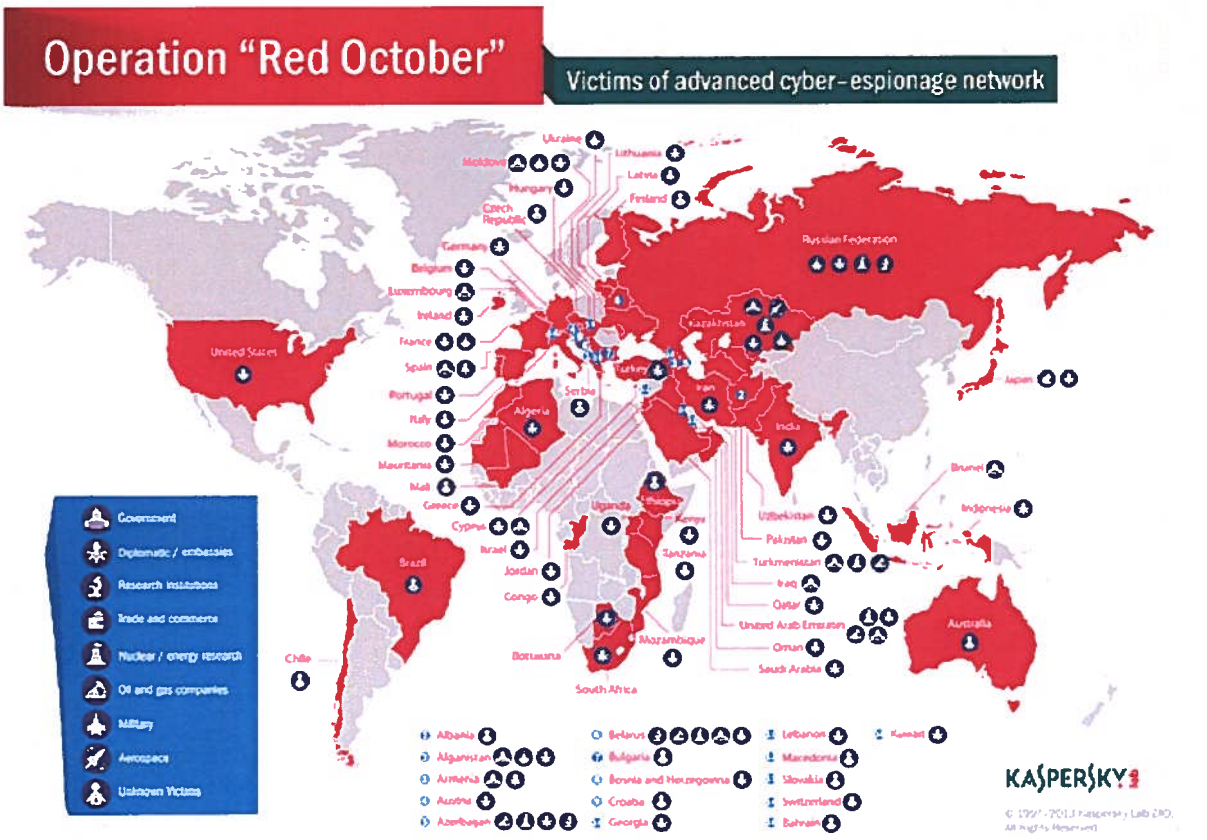


Figura 11- Operação Outubro Vermelho

O *NetTraveler* usou um *exploit* de CVE-2013-2465, que é uma vulnerabilidade das versões Java 5, 6 e 7 que só foi corrigida pela *Oracle* em Junho de 2013.

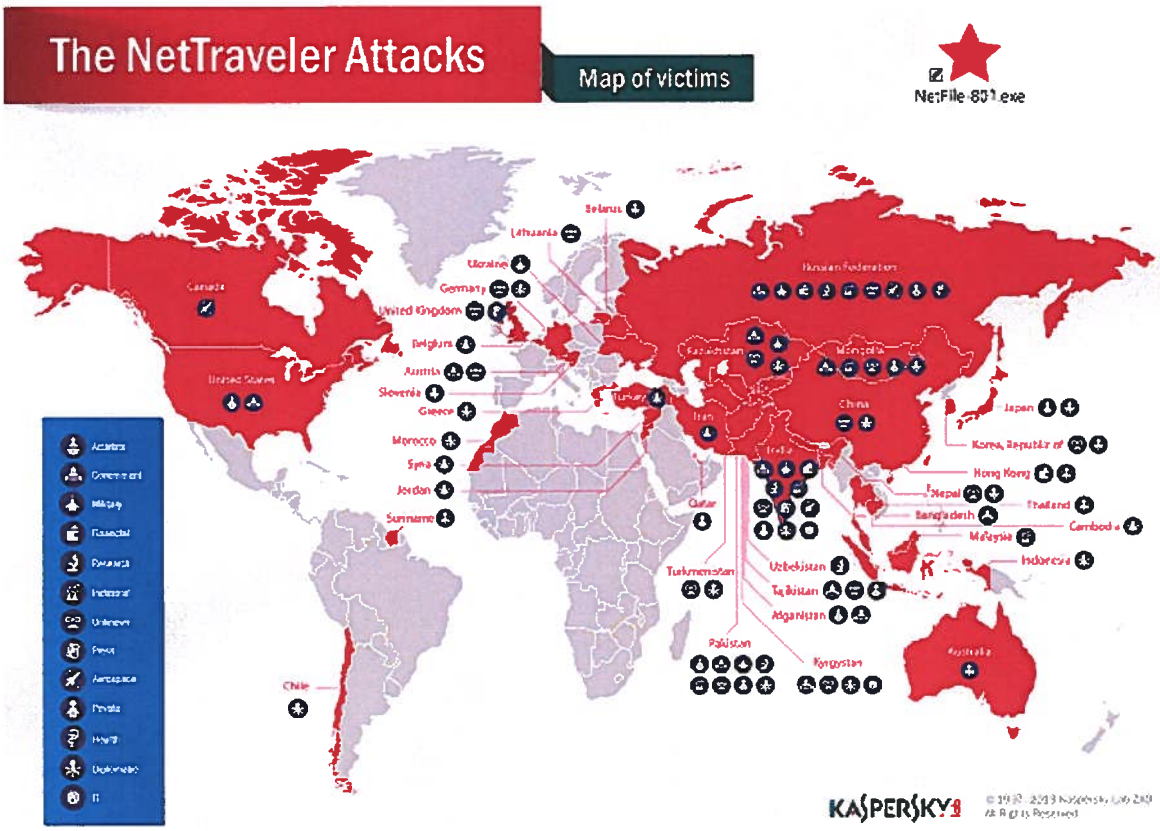


Figura 12 - Ataque *NetTraveler*

No entanto, as vulnerabilidades mais perigosas são as chamadas *zero-day*, actualmente desconhecidas para o fabricante do *software*, os cibercriminosos procuram continuamente vulnerabilidades de *software* conhecido para criar *exploits*.

De acordo com dados do *Kaspersky Security Network*, em 2013 os produtos da *Kaspersky Lab* neutralizaram 5.188.740.554 ciberataques em computadores de utilizadores e dispositivos móveis e 1.700.870.654 ataques lançados a partir de recursos on-line localizados em todo o mundo, detectaram 104.427 novas modificações de programas maliciosos para dispositivos móveis e quase três bilhões de ataques de *malware* nos computadores dos utilizadores. Nestes ataques detectaram-se um total de 1,8 milhões de programas maliciosos e potencialmente indesejados.

III - Ameaças à Segurança Informática

Os primeiros ataques surgiram sob a forma de vírus, que ao longo dos anos têm aumentado exponencialmente a sua capacidade de destruição, mas não foram os únicos, Cavalos de Tróia, *Worms*, *Spyware*, entre outros, tornaram-se ameaças à segurança informática.

Segundo Stallings (2011), as principais ameaças à Segurança Informática, poderão ser concretizadas através de ataques passivos ou activos.

Os ataques passivos tentar fazer uso das informações do sistema, sem alterar qualquer tipo de informação, nem afectar qualquer recurso do sistema, têm como natureza escutar e monitorizar transmissões.

Os ataques activos pretendem intervir no normal fluxo da informação, alterando os conteúdos da mesma e afectando recursos e o correcto funcionamento dos SI.

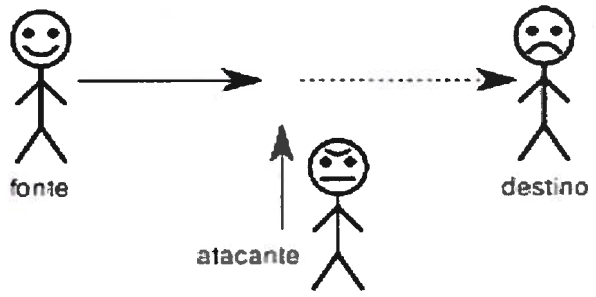
Para Pfleeger & Pfleeger (2006), as ameaças poderão ser representadas por quatro tipos de ataque: intercepção, interrupção, modificação e fabricação, na exploração das vulnerabilidades do sistema de informação.

Os ataques de intercepção podem ser considerados como ataques à confidencialidade de um sistema. Este ocorre quando um atacante obtém acesso indevido a informação do sistema de informação.

Fonte: http://pt.scribd.com/doc/65807740/Arquitetura-S-O-5

Figura 13 - Ataque básico com Interceptação

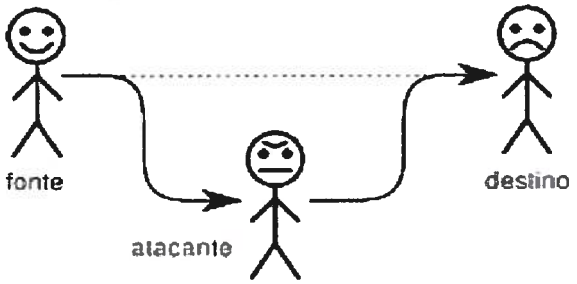
Os ataques de interrupção podem ser considerados como ataques à disponibilidade de um sistema. Estes ocorrem quando um atacante consegue interromper o normal fluxo de informações.



Fonte: http://pt.scribd.com/doc/65807740/Arquitetura-S-O-5

Figura 14 - Ataque básico por Interrupção

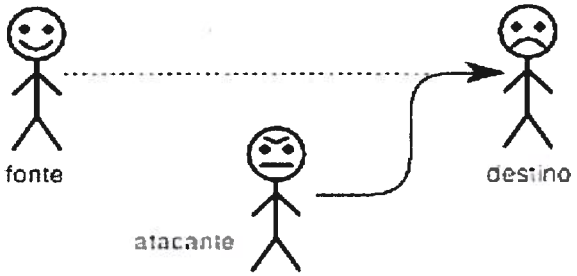
Os ataques de modificação podem ser considerados como ataques à integridade de um sistema. Ocorrem quando um atacante consegue modificar o conteúdo de uma informação.



Fonte: http://pt.scribd.com/doc/65807740/Arquitetura-S-O-5

Figura 15 - Ataque básico por Modificação

Os ataques de fabricação podem ser considerados como ataques à autenticidade de um sistema. Ocorrem quando um atacante consegue introduzir falsas informações num sistema de informação.



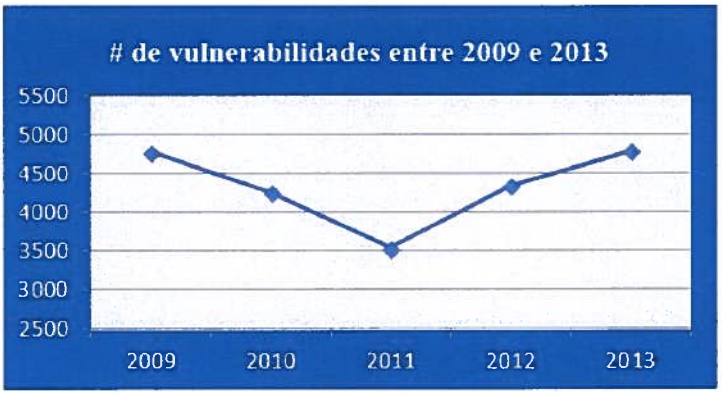
Fonte: http://pt.scribd.com/doc/65807740/Arquitetura-S-O-5

Figura 16 - Ataque básico por Fabricação

Os ataques tendem a aproveitar as vulnerabilidades de *hardware* ou *software,* de modo a permitir que um atacante comprometa a segurança desse SI, através de deficientes concepções ou deficiências acidentais dos produtos.

Segundo Florian (2014), o número de vulnerabilidades de segurança reportadas em 2013 continuou a aumentar em comparação com 2012. Em média em 2013, foram relatadas treze novas vulnerabilidades por dia, para um total de quatro mil setecentos e noventa e quatro vulnerabilidades de segurança, o valor mais elevado nos últimos cinco anos.

Ano	# de vulnerabilidades
2009	4783
2010	4258
2011	3532
2012	4347
2013	4794

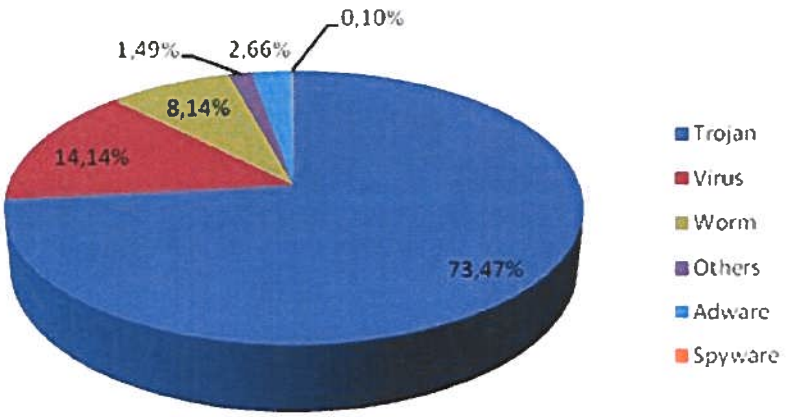


Fonte adaptada: http://www.gfi.com/blog/report-most-vulnerable-operating-systems-and-applications-in-2013/

Figura 17 - Evolução das vulnerabilidades de segurança reportadas nos últimos cinco anos

3.1. *Software* Malicioso

A ameaça surge quando pessoas mal-intencionadas conseguem instalar *software* malicioso sem autorização da organização, dos quais se destacam: *Trojans*, Vírus, *Worms*, Cavalos de Tróia e *spyware*.



Fonte: http://www.pandasecurity.com/angola/homeusers/media/press-releases/viewnews?noticia=10474

Figura 18 - Distribuição dos principais tipos de ataque por *software* malicioso

Os mais frequentes os Cavalos de Tróia também designados *Trojan* ou *Trojan Horses* são ainda conhecidos como *Backdoors* (porta dos fundos). São programas que simulam programas autênticos, mas contém código oculto criado com o intuito de aceder às credenciais de um utilizar legítimo deforma a controlar, explorar e danificar o computador da vítima. Se o ataque for bem-sucedido esta porta dos fundos permite o acesso do atacante a um sistema protegido, originando o comprometimento de informações confidenciais ou pessoais. Este tipo de *malware* permite ainda outras actividades ilícitas como a monitorização de todo o SI bem como a corrupção e desactivação de recursos do sistema. Estes programas são usualmente distribuídos aos utilizadores da rede através de mensagens de e-mail que se afiguram como ferramentas legítimas.

Os vírus são programas que se anexam a outros programas para infectar e executar acções indesejadas como danificar e eliminar dados num computador. Alguns vírus são de fácil detecção e remoção, mas outros poderão ser mais avançados através da utilização de mecanismos polimórficos, prolongando assim a infecção do sistema e evitando a sua detecção. Para um vírus se propagar necessita da acção do utilizador para executar a aplicação ou script infectado. Por regra, um utilizador não se apercebe da instalação de um vírus que ocorre na execução de uma aplicação tida como legítima.

Semelhante a um vírus, os *Worms* são programas capazes de se propagarem automaticamente através de uma rede, enviando cópias de si mesmo para outros computadores. Propagam-se através da sua grande capacidade de se replicar explorando as vulnerabilidades do *software* instalado sem necessidade de uma acção do utilizador. Por regra, este tipo de *malware* não infecta nem corrompe os ficheiros, no entanto consegue consumir inúmeros recursos de uma rede degradando-a com o passar do tempo.

O S*pyware* é uma categoria de *software* que se pode instalar no computador sem o conhecimento ou consentimento do utilizador legítimo. O S*pyware* pode não apresentar sintomas após infectar o seu computador. Permite ao atacante monitorizar o comportamento online, identificando as páginas de Internet (URL) acedidas, endereços de e-mail, número de cartões de crédito e até identificar sequências de teclas pressionadas pelo utilizador. Este *malware* tem ainda capacidade para alterar definições de um computador abrandando o seu normal funcionamento.

Sendo estes os mais vulgarmente referenciados, existem outros com os mesmos intuitos de afectar os SI como é o caso dos *Bot*, *Botnets*, *RootKit Keyloger*, *Screenlogger*, *Adware, Exploits*, entre outros[12].

3.2. Negação de Serviço

Os ataques por negação de serviço são uma tentativa de impedir que utilizadores legítimos de uma rede ou serviço, sejam privados da sua utilização. Quando este ataque é efectuado apenas por um único hospedeiro, podemos classifica-lo como um ataque de negação de serviço (DoS).Quando o ataque negação de serviço é distribuído (DDoS), a ameaça torna-se mais grave, pois neste caso o ataque é feito através do recrutamento de inúmeros hospedeiros por toda a internet, de forma a coordenar um ataque a um determinado alvo (Stallings, 2011).

3.2.1. Ataques típicos de DoS

O *Smurf* e o *Fragle* são típicos ataques de negação de serviço e ocorrem quando o *ping* (uma ferramenta de *software* disponível na maioria dos sistemas operativos) é executado com o intuito de testar a conectividade de um computador específico. Quando a ferramenta de *ping* é executada, um pacote de solicitação de eco do ICMP (*Internet Control Message Protocol*) é enviado ao computador de destino. Se o computador de destino receber o pacote do TCP (*Transmission Control Protocol*), ele responderá para confirmar a solicitação de ping. No caso de um ataque de negação de serviços *Smurf*, o endereço IP (*Internet Protocol*) de retorno do pacote do ping é forjado com o IP do computador de destino. 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 é chamado *Smurf*[13].

O conceito do ataque *Fraggle* é semelhante ao *Smurf*, mas é efectuado com pedidos de solicitações através do protocolo UDP (*User Datagram Protocol*).

---

[12] http://pt.wikipedia.org/wiki/Malware acedido em 01 de Maio de 2014

[13] http://pt.norton.com/security_response/glossary/define.jsp?letter=s&word=smurf-dos-attack acedido em 01 de Dezembro de 2013

O *ping of death* é uma forma de ataque que consiste no envio de um pacote de informação com um tamanho superior a 65.535 *bytes* (acima do suportado pelo protocolo TCP/IP[14]) em pequenos fragmentos de informação, de tamanho inferior ao suportado, de forma a enganar o computador que os recebe e bloqueando-o quando procede à montagem desses fragmentos.

O ataque por SYN flood utiliza o *3-Way handshake*[15] para sobrecarregar a máquina da vítima com solicitações (SYN) de reconhecimento (ACK) em aberto, através de dois métodos distintos. Numa das hipóteses, é enviado um SYN através de um endereço de IP falso para que quando a vítima devolve o SYN-ACK não obtenha resposta. Na outra hipótese, o atacante envia o SYN com o verdadeiro IP, mas opta por não enviar o ACK. Ambas as situações deixam inúmeros pedidos em aberto causando o congestionamento e consequente bloqueio da máquina vitima do ataque.

3.3. Mensagem de Correio Electrónico Não Solicitado (*SPAM*)

Entende-se por SPAM todas as mensagens de correio electrónico enviadas por remetentes desconhecidos para um grande número de destinatários sem o consentimento destes. Normalmente o SPAM consiste no envio de publicidade não solicitada e informação sem qualquer conteúdo de interesse, que por vezes podem conter *links* para propagação de *software* malicioso.

3.3.1. *Phising*

Um ataque por *phising* é um tipo de fraude electrónica, que consiste através no envio de uma mensagem de correio electrónico, com o objectivo de encaminhar um utilizador para uma página de internet fictícia semelhante à real, de forma a obter informação sensível ou confidencial como palavras-chave ou números de cartões de crédito permitindo deste modo através da informação recolhida praticar burlas em nome da vítima (Magalhães & Grilo, 2006).

De forma a combater este tipo de fraude, cada vez mais se recorre a técnicas sofisticadas e difíceis de detectar. A *Kaspersky Lab*[16] recomenda: não abrir anexos ou *links* se o remetente não for totalmente seguro e em nenhum caso abrir e-mails da pasta de

[14] http://www.ietf.org/rfc/rfc791.txt acedido em 08 de Dezembro 2014
[15] É um processo de reconhecimento entre duas máquinas de forma a estabelecerem uma comunicação.
[16] Empresa de *software* de segurança para as Tecnologias de Informação

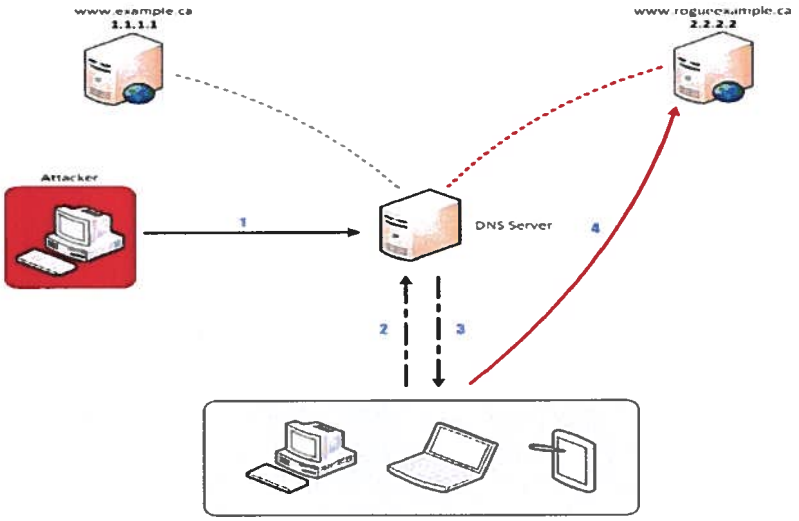
"correio não solicitado[17]"; ter especial atenção quando iniciar uma sessão com um utilizador com permissões de administrador; escolher uma palavra-chave forte para diminuir a hipotese de esta ser capturada pelos atacantes; proceder à instalação *software* antivírus devidamente actualizado e, sobretudo muito senso comum sempre que navegar na Internet[18].

3.4. *Man-in-the Middle*

Um ataque *Man-in-the Middle* ocorre quando um indivíduo que se coloca à "escuta" com o intuito de interceptar mensagens trocadas por utilizadores legítimos. Quando este ataque é bem-sucedido, permitirá ao atacante alterar e bloquear partes da informação trocadas entre os dois utilizadores legítimos sem que estes se apercebam que os dados foram alterados.

3.5. Envenenamento cache DNS (*DNS Spoofing*)

O ataque por envenenamento da *cache* do Domain Name Server (DNS) é feito quando o atacante altera a *cache* dos servidores de DNS dos provedores de serviços de internet (ISP). Este tipo de ataque pretende o encaminhamento de pedidos legítimos efectuados pelos utilizadores a determinadas URLs, sejam direccionados para URLs falsas controladas pelo atacante (Olzak, 2006).



Fonte: http://www.cira.ca/knowledge-centre/technology/dnssec/faq/

Figura 19 - DNS *Spoofing*

[17] Correio automaticamente classificado como SPAM pelos provedores de e-mail (Gmail, Hotmail, etc)

[18] http://www.kaspersky.com/pt/about/news/virus/2013/A_maioria_das_pessoas_continua_sem_saber_identificar_uma_mensagem_de_Phishing_ acedido em 07 de Dezembro de 2013

3.6. Ataques por Palavras-Chave

Ataque de Força Bruta (*Brute Force*) - Um ataque de força bruta ocorre quando o atacante tenta adivinhar, por tentativa e erro ou *software*, a palavras-chave de um utilizador legítimo, de forma a obter o acesso autorizado a dados e recursos de uma organização. Quanto maior for a complexidade da palavra-chave melhor.

Ataque de Dicionário – Este tipo de ataque tenta aproveitar o facto da maioria dos utilizadores recorrerem a palavras-chave com palavras existentes no dicionário. Deste modo o atacante pode limitar o universo de procura apenas a palavras de dicionário, permitindo a sua descoberta em poucos minutos.

Nos próximos capítulos serão feitas diversas abordagens das principais políticas de segurança a serem tomadas de forma a proteger os SI das principais ameaças neste capítulo identificadas.

IV - Protecção da informação

As políticas de segurança têm como princípios garantirem a prevenção e protecção de qualquer SI, no qual a preservação da confidencialidade, integridade e disponibilidade destes sistemas garanta também a autenticidade e o não repúdio das comunicações. Esta política de segurança deverá ser dinâmica capaz de se adaptar e acompanhar as novas tecnologias e novas realidades da organização. A formalização de um documento de acesso com indicação das regras e tecnologias disponíveis dentro de uma organização deve estar disponível para todos os utilizadores de forma a proteger os activos de uma organização.

4.1. Protecção Física

A protecção física pretende impedir acessos físicos não autorizados à infraestrutura de rede, prevenindo o roubo ou destruição de equipamentos, obtenção de informação sigilosa, entre outros danos passíveis quando se obtem o acesso físico ao local. Assim a protecção física pode ser dividida da seguinte forma: protecção dos utilizadores e protecção dos equipamentos (Magalhães & Grilo, 2006).

4.1.1. Protecção dos Utilizadores

O sucesso de qualquer organização depende dos seus colaboradores, para isso uma correcta política de recrutamento é essencial na contratação de pessoas idóneas salvaguardando no contrato uma cláusula de confidencialidade.

É necessária uma disponibilização regular de acções de formação aos colaboradores de modo a estes serem informados das políticas e procedimentos de segurança da organização e sensibiliza-los para as ameaças inerentes à segurança da informação de forma a prevenir comportamentos de risco.

Uma rápida execução de medidas disciplinares adequadas de acordo com eventual violação das políticas e procedimentos de segurança ou quebra do dever de sigilo, deve ser tomada de forma a dissuadir outros comportamentos de risco, praticados por outros colaboradores.

4.1.2. Protecção dos Equipamentos

Neste dominio o controlo de acessos é essencial de forma a prevenir o acesso de pessoas não autorizadas a locais com equipamentos e informações sensíveis. Equipamentos

sensíveis como os servidores, deverão estar alojados numa sala fechada e devidamente climatizada acessível apenas por código, cartãoes magnéticos ou sistemas biometricos. Outros equipamentos menos sensíveis deverão ser inventariados e protegidos de forma a minimizar a possibilidade de furto e perda de informação.Um sistema contra incêndios, danos por água e falhas de corrente electica tambem deverá ser tido em conta.

4.2. Protecção Lógica

A informação é disponibilizada por um processo de autenticação, no qual é verificado se o utilizador tem ou não permissão para aceder a esse recurso da rede.

4.2.1. Controlo de Acessos

O controlo de acessos pretende garantir que somente utilizadores autorizados tenham acesso a dados sensíveis. O princípio do menor privilégio exige que haja algum mecanismo para garantir que o acesso só seja concedido de acordo com as necessidades necessárias para execução do seu trabalho, conforme determinado pela política organizacional. Implícitos nessa definição são as capacidades funcionais referidos como "os 4As" (O'Hanley & Tiller, 2014): autenticação, autorização, administração e auditoria.

A Autenticação consiste na verificação da identidade do utilizador com base nas credenciais de acesso à rede. O controlo de acesso através das credenciais *login* e *palavra-chave*, e sistemas biométricos são necessários na validação da identidade do utilizador.

A Autorização consiste na definição dos recursos que o utilizador tem acesso após autenticação no sistema.

A administração consiste na gestão e alteração dos dados da organização, e em garantir a desactivação ou remoção de contas quando estas não são mais necessárias, obrigando à coordenação de um complexo conjunto de tarefas. Entre estas se destacam: determinar que os direitos de acesso para um determinado utilizador sejam os adequados, reunindo aprovações para execução desses direitos; garantir que as políticas da organização não são violadas; certificar que os privilégios existentes ainda são justificados com base numa análise periódica; interagir com os vários sistemas operativos, aplicações, bancos de dados, servidores Web, sistemas de autenticação e assim por diante para realmente criar ou excluir contas e gestão dos níveis de privilégio.

A auditoria verifica as acções realizadas nos primeiros "3As" e se estas foram efectuadas correctamente. Um processo de auditoria eficaz pode identificar falhas de autenticação, anomalias de autorização e acções administrativas que excedem limites predeterminados. Quando estes ocorrem, podem ser gerados alertas de forma a notificar o pessoal responsável das acções correctivas a tomar.

4.2.2. Políticas de criação e utilização de palavras-chave

Um monitor de acessos eficaz deve ter em conta uma boa política quanto à criação e utilização de palavras-chave, nomeadamente quanto a criação e utilização de palavras-chave.

Quanto à criação de palavras-chave deverão ser tidos em conta os seguintes critérios: mínimos de oito caracteres; letras maiúsculas e minúsculas; caracteres especiais e números; evitar a criação de palavras-chave com base em informações pessoais, como: nome do utilizador, nomes de familiares, datas, ou palavras existentes no dicionário; evitar sequências de letras do teclado; obrigatoriedade de renovação da palavra-chave a cada noventa dias, não permitindo a sua substituição por outra anteriormente utilizada; evitar a utilização da mesma palavra-chave para diferentes serviços.

Quanto à utilização de palavras-chave deverão ser seguidos os seguintes princípios: manter a confidencialidade das palavras-chave; no momento da sua digitalização, não permitir a sua visualização por outra pessoa; evitar escrever as palavras-chave em papéis que facilitem a identificação do seu contexto.

4.2.3. Antivírus

Um programa de antivírus actualizado e centralizado pode garantir protecção para a globalidade de *software* malicioso. Este tipo de *software* propaga-se através da Internet, na recepção de e-mails, redes sociais e utilização de programas de mensagens instantâneas. Quando instalado o programa de antivírus, a sua actualização deverá ser feita de forma automática e distribuída simultaneamente a todos os equipamentos suportados. A instalação deste *software* malicioso é também potenciada pelo uso de unidades de armazenamento externas, leitores de áudio e vídeo ou disquetes.

4.3. Protecção do Perímetro

A protecção do perímetro pretende impedir acessos externos e internos não autorizados à rede interna da organização.

4.3.1. *Proxy*

A implementação de um servidor *Proxy* é um importante mecanismo de segurança, semelhante ao funcionamento de uma *firewall*. Permite delimitar uma barreira entre a rede interna e a rede externa ou entre duas redes através da instalação de *software* próprio. Operando na camada de aplicação do Modelo OSI, o servidor *Proxy* permite configurar o acesso de determinados protocolos, HTTP, FTP, SMTP, IMAP, entre outros, à rede.

Os servidores *proxy* permitem melhorar o desempenho da rede gerida ao proceder ao armazenamento (*cache*) das solicitações efectuadas pelos utilizadores na internet, deste modo futuras solicitações já se encontrarão armazenadas no servidor *proxy* diminuído o seu tempo de resposta bem como a largura de banda[19] da rede

4.3.2. *Firewall*

Numa primeira instância podemos considerar a *firewall* como a primeira barreira de segurança na delimitação do perímetro de uma organização.

Independentemente da sua forma de implementação uma *firewall* veio permitir separar diversos segmentos de rede, quer públicos ou privados associando diferentes graus de segurança através de conjuntos de regras diferenciados, que permitem autorizar negar ou descartar a informação direccionada a um segmento de rede de acordo com o sentido de tráfego.

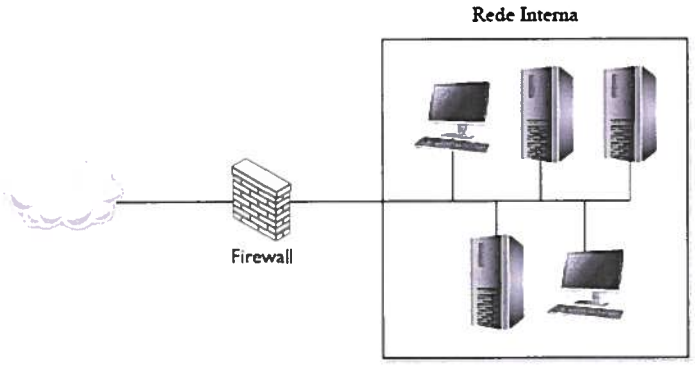
Por regra uma *firewall* corresponde a *software*, podendo ser também uma peça de *hardware*, que tem como principal função a filtragem de pacotes. Sendo esta uma das principais ferramentas de segurança, permite-nos, quando bem configurada, auditar, proteger e controlar todo o tráfego interno e externo num único ponto de uma organização.

[19] Largura de banda é a capacidade de transmissão de dados dentro de uma rede.

4.3.3. Tipologias de *Firewall*

De acordo com as necessidades da organização a implementação de uma *firewall* pode ser realizada com base em três tipos de tipologias: *Dual-Homed Host, Screened Host e Screened Subnet.*

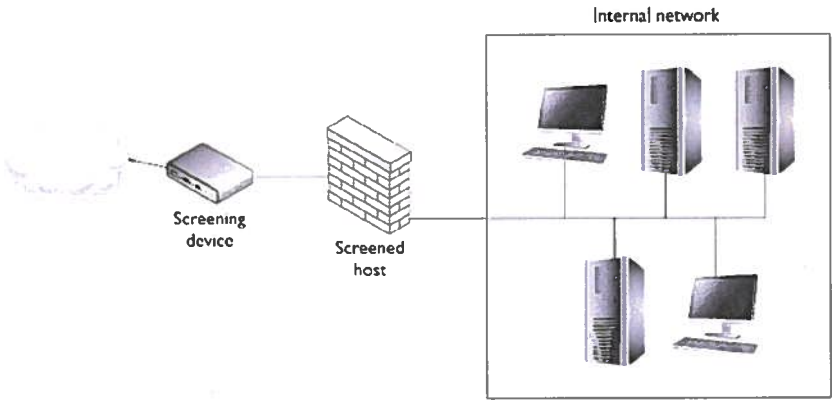
Arquitetura *Dual-Homed Host*, simples e económica, a *firewall* é constituída por uma única máquina (*Bastion host*) com duas ou mais placas de rede, separando a rede interna da rede externa. A desvantagem deste tipo de arquitectura deve-se à grande concentração de tráfego num único ponto de entrada e saída da rede. Uma falha nesta máquina poderá por em risco o tráfego e segurança de uma organização.



Fonte adaptada: http://www.internetsegura.org/nsegura/firewall.asp

Figura 20 - Arquitetura *Dual-Homed Host*

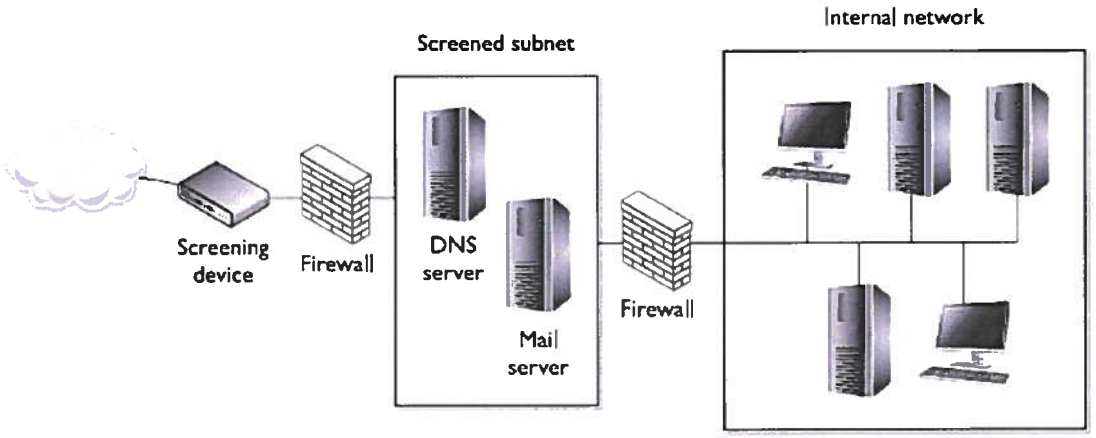
Numa arquitectura *Screened Host* é adicionada uma segunda máquina na separação da rede interna à rede externa. Neste caso uma firewall com funções de *router* para filtragem de pacotes, redireciona o tráfego para um *Bastion Host* que actua entre o *router* e a rede interna fornecendo protecção extra da rede interna.



Fonte: http://www.infowester.com/firewall.php

Figura 21 - Arquitetura *Screened Host*

Numa arquitectura *Screened Subnet* é adicionado um segundo *router* entre a rede interna e um *Bastion Host*, posicionados em conjunto com um primeiro *router* de forma a formar uma sub-rede, denominada DMZ. Com uma arquitectura mais complexa e mais cara, fornece melhor protecção da rede interna, permitindo separar os servidores de internet, de e-*mail*, e DNS da rede interna.



Fonte: http://www.infowester.com/firewall.php

Figura 22 - Arquitetura *Screened Subnet*

4.3.4. Funcionalidades de uma *Firewall*

De acordo com as tipologias referidas, uma *firewall* pode disponibilizar cumulativamente as seguintes funcionalidades: Filtro de Pacotes, Filtro Aplicacional, *DeMilitarized Zone* (DMZ) e *Network Address Translation* (NAT).

Com o filtro de pacotes, o controlo de acesso é efectuado através de um conjunto de regras parametrizáveis com base na análise do conteúdo do pacote IP e com base na informação do cabeçalho deste. Um filtro aplicacional é semelhante ao controlo de acesso efectuado por um *Proxy,* mas configurado na firewall.

Uma DMZ funciona como uma rede de perímetro (ver fig.20), onde os recursos têm endereços IP públicos, para que sejam acedidos através da Internet. Recursos da organização como os servidores de internet, e-mail ou um servidor de nomes de domínio (DNS) são colocados na DMZ, enquanto que os restantes recursos da organização encontram-se escondidos atrás de um *router*. Os recursos nas DMZ podem estar mais expostos a ataques uma vez que se encontram disponiveis para serem acedidos pelos utilizadores na Internet. As portas relativas aos protocolos TCP e UDP dos servidores da DMZ têm que ficar disponíveis para tráfego de entrada e saída (Vacca, 2009).

A conversão de endereços de IP privados para públicos é realizada pelo *Network Address Translation* (NAT) através do mapeamento interno do endereço IP e a porta local do computador, permitdo deste modo que os utilizadores de uma rede interna enviem solicitações e recebam respostas de utilizadores externos à rede.

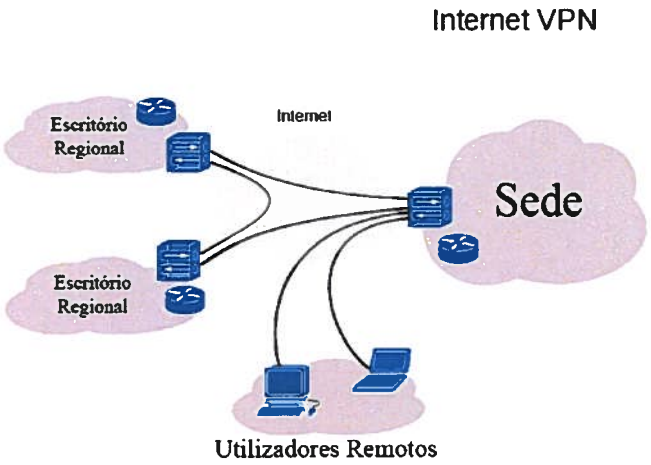
4.3.5. Implementação de uma *Firewall*

A implementação de uma *firewall* deve ter em conta as necessidades de uma organização. Pode ser efectuada com recurso a *software* ou *hardware*, no qual a necessidade de protocolos a suportar, filtro de pacotes estáticos ou dinâmicos[20], qualidade de serviço (QOS)[21] e disponibilidade são factores a considerar. Actualmente existem no mercado várias soluções para implementar um sistema de *firewall*, através do uso de *software* livre ou proprietário ou *hardware*, mais dispendioso neste último caso.

4.3.6. *Virtual Private Network* (VPN)

A utilização de VPN pode ser um factor de grande importância para as organizações, principalmente quanto ao aspecto económico, uma vez que permitem que as conexões físicas dedicadas de longa distância sejam feitas através da rede pública. Uma VPN permite também a substituição das estruturas de conexões remotas, que podem ser eliminadas em função da utilização dos clientes e provedores VPN. Porém, o facto das informações das organizações passarem a trafegar por meio de uma rede pública requer uma série de considerações em relação à segurança. A criptografia associada aos principais protocolos disponíveis (PPTP, L2TP, *Ipsec*) poderá garantir uma comunicação segura entre as organizações por intermédio de túneis virtuais (Nakamura & Geus, 2007).

[20] Filtro de pacotes semelhantes, com controlo de acessos com base em parâmetros de um pacote IP, não controlando o estado da ligação, no caso dos filtros de pacotes estático.
[21] Determina a qualidade de uma conexão com base em quatro parâmetros: largura de banda, atraso, *jitter* e perda (Tanenbaum & Wetherall, 2011).



Fonte adaptada: http://www.infowester.com/firewall.php

Figura 23 - *Virtual Private Network*

Segundo Braun, Günter, Kasumi, & Khalil (1999), a maioria dos fornecedores de soluções de VPN como a IBM ou a Cisco, identificou três cenários possíveis do seu uso no qual uma Intranet de uma organização se conecta com entidades legítimas sobre a Internet.

Uma rede de acesso remoto onde um utilizador no exterior da sua organização pode necessitar de acesso a determinados recursos da sua empresa. Este cenário permitirá ao utilizador remoto trabalhar como se este estivesse no seu posto de trabalho no escritório. Autenticação, transparência e facilidade de uso para o utilizador remoto são factores cruciais para este cenário.

Uma conexão de rede de filiais onde, duas ou mais Intranets de confiança estão ligadas. Normalmente, as Intranets são protegidas por *firewalls* que são o local ideal para implantar o *software* VPN. Deste modo, o utilizador externo à rede não tem que se preocupar com a sua instalação cabendo ao administrador de rede a certeza de que toda a troca de tráfego de Internet entre os dois, é seguro. Embora este seja o cenário mais simples, podem surgir problemas no gerenciamento de endereços IP não registados.

Uma conexão de rede de parceiros de negócios (também designado de extranet) tem representado recentemente a maior tendência para o uso de uma VPN. As empresas podem conceder aos seus fornecedores, clientes e outras empresas acesso temporal e limitado à sua Intranet. A ampla disponibilidade da Internet e o seu relativo baixo custo permite novos modelos de negócios, incluindo o contacto inicial do cliente, negociação de vendas, atendimento de pedidos e suporte contínuo. Além disso, essa solução permite automatizar a cadeia de abastecimento e facilitar projectos de colaboração com parceiros.

4.3.6.1. Protocolos da VPN

Com suporte para a maioria dos dispositivos, as ligações com base em *Point-to-Point Tunneling Protocol* (PPTP) permitem a transferência segura de dados de um dispositivo remoto para um servidor privado através de redes públicas como a Internet. Fáceis de configurar as ligações baseadas em PPTP oferecem uma segurança básica permitindo a confidencialidade dos dados, sem garantir a integridade e autenticidade dos mesmos.

O protocolo *Layer Two Tunneling Protocol* (L2TP), mais seguro do que PPTP, é utilizado em conjunto com o *IPSec* que dispõe de algoritmos de criptografia mais seguros. Exige um certificado ou chave pré-compartilhada. Tem um nível mais forte de criptografia tendo em conta o uso de chaves de 168 bits, e um algoritmo de criptográfico DES. Promove a integridade dos dados e autenticação de verificação de origem projectada para impedir os hackers de comprometer o sistema. No entanto, o aumento da sobrecarga necessária para gerir o aumento de segurança significa que este é executado num ritmo mais lento do que PPTP.

O *Internet Protocol Security* (Ipsec), com suporte a todos os algoritmos criptográficos usados actualmente, foi também desenvolvido de forma a suportar novos e mais desenvolvidos algoritmos, à medida que estes forem surgindo, abrangendo os seguintes requisitos de segurança: a autenticação da origem de dados; a integridade dos dados; a confidencialidade de dados; a protecção de repetição; a gestão automática de chaves criptográficas e associações de segurança.

Uma VPN pode utilizar dois protocolos IPSec para proteger os dados à medida que estes circulam pela VPN: Cabecalho de autenticação (AH) e *Encapsulating Security Payload* (ESP). A outra parte da implementação dos *Ipsec* é o protocolo *Internet Key Exchange* (IKE) que permite o gerenciamento automático de chaves. Enquanto os *Ipsec* codificam os dados, o IKE suporta a negociação automática das associações de segurança (SAs) e a geração e actualização automática das chaves criptográficas (IBM Corporation 1998, 2014).

No protocolo *Ipsec*, são definidos dois modos de operação: o modo de transporte e o modo de túnel. O modo de transporte é mais simples e é utilizado no estabelecimento de comunicações seguras entre redes e terminais, no qual apenas os dados do pacote são encriptados. O modo túnel é utilizado para o estabelecimento de ligações seguras entre duas ou mais redes, permitindo o encapsulamento de todo o pacote IP.

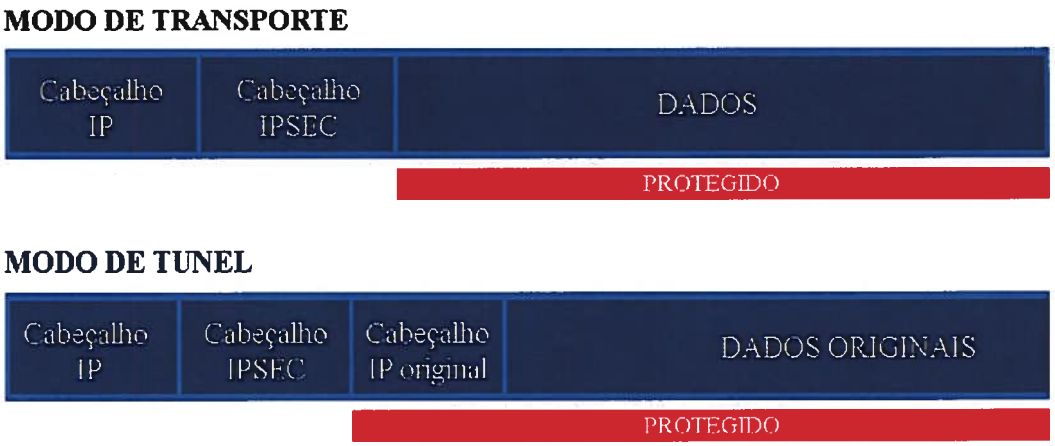


Figura 24 - Modo de Operação do protocolo Ipsec

V - Detecção

A detecção de potenciais ameaças de um sistema de segurança é fundamental na tomada de medidas preventivas de forma a proteger a organização.

5.1. IDS

Um IDS (*Intrusion Detection System*) consiste num processo de monitorização dos eventos que ocorrem num computador ou rede analisando-os em busca de possíveis incidentes. Regista incidências de ataque na tentativa de detê-los, e denunciá-los aos administradores de sistema. A utilização destes sistemas permite também a identificação de problemas relacionados com as políticas de segurança documentando ameaças existentes e dissuadindo as pessoas de violar as políticas de segurança. Muitos IDS podem reagir a uma ameaça detectada tentando impedi-la de ser bem sucedido de forma activa ou passiva. Os IDS activos actuam com o intuito de travar a ameaça enquanto os IDS passivos apenas alertam os administradores das ocorrências anómalas. O principal problema na utilizaçãodos IDS é a geração de falsos alarmes activados contra acções legítimas que diferem do padrão normal, determinada por novos tipos de ataque ou por bugs do próprio *software*.

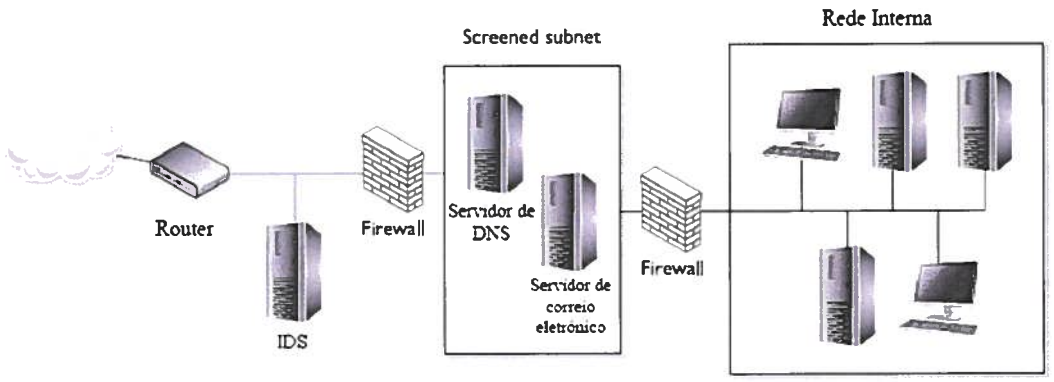


Figura 25 - IDS

5.1.1. Tecnologias de IDS

Os quatro tipos de tecnologias de IDS são diferenciados principalmente pelos tipos de eventos que eles monitorizam e pelas formas como estão implantados (Scarfone & Mell, 2007).

O *Network-Based* monitoriza o tráfego da rede para segmentos de rede específicos ou dispositivos e analisa a actividade de rede e o protocolo de aplicação para identificar actividade suspeita.

O *Wireless* monitoriza o tráfego de rede sem fio e analisa-o de forma a identificar actividade suspeita na rede e respectivos protocolos

O *Network Behavior Analysis* (NBA) analisa o tráfego de rede para identificar as ameaças que geram fluxos de tráfego incomuns, como negação de serviço distribuída (DDoS), certas formas de *malware* e violações das políticas de segurança

O *Host-Based* monitoriza as características de um único *host* e os eventos suspeitos que ocorrem dentro deste.

5.1.2. Componentes do IDS

Segundo o *Common Intrusion Detection Framework Architecture* (CIDF)[22], um sistema de detecção de intrusão consiste em quatro tipos de componentes que se comunicam entre si: geradores de eventos, analisadores de eventos, bancos de dados de eventos e unidades de resposta.

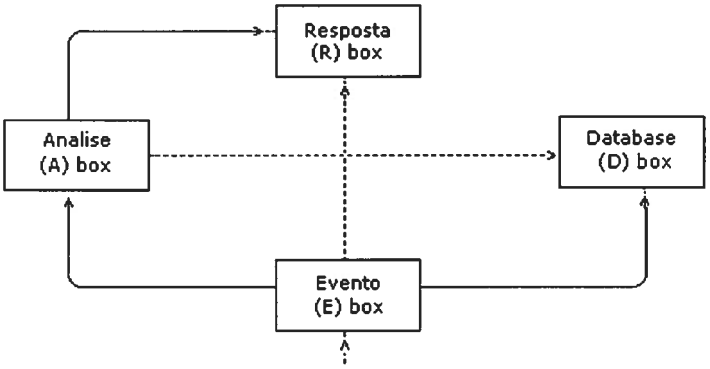
Os geradores de eventos ("E- boxes") têm como função obter os eventos a partir do meio externo ao CIDF, ou seja, produz os eventos mas não os processa, isso fica a cargo do componente especializado na função de processamento, que por sua vez após analisar os eventos (violação de política, anomalias, intrusão) envia os resultados para outros componentes.

Os analisadores de eventos ("A- boxes") têm como função receber e analisar informações de outros componentes e posteriormente enviar informação relevante.

Os bancos de dados de eventos ("D- boxes") têm como função armazenar os eventos e resultados para uma necessidade futura.

As unidades de resposta ("R- boxes") tem como função reagir a uma ameaça detectada tentando impedi-la de ser bem sucedida, como por exemplo, fechar uma ligação, terminar um processo, alterar permissões de arquivo, notificação do administrador de sistemas.

[22] http://gost.isi.edu/cidf/drafts/architecture.txt, acedido em 30 de Novembro de 2013.



Fonte: http://www.absoluta.org/seguranca/seg_ids.htm

Figura 26 - Modelo de componentes do IDS

Como complemento e visto como uma evolução dos IDS, o IPS junta as capacidades de detecção do IDS e a capacidade de bloqueio de uma *firewall* diminuindo os falsos alertas.

5.2. *Honeypot*

Um *honeypot* é utilizado com o intuito de criar zonas passíveis de ser atacadas onde a informação contida é irrelevante para a organização, permitindo obter informações sobre o atacante e suas técnicas de ataque, desviando o atacante dos sistemas em produção. Não geram falsos alertas como os identificados no IDS, capturam tráfego malicioso criptografado e concomem menos recursos de *hardware* em comparação com os IDS.

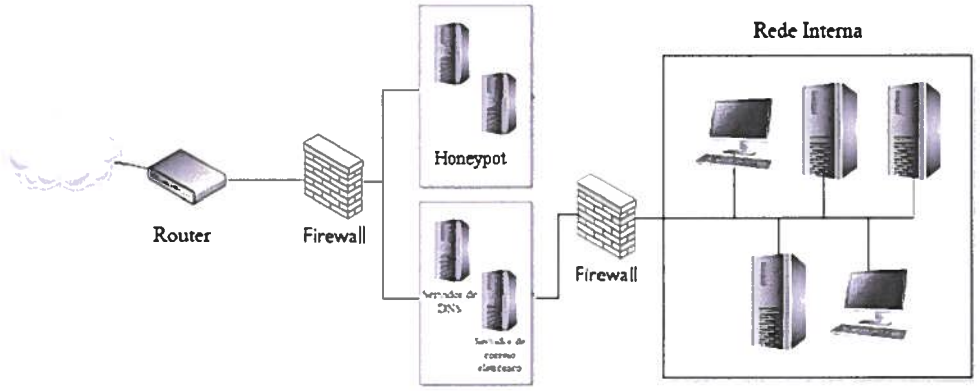


Figura 27 - *Honeypot*

Segundo Spitzner, os honeypots podem ser de dois tipos (Spitzner, 2003), de produção ou pesquisa.

5.2.1. *Honeypots* de produção

Visam proceder a protecção da organização, identificando e minimizando as ameaças praticadas pelos atacantes. *Honeypots* de produção geralmente são mais fáceis de construir e

implementar que os *honeypots* de pesquisa, porque exigem menos funcionalidades. Devido a esta relativa simplicidade, estes geralmente têm menos riscos para a segurança de uma organização. É muito mais difícil usar um *honeypot* de produção para atacar e prejudicar outros sistemas. No entanto, eles também dão geralmente menos informações sobre os ataques ou os atacantes, que os *honeypots* de pesquisa (Spitzner, 2003).

5.2.2. *Honeypots* de pesquisa

Honeypots de pesquisa são projectados para obter informações sobre os atacantes. A sua principal missão é pesquisar as ameaças que as organizações podem enfrentar como identificar o tipo de atacantes, a forma como estão organizados, os tipos de ferramentas usam para atacar outros sistemas, e onde obtiveram essas ferramentas. Este tipo de *honeypot* normalmente é utilizado em organizações de pesquisa como universidades, agências militares e governamentais e empresas de pesquisa de segurança. Disponibilizando mais funcionalidades, tornam-se mais complexos exigindo mais recursos e manutenção, potenciam a reduzir a segurança de uma organização (Spitzner, 2003).

5.3. Auditoria

A necessidade de um cuidadoso planeamento das actividades de auditoria pode minimizar os riscos de potenciais ameaças. Na implementação de um processo de auditoria aos SI devem ser observadas as seguintes directivas[23]: requisitos de auditoria devem acordados com o nível apropriado da administração; a verificação esteja limitada ao acesso para leitura de *software* e dados; outros acessos diferentes de apenas leitura sejam permitidos somente através de cópias isoladas dos arquivos do sistema, e sejam apagados ao final da auditoria, ou dada protecção apropriada quando existir uma obrigação para guardar tais arquivos como requisitos da documentação da auditoria; recursos para execução da verificação sejam identificados explicitamente e tornados disponíveis; requisitos para processamento adicional ou especial sejam identificados e acordados; todo o acesso seja monitorizado e registado de forma a produzir um histórico de acessos; convém que o uso do histórico de acessod seja considerado para os sistemas ou dados críticos; todos os procedimentos, requisitos e responsabilidades sejam documentados; as pessoas que executem a auditoria sejam independentes das actividades auditadas.

[23] Norma ABNT ISO/IEC 17799:2005

VI - Recuperação

A definição de um plano de recuperação dos SI é importante de forma a manter e salvaguardar a integridade e disponibilidade dos dados e recursos de um sistema de informação de uma organização.

7.1. *Backup*

A existênciade recursos adequados para a geração de cópias de segurança deve ser disponibilizada de forma a garantir que toda informação e *software* essenciais da organização possam ser recuperados após um desastre ou a falha de uma média. De acordo com as necessidades e recursos adequados as políticas de *backup* deverão ter em conta diversas considerações: a definição das necessidades de cópias de segurança; a formalização de um documento completo com informação de todos os processos à restauração do backup; definir o tipo de cópia de segurança e a frequência da sua realização de acordo com o conteúdo da informação e necessidades da organização; o armazenamento das cópias de segurança deverá ser feito em local seguro diferentes do local de origem, de forma a não serem afectadas na ocorrência de um desastre no local principal; os sistemas de *backup* deverão ser regularmente testados de forma a garantir a sua utilização em caso de desastre ou resposta a uma crise; os procedimentos de recuperação devem ser verificados e testados regularmente, de forma a garantir que estes são efectivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação; em situações onde a confidencialidade é importante, cópias de segurança devem ser protegidas com recurso a técnicas de encriptação.

7.2. Redundância

Um sistema RAID (Conjunto Redundante de Discos Independentes) permite simular uma unidade lógica de armazenamento através da combinação de duas ou mais unidades físicas. A implementação de um sistema RAID através da combinação de discos de baixo custo permite ganhos significativos de segurança e desempenho de todo o sistema. Os objectivos principais deste sistema consistem num acesso aos dados de forma mais rápida e uma maior tolerância a falhas, de acordo com a figura seguinte.

	RAID 0	RAID 1	RAID 5	RAID 10
Nº mínimo de unidades	2	2	3	4
As vantagens	Taxas mais altas de transferência	100% de redundância de dados. Um disco pode falhar, mas os dados continuarão acessíveis. É recomendada uma nova montagem em um novo disco para manter a redundância dos dados.	Porcentagem mais alta de capacidade utilizável e alto desempenho, leitura e tolerância a falhas.	Combina o desempenho de leitura da RAID 0 com a tolerância a falhas da RAID 1.
Tolerância a falhas	Nenhuma - se um disco falhar todos os dados serão perdidos	Excelente - o espelhamento de disco significa que todos os dados em um disco são duplicados no outro.	Excelente - as informações de paridade permitem a reconstrução dos dados após a substituição de uma unidade de disco falha por uma nova.	Excelente - o espelhamento de disco significa que todos os dados em um disco são duplicados no outro.
Aplicativo	Usado em desktops e workstations para o desempenho máximo de dados temporários e taxa alta de E/S	Usada em sistemas menores em que a capacidade de um disco é suficiente e para os aplicativos que exigem muito alta disponibilidade.	Armazenamento de grandes quantidades de dados críticos.	Aplicativos de alto desempenho que requerem proteção de dados, como, por exemplo, edição de vídeo.

Fonte: http://www.intel.com/support/pt/chipsets/imsm/sb/CS-009337.htm

Figura 28 - RAID

VII - Redes sem Fios

A utilização das redes sem fios tornaram-se nos últimos anos bastante populares, tanto em redes privadas como públicas. A rapidez e baixo custo de instalação, mobilidade e escalabilidade, levaram a uma grande adesão de pessoas e organizações, contribuindo assim para a sua massificação. Uma rede sem fios é composta por dispositivos identificados por um endereço MAC[24] (Media Acess Control), capazes de se ligarem a uma rede sem fios, e um AP permitindo a ligação desses dispositivos e outros equipamentos da rede (Clark & Wilson, 1987).

7.1. Principais ameaças às redes sem fios

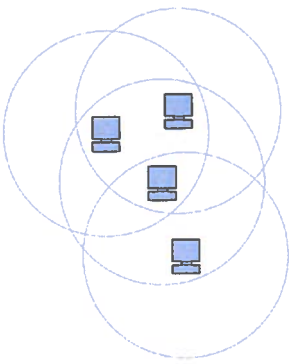
Apesar da sua popularidade, existem problemas de segurança inerentes à utilização das redes sem fios, alguns destes riscos são similares aos encontrados nas redes com fios outros advém do carácter não guiado do meio de transmissão. Os ataques à autenticação e os ataques de negação de serviço são os principais riscos de segurança associados às redes de comunicações sem fio.

7.2. Arquitecturas das Redes sem Fios

A arquitectura da WLAN pode ser operada de dois modos (The Institute of Electrical and Electronics Engineers, Inc., 1999): *Ad-hoc* e *Infrastructure network*.

7.2.1. *Ad-hoc*

Numa arquitectura *Ad-hoc* todos os dispositivos comunicam directamente entre si sem recurso a um AP desde que encontrem no seu raio de acção.



Fonte adaptada: http://pt.kioskea.net/contents/792-os-modos-de-funcionamento-do-wifi-802-11-ou-wi-fi

Figura 29 - Arquitectura *Ad-hoc*

[24] Endereço físico associado à interface de comunicação, que conecta um dispositivo à rede.

7.2.2. *Infrastructure network*

Numa arquitectura *Infrastructure network*, todos os dispositivos comunicam entre si, através do AP compartilhando o mesmo *Service Set Identifier* (SSID[25]).

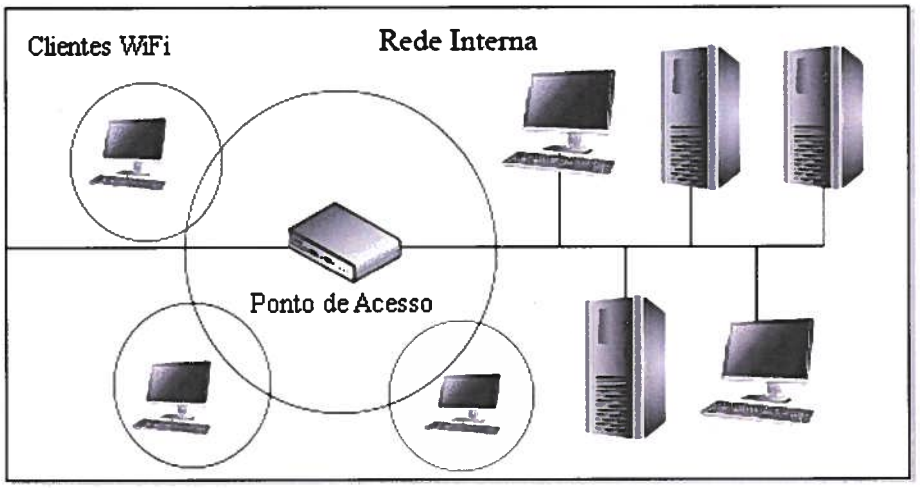


Figura 30 - Arquitectura *Infrastructure network*

7.3. Protocolos das Redes sem Fios

Como utilizam o ar para transmissão, estas redes devem preencher requisitos de segurança mais exigentes apesar de estasestarem menos expostas a desastres de origem natural, as escolhas do protocolo de segurançaa utilizar são fundamentais neste campo.

7.3.1. WEP

WEP é o protocolo padrão da norma 802.11, um mecanismo de autenticaçãoque pretendia garantir confidencialidade através do algoritmo RC4 com utilização de uma chave secreta estática e verificação de integridade através de um *checksum*. Desde cedo começaram a ser detectadas algumas vulnerabilidades que fizeram com que a credibilidade deste protocolo fosse posta em causa (Fluhrer, Mantin , & Shamir, 2001).

7.3.2. WAP

Este protocolo foi desenvolvido pela Wi-Fi Alliance, de forma a oferecer um melhor padrão de segurança para redes sem fios tendo em conta todas as vulnerabilidades conhecidas do protocolo WEP, oferecendo uma melhor protecção de dados e controlo de acesso à rede. Oferece melhorias no algoritmo da criptografia, possibilitando a constante

[25] SSID identica o nome da rede sem fios

mudança de chaves no envio de novos pacotes através da utilização de um protocolo de chave temporária TKIP (*Temporary Key Integrity Protocol*) e melhoria nosmecanismos de autenticação de utilizador baseada no padrão IEEE 802.1X e no EAP (*Extensible Authentication Protocol*) através de um servidor de autenticação. O WAP foi concebido de forma a ser implementado em conjunto com WEP e ser compatível com todas as versões implementadas nos dispositivos 802.11.

Este protocolo pode ser habilitado em duas versões: na versão WPA-Pessoal permite uma forte protecção dos dados e impede o acesso não autorizado de rede para pequenas organizações Utiliza um algoritmo de criptografia TKIP (*Temporary Key Integrity Protocol*), baseado em chaves e protege contra os acessos não autorizados de rede através do uso de uma chave pré-compartilhada PSK (*Pré-Shared Key*); na versão WPA-Empresa permite a autenticação dos utilizadores na rede através de uma estrutura de autenticação IEEE 802.1X e um algoritmo de criptografia TKIP.

PSK é um mecanismo de WAP-Pessoal, que permite o uso de chaves introduzidas manualmente para iniciar em segurança uma comunicação. A PSK é definida no ponto de acesso e posteriormente introduzida no computador de forma a autenticar-se na rede Wi-Fi prevenindo o acesso de utilizadores não autorizados à rede.

7.3.3. WAP2

Semelhante ao WPA o protocolo WAP2 fornece ainda maior protecção dos dados e controlo de acesso à rede sem fio. Com base no padrão IEEE 802.11i, este protocolo incorpora as correcções do efectuadas no WAP no que diz respeito ao combate às vulnerabilidades do WEP e implementa um novo algoritmo de encriptação o Advanced Encryption Standard (AES)[26] compatível com autenticação baseada em 802.1X.

Tal como na versão WAP, pode ser habilitado de dois modos: WPA2–Pessoal que à semelhança do WAP protege a rede contra os acessos não autorizados de rede através do uso de uma chave pré-compartilhada PSK e oferece melhor protecção da rede contra acessos não autorizados, através da utilização do algoritmo criptográfico AES; WAP2–Empresa que procede à verificação dos utilizadores da rede através de um servidor de autenticação.

---

[26] O AES é uma cifra de bloco de chaves simétricas que através de operações matemáticas e lógicas transforma uma chave e um bloco de dados não cifrados, num bloco de dados cifrados.

O WAP2 é compatível com o WAP e como tal utiliza a estrutura 802.1X/EAP como parte da infraestrutura que garante a autenticação mútua centralizada e gerenciamento de chave dinâmica, oferece ainda, uma chave pré-compartilhada para uso em ambientes domésticos e de pequenos escritórios.

Conclusão

Actualmente a segurança informática tem-se mostrado um tema bastante abrangente que incorpora diversas áreas do ramo da Informática. Identificar todas as ameaças e medidas para prevenção, detecção e recuperação dos sistemas de informação, num único documento é extremamente complexo.

Pretendeu-se com este projecto disponibilizar às organizações as principais abordagens relacionadas com a segurança da Informação.

Assim, a elaboração de um plano de segurança de acordo com as necessidades da organização, identificando os pontos críticos do sistema de informação e organiza-los por grau de impacto e ocorrência é de extrema relevância para a protecção dos sistemas de informação.

Também a componente humana tem-se demonstrado um dos factores mais críticos na segurança dos sistemas de informação, deste modo a consciencialização dos utilizadores internos e externos para uma adequada utilização desses recursos e divulgação da política de segurança implementada pela organização, é fundamental de forma a minimizar os comportamentos de risco.

Nenhum sistema de informação está verdadeiramente seguro e a informação, como um activo valioso de uma organização, deverá ser protegida atravéz da definição de uma solução de segurança tendo em conta o custo da sua implementação, face o real valor da informação a proteger.

Para trabalho futuro e com base neste projeto, poderá ser desenvolvida uma simulação aplicada a uma situação real de uma organização fictícia, de modo a aplicar os principais objetivos deste projeto através da elaboração de documentação própria das políticas de segurança a ser tidas em conta, bem como o funcionamento da infraestrutura de rede através da criação de máquinas virtuais.

Bibliografia

Braun, T., Günter, M., Kasumi, M., & Khalil, I. (1999). *Virtual Private Network Architecture.* Universidade de Berna.

Clark, D., & Wilson, D. (1987). A Comparison of Commercial and Military Computer Security Policies. *in Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy,* pp. 184-193.

Festa, L. M. (04 de Setembro de 2013). *Política de Controlo de Acesso Chinese Wall.* Obtido em 11 de Maio de 2014, de Scribd: http://pt.scribd.com/doc/165287934/Brewer-Nash-Chinese-Wall

Florian, C. (3 de Fevereiro de 2014). *Report: Most vulnerable operating systems and applications in 2013.* Obtido em 1 de Maio de 2014, de GFI: http://www.gfi.com/blog/report-most-vulnerable-operating-systems-and-applications-in-2013/

Fluhrer, S., Mantin , I., & Shamir, A. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4.* Obtido em 21 de 11 de 2013, de CiteSeerX: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.2652&rep=rep1&type=pdf

Fraser, B. (1997). *RFC: 2196 - Site Security Handbook.* Pittsburgh: Barbara Y. Fraser - Software Engineering Institute - Carnegie Mellon University.

Harris, S. (2013). *CISSP All in one - Exam Guide Sixth Edition.* Nova Iorque: McGraw-Hill Companies.

Harrison, M. A., Ruzzo, W. L., & Ullman, J. D. (8 de Agosto de 1976). Protection in Operating Systems. (R. Gaines, Ed.) *Communications of the ACM, 19,* 461-471.

IBM Corporation 1998. (2014). *IBM i: Funcionamento em Rede Privada Virtual.* Obtido em 08 de Dezembro de 2013, de IBM Knowledge Center: http://www-01.ibm.com/support/knowledgecenter/api/content/ssw_ibm_i_72/rzaja/rzajapdf.pdf

Kamluk, V., & Lozhkin, S. (2013). Corporate Threats. *Kaspersky Security Bulletin 2013,* 22-31.

Lampson, B. W. (Janeiro de 1971). Proc. 5th Princeton Conf. on Information Sciences and Systems. *Protection* , pp. 18-24.

Landwehr, C. (Setembro de 1981). ACM Computing Surveys. *Formal Models for Computer Security, 13,* 247-278.

Magalhães, H., & Grilo, A. (2006). *A Segurança Informática e o Negócio Electrónico.* (S. P. Inovação, Ed.) Porto: Princípia.

Marques, J. A., Ferreira, P., Ribeiro, C., Veiga, L., & Rodrigues, R. (2012). *Sistemas Operativos* (2ª ed.). Lisboa: FCA - Editora de Informática.

Nakamura, E. T., & Geus, P. L. (2007). *Segurança de Redes em Ambientes Cooperativos.* São Paulo: Novatec Editora.

O'Hanley, R., & Tiller, J. S. (2014). *Information Security Management Handbook* (6ª ed., Vol. 7). Boca Raton, Flórida: Taylor & Francis Group.

Olzak, T. (March de 2006). *DNS Cache Poisoning: Definition and Prevention.* Obtido em 1 de Dezembro de 2013, de http://adventuresinsecurity.com/Papers/DNS_Cache_Poisoning.pdf

Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing* (4ª ed.). New Jersey: Prentice Hall.

Sandhu, R., & Samarati, P. (Setembro de 1994). Access Control: Principles and Practice. *IEEE Comunications Magazine*, 40-48.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).* Gaithersburg: National Institute of Standards and Technology.

Spitzner, L. (2003). *Honeypots: Tracking Hackers.* Boston: Pearson Education, Inc.

Stallings, W. (2011). *Network Security Essentials: Aplications and Standards* (4ª ed.). Nova Jersey: Prentice Hall.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5ª ed.). Boston: Prentice Hall.

The Institute of Electrical and Electronics Engineers, Inc. (1999). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* Nova Iorque: IEEE.

Vacca, J. R. (2009). *Computer and Information Security Handbook.* Burlington: Morgan Kaufmann Publishers.

Veiga, P. (2004). *Tecnologias e Sistemas de Informação, Redes e Segurança.* (S. –S. Inovação, Ed.) Porto: Principia.