



Segurança de Infraestrutura de TI

Bootcamp Online: Analista em Cibersecurity

Maximiliano de Carvalho Jacomo

2020

Segurança de Infraestrutura de TI

Maximiliano de Carvalho Jacomo

© Copyright do Instituto de Gestão e Tecnologia da Informação.

Todos os direitos reservados.

Sumário

Capítulo 1.	Introdução a Segurança da Infraestrutura de TI.....	5
1.1.	De onde vêm a Estratégia de Defesa em Profundidade?	8
1.2.	Controles da Estratégia de Defesa em Profundidade	11
Capítulo 2.	Arquitetura da Estratégia da Defesa em Profundidade	13
2.1.	Camada 1: Política, Procedimentos e Conscientização.....	14
2.2.	Camada 2: Segurança Física.....	18
2.3.	Camada 3: Segurança de Perímetro	19
2.4.	Camada 4: Segurança Rede Interna	20
2.5.	Camada 5: Segurança de Host (dispositivos)	21
2.6.	Camada 6: Segurança Aplicação.....	22
2.7.	Camada 7: Segurança Dados.....	23
Capítulo 3.	Mecanismos de Proteção – DID.....	25
3.1.	Segurança Perímetro	25
3.2.	Roteadores, Switchs e ACLs	26
3.3.	Firewall.....	31
3.3.1.	Tipos de Firewall	34
3.3.2.	Filtragem de Pacotes (packet filtering)	35
3.3.3.	Firewall de Aplicação ou Proxy de Serviço	37
3.3.4.	Firewall: Inspeção de Estado (Stateful Inspection)	38
3.3.5.	Firewall de Aplicações WEB (WAF)	38
3.3.6.	Firewall Pessoal e UTM	41
3.4.	DMZ – Zona Desmilitarizada (Demilitarized Zone)	42
Capítulo 4.	Proteção: Rede Interna	45
4.1.	Switches Layer 2 e 3.....	45
4.2.	VLANs – Redes Locais Virtuais	47

Capítulo 5. Camada: Proteção Hosts (Segurança de Host)	50
5.1. Baselines, Bugs, Atualizações e Correções.....	51
5.2. Exploit, Antivírus, AntiSpam e Antimalware's.....	56
5.3. RootKits, BackDoors e HIDS	59
5.4. Whitelisting, Blacklist e EndPoint Security	61
Capítulo 6. IPS, IDS e VPN	65
6.1. IPS e IDS (Prevenção ou Detecção de Intrusão).....	65
6.2. VPN – Virtual Private Network	69
Referências.....	73

Capítulo 1. Introdução a Segurança da Infraestrutura de TI

De acordo com o *ITIL v3* o termo infraestrutura de TI é definido como um conjunto de elementos que incluem computadores, servidores, redes, dados, armazenamento, instalações físicas e virtuais, bem como softwares, processos, políticas, equipes, treinamento, segurança, funcionalidade móvel e virtual e serviços baseados em nuvem que compõem a infraestrutura de TI. Nesse contexto, podemos dizer que a infraestrutura de TI consiste em todos os elementos que suportam o gerenciamento e a usabilidade de dados e informações, incluindo o hardware físico e instalações físicas no qual estão alocados, o armazenamento e recuperação desses dados e informações, os sistemas de rede, as interfaces e os softwares para suportar as operações e os objetivos de negócio que a empresa e seus colaboradores realizam em seu dia a dia, para suprir as necessidades e expectativas de seus clientes e consumidores de seus produtos e serviços.

Na medida em que o modelo de negócio de uma empresa evolui, percebe-se claramente que a infraestrutura de TI passa a ter um papel crucial e estratégico. Isto porque, permite aos gestores criarem um ambiente corporativo mais flexível e preparado para enfrentar as diversas adversidades e ameaças vindas do meio social, político ou econômico em que a empresa está inserida.

Garantir que todos esses elementos pertencentes a uma infraestrutura de TI, operem dentro do ambiente organizacional de maneira eficiente e eficaz, alinhados as operações, estratégias e metas corporativa com segurança, torna-se uma tarefa complexa e importante para as equipes de infraestrutura de TI, redes e segurança da informação. Ou seja, pode-se dizer que tais equipes têm como principal objetivo garantir que todos os elementos que compõem uma infraestrutura de TI, estejam funcionando no nível máximo de eficiência e segurança para suprir todas as necessidades operacionais, gerenciais e estratégicas de uma empresa.

Pois bem, sabendo agora que uma infraestrutura de TI possui um grande valor operacional e estratégico para uma empresa e, que essa infra é composta por diversos elementos de TI diversificados, doravante denominados de ativos de TI, perguntas do tipo: Como realizar a proteção desses ativos de TI? Como impedir que

ameaças paralitem de forma parcial ou total o funcionamento desses ativos de TI? Ou, como garantir que esses ativos de TI estejam disponíveis, íntegros e, se mantenham confidenciais em um meio ambiente cada vez mais integrado, interativo e compartilhado? Se tornam imperativas e essenciais, e requer das equipes de TI uma resposta rápida e eficiente.

Neste contexto, as equipes de TI e segurança da informação e segurança cibernética, devem pensar em uma estratégia que permita a implementação de mecanismos de proteção que respondam de forma eficiente os questionamentos levantados anteriormente. Ou seja, as diversas ameaças que podem comprometer parcialmente ou totalmente, pelo funcionamento operacional de uma empresa ou organização seja ela de pequeno, médio ou grande porte e de qualquer modelo de negócio.

A Defesa em Profundidade é uma estratégia de segurança da informação e da segurança cibernética que se baseia na aplicação de uma série de medidas defensivas redundantes em camadas que tem como objetivo implementar controles administrativos, físicos e tecnológicos, utilizando-se de políticas, controles, mecanismos e ferramentas tecnológicas redundantes disposta em camadas. Essa abordagem de implementar várias camadas é conhecida como “*segurança em camadas*” e objetiva aumentar a segurança de uma infraestrutura de TI como um todo. Isto porque, a segurança em camadas possibilita realizar o tratamento de diversas ameaças vindas de muitos vetores de ataque diferentes, tendo como princípio o conceito que: se um mecanismo de segurança falhar, outro será acionado imediatamente para impedir um ataque.

Para entender melhor a estratégia de Defesa em Profundidade e sua proposta de segurança em camadas, é preciso voltarmos ao tempo medieval e entendermos os mecanismos de proteção e defesa de um castelo. Observe a figura a seguir e tente reconhecer os mecanismos que proporciona a segurança do castelo contra ataques e invasões.

Figura 1 - Representação de um castelo medieval.



Conseguiu encontrar os mecanismos que proporcionam a segurança do castelo contra ataques e invasões? Sim, Não! Vamos lá...

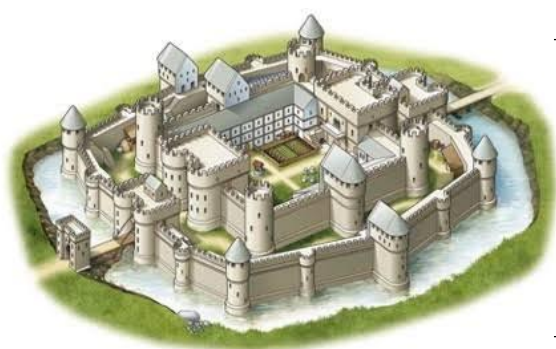
Para que um exército inimigo consiga invadir o castelo para conquistá-lo e roubar seus tesouros preciosos, primeiramente precisará vencer as barreiras e mecanismos de proteção do castelo. Como exemplo de tais barreiras e mecanismos de proteção, podemos citar: os portões de entrada e saída do castelo que interligam o mundo exterior com o ambiente interno do castelo; o fosso d'água que circula todo o castelo; a ponte levadiça, os portões internos do castelo, os muros e as torres de vigilância interna e externa do castelo, as guarnições de soldados (arqueiros, lanceiros e cavaleiros) que estão nos portões, muros, torres e áreas internas do castelo, etc. Cada um desses elementos de proteção pertencerão a uma ou mais conjuntos de elementos de segurança e, estarão dispostos (ou seja, distribuídos) em seções específicas do castelo e, estarão trabalhando em conjunto (unificada) e de forma redundante, no qual, caso uma seção seja vencida a próxima seção logo entra em ação para inibir ou impedir o ataque.

Essa disposição em seções na segurança da informação ou na segurança cibernética é conhecida como camadas de segurança. Sendo assim, cada seção do castelo será uma camada de segurança que possui um conjunto de mecanismos de proteção específicos aquela camada e que atuam com o propósito de inibir ou impedir que ameaças roubem dados ou informações ou comprometam o parcialmente ou

totalmente o funcionamento de um ou mais ativos de TI de uma infraestrutura de TI e consecutivamente as operações, estratégias e metas corporativas de uma empresa.

Ao penetrar em um castelo, você se depara com diversos mecanismos de defesa como o fosso e as muralhas em volta do castelo, a ponte levadiça, as torres de vigilância e os soldados arqueiros e assim por diante.

Figura 2 - Camadas de Proteção de um Castelo.



Mecanismos de Defesa do Castelo

- Portões Externos e Internos;
- Ponte Levadiça e Fosso D'água
- Muros e Torres Externos e Internos;
- Guarnições de Soldados;
- Etc...

É importante ressaltar que o mundo digital revolucionou a forma como vivemos, trabalhamos e nos divertimos. No entanto, é um mundo digital constantemente aberto a riscos e ameaças. Assim, um analista de segurança da informação ou segurança cibernética ou uma equipe de TI ou segurança, precisa garantir que as medidas implementadas e adotadas sejam as melhores possíveis e as mais assertivas para impedir que as suas infraestruturas de TI e, respectivamente, os ativos de TI, sejam comprometidos. Porém, infelizmente, não existe um método ou medida única que possa proteger com êxito contra todos os tipos de riscos e ameaças e, é aqui que entra em cena a proposta da estratégia de defesa em profundidade e segurança em camadas!

1.1. De onde vêm a Estratégia de Defesa em Profundidade?

A estratégia de defesa em profundidade vem da Agência de Segurança Nacional dos EUA a NSA – USA e, foi concebido como uma abordagem abrangente para segurança da informação e segurança cibernética. O conceito foi inspirado por

uma estratégia militar do exército do EUA com o mesmo nome. Porém, na prática, a estratégia militar criada pelo exército americano e a estratégia de segurança da informação e segurança cibernética criada pelo NSA se diferem.

A estratégia de defesa em profundidade, como estratégia militar, gira em torno de ter uma defesa de perímetro mais fraca no qual o propósito é ceder intencionalmente espaço (terreno) para ganhar tempo para construir uma estratégia de contra-ataque e reconquistar o espaço perdido e vencer o exército oponente. Já como estratégia de segurança da informação e segurança cibernética, a estratégia de defesa em profundidade envolve a implementação de sistemas/mecanismos paralelos de defesa/proteção que atuam como contramedidas por meio de controles físicos, técnicos e administrativos, que em conjunto visam inibir ou impedir que uma ameaça não comprometa um ou mais ativos de TI. Ou seja, não cedem o espaço (terreno) para um invasor ou ameaça e, muito menos, permitem que tal invasor ou ameaça comprometa um ou mais princípios básicos que regem a segurança da informação – disponibilidade, integridade, confidencialidade ou autenticidade.

Um dos pontos mais importante que deve ser compreendido sobre o conceito da estratégia de defesa em profundidade é que um ataque em potencial deve ser interrompido por vários métodos de proteção independentes, mas que em conjunto atuam como um grande sistema de segurança.

A sofisticação crescente dos ataques cibernéticos significa que as empresas não podem mais confiar em um produto único de segurança para protegê-las. Os profissionais de segurança precisam aplicar a estratégia de defesa em profundidade em todos os ativos de TI. Desde laptops de funcionários, que precisam de proteção contra ameaças e ataques do tipo intermediário advindos das redes Wi-Fi, até prevenção de sequestro de dados e informações.

Não existe uma única camada de segurança que proteja contra todos os riscos e ameaças cibernéticas, os criminosos virtuais estão se tornando cada vez mais sofisticados em seus ataques e as empresas por meio de suas equipes de segurança de TI, precisam responder de forma rápida e eficiente a essas ameaças,

além de estar em constante processo de melhoria contínua de seus mecanismos de proteção e defesas.

Acessos não autorizados, golpes cibernéticos baseados em técnicas de phishing, falsificação de e-mails, ransomware, violação de dados, vazamento de dados, negação de serviços e outros tipos diferentes de ameaças e ataques podem ser usados separadamente ou em conjunto, para atacar uma infraestrutura de TI de uma empresa. As equipes de segurança precisam de implementar várias camadas de segurança, cada qual com seus conjuntos de ferramentas específicas ao tratamento de cada vulnerabilidade e ameaça presente aquela camada e respectivamente a proteção dos ativos de TI contidos na referida camada.

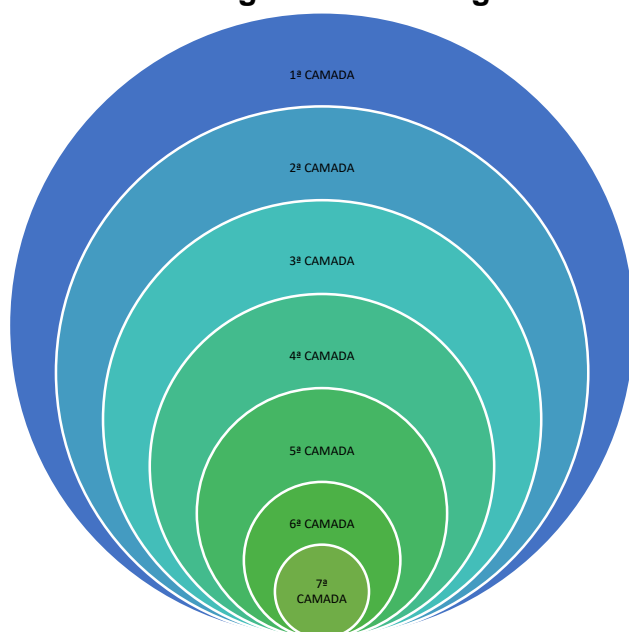
Para compreender melhor o funcionamento da estratégia de defesa em profundidade aplicada à segurança da informação e à segurança cibernética, vamos relembrar o exemplo das proteções contidas em um castelo medieval. Um invasor se depara com diversos mecanismos de defesa como o fosso e as muralhas em volta do castelo, a ponte levadiça, as torres de vigilância e os soldados arqueiros e assim por diante, conforme mencionado anteriormente. Cada um destes mecanismos de defesa estará distribuído em camadas e, cada camada será uma barreira responsável por realizar uma proteção específica para impedir que o invasor conquiste o castelo.

Por exemplo, os primeiros mecanismos de defesa a serem vencidos pelo invasor serão os controles de acesso físico como os portões externos antes da ponte levadiça, que podem conter soldados que exercem a função de identificar e controlar o primeiro acesso ao castelo. Ou seja, quem entra ou sai do castelo. Temos ainda nesta primeira camada de proteção a ponte levadiça e o fosso d'água que são considerados outros mecanismos de segurança que limitam o acesso ao castelo.

Bem, caso o invasor consiga superar os mecanismos presentes na camada de segurança física do castelo, ele terá que enfrentar uma próxima camada de proteção, no caso podemos citar as torres externas de vigilância e os soldados arqueiros.

Percebe-se neste momento, que na segunda camada de proteção há a presença de outros mecanismos de segurança que possuem um grau de dificuldade maior se comparados aos primeiros mecanismos presentes na primeira camada de proteção. Isto faz com que, o invasor tenha uma maior dificuldade em superá-los. Porém, caso ele consiga superar essa segunda camada de proteção, haverá uma terceira camada de proteção, composta por outros mecanismos de segurança com maiores níveis de dificuldade. Este aumento do nível de dificuldade irá se repetir de forma exponencial a cada camada de proteção. Ou seja, a próxima camada de proteção, a quarta camada possuirá novos mecanismos de proteção superiores a terceira camada e, assim por diante, dificultado e impedindo o acesso do invasor ao tesouro contido dentro do interior castelo, ou fazendo com que ele desista de invadir o castelo.

Figura 3 - Estratégia em Defesa de Profundidade.



Lembre-se: Quanto mais funda for a camada de proteção, maior será o nível de proteção. Ou seja, maior será o fator dificultador para o invasor.

1.2. Controles da Estratégia de Defesa em Profundidade

A estratégia de defesa em profundidade é pautada em três tipos de controles, a saber:

Controles Físicos – correspondem a medidas de proteção que impedem o acesso físico aos ativos de TI de uma infraestrutura de TI. Como exemplo de medidas de proteção correspondente aos controles físicos, citamos: cercas, muros, catracas, portas com controle de acesso, sistemas de CFTV, guaritas com vigilância física, etc.;

Controles Técnicos – correspondem a medidas de proteção que irão garantir a segurança dos ativos de TI e visam proteger os conjuntos de hardware, os conjuntos de softwares e a rede. Como exemplo de medidas de proteção correspondentes aos controles técnicos, citamos: sistemas de proteção contra intrusões (IDS, IPS), sistemas de proteção de borda – Firewall, sistemas de gerenciamento de identidade e acesso (IAM), VPN, VLans, sistema de Antivírus, AntiSpam, DMZ, DLP, ACLs, criptografia de dados, sistemas de backup, dentre outros;

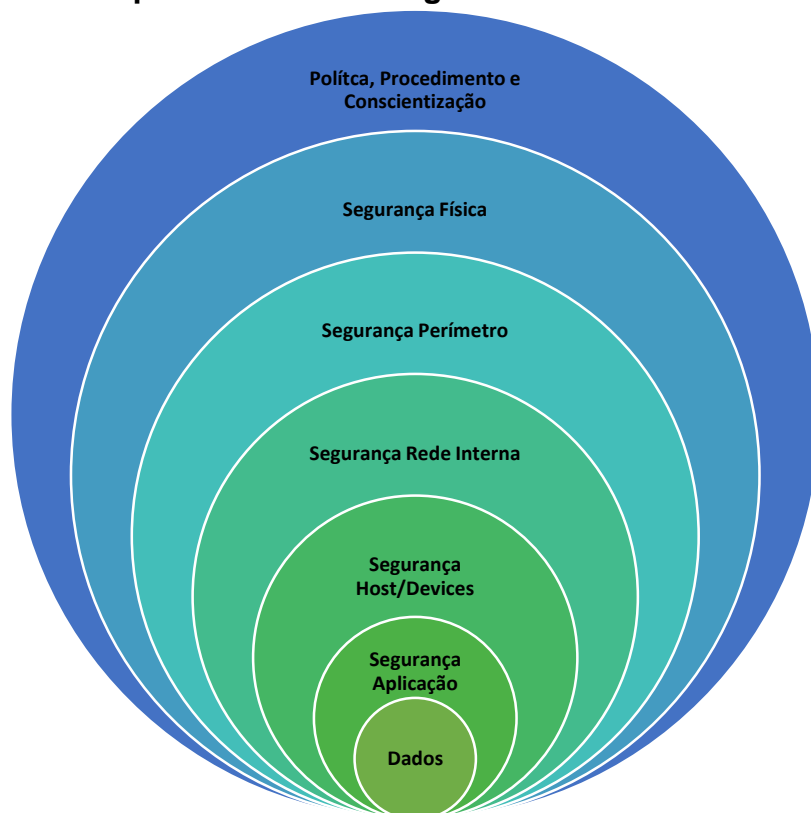
Controles Administrativos – correspondem a medidas de proteção administrativas, que irão orientar, reger e monitorar os controles físicos e controles técnicos, por meio de políticas e procedimentos direcionados a todos os clientes, colaboradores, fornecedores e parceiros comerciais aos funcionários de uma organização e seus fornecedores e parceiros comerciais que devem ser cumpridos e respeitados por todos. Como exemplo, citamos: as políticas de segurança da informação, as políticas de segurança cibernética, as políticas de privacidade e proteção de dados pessoais, o gerenciamento de risco e compliance; as estruturas de governança corporativa e governança de TI; a avaliações de riscos e ameaças aos ativos de TI e a toda segurança da informação e segurança cibernética, as políticas de treinamento e conscientização de clientes, colaboradores ou usuários, fornecedores e parceiros comerciais, a adoção de metodologias para promover a melhoria continua e garantir a adoção das melhores práticas, etc.

Capítulo 2. Arquitetura da Estratégia da Defesa em Profundidade

Até aqui, já percebemos que a estratégia de defesa em profundidade está fundamentada no conceito de segurança em camadas, na qual cada camada terá um conjunto de controles, mecanismos e ferramentas tecnológicas projetados para proteger os ativos de TI de uma infraestrutura de TI.

Com base no conceito de segurança em camadas, a arquitetura de uma estratégia de defesa em profundidade em consonância com as boas práticas de segurança propostas por normas internacionais como por exemplo as normas ISO/IEC 17799:2005; BS 7799; ISO/IEC 27000; RFC 2196 entre outras, possui sua arquitetura composta por sete camadas de proteção (Figura 4).

Figura 4 - Arquitetura da Estratégia em Defesa de Profundidade.



A seguir, iremos compreender melhor a função e funcionalidade de cada camada em relação à segurança da informação e segurança cibernética dos ativos de TI de uma infraestrutura de TI.

2.1. Camada 1: Política, Procedimentos e Conscientização

Trata-se da camada responsável por implementar os controles administrativos propostos na estratégia de defesa em profundidade. Aqui as equipes de segurança da informação deverão criar e implementar as diversas políticas e procedimentos que irão governar as práticas de segurança da informação e segurança cibernética de uma empresa, incluindo as ações de conscientização, treinamento e educação dessas práticas que deverão ser compreendidas, aceitas, seguidas e desempenhadas por todos os clientes, funcionários, fornecedores e parceiros comerciais da empresa.

Seja qual for a ação, controle, mecanismo ou ferramenta tecnológica que uma empresa adote em sua infraestrutura de TI e em seu ambiente corporativo, estes precisam de normas, políticas e procedimentos que irão garantir que todas as medidas de segurança estão sendo realizadas da forma correta ao longo do tempo por todos os funcionários, fornecedores e parceiros comerciais.

As políticas e procedimentos, precisam ser divulgados, seguidos e principalmente compreendidos pelos funcionários, fornecedores e parceiros comerciais e, para tal, é preciso que a alta administração da empresa em conjunto com a área de segurança e, por meio dos seus processos de governança corporativa, governança da tecnologia da informação e, da gestão de segurança da informação, implemente programas de conscientização, treinamento e educação junto a todos os colaboradores internos e externos ligados a empresa.

Existem vários motivos para a criação e implementação de políticas e procedimentos voltados à segurança da informação e segurança cibernética, dentre os quais destacamos: Estabelecer os requisitos necessários para impedir ou minimizar o acesso não autorizado acidental ou intencional aos ativos de TI – dados, informações, sistemas, dispositivos, etc.; Fornece diretrizes consistentes para as melhores práticas de segurança da informação e segurança cibernética; Comunicar a importância da segurança da informação e segurança cibernética a todos os colaboradores; Satisfazer aos requisitos legais inerentes ao modelo de negócio realizado pela empresa, tais como: normas e regulamentações de órgãos reguladores

de mercado, leis e legislações impostas por órgãos municipais, estaduais e federais, normas e regulamentações internas e de compliance, dentre outros.

Uma vez que as políticas e procedimentos estejam claramente definidos e divulgados, os programas de conscientização, treinamento e educação devidamente disseminados junto a todos os setores e colaboradores internos e externos à empresa, faz-se necessário a implementação de medidas de monitoramento das atividades realizadas por todos os membros que compõe o ambiente organizacional, para verificar se tais atividades estão de acordo com as políticas e procedimentos de segurança criados e vice-versa.

É importante que sejam definidos pela governança corporativa ou pela alta administração da empresa, as ações e medidas disciplinares a serem aplicadas aos colaboradores que descumprirem as políticas e procedimentos de segurança da informação e segurança cibernética.

Mas como criar uma política de segurança da informação ou segurança cibernética em concordância com as operações, estratégias e metas corporativas? Essa talvez seja um dos questionamentos mais comuns para aquelas equipes que iniciam a sua jornada rumo a conquista de uma infraestrutura de TI segura e uma governança da segurança da informação.

Por experiência própria confesso a você, que construir qualquer tipo de política destinada a proteger os ativos de TI de uma empresa, não é uma tarefa fácil. Muito pelo contrário, requer muita dedicação e trabalho de campo junto aos gestores das demais áreas operacionais da empresa. Por esse motivo, vou passar a você, algumas dicas que podem ajudar na construção de uma política de segurança da informação ou segurança cibernética. Preparados, vamos lá...

O primeiro passo para a construção de uma PSI é entender os motivos pelos quais a mesma deve ser criada e implementada dentro de uma empresa. A política de segurança da informação tem relação direta com a proteção de dados, para resguardar as informações da empresa. Esse conceito não inclui apenas a segurança de dados, mas todo o sistema da empresa em si. A proposta de uma PSI é

empreender esforços mais globais dentro do negócio. Ou seja, uma PSI em uma empresa, deve agregar iniciativas, normas, posturas e métricas ligadas à segurança da informação que se relacionem com todos os departamentos ou setores da empresa. A proposta é registrar princípios que possam reduzir ocorrência de incidentes de segurança da informação ou segurança cibernética ou mitigar os danos causados caso o incidente ocorra.

Criar uma política de segurança da informação, requer alguns cuidados básicos e inicialmente é preciso que se faça um diagnóstico de todo o ambiente corporativo. Ou seja, é preciso “ouvir” toda a empresa para buscar as vulnerabilidades que estão presentes no ambiente, incluindo um exame detalhado sobre os ativos de TI, estruturas, procedimentos e hábitos culturais da empresa e de seus colaboradores. Outro item importante na criação de uma PSI é a “integração”. Ou seja, o engajamento e a mobilização de todos os departamentos e colaboradores da empresa no processo de criação. Isto porque, uma PSI não deve ser construída somente pela equipe de segurança da informação ou de TI. Mas, sim com a colaboração de todos os colaboradores, mesmo que alguns deles não participem do processo de decisão. Afinal serão eles que irão auxiliar as equipes de TI e segurança no diagnóstico das falhas e na aplicação da melhoria contínua da segurança da informação. Como dica, produza algum tipo de campanha interna para sensibilizar e informar os colaboradores sobre as mudanças em relação à segurança da informação. Ações como essa irão contribuir para a criação ou mudança da cultura organizacional em relação a proteção dos ativos de TI.

Bem, agora que todos os colaboradores dentro da empresa estão engajados no processo de criação da PSI e, as equipes de TI ou segurança da informação realizaram o diagnóstico necessário para reconhecimento das vulnerabilidades de seus ativos de TI e de toda a infraestrutura de TI, é o momento de traçar os “objetivos”. No geral, sabemos que existem três conceitos básicos que guiam um bom plano de segurança da informação - disponibilidade, integridade e confidencialidade. Neste contexto, deve-se estabelecer vários objetivos, dos quais destacamos: (a) a criação de uma série de medidas que garantam a proteção dos ativos de TI, incluindo dados e informações; (b) a criação de uma série de medidas que impeçam ou mitiguem os

riscos relacionados as ameaças cibernéticas; (c) a criação de planos que respondam de forma eficiente e eficaz os possíveis incidentes de segurança; (d) a criação de medidas que impeçam o vazamento de dados e informações, mas que não engessem o acesso aos mesmos a ponto de prejudicar a fluidez dos processos organizacionais, as operações e estratégias corporativas e o próprio modelo de negócio realizado pela empresa.

Lembre-se, seja qual for a política a ser criada - segurança da informação, segurança cibernética, privacidade e proteção de dados pessoais, etc., a mesma deverá ser um “movimento contínuo” dentro da empresa. Ou seja, precisa estar disponível a todos os colaboradores e em versões adaptadas a cada nível organizacional de forma clara e objetiva. Em caso de dúvidas a política deve fornecer respostas claras, diretas e rápidas para solucionar imprevistos.

Definido os objetivos, é hora de partir para a “elaboração”. Neste momento, as equipes de TI ou segurança da informação devem consolidar as políticas com as normas, diretrizes e procedimentos que direcionem os colaboradores de forma clara e correta a utilização dos ativos de TI, incluindo as instruções para momentos de crise, proibições e procedimentos caso ocorra o descumprimento das normas e diretrizes estabelecidas na política e, por fim, os parâmetros de monitoramento, auditoria, fiscalização, métricas de conformidade e revisão da política e de todas as diretrizes e normas estabelecidas. Lembre-se que a elaboração de qualquer tipo de política, deve ser realizada em parceria com os diversos departamentos da empresa e parceiros estratégicos. Essa ação integrada permite a elaboração sólida das normas e diretrizes a serem seguidas por todos na empresa e promove a mudança cultural.

Por fim, mas não menos importante, há outras duas etapas que devem ser seguidas. São elas a etapa de treinamento e conscientização, na qual busca-se capacitar todos os colaboradores com o propósito de fazer com que a recém-criada política de segurança da informação saia do papel e traga bons resultados. É importante realizar um bom trabalho de treinamento e conscientização para garantir o sucesso da PSI e sua disseminação junto aos colaboradores. #ficadica: durante a fase de treinamento é preciso incluir os procedimentos básicos de segurança, com o

propósito de nivelar o conhecimento de todos os colaboradores quanto a esses princípios. E a etapa de monitoramento e revisão, no qual as equipes de TI e segurança realizam o monitoramento constante das normas e diretrizes estabelecidas visando o compliance da política com a realidade em que se encontra a empresa e os respectivos ajustes necessários as mudanças proporcionadas nos processos operacionais, gerenciais e estratégicos do modelo de negócio e do ambiente ou mercado ao qual a empresa está inserida.

2.2. Camada 2: Segurança Física

Considerada a primeira barreira de proteção de uma infraestrutura de TI, a camada de segurança física tem como objetivo garantir que as ameaças não tenham acesso físico aos ativos tangíveis, como pessoas, servidores, desktops, dispositivos de rede – switches, roteadores, racks de telecomunicação, racks de redes – path panéis, painéis de controle elétricos, painéis de controle de climatização, dispositivos de armazenamento de dados e outros recursos valiosos.

A ausência de controles e mecanismos de proteção físico e redundante, que impeçam as ameaças de acessarem fisicamente uma infraestrutura de TI e/ou o ambiente interno corporativo da empresa, bem como outros que impeçam que uma infraestrutura de TI se torne indisponível ou perca a sua integridade, pode afetar a confiabilidade dos processos operacionais realizados no dia a dia dentro do ambiente corporativo e, causar danos e perdas financeiras, perdas materiais e de imagem/reputação perante ao mercado, ao meio ambiente, a sociedade e junto aos seus clientes, consumidores, fornecedores e parceiros comerciais.

A ideia principal desta camada é a de criar um perímetro de segurança físico no qual busca-se estabelecer níveis de segurança física na infraestrutura de TI e em todo ambiente da empresa de forma segmentada. No geral, o perímetro de segurança física é composto por mecanismos de proteção e segurança tais como: muros, cercas e pontos de controle de acesso físico nas partes mais externas da empresa; sistemas de alarme, sensores de movimento, circuitos fechados de TVs, fechaduras

eletrônicas, cartões de acesso, dispositivos de segurança biométrica, vigilantes, porteiros, dentre outros nas partes externas e internas da empresa.

2.3. Camada 3: Segurança de Perímetro

A camada segurança de perímetro, tem como objetivo implementar a proteção necessária entre o mundo exterior e a infraestrutura de TI interna do ambiente corporativo. Ou seja, o perímetro é a fronteira da rede onde os dados fluem de e para outra rede, incluindo a internet. Portanto, é essencial fortalecer as defesas ao longo da borda da rede para promover uma proteção mais abrangente. A defesa de perímetro permite a entrada de dados autorizados, bloqueando o tráfego suspeito e é composta por vários mecanismos e ferramentas tecnológicas diferentes.

É importante que as empresas por meio das suas equipes de TI ou segurança da informação, criem um ponto de estrangulamento, ou seja, um funil ou ponto único por onde todos os dados entrem e saiam de suas redes. Este caminho único tem como principal objetivo analisar em profundidade todos os dados que trafegam nesta única via, evitando que algum tipo de ameaça perpassasse para dentro da rede ou que algum dado ou informação vaze para fora, ou seja, para o ambiente externo.

Nesta camada encontramos como mecanismos e ferramentas de proteção, dispositivos de borda tais como: roteadores, switches do tipo layer 3, appliances de firewall (UTM), sistemas de IDS e IPS para detecção e prevenção de intrusos, sistemas DLPs que previnem a perda de dados. Além de esquemas como DMZ – zonas desmilitarizadas de rede –, sistemas de proxy e conversão de endereços de rede (NAT), VPN – redes virtuais privadas –, para prover acesso externo aos ativos de TI de forma segura, dentre outras tecnologias de proteção.

É importante ressaltar que alguns desses mesmos dispositivos de proteção podem também estar presentes dentro da rede interna da empresa, realizando a proteção entre as redes e os ativos internos de TI da empresa e podem também fazer parte de outras medidas de proteção dispostas nas outras camadas da estratégia de defesa em profundidade.

2.4. Camada 4: Segurança Rede Interna

“Não pense nos oponentes que não estão atacando; se preocupe com sua própria falta de preparação”. Esta frase retirada do livro Os Cinco Anéis de Miyamoto Musashi, ilustra bem o conceito, que devemos considerar que não existem apenas ameaças externas. Ou seja, ameaças que vêm somente do lado de fora do ambiente corporativo. Mas sim, também podem existir ameaças internas, que vêm de dentro do ambiente interno da empresa. Ou seja, de dentro da rede corporativa da empresa.

A camada de segurança rede interna da estratégia de defesa em profundidade, deve possuir mecanismos e ferramentas de proteção capazes de lidar com a identidade e autenticação dos usuários da rede, autorizando ou não, o acesso destes usuários aos recursos computacionais e de redes disponíveis na infraestrutura de TI. Devem também realizar a proteção dos dados e informações que fluem pela rede, por meio de mecanismos de monitoramento e filtragem que realizem de forma automática a análise consistente de todos os pacotes de dados que circulam na rede e respectivamente os protocolos e portas utilizadas durante o processo de transmissão e recepção de dados.

Há ainda outros dispositivos de proteção utilizados que podem estar dispostos em outras camadas, que farão também parte do conjunto de mecanismos e ferramentas de proteção da camada de segurança de rede interna. Como exemplo de tais dispositivos, citamos: os sistemas de firewall internos que cuidam do tráfego dos pacotes de dados que circulam dentro da rede interna, os sistemas de IPS e IDS que buscam detectar e mitigar acessos não autorizados, os sistemas de Proxy que realizam o conceito de NAT (Network Address Translation), a conversão de um endereçamento IP público para um endereçamento IP privado, um sistema de DLP (Data Loss Prevention) que permite de forma automática o monitoramento dos dados com o propósito de prevenir a perda ou vazamento de dados ou informações confidenciais ou pessoais, além de outras tecnologias como, sistemas que realizam autenticação de usuários e dispositivos baseados no protocolo IEEE 802.1x; sistemas que implementam o protocolo IPSec (conjunto de protocolos que tem como objetivo proteger a comunicação IP, autenticando e criptografando cada pacote IP de uma

sessão de comunicação), NAC – protocolo que permite a restrição de disponibilidade de recursos de rede, VLans ou redes locais virtuais que possibilita as equipes de segurança da informação realizar a segmentação de redes internas, isolando e realizando um controle maior do domínio de broadcast, dentre outras soluções e ferramentas.

É importante ressaltar que, além dos mecanismos e ferramentas citada anteriormente, esta camada tem como missão realizar o levantamento, avaliação e o gerenciamento de vulnerabilidades presentes em um ambiente de infraestrutura de TI, permitindo assim, que as equipes de segurança da informação e segurança cibernética descubram os possíveis vetores de ataque e falhas junto aos seus ativos de TI e que possam ser explorados por ameaças e gerar riscos ao ambiente corporativo e toda a infraestrutura de TI.

2.5. Camada 5: Segurança de Host (dispositivos)

A camada de segurança de host, concentra-se em manter a proteção dos hosts e respectivamente dos sistemas operacionais que controlam estes hosts. Para aqueles que não sabem a definição de host, podemos dizer que um “host” é qualquer dispositivo computacional – computador, servidor, impressora, ou outro qualquer que possua um protocolo de comunicação, receba um endereçamento IP e, que possa ser ligado a uma rede de computadores pública ou privada.

Prover mecanismos e ferramentas de proteção nessa camada, é uma tarefa especialmente desafiadora, pois esses dispositivos são projetados para realizar multitarefas e interagir com vários outros dispositivos, aplicativos, protocolos e serviços, simultaneamente. Outro fator desafiador e relevante a essa camada está associado ao universo de dispositivos de diversas marcas, modelos e fabricantes que em alguns casos requer uma atenção especial quanto as vulnerabilidades que podem existir no dispositivo em si e que podem comprometer toda a segurança da infraestrutura de TI, mas também as possíveis incompatibilidades entre tais

dispositivos e os mecanismos e ferramentas de proteção implementados na referida camada e em toda a infraestrutura de TI.

Dentre os mecanismos e ferramentas tecnológicas que podem ser implementadas nessa camada, destacam-se: sistemas de firewall desenvolvidas para computadores pessoais; sistemas de detecção e prevenção de intrusão baseados em host (HIPS ou HIDS); sistemas de gestão ou gerenciamento de identidades e acessos; sistemas de detecção de vírus, malwares e outras ameaças virtuais; sistemas de gerenciamento de patches e atualizações de segurança, sistemas de registro e auditoria de logs; sistemas de controle de inventário e monitoramento de hardware, etc.

2.6. Camada 6: Segurança Aplicação

Não muito diferente da camada anterior em termos de diversidade, a camada de segurança aplicação, da estratégia de defesa em profundidade, tem como objetivo manter os aplicativos, os sistemas de informação e demais outros softwares (dos mais variados tipos e aplicabilidades) mais seguros e protegidos contra falhas sistêmicas, operacionais e ameaças virtuais. Lembre-se que essa camada irá cuidar da proteção de “todos” os tipos de softwares e aplicativos, incluindo os sistemas de informação, tais como: CRM, ERP, BI etc., que manipulam e processam todos os dados e informações em um ambiente corporativo.

Um aplicativo ou sistema de informação mal protegido dentro de um ambiente corporativo, podem fornecer para as ameaças, o acesso e controle de forma fácil ao seus dados e informações, comprometendo não só os ativos de TI, mas também levando riscos a empresa e seu modelo de negócio.

Nesta camada, encontramos diversos mecanismos e ferramentas de proteção, tais como: gateway de aplicação (Proxy); sistemas de gerenciamento de identidade e acessos (IAM) a aplicativos e demais softwares e recursos computacionais; sistemas de filtragem de conteúdo, ACLs (regras) de liberação de

acesso, além de sistemas de monitoramento de serviços, de updates de patches de correção de bugs e falhas do tipo 0-day, entre outros.

2.7. Camada 7: Segurança Dados

Considerada a camada de segurança mais profunda da estratégia de defesa em profundidade e a mais valiosa em termos de ativos de TI, a mesma tem como principal objetivo proteger os “dados” que estão armazenados nos sistemas de gerenciamento de banco de dados, bem como o seu processamento, transmissão e descarte.

Atualmente, os dados são considerados o novo “petróleo” do mundo digital. Isto porque eles são fonte essenciais para a formação de informações que permitem as empresas conhecer seus clientes e concorrentes, realizar o planejamento estratégico, conquistar novos mercados, criar ou aperfeiçoar produtos e serviços e, principalmente garantir a sua sobrevivência em um mercado cada vez mais competitivo. Assim sendo, os dados são considerados o objetivo final de quase todas as medidas de segurança de TI e, alvo principal dos criminosos e ameaças cibernéticas.

As estratégias de proteção nessa camada devem se concentrar nos dados armazenados, incluindo os dispositivos de armazenamento, nos dados em trânsito e no descarte desses dados quando não forem mais necessários.

É importante ressaltar que nos últimos anos, devido à valorização dos dados, principalmente dos dados pessoais, muitas nações vêm impondo leis rigorosas como a GDPR – lei geral de proteção de dados da união europeia e a LGPD – lei geral de proteção de dados pessoais no Brasil, com o objetivo de fazer com que as empresas adotem medidas, controles administrativos e técnicas que garantem a proteção e a privacidade de dados pessoais, contra o tratamento indevido, roubo ou vazamento de informações que possam colocar em risco a integridade física ou causar qualquer dano moral, social ou de vida de um indivíduo – pessoa física.

Como exemplo de mecanismos e ferramentas de proteção que devem ser implementados nessa camada, podemos citar, a criptografia de disco, por meio de sistemas como Bitlocker, a criptografia de dados, realizada nos sistemas de gerenciamento de banco de dados e aplicações, os esquemas de proteção de disco baseados em matriz redundante de discos independente – RAID, o gerenciamento de identidade e acessos (IAM), já mencionado DLP, sistemas utilizados para prevenir a perda e vazamento de dados, os esquemas e sistemas de cópia de segurança (backup e restore), esquemas de fail over, sistemas de verificação de integridade de dados, sistemas de classificação de dados, sistema de Data Wiping e Cleansing, sistemas de gerenciamento de risco de dados, sistemas de proteção de dados móveis (aplicações mobile) - DLP para dados em repouso, DLP para dados em uso e DLP para dados em movimento.

Capítulo 3. Mecanismos de Proteção – DID

Antes de começarmos a apresentar alguns mecanismos de proteção que podem ser utilizados na estratégia de defesa em profundidade – segurança em camadas, as equipes de segurança da informação e segurança cibernética, devem estar atentas a dois pontos importantes: o primeiro ponto é reconhecer os caminhos pelos quais uma ameaça cibernética pode percorrer para tentar comprometer a infraestrutura de TI de uma empresa, e o segundo é compreender quais seriam seus possíveis objetivos.

Compreender esses dois pontos torna as equipes de segurança mais preparadas para identificar, responder e proteger todos os ativos de TI contra a diversos tipos de ameaças, mitigando os pontos passíveis de ataque. Ou seja, realizando o tratamento adequado das vulnerabilidades presentes em uma infraestrutura de TI.

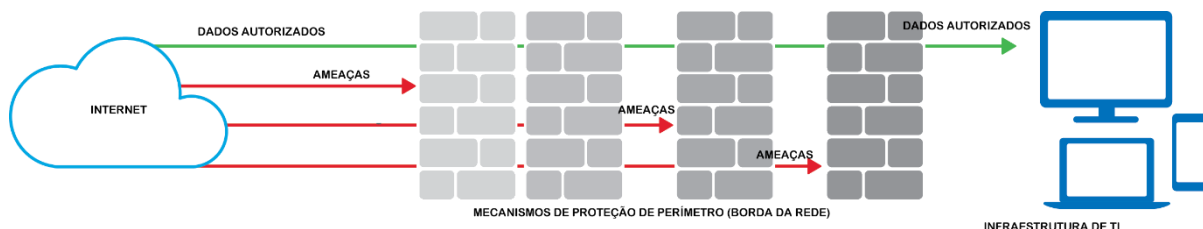
Bem, pensando nos dois pontos importantes apresentados, vamos começar a apresentar alguns mecanismos de proteção que podem fortalecer a segurança de uma infraestrutura de TI.

3.1. Segurança Perímetro

Conforme observamos no capítulo anterior, a camada segurança de perímetro ou, em alguns casos, denominada proteção de borda na estratégia de defesa em profundidade, tem como objetivo estabelecer e garantir a proteção necessária entre o mundo exterior e a infraestrutura de TI interna de uma empresa. Ou seja, sua missão é fazer com que as ameaças que estão do lado de fora não consigam acessar o ambiente interno da empresa. Essa proteção é realizada através da implementação de mecanismos e ferramentas tecnológicas que realizam o monitoramento, controle e proteção de todos os pontos de entrada e saída de dados e informações que a empresa possui. Em termos técnicos, a segurança do perímetro visa monitorar, controlar e proteger a comunicação dos dados e as conexões

existentes entre a rede pública conhecida como “WAN” e a rede local privada, denominada de “LAN”.

Figura 5 - Proteção Segurança Perímetro.

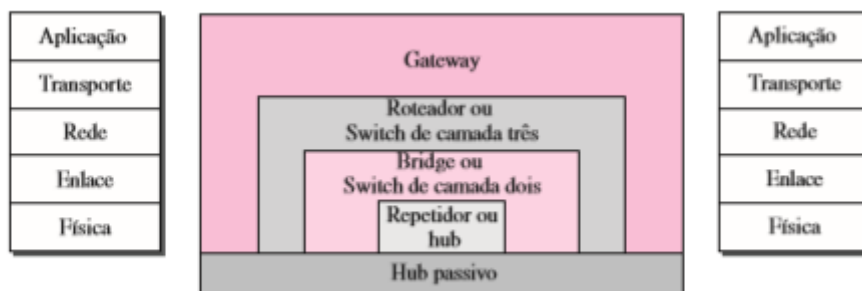


3.2. Roteadores, Switchs e ACLs

Em uma infraestrutura de TI de qualquer empresa, iremos encontrar as redes de computadores locais ou LAN. Normalmente as LANs não operam dentro de uma infraestrutura de TI de forma isolada. Elas são conectadas entre si ou à internet. Para que essa interligação aconteça os segmentos de LANs usam dispositivos de conexão que podem operar em diferentes camadas do modelo de arquitetura TCP/IP.

Os dispositivos de conexão, podem ser classificados em cinco categorias, que definimos como: (a) Aqueles que operam abaixo da camada física da arquitetura TCP/IP, por exemplo, um hub; (b) Aqueles que operam na camada física da arquitetura TCP/IP, por exemplo um repetidor ou hub ativo; (c) Aqueles que operam nas camadas física e de enlace da arquitetura TCP/IP, por exemplo uma bridge (ponte) ou um switch L2 (camada dois); (d) Aqueles que operam nas camadas física, de enlace e de rede da arquitetura TCP/IP, por exemplo um roteador ou switch L3 (camada três); e (e) Aqueles que operam em todas as cinco camadas da arquitetura TCP/IP, por exemplo um gateway. Em nossos estudos vamos abordar os dispositivos de conexão que atuam nas camadas física, de enlace e de rede, do modelo de arquitetura TCP/IP especificamente os roteadores e switch L3.

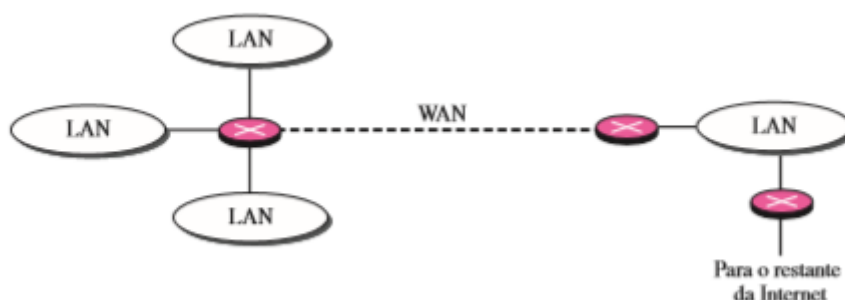
Figura 6 - Relacionamento Arquitetura TCP/IP vs. Dispositivos de Conexão.



Um roteador é um dispositivo de conexão utilizado em redes de computadores que direciona pacotes de dados a partir da leitura de seus protocolos e endereços lógicos. Além de realizar o direcionamento de pacotes de dados, um roteador também interliga redes de computador distintas (LAN e WAN), promovendo a comunicação entre essas redes.

Um roteador possui uma tabela de roteamento, que é usada para tomar decisões sobre a rota pela qual esses pacotes irão seguir até chegarem ao seu destino. As tabelas de roteamento podem ser do tipo estático, no qual os administradores de redes realizam as configurações das rotas (endereços pelos quais os pacotes irão seguir na rede) de forma manual e dinâmico, no qual as rotas são obtidas e atualizadas de forma automática, usando-se os protocolos de roteamento.

Figura 7 - Rede Interligada por Roteadores.



Exercendo os papéis de interligação, encaminhamento e controle do fluxo de pacote dados, que são transmitidos entre redes de computadores distintas, na

estratégia de defesa em profundidade, o roteador é considerado o primeiro mecanismo de proteção da infraestrutura TI. Atuando em conjunto com o roteador, em alguns casos podemos encontrar o switch de camada três ou simplesmente switch L3.

Os switches L3, possuem funções e funcionalidades similares a de um roteador. Porém, possuem recursos computacionais e de configurações mais sofisticados, possibilitando as equipes de TI realizarem a segmentação de suas redes LANs e estruturas de redes virtuais conhecidas como VLANs. Essa segmentação em VLANs, proporciona um maior gerenciamento, controle e proteção dos hosts conectados a essa LAN ou VLAN. Mas, atenção, quanto utilizamos o termo Switch, temos que ter cuidado. Isto porque, um switch pode significar duas coisas distintas. Por isso é importante no ato do esclarecimento do termo, acrescentarmos o nível no qual o dispositivo opera na rede LAN e, consecutivamente, na arquitetura do modelo TCP/IP.

Para entender melhor esse significado, podemos ter em uma infraestrutura de redes de computadores, um switch de camada dois, também denominado de switch L2, que opera nas camadas física e de enlace da arquitetura TCP/IP, e que possui o papel de uma bridge (ponte) com muitas portas que possibilita alocar em cada porta um único host de maneira que esse possua a sua própria independência na LAN ou VLAN, mas este tipo de switch não possui funções de encaminhamento de pacotes entre duas redes distintas. Ou seja, não possui funções de roteamento de pacotes de dados de rede. Já um switch de camada três - switch L3, além de atuar nas camadas física e de enlace, também atua na camada de redes da arquitetura TCP/IP, proporcionando outras funções e funcionalidades similares a de um roteador. Ou seja, realizando a interligação de redes LANs e VLANs e, encaminhando os pacotes de dados entre essas redes, através da tabela de roteamento e seus protocolos de conexão.

Bem, voltando aos roteadores, os mesmos podem ser arranjados em uma infraestrutura de TI, de acordo com a sua função ou funcionalidade na rede LAN ou WAN. Como exemplo podemos citar: (a) os roteadores de núcleo de rede interna, que

são utilizados para estabelecer conexões internas, ou seja, somente entre as redes LANs de uma empresa, não se comunicando com as redes WANs; (b) os roteadores de borda que estão localizados nas “bordas” de uma rede e são responsáveis em realizar a interligação entre várias redes LAN/WAN e WAN/WAN; e (c) os roteadores sem fio, que possibilitam interligar redes cabeadas e redes sem cabo, possibilitando a interconexão de diversos tipos de dispositivos sem fio.

Figura 8 - Exemplificação Core Router.

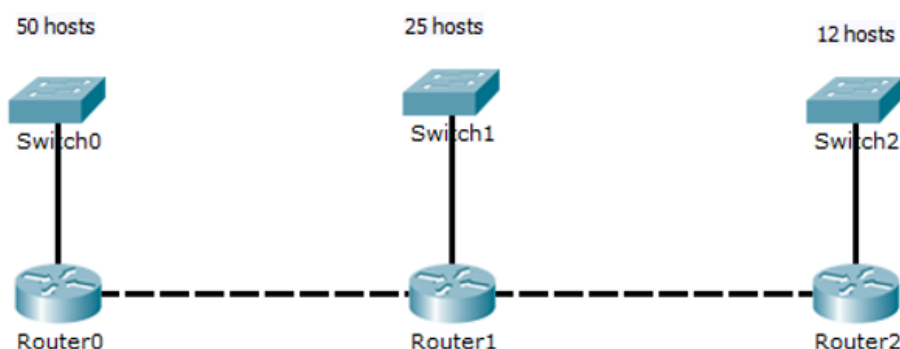


Figura 9 - Exemplificação Roteadores de Borda.

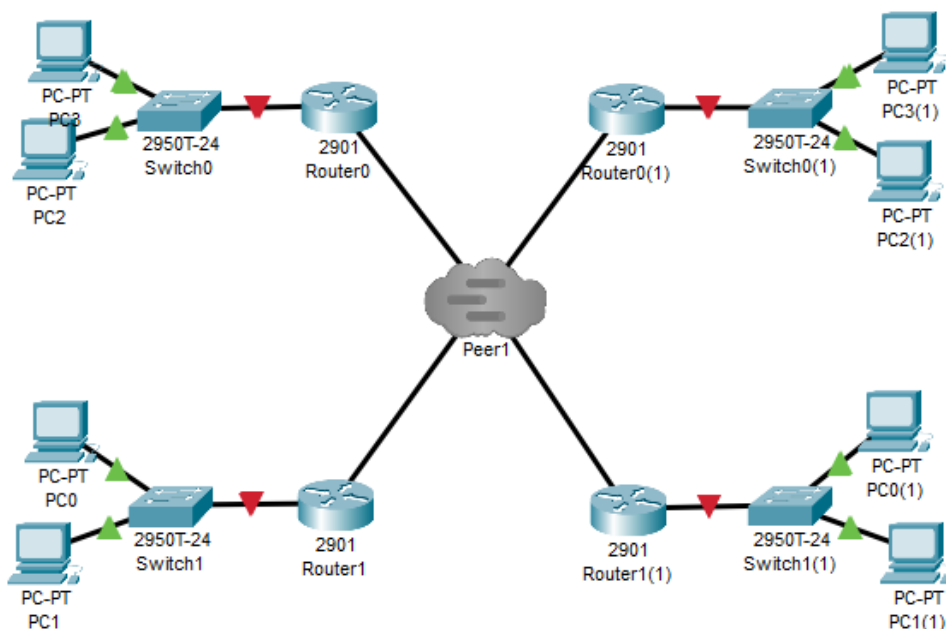
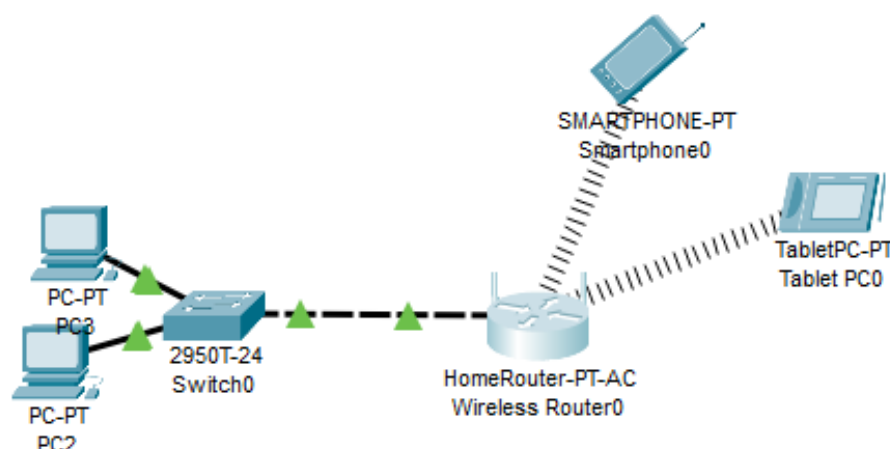


Figura 10 - Exemplificação Roteador sem fio.



No geral, as equipes de segurança da informação, segurança cibernética e de administração de redes, podem aumentar os níveis de proteção na camada de perímetro, por meio da aplicabilidade de ACLs – Access Control List ou Lista de Controle de Acessos, em seus roteadores e switches L3 ou L2. Essas listas de controle são utilizadas para classificar e controlar o tráfego dos pacotes que passam pelas interfaces dos roteadores ou switches. As ACLs são configuradas de acordo com critérios estabelecidos por essas equipes e suas políticas, sendo na maioria dos casos utilizada para determinar se um pacote será encaminhado ou descartado em uma interface ou porta do roteador ou switch.

Tais ações realizadas por uma ACL devem seguir por padrão uma definição do que se deve permitir ou negar, tendo como base o endereço de origem do tráfego, o endereço de destino do tráfego e o protocolo/porta a ser utilizado.

Além, de realizar a validação dos pacotes de dados, permitindo ou não o envio ou recebimento dos mesmos entre as redes LAN e WAN, as ACLs também possibilitam as equipes de TI realizar a priorização do envio ou recebimento dos pacotes de dados, através da implementação de QoS junto aos protocolos, bem como o balanceamento de carga e consecutivamente a aplicabilidade de mecanismos de redundância contra quedas ou perdas de conexão de links de comunicação.

Atualmente vários modelos de roteadores e switch L3 e L2 possuem uma interface gráfica que pode ser acessada localmente ou remotamente por meio de navegadores de internet, possibilitando as equipes de TI habilitarem inúmeras funções e configurar diversas funcionalidades de maneira bem prática e intuitiva.

#Dica: Uma boa maneira de aprender a dominar a criação de ACLs em roteadores é montando laboratórios por meio da utilização do software Cisco Packet Trace, disponível no website do fabricante Cisco Network no endereço <https://www.netacad.com/pt-br/courses/packet-tracer>. Lá você encontrará uma série de exercícios práticos que permitirão você aumentar o conhecimento de como criar e trabalhar com ACLs.

3.3. Firewall

O firewall é um dos principais componentes de segurança de uma empresa, como também o mais conhecido e antigo. O termo firewall significa “barreira de fogo” e sua missão é impedir que dados, sistemas e ameaças externas vindas da rede WAN – no geral a internet – não acessem o ambiente dados, sistemas e dispositivos conectados à rede interna (Lan) da empresa, limitando o caminho das conexões, como as permissões de cada uma. Ou seja, podemos dizer que um firewall é a barreira que permite ou não o fluxo de dados entre duas redes distintas.

Para que você possa compreender melhor o funcionamento de um firewall em uma infraestrutura de TI, imagine-o como sendo uma portaria de um prédio com um porteiro. Para que você tenha acesso aos apartamentos desse prédio, você precisa obedecer as regras estabelecidas pelo condômino do prédio, como por exemplo se identificar, dizer em qual apartamento você vai, ser esperado pelo morador do apartamento, ser autorizado por esse morador para entrar no prédio e na maioria dos casos, não portar qualquer tipo de objeto que possa trazer risco à segurança do prédio; para sair, não se pode levar nada que pertence aos moradores ou ao prédio sem a devida autorização. Pois bem, o firewall é exatamente essa

portaria e porteiro em nossa infraestrutura de TI, mas especificamente na rede interna da empresa.

Um firewall pode impedir uma série de ações maliciosas, como por exemplo, inibir que uma ameaça qualquer que tente se conectar a um computador dentro da rede LAN, sem a devida autorização, ou bloquear um determinado aplicativo que esteja enviando ou solicitando dados ou conexões não autorizadas.

Firewall é um ponto entre duas ou mais redes no qual circula todo o tráfego. A partir deste tráfego é possível controlar e autêntica o tráfego, além de registrar por meio de logs, todo o tráfego da rede, facilitando sua auditoria. É um dos maiores destaques para hackers, pois se ele conseguir acessá-lo, pode alterar suas permissões e alcançar o bem mais valioso das empresas – a informação”. Podendo ser também definido como um componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre conjuntos de redes. (CHAPMAN, CHESWICK, STEVEBELLOVIN, 2016).

Os primeiros modelos de firewall foram inseridos em roteadores, no final da década de 80, por estarem em posição privilegiada, conectando redes distintas. As regras eram baseadas em ACLs de origem, destino e tipo de pacote. Porém, com o advento da WEB, foi necessário separar as funcionalidades do firewall dos roteadores.

No geral, o uso mais comum do firewall é proteger uma rede privada, normalmente considerada segura e confiável, com dados e informações importantes, porém de acesso restritivo, contra acessos das inúmeras ameaças que podem tentar, sem autorização, acessar à rede privada para realizar ações mal-intencionadas como por exemplo: o roubo de dados e informações, a negação de serviços que possam comprometer as operações da empresa, etc.

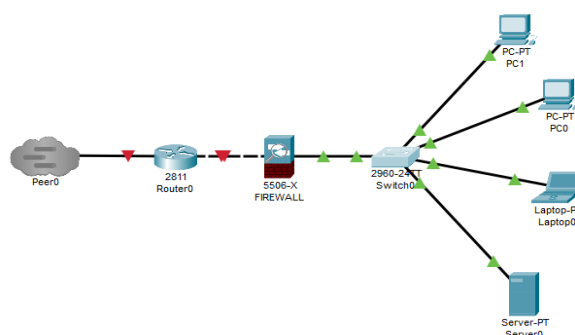
Tecnicamente falando, um firewall é um dispositivo de hardware composto por duas ou mais interfaces de rede no qual após ser configurado de acordo com as políticas de segurança da informação e interligado as redes interna e externa (LAN e

WAN), realizam o monitoramento e o controle de todos os pacotes de dados recebidos e transmitidos, incluindo os protocolos utilizados por esses pacotes, permitindo ou não que os mesmos sigam a diante e alcancem o seu destino. Neste contexto, é importante dizer que todo pacote de dados enviados de uma rede para a outra deverá passar obrigatoriamente pelo firewall e esse, por sua vez, terá que analisar esse pacote com o propósito de verificar se o mesmo representa ou não algum perigo a rede interna e, se for o caso, descarta-lo antes que esse pacote possa alcançar seu destino.

No geral, um firewall é configurado para prover uma filtragem controlada do tráfego da rede, permitindo acessos restritos a certos protocolos e portas de comunicação na internet, e bloqueando o acesso a quase todo o resto das outras conexões e garantir a segurança da rede LAN contra acessos interativos que possam ser autenticados, geralmente provenientes de ameaças externas que estão presentes nas redes WAN, especialmente nas internets.

Diversos especialistas em segurança da informação e cibersegurança costumam dizer que implementar um sistema de firewall em uma rede LAN corporativa é essencial e vital à segurança dessa rede contra ameaças externas. Isto porque, torna-se o único meio de acesso existente entre a rede externa e a rede interna e promove o controle do tráfego que chega e sai entre essas redes, protegendo e restringindo acessos indevidos à hosts e aplicativos contidos dentro da rede LAN ou também da rede WAN.

Figura 11 - Função do Firewall.



Lembre-se, o objetivo de um firewall é formar uma linha fechada de defesa projetado para proteger os ativos de TI de uma empresa e sua infraestrutura de TI. Para tal, o mesmo deve atender a algumas condições: (a) deve ser parte integrante da política global de segurança da informação da empresa, de modo a evitar ser contornado facilmente por meios disponíveis a qualquer dos colaboradores internos; (b) todo o tráfego de dados para dentro ou fora da rede corporativa deve passar obrigatoriamente pelo firewall, para poder ser inspecionado; (c) deve permitir apenas a passagem do tráfego especialmente autorizado e bloquear imediatamente qualquer outro; (e) deve ser imune à penetração, uma vez que não pode oferecer nenhuma proteção ao perímetro interno uma vez que um atacante consiga atravessá-lo ou contorna-lo.

3.3.1. Tipos de Firewall

Percebe-se que, a julgar pela variedade de tipos, os firewalls podem ser implementados de várias formas para atender às mais diversas necessidades. Este aspecto leva a outra característica importante do assunto: a arquitetura de um firewall.

Quando falamos de arquitetura, nos referimos à forma como o firewall é projetado e implementado. Há, basicamente, três tipos de arquitetura. Veremos elas a seguir.

Arquitetura **Dual-Homed Host** – nesta arquitetura, o firewall fica disposto entre a rede LAN e a rede WAN. O nome da arquitetura se deve ao fato de este firewall possuir ao menos duas interfaces de rede, uma para cada “lado”. Perceba que não há outro caminho de comunicação, portanto, todo o tráfego passa por este firewall, não havendo acesso da rede interna para a rede externa (e vice-versa) diretamente. A principal vantagem desta abordagem é que há grande controle do tráfego. A desvantagem mais expressiva, por sua vez, é que qualquer problema com o dual-homed – uma invasão, por exemplo – pode pôr em risco a segurança da rede ou mesmo paralisar o tráfego. Por esta razão, o seu uso pode não ser adequado em redes cujo acesso à internet é essencial. Este tipo de arquitetura é bastante utilizado para firewalls do tipo proxy.

Arquitetura **Screened Host** – na arquitetura Screened Host, em vez de haver um único firewall servindo de intermediador entre a rede LAN e a rede WAN, há duas: uma que faz o papel de roteador (*screening router*) e outra chamada de *bastion host*. O bastion host atua entre o roteador e a rede LAN, não permitindo comunicação direta entre ambos os lados. Perceba então que se trata de uma camada extra de segurança: a comunicação ocorre no sentido *rede interna – bastion host – screening router – rede externa* e vice-versa. O roteador normalmente trabalha efetuando filtragem de pacotes, sendo os filtros configurados para redirecionar o tráfego ao bastion host. Este, por sua vez, pode decidir se determinadas conexões devem ser permitidas ou não, mesmo que tenham passado pelos filtros do roteador. Sendo o ponto crítico da estrutura, o bastion host precisa ser bem protegido, do contrário, colocará em risco a segurança da rede interna ou ainda poderá torná-la inacessível.

Arquitetura **Screened Subnet** – este tipo de arquitetura também conta com a figura do bastion host, mas este fica dentro de uma área isolada de nome interessante: a *DMZ*, sigla para *Demilitarized Zone* – Zona Desmilitarizada. A DMZ, por sua vez, fica entre a rede interna e a rede externa. Acontece que, entre a rede LAN e a DMZ há um roteador que normalmente trabalha com filtros de pacotes. Além disso, entre a DMZ e a rede WAN, há outro roteador do tipo. Note que esta arquitetura se mostra bastante segura, uma vez que, caso o invasor/ameaça passe no primeiro roteador, terá ainda que lidar com a zona desmilitarizada. Esta inclusive pode ser configurada de diversas formas, com a implementação de proxies ou com a adição de mais bastion hosts para lidar com requisições específicas, por exemplo. O nível segurança e a flexibilidade de configuração fazem da Screened Subnet uma arquitetura normalmente mais complexa e, conseqüentemente, mais cara.

3.3.2. Filtragem de Pacotes (*packet filtering*)

As primeiras soluções de firewall surgiram na década de 1980 baseando-se em **filtragem de pacotes** de dados (***packet filtering***), uma metodologia mais simples e, por isso, mais limitada, embora ofereça um nível de proteção significativo.

Para compreender, é importante saber que cada pacote de dados transmitido ou recebido na rede, possui um cabeçalho com diversas informações a seu respeito,

como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros. O Firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log.

A transmissão dos dados é feita com base no padrão TCP/IP (***Transmission Control Protocol/Internet Protocol***), que é organizado em camadas. A filtragem normalmente se limita às camadas de rede e de transporte: a primeira é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e processos de roteamento, por exemplo; a segunda é onde estão os protocolos que permitem o tráfego de dados, como o TCP e o UDP.

Com base nisso, um firewall de filtragem pode ter, por exemplo, uma regra que permita todo o tráfego da rede local que utilize a porta UDP 123, assim como ter uma política que bloqueia qualquer acesso da rede local por meio da porta TCP 25.

Podemos encontrar dois tipos de firewall de filtragem de pacotes. O primeiro utiliza o que é conhecido como ***filtros estáticos***, enquanto o segundo é um pouco mais evoluído, utilizando ***filtros dinâmicos***.

Na filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro. A princípio, esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão. É possível então que os filtros contenham regras que permitem o tráfego destes serviços, mas ao mesmo tempo bloqueiem as respostas/requisições necessárias, impedindo a execução da tarefa. Esta situação é capaz de ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, aumentando os riscos de o firewall não filtrar pacotes que deveriam ser, de fato, bloqueados.

A filtragem dinâmica surgiu para superar as limitações dos filtros estáticos. Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para “criar” regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente. Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

3.3.3. Firewall de Aplicação ou Proxy de Serviço

O firewall de aplicação, também conhecido como “proxy de serviços” ou apenas “proxy” é uma solução de proteção que atua como um ponto intermediário entre um host ou uma rede interna e outra rede, externa, no geral a internet. Normalmente, trata-se de um dispositivo “appliance” que possui um hardware com poder de processamento e memória superior, devido ao tratamento que deve ser realizado ao lidar com muitas requisições.

Firewall deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino. Por exemplo, em vez de a rede LAN (interna) se comunicar diretamente com a rede WAN (externa), há um dispositivo (proxy) entre ambas as redes, criando duas conexões – a primeira entre a LAN e o Proxy e, a segunda entre o Proxy e a WAN.

Todo o fluxo de dados necessita passar pelo proxy. Desta forma, é possível, por exemplo, estabelecer ACLs (regras) que impeçam o acesso de determinados endereços externos, assim como que proíbam a comunicação entre hosts internos e determinados serviços remotos. Este controle amplo também possibilita o uso do proxy para tarefas complementares: o equipamento pode registrar o tráfego de dados em um arquivo de log; conteúdo muito utilizado pode ser guardado em uma espécie de cache (uma página Web muito acessada fica guardada temporariamente no proxy, fazendo com que não seja necessário requisitá-la no endereço original a todo instante, por exemplo); determinados recursos podem ser liberados apenas mediante autenticação do usuário; entre outros.

A implementação de um proxy não é tarefa fácil, haja visto a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que,

dependendo das circunstâncias, este tipo de firewall não consiga ou exija muito trabalho de configuração para bloquear ou autorizar determinados acessos.

3.3.4. Firewall: Inspeção de Estado (*Stateful Inspection*)

Sendo tratado por alguns especialistas no assunto como uma evolução dos filtros dinâmicos, os firewalls de **inspeção de estado** (*stateful inspection*) trabalham fazendo uma espécie de comparação entre o que está acontecendo e o que é esperado para acontecer.

Para tanto, firewalls de inspeção analisam todo o tráfego de dados para encontrar estados, isto é, padrões aceitáveis por suas regras e que, a princípio, serão usados para manter a comunicação. Estas informações são então mantidas pelo firewall e usadas como parâmetro para o tráfego subsequente.

Para entender melhor, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um cliente e um servidor. Os pacotes de dados iniciais informam quais portas TCP serão usadas para estas tarefas. Se de repente o tráfego começar a fluir por uma porta não mencionada, o firewall pode então detectar esta ocorrência como uma anormalidade e efetuar o bloqueio.

3.3.5. Firewall de Aplicações WEB (WAF)

O WAF é um novo tipo de firewall criado para combater as ameaças que estão além das capacidades dos firewalls tradicionais. Ele cria uma barreira entre o seu serviço baseado na web e todo o resto da internet, bloqueando e protegendo a aplicação de ações criminosas, como manipulação de conteúdo exibido, conhecida como “pichação”, injeções indevidas em banco de dados de padrão SQL ou simplesmente “SQL Injection”, determinados tipos de fraudes em acesso administrativo e várias outras espécies de ciberataques.

A maneira como o WAF atua, garante que todos os tipos de negócio/empresas tenham suas redes protegidas adequadamente, ajudando as equipes de segurança da informação e segurança cibernética no combate às principais ameaças e assegurando a continuidade das operações da empresa.

O Web Application Firewall trabalha para impedir qualquer exposição de dados não autorizada em um site ou aplicativo baseado na web. Não é exagero algum dizer que um ataque organizado a um site é capaz de arruinar um modelo de negócio ou uma empresa, especialmente lojas virtuais que armazenam os dados dos usuários: sem a segurança adequada, essas informações podem facilmente cair nas mãos de criminosos cibernéticos.

Neste contexto, o WAF trabalha monitorando, filtrando e bloqueando automaticamente o tráfego de dados potencialmente maliciosos, liberando a TI da sua empresa para decidir quem terá o acesso impedido. Além disso, ele também é altamente escalável, permitindo a definição de um conjunto de regras para evitar os ataques mais comuns. O WAF pode ser executado como uma aplicação de rede, plug-in de servidor ou serviço na nuvem. Cada tipo apresenta suas vantagens e desvantagens, como você pode ver a seguir.

WAF de Rede - esse modelo é normalmente baseado em hardware e, por ser instalado localmente, tende a ser mais rápido. Seu gerenciamento é normalmente oferecido como um serviço, o que pode tornar as coisas mais simples — e, por ter um conjunto central de assinaturas e opções de configuração, vários aplicativos podem ser protegidos com menos esforço. Como ponto negativo dos WAFs de rede, podemos ressaltar os altos custos não apenas do hardware necessário para a implementação da tecnologia, mas de todas as suas dependências, tais como contingência de energia por gerador e links redundantes de internet de altíssima largura.

WAF de Host - a maior vantagem desse modelo é a possibilidade de incluir opções de personalização a um custo baixo — afinal, como é totalmente baseado em software, ele pode ser integrado no próprio código do aplicativo. Porém, a tarefa de gerenciar os WAFs de host pode ser um tanto desafiadora, já que eles demandam bibliotecas locais, ambientes compatíveis (como Java ou .net) e são dependentes de recursos de servidores locais para funcionarem de forma eficaz.

WAF na Nuvem - já os WAFs hospedados na nuvem são geralmente administrados pelos provedores do serviço, que disponibilizam uma interface de

configuração adequada às necessidades do cliente. Além de fáceis de implantar, são oferecidos em modelo de assinatura — o que os transforma na opção mais econômica e escalável de todas.

Independentemente do tipo de WAF que for implementado, é recomendável que a equipe de segurança faça alguns treinamentos de administração. Em muitos casos, quanto mais uma empresa desejar ter um papel profundo nas configurações de gerenciamento, mais treinos serão necessários. Seja quem for que administre o Web Application Firewall, é importante ter ainda um time de desenvolvimento envolvido na tarefa, já que um WAF configurado incorretamente pode ter impacto negativo na performance e disponibilidade da aplicação que protege.

Uma alternativa para eliminar a necessidade desses esforços pela empresa é contratar os serviços de um IaaS (Infrastructure as a Service, ou Infraestrutura como um Serviço). Por uma taxa fixa mensal, você pode contar com o auxílio de profissionais especializados que cuidarão de todas as tarefas relacionadas ao WAF, liberando o seu time de TI para as tarefas estratégicas da companhia.

O WAF fornece proteção garantida contra as dez ameaças de segurança mais críticas identificadas pela comunidade on-line OWASP (*Open Web Application Security Project*, ou Projeto Aberto de Segurança em Aplicações Web). São elas:

1. Injection;
2. Broken Authentication and Session Management;
3. Cross-Site Scripting (XSS);
4. Broken Access Control;
5. Security Misconfiguration;
6. Sensitive Data Exposure
7. Insufficient Attack Protection;
8. Cross-Site Request Forgery (CSRF);
9. Using Components with Known Vulnerabilities;

10. Underprotected APIs.

O tráfego proveniente de ataques consome banda de internet, infraestrutura e recursos operacionais. Como o WAF bloqueia esses acessos inconvenientes, sua empresa acaba evitando todos esses gastos desnecessários.

Por fim, é importante ressaltar que qualquer tipo de firewalls terá limitações, sendo que estas variam conforme o tipo de solução e a arquitetura utilizada. De fato, firewalls são recursos de segurança bastante importantes, mas não são perfeitos em todos os sentidos. Resumindo este aspecto, podemos mencionar as seguintes limitações: (a) um firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede (ou mesmo de um computador). Esta situação pode gerar mais gastos para uma ampliação de infraestrutura capaz de superar o problema; (b) A verificação das políticas e regras contidas no firewall precisam ser revisadas periodicamente para não prejudicar o funcionamento de novos serviços; (c) Novos serviços ou protocolos podem não ser devidamente tratados por proxies já implementados; (d) Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede LAN; (e) Um firewall pode não ser capaz de identificar uma atividade maliciosa que acontece por descuido do usuário – quando este acessa um site falso de um banco ao clicar em um link de uma mensagem de e-mail, por exemplo; (f) Firewalls precisam ser “vigiados”. Malwares ou atacantes experientes podem tentar descobrir ou explorar brechas de segurança em soluções do tipo; (g) Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma conexão 4G (justamente para burlar as restrições da rede, talvez), o firewall não conseguirá interferir.

3.3.6. Firewall Pessoal e UTM

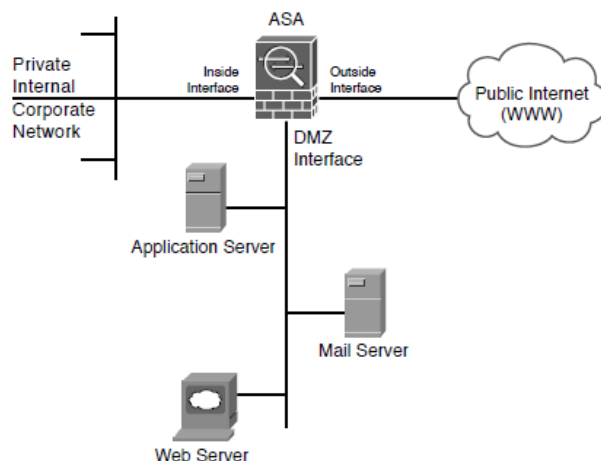
Conforme observamos, as arquiteturas de firewall nos mostram as opções de configuração de firewalls em redes. Mas, como você provavelmente sabe, há firewalls mais simples destinados a proteger o seu computador, seja ele um desktop, um laptop, um tablet, enfim. São os **firewalls pessoais** (ou domésticos), que **DEVEM** ser utilizados por qualquer pessoa.

Felizmente, sistemas operacionais atuais para uso doméstico ou em escritório costumam conter firewall interno por padrão, como é o caso de distribuições Linux, Windows ou Mac OS X. Além disso, é comum desenvolvedores de antivírus oferecerem outras opções de proteção junto ao software, entre elas, um firewall.

Existem ainda outras soluções de firewall que podem ser utilizadas para proteger a infraestrutura de TI da empresa. Estas por sua vez, são soluções “embarcadas”, ou seja, que possuem um conjunto de hardwares e softwares específicos e projetados exclusivamente para atuar com firewall. A grande vantagem de um firewall deste tipo “firewall de hardware” é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para lidar com grandes volumes de dados e não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional (por conta de uma falha em outro software, por exemplo).

3.4. DMZ – Zona Desmilitarizada (Demilitarized Zone)

DMZ é uma sigla para Demilitarized Zone (Zona Desmilitarizada em português), trata-se de uma sub-rede que se situa entre uma rede confiável (a rede da sua empresa, por exemplo) e uma rede não confiável (geralmente a internet), provendo assim isolamento físico entre as duas redes, garantido por uma série de regras de conectividade mantidas no firewall. O aspecto do isolamento físico do DMZ é importante pôr ele garantir que a rede WAN (a internet no caso) acesse apenas os servidores isolados no DMZ, ao invés de acessar diretamente a rede interna (LAN) da empresa, como pode ser visto a seguir. Os servidores mais comumente encontrados no DMZ são os que prestam algum tipo de serviço externo como por exemplo os servidores de e-mail, arquivos FTP, e páginas HTML.



Apenas por curiosidade: O termo DMZ surgiu no meio militar, e significava uma área entre as áreas aliadas e inimigas. A DMZ (no sentido original, não computacional) mais famosa do mundo fica entre as fronteiras da Coreia do Norte e Coreia do Sul, que desde o fim da Guerra da Coreia (1953) ainda não assinaram um tratado de paz.

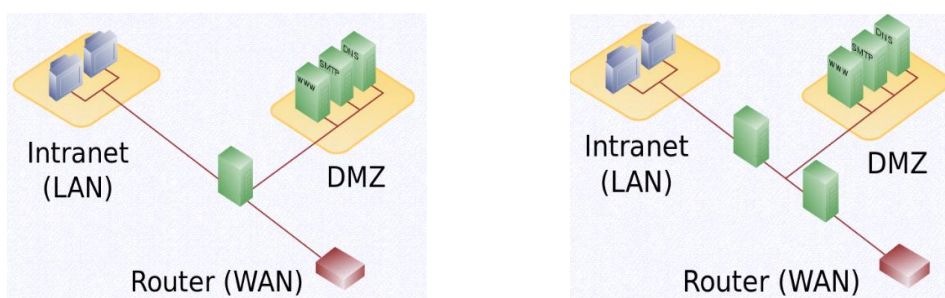
Quanto as arquiteturas do DMZ, podemos implementar as seguintes:

(a) **Single Firewall** – trata-se de uma arquitetura comumente encontrada nas infraestruturas de TI das empresas. Qualquer firewall com pelo menos 3 interfaces de rede pode formar uma arquitetura desse tipo. Neste caso, A primeira interface de rede conecta o firewall à internet através do provedor de acesso (ISP), a segunda interface forma a rede interna (LAN) e a terceira interface é usada para criar a DMZ. Esse tipo de arquitetura é considerado vulnerável devido ao fato de o firewall ter que lidar com as requisições para a rede interna e o DMZ, sendo um ponto óbvio de ataque na arquitetura de segurança da rede.

(b) **Multiple Firewall** – considerada a arquitetura DMZ a mais segura. Utiliza mais de um firewall (geralmente dois), onde o primeiro, também chamado de firewall exterior ou de "front-end" é utilizado para direcionar o tráfego da internet para a DMZ apenas, enquanto os demais são utilizados para direcionar o tráfego da DMZ para a rede interna (LAN). Esse tipo de arquitetura é considerado mais seguro pois para que a rede interna seja comprometida, é necessário que os dois firewalls sejam comprometidos. Por isso, quando essa arquitetura é utilizada, é comum que se

usem firewalls de fabricantes diferentes, pois é mais difícil que as falhas de segurança encontradas no produto de um fabricante sejam encontradas no produto de outro, tornando assim a rede mais segura e confiável. Um exemplo dessa arquitetura pode ser visto na figura a seguir.

Figura 12 - DMZ: Single Firewall e Multiple Firewall.



Capítulo 4. Proteção: Rede Interna

Nesta camada podemos adotar diversos tipos de mecanismos e ferramentas tecnológicas para garantir a proteção da rede LAN da empresa. A seguir iremos estudar os mais utilizados e implementados pelas equipes de segurança da informação e segurança cibernética.

4.1. Switches Layer 2 e 3

De acordo com a estratégia de defesa em profundidade “segurança em camadas”, precisamos garantir que a rede interna “LAN” da empresa possua barreiras que possam impedir, dificultar e inibir o acesso de ameaças (invasores) aos ativos de TI internos, caso as barreiras de proteção de borda sejam vencidas.

No passado as conexões locais entre os hosts da rede eram realizadas por meio de dispositivos denominados “HUBs” ou repetidores. Estes dispositivos eram extremamente inseguros e não possuíam inteligência para tratar os pacotes de dados que passam por eles. Ou seja, apenas realizam a repetição da transmissão dos pacotes de dados por toda a rede. E, o pior, replicando essa transmissão aos hosts de toda rede. Isso sem dúvida apresentava um risco de segurança enorme, uma vez que uma ameaça poderia ser replicada a todos os hosts da rede.

Atualmente o envio e recebimento dos pacotes de dados em uma rede local é realizada por roteadores ou switches, que por possuírem uma “inteligência”, possibilitam a otimização de todo o tráfego da rede local, realizando a transmissão dos pacotes de dados de forma isolada, host a host sem mais replicar essa transmissão a todos os hosts da rede e, única exclusivamente, a aquele host que requisitou a transmissão e está autorizado a recebê-la. Esse novo modelo proporcionou uma maior proteção e segurança as redes locais.

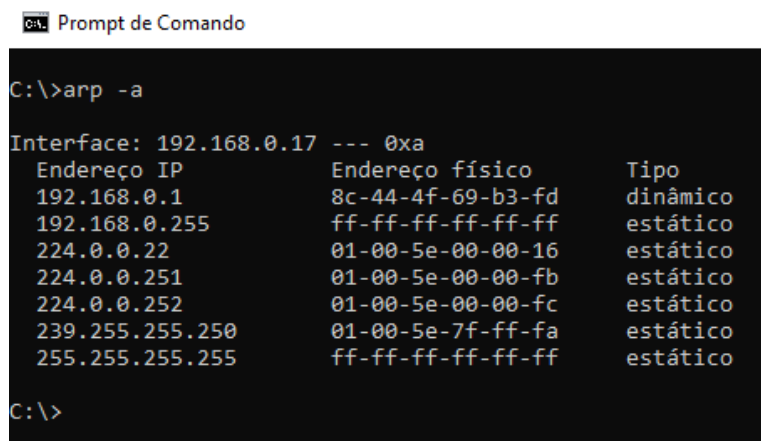
Os switches layer 2 e layer 3 são dispositivos computacionais que possuem mecanismos de gerenciamento que podem ser configurados de acordo com as necessidades de proteção e segurança desenhadas pelas equipes de TI. São

conhecidos comumente como switches gerenciáveis de camada 2 ou camada 3 do modelo de arquitetura TCP/IP.

A utilização de switches gerenciáveis como mecanismos de proteção a rede interna possibilita inúmeras vantagens, dentre as quais destacamos:

- Otimização das transmissões dos pacotes de dados por evitar problemas de colisão de dados durante a transmissão;
- Proteção da transmissão de pacotes de dados entre os host conectados à rede, através de um controle de endereçamento físico entre os hosts e as redes conhecido como endereços MAC – Media Access Control, um endereço físico configurado pelo fabricante em um hardware que possui conectividade à rede por meio do protocolo ethernet que fica armazenado em uma tabela denominada tabela ARP no switch que tem como função principal realizar o relacionamento entre o endereçamento IP utilizados junto as aplicações e o endereço físico “MAC” utilizado na camada enlace do modelo de arquitetura TCP/IP.

Figura 13 - Representação da Tabela ARP contida em um Host.



```

C:\>arp -a

Interface: 192.168.0.17 --- 0xa
Endereço IP      Endereço físico      Tipo
192.168.0.1      8c-44-4f-69-b3-fd    dinâmico
192.168.0.255    ff-ff-ff-ff-ff-ff    estático
224.0.0.22       01-00-5e-00-00-16    estático
224.0.0.251      01-00-5e-00-00-fb    estático
224.0.0.252      01-00-5e-00-00-fc    estático
239.255.255.250  01-00-5e-7f-ff-fa    estático
255.255.255.255  ff-ff-ff-ff-ff-ff    estático

C:\>
  
```

- A criação de redes virtuais denominada VLANs – redes locais virtuais que possibilitam a criação de sub-redes (redes distintas), fortalecendo a proteção e a segurança da rede local, tema que iremos estudar a seguir.

4.2. VLANs – Redes Locais Virtuais

Existem inúmeras definições para uma rede local virtual, como pode ser observado na bibliografia.

- Varadarajan as define como *"estruturas capazes de segmentar, logicamente, uma rede local em diferentes domínios de broadcast"*.
- Já Molinari diz que *"uma rede virtual é um grupo de estações e servidores que se comunica independentemente de sua localização física ou topologia, como se fosse um único domínio broadcast, ou uma rede lógica."*

De acordo com as definições apresentadas, a implantação de VLANs possibilita a partição de uma rede local em diferentes segmentos lógicos (criação de novos domínios broadcast), permitindo que usuários fisicamente distantes (por exemplo, um em cada local ou andar da empresa) estejam conectados à mesma rede.

Como fatores motivadores a criação de VLANs em uma infraestrutura de TI no ambiente corporativo, imagine uma empresa, cujo crescimento acelerado impossibilitou um projeto ordenado de expansão, que possua uma dezena de departamentos conectados a uma rede local interna. Ao contrário do que se pensa, os funcionários de cada departamento estão espalhados pelos andares da sede. Como organizar um domínio para cada setor da empresa? Uma solução possível seria a segmentação da rede interna em redes virtuais, uma para cada departamento.

Outro exemplo é a formação de grupos temporários de trabalho. Hoje em dia é comum o desenvolvimento de projetos envolvendo diversos setores de uma empresa, como marketing, vendas, contabilidade e comercial. Durante o período do projeto, a comunicação entre seus membros tende a ser alta. Para conter o tráfego broadcast, pode-se implementar uma VLAN para este grupo de trabalho.

Os exemplos anteriores mostram que as VLAN proporcionam uma alta flexibilidade a uma rede local. Isto é ideal para ambientes corporativos, onde a todo momento ocorrem mudanças de empregados, reestruturações internas, aumento do

número de usuários, entre outras situações. Entre os benefícios proporcionados pela implantação de redes virtuais podemos citar:

- **Controle do tráfego broadcast** – as VLANs apresentam um desempenho superior as tradicionais redes locais, principalmente devido ao controle do tráfego broadcast. Tempestades de quadros broadcast (*broadcast storms*) podem ser causadas por mal funcionamento de placas de interface de rede, conexões de cabos malfeitas e aplicações ou protocolos que geram este tipo de tráfego, entre outros. Em redes onde o tráfego broadcast é responsável por grande parte do tráfego total, as VLANs reduzem o número de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede. De um outro ponto de vista, em uma rede local segmentada, os domínios de broadcast são menores. Isto porque cada segmento possui um menor número de dispositivos conectados, comparado ao existente na rede sem segmentação. Com isso, trafegam menos quadros broadcast tanto em cada segmento, quanto em toda rede.
- **Segmentação lógica da rede** – como visto anteriormente, redes virtuais podem ser criadas com base na organização setorial de uma empresa. Cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isto proporciona uma segmentação lógica da rede.
- **Redução de custos e facilidade de gerenciamento** – grande parte do custo de uma rede se deve ao fato da inclusão e da movimentação de usuários dela. Cada vez que um usuário se movimenta é necessário um novo cabeamento, um novo endereçamento para estação de trabalho e uma nova configuração de repetidores e roteadores. Em uma VLAN, a adição e movimentação de usuários pode ser feita remotamente pelo administrador da rede (da sua própria estação), sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade.

- **Independência da topologia física** – VLANs proporcionam independência da topologia física da rede, permitindo que grupos de trabalho, fisicamente diversos, possam ser conectados logicamente a um único domínio broadcast.
- **Maior segurança** – as redes locais virtuais limitam o tráfego a domínios específicos proporcionando mais proteção e segurança a estes. O tráfego em uma VLAN não pode ser "escutado" por membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas. Desta forma, o acesso a servidores que não estejam na mesma VLAN é restrito, criando assim "*domínios de segurança no acesso a recursos*".

Dispositivos em uma rede local virtual podem ser conectados de três maneiras diferentes, sendo:

- **Enlace tronco (*Trunk Link*)** – todos os dispositivos conectados a um enlace deste tipo, incluindo estações de trabalho, devem, obrigatoriamente, ter suporte à VLANs. Todos os pacotes de dados transmitidos em quadros em um *trunk link* possuem um rótulo VLAN.
- **Enlace de Acesso (*Access Link*)** – um enlace de acesso conecta um dispositivo sem suporte a VLAN a uma porta de um switch. Todos os pacotes de dados transmitidos em quadros neste tipo de enlace, obrigatoriamente, não devem possuir rótulo;
- **Enlace Híbrido (*Hybrid Link*)** – este é uma combinação dos dois enlaces anteriores. Em um enlace híbrido são conectados tanto dispositivos com suporte a VLANs, quanto os sem. Num enlace desta natureza pode haver quadros com (*tagged frames*) e sem rótulo (*untagged frame*), mas todos os quadros para uma VLAN específica têm de ser com rótulo VLAN ou sem rótulo.

Capítulo 5. Camada: Proteção Hosts (Segurança de Host)

Conforme estudamos no capítulo 2, a camada de segurança de host, concentra-se em manter a proteção dos hosts e respectivamente dos sistemas operacionais que controlam estes hosts. Porém, prover mecanismos e ferramentas de proteção nessa camada é uma tarefa especialmente desafiadora para as equipes de segurança da informação e segurança cibernética. Isto porque, esses dispositivos são projetados para realizar multitarefas e interagir com vários outros dispositivos, aplicativos, protocolos e serviços, simultaneamente.

Neste contexto é importante que as equipes de segurança busquem implementar dispositivos de fabricantes de hardware e software que seguem o conceito de segurança por design e segurança por default. Estes dois conceitos expressam a responsabilidade dos fabricantes de hardwares e desenvolvedores de softwares acerca da preocupação em aumentar os níveis de segurança no planejamento, fabricação e desenvolvimentos de dispositivos de hardware ou softwares.

Segurança por design significa que o hardware ou a aplicação (software) deve ser desenhado (planejado) para prover segurança desde sua concepção, passando por um processo de modelagem de ameaças como parte de sua análise, uma inspeção regular de código durante e ao término do desenvolvimento e testes de invasão durante a homologação das versões. Já a segurança por default significa que o hardware ou a aplicação (software) quando é entregue ao usuário, deve ser configurado com a menor superfície de ataque possível, e seguindo a recomendação de privilégio mínimo, ou seja, com o mínimo de recursos habilitados e com usuários configurados para terem permissão de executar somente o necessário para a operação normal do sistema ou do dispositivo. Qualquer recurso ou privilégio adicional deve ser habilitado pelo usuário administrador, de acordo com sua demanda ou políticas de segurança.

Outro exemplo sobre segurança por design e por default, vem sendo divulgado e implementado quanto ao quesito “proteção à privacidade dos dados pessoais”. Neste caso, podemos citar como exemplo a Lei Geral de Proteção de

Dados Pessoais brasileira – LGPD que tem como um dos princípios a serem seguidos pelas empresas, a adoção de segurança baseada em privacidade por design e privacidade por default.

Bem, considerando que o fabricante de hardware ou o desenvolvedor de software teve o cuidado de seguir estes dois princípios, resta as equipes de segurança manter a infraestrutura de TI fortalecida, ou ainda, reforçar a proteção e a segurança dela, de acordo com a classificação de risco que esta infraestrutura receber. Para manter o host fortalecidos, ou seja, devidamente protegidos, devemos:

- (a) Sempre manter atualizado **todos** os sistemas operacionais e ativos de rede;
- (b) Eliminar **todos** os serviços desnecessários ou não utilizados pelos usuários;
- (c) **Utilizar** baselines de fontes confiáveis;
- (d) **Dividir** as funções entre servidores para reduzir a superfície de ataque;
- (e) **Remover** funcionalidades ou recursos desnecessários ou não utilizados pelos usuários.

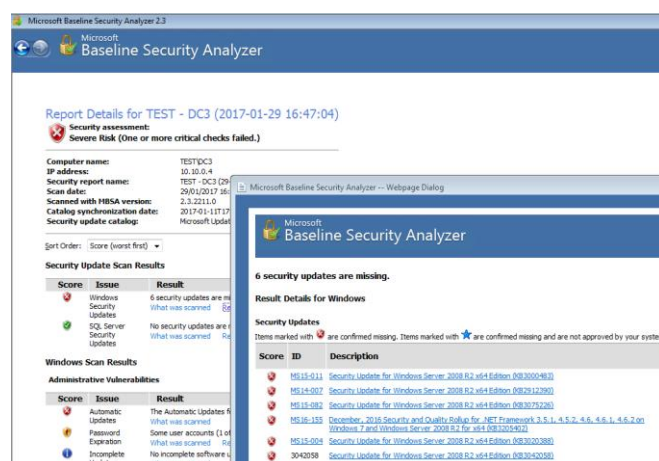
5.1. Baselines, Bugs, Atualizações e Correções

Para que as equipes de segurança da informação e segurança cibernética possam fortalecer a proteção dos hosts existentes em suas redes internas, existem diversos guias que fornecem orientações sobre as melhores práticas para realizar configurações nos hosts, proporcionando aumentar a proteção e a segurança nos mesmos, sejam eles roteadores, switches, desktops, servidores ou servidores de alta criticidade. Porém, é importante termos em mente que cada configuração de segurança aplicada ao host pode dificultar a usabilidade dele, e até mesmo fazer com que algumas aplicações ou sistemas parem de funcionar. Por este motivo as equipes de segurança ou as equipes de TI, devemos analisar estes guias de *Hardening* minuciosamente, verificando quais configurações podem ou não ser aplicadas em suas infraestruturas de TI e consecutivamente nos hosts pertencentes a mesma.

Além dos guias, existem alguns softwares que nos ajudam as equipes de segurança e de TI, na tarefa de verificar a configuração dos hosts e compará-las a um baseline estabelecido pelo fabricante do hardware ou software. Uma das ferramentas

de baseline mais utilizadas por inúmeras equipes de TI e que serve para tal propósito é o MBSA (*Microsoft Baseline Security Analyser*), um programa gratuito que pode ser baixado do site da Microsoft, que permite a equipe de TI realizar uma análise acurada de um ou mais hosts na rede, indicando quais configurações estão de acordo com o Baseline da Microsoft e quais não estão.

Figura 14 - Resultado obtido após a execução do MBSA.

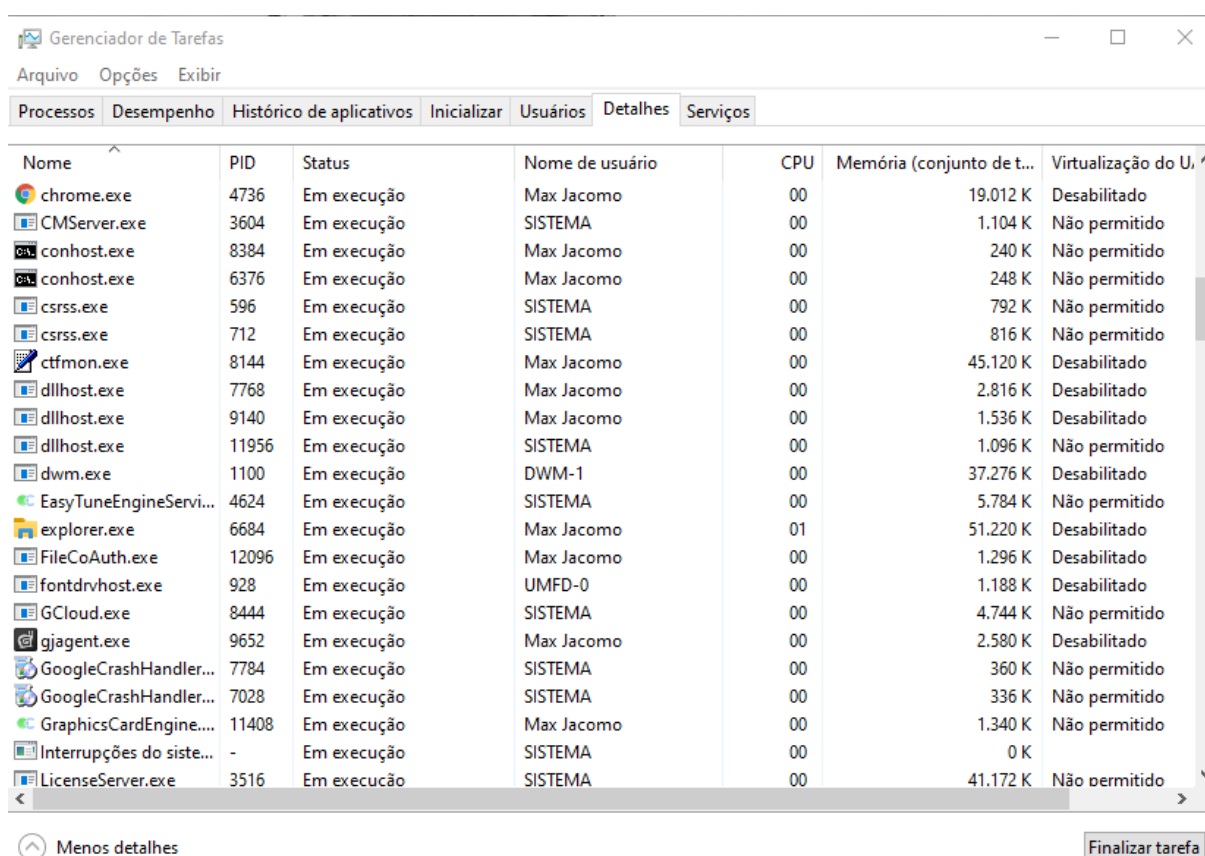


Bugs são tão antigos como a própria computação e receberam este nome porque os primeiros defeitos nos computadores foram causados por pequenos insetos que causavam curtos nas placas de circuitos deles. Segundo a Wikipédia, um bug é um erro no funcionamento comum de um software ou hardware, também chamado de falha na lógica de um programa que pode causar comportamentos inesperados, como resultado incorreto ou comportamento indesejado. São, geralmente, causados por erros no próprio código-fonte, mas também podem ser causados por algum framework, interpretador, sistema operacional ou compilador.

O problema com os bugs é que eles podem levar ao comprometimento da segurança de todo o sistema. Quando um pesquisador consegue encontrar um Bug em um sistema ele pode explorar este Bug para fazer com que o sistema saia de seu comportamento normal e execute o código desejado pelo invasor.

Um dos Bugs mais comuns é o **Buffer Overflow**. O Buffer é a memória utilizada para guardar as entradas de um usuário, e geralmente tem um tamanho pré-

fixado. Quando um usuário envia mais dados que o Buffer foi programado para suportar, estes dados passam então a ocupar um espaço de memória destinado a guardar outras entradas de usuários e até mesmo um ponteiro, destinado a guardar o endereço de memória onde o programa deve executar a próxima instrução. Um buffer overflow é realizado em cima de uma função de uma aplicação e como consequência ele se apodera de todos os recursos que o sistema operacional destina àquele processo. Uma informação importante a ser feita para avaliar o impacto do buffer overflow em um programa, é saber com quais privilégios este programa é executado. Para entender melhor como uma ameaça pode explorar um buffer overflow, observe a figura a seguir:



Nome	PID	Status	Nome de usuário	CPU	Memória (conjunto de t...	Virtualização do U...
chrome.exe	4736	Em execução	Max Jacomo	00	19.012 K	Desabilitado
CMServer.exe	3604	Em execução	SISTEMA	00	1.104 K	Não permitido
conhost.exe	8384	Em execução	Max Jacomo	00	240 K	Não permitido
conhost.exe	6376	Em execução	Max Jacomo	00	248 K	Não permitido
csrss.exe	596	Em execução	SISTEMA	00	792 K	Não permitido
csrss.exe	712	Em execução	SISTEMA	00	816 K	Não permitido
ctfmon.exe	8144	Em execução	Max Jacomo	00	45.120 K	Desabilitado
dllhost.exe	7768	Em execução	Max Jacomo	00	2.816 K	Desabilitado
dllhost.exe	9140	Em execução	Max Jacomo	00	1.536 K	Desabilitado
dllhost.exe	11956	Em execução	SISTEMA	00	1.096 K	Não permitido
dwm.exe	1100	Em execução	DWM-1	00	37.276 K	Desabilitado
EasyTuneEngineServi...	4624	Em execução	SISTEMA	00	5.784 K	Não permitido
explorer.exe	6684	Em execução	Max Jacomo	01	51.220 K	Desabilitado
FileCoAuth.exe	12096	Em execução	Max Jacomo	00	1.296 K	Desabilitado
fontdrvhost.exe	928	Em execução	UMFD-0	00	1.188 K	Desabilitado
GCloud.exe	8444	Em execução	SISTEMA	00	4.744 K	Não permitido
gjagent.exe	9652	Em execução	Max Jacomo	00	2.580 K	Desabilitado
GoogleCrashHandler...	7784	Em execução	SISTEMA	00	360 K	Não permitido
GoogleCrashHandler...	7028	Em execução	SISTEMA	00	336 K	Não permitido
GraphicsCardEngine...	11408	Em execução	Max Jacomo	00	1.340 K	Não permitido
Interrupções do siste...	-	Em execução	SISTEMA	00	0 K	
LicenseServer.exe	3516	Em execução	SISTEMA	00	41.172 K	Não permitido

Podemos perceber que em um sistema operacional de um host, haverá diversas aplicações, serviços e funcionalidades sendo executadas simultaneamente e, que rodam de acordo com os privilégios de cada usuário. Como exemplo na figura a seguir é possível visualizar a aplicação “chrome.exe” sendo executada sob o

privilégio do usuário “max jaco””. Enquanto a aplicação “CMServer.exe” está sendo executado sob e com os privilégios do usuário “sistema”.

Figura 15 - Usuário Privilegiado e Não Privilegiado.

Arquivo Opções Exibir						
Processos Desempenho Histórico de aplicativos Inicializar Usuários Detalhes Serviços						
Nome	PID	Status	Nome de usuário	CPU	Memória (conjunto de t...	Virtualização do U. ^
chrome.exe	4736	Em execução	Max Jacomo	00	19.012 K	Desabilitado
CMServer.exe	3604	Em execução	SISTEMA	00	1.104 K	Não permitido
conhost.exe	8384	Em execução	Max Jacomo	00	240 K	Não permitido
conhost.exe	6376	Em execução	Max Jacomo	00	248 K	Não permitido

No caso da primeira aplicação, como o usuário “max jaco” possui menos privilégios se comparado com um usuário do tipo sistema, caso este usuário seja alvo de alguma ameaça, o impacto junto ao sistema operacional do host será menor. Tendo em vista que o “max” não possui acesso privilegiado. Agora caso ocorra um buffer overflow provocado por uma ameaça/invasor no aplicativo CMServer.exe que por sua vez foi escalonado para ser utilizado pelo usuário “sistema” que possui privilégios maiores se comparado com os privilégios configurados ao usuário “max jaco”, o resultado poderia ser catastrófico visto que por se tratar de um aplicativo “serviço” que está escalonado para um usuário com “poder” ou melhor “acesso” privilegiado, este invasor ou ameaça poderia adquirir o acesso e controle total do sistema operacional, o que causaria uma grande falha de segurança no host.

No caso de atualizações e/ou correções, é comum que muitos dispositivos de hardware e aplicativos “softwares” logo após o seu lançamento possua uma vulnerabilidade que não foi descoberta durante as fases de teste e homologação. Assim sendo, tal vulnerabilidade ficará em um estado latente até que algum pesquisados – geralmente um hacker – contratado ou não pelo fabricante ou desenvolvedor a encontre. A índole do pesquisador vai ditar as regras de quando ele irá publicar a vulnerabilidade encontrada. Se o pesquisador estiver apoiando o fabricante ou desenvolvedor, e este tratar segurança como algo sério, a vulnerabilidade somente será publicada após uma correção estar disponibilizada para os usuários. Caso ele não se importe com o fabricante ou com os usuários, a

vulnerabilidade pode ser publicada assim que ele a descobrir ou quando ele já tiver um código que a explore.

Porém, existe ainda uma outra possibilidade, a que ele “os pesquisadores” não venha a publicá-la, e sim disponibilizá-la para um criador de vírus que se utilizam de “0-days”, ou seja, exploração de vulnerabilidades zero ou menos dias antes da publicação da correção, para causar algum tipo de dano ao hardware ou ao software no intuito de obter algum benefício para si. Uma vez que a correção é publicada, inicia-se o período de homologação por parte do usuário, que pode levar de horas a dias. Os últimos estudos mostram que os vírus baseados em 0-days, ou em correções recém-lançadas, têm tido uma penetração maior em empresas do que em usuários domésticos, porque estes contam com um serviço de atualização automática, e as organizações perdem um tempo valioso em seu processo de homologação, que apesar de importante deve ser tratado com prioridade para que essa não fique exposta a ameaças durante muito tempo. Como dica para o gerenciamento de atualizações e/ou correções de vulnerabilidades, destacam-se: (a) utiliza fontes externas confiáveis para identificar vulnerabilidades; (b) estabelecer uma escala de atualização de 24 horas a 30 dias de acordo com a exposição e criticidade do sistema; (c) possuir um ambiente completo de homologação e testes.

A título de curiosidade, as vulnerabilidades 0-day (ou de dia zero) são aquelas em que hackers encontram, e que poderiam ser exploradas antes que os desenvolvedores tenham tempo de reagir a respeito. Mas é claro que nem todas as vulnerabilidades descobertas são do tipo 0-day. A maioria das falhas de segurança são descobertas por outros desenvolvedores ou hackers em programas de Bug Hunting, por exemplo. Grandes players desenvolvedores de softwares como a Microsoft e a Google, possuem projetos voltados a descobrir falhas de segurança em seus softwares e em softwares de outras empresas antes que elas se tornem públicas.

Estes projetos possuem como objetivo tornar a internet mais segura. Isso porque, com tempo suficiente para consertar as vulnerabilidades, os desenvolvedores podem lançar um patch de correção para que os usuários atualizem seus sistemas e

fiquem seguros. Afinal, uma premissa muito atestada no universo da segurança da informação é de que o usuário é o elo mais fraco da corrente e, isto por si só, já justifica o porquê de os criminosos virtuais estarem aumentando significativamente o alvo em usuários finais, uma vez que a falta de conhecimento e educação necessária em relação às boas práticas de segurança abrem diversas brechas para os criminosos virtuais adentrarem no ambiente corporativo das empresas.

5.2. Exploit, Antivírus, AntiSpam e Antimalware's

Me permita uma pergunta: Você sabe o que é um exploit? Bem, as habituais definições falam de um programa ou código que se aproveita de uma brecha de segurança (vulnerabilidade) em um aplicativo ou sistema, de forma que um atacante pode usá-la em benefício próprio.

Passando para a vida real, seria como se um modelo de fechadura (sistema ou aplicativo) tivesse uma falha que permitisse criar chaves que a abrissem a fechadura (exploit), permitindo que alguém (malware) possa acessar ao local e realizar atos ilícitos. Existe muita confusão entre os usuários e certo mito de que um exploit pode considerar-se malware. A realidade é que, como vimos no exemplo acima, exploit não é um código malicioso em si mesmo, mas apenas uma “chave” para que algum malware acesse ao sistema. Dessa forma, podem ser dadas as permissões necessárias para que o exploit possa executar-se em um sistema, aproveitando-se de uma vulnerabilidade.

Agora que você já sabe o que é um exploit, podemos distingui-lo entre dois tipos: os conhecidos ou desconhecidos (0-day).

Os exploits conhecidos são aqueles que estão mais presentes e podemos tomar medidas efetivas de proteção para evitar que os sistemas sejam afetados. Na verdade, costumam ser os que aparecem na maioria das notícias sobre segurança e, além disso, a cada dia surgem novos, da mesma forma que também vão aparecendo novas vulnerabilidades.

Por este motivo, é importante que as equipes de segurança da informação e segurança cibernética estejam informadas sobre quais vulnerabilidades estão sendo aproveitadas pelos exploits e possam ter certeza de que estão com todos os seus hosts, sistemas e aplicativos atualizados. Caso ainda não exista uma atualização disponível, a equipe de segurança deve buscar medidas técnicas que ajudem a mitigar as possíveis ameaças.

No geral, vários desenvolvedores de softwares de proteção e segurança, principalmente os desenvolvedores de sistemas de antivírus, disponibilizam ótimas ferramentas de informação, constantemente atualizada sobre as falhas, correções e novidades, embora também existam sites especializados em identificar e informar as mudanças que aparecem a cada dia, como o Exploit Data base.

Por outro lado, falamos dos exploits desconhecidos ou 0-days, os quais vemos muitas vezes nas notícias sobre segurança. Estes se utilizam das vulnerabilidades que ainda não tenham sido informadas ao público em geral e, portanto, podem representar uma grave ameaça, especialmente quando utilizam ataques dirigidos às empresas ou governos. Quando são utilizados, não é comum haver medidas que possam bloquear o malware que o aproveita e isso os converte em uma ameaça praticamente indetectável. É por isso que são bastante utilizados entre os cibercriminosos, permitindo roubar informações importantes de uma empresa ou governo e, em casos extremos, atacar certo tipo de infraestruturas críticas.

Por fim, a seguir apresentamos algumas medidas que precisam ser adotadas pelas equipes de segurança da informação e segurança cibernética para evitar que suas infraestruturas de TI sejam contaminadas por meio de malwares que utilizam de exploit:

- Manter todos os aplicativos e sistemas atualizados – sabendo que os exploits se aproveitam das brechas de segurança, é fundamental fechá-las o quanto antes. Além disso, o ideal é manter uma política de atualizações eficaz, evitando deixar uma “janela de tempo” que possa ser aproveitada pelos atacantes;

- Diminuir os efeitos de possíveis exploits usados contra nós ou contra as empresas. Pode ser que o fabricante do sistema ou aplicativo vulnerável não tenha lançado ainda uma atualização que solucione o problema. Nesse caso, pode-se utilizar ferramentas específicas e destinadas ao reconhecimento de bugs e anomalias sistêmicas. Isso ajuda a evitar que o sistema seja infectado até que apareça uma solução definitiva.
- Contar com soluções de segurança avançadas, disponibilizadas por grandes players especializados em segurança da informação e segurança cibernética, que são capazes de detectar e bloquear exploits projetados para aproveitar vulnerabilidades em navegadores web e leitores de PDF, entre outros.

Para compreendermos mais facilmente o grande número de definições referentes ao malware, é melhor dividi-lo em duas partes, sendo elas:

- Vetor de ataque é o método que o agente ameaçador utiliza para atacar um sistema. Como exemplos, podemos citar: Trojam, Phising etc.
- Payload é uma atividade mal-intencionada exercida pelo malware. O payload é uma ação separada da instalação e da propagação que o malware realiza. Como exemplo, podemos citar: Spyware, Ransomware, Rootkit etc.

Dessa forma, é comum encontramos duas classificações ao definir essas ameaças. Um malware pode ser, por exemplo, um **Trojam-Ransomware**.

Spam é o termo utilizado para se referir aos e-mails não solicitados, que geralmente são enviados para muitas pessoas. O nome Spam é a abreviação do nome de um produto alimentício, o Spiced Ham (presunto condimentado). Em 1970, a trupe do Monty Python fez um quadro onde a atendente tentava adicionar o SPAM a qualquer tipo de comida. Isso transformou o termo em uma gíria que significa uma coisa chata, que é empurrada para você.

Além de atentar contra a disponibilidade de banda das organizações, o SPAM também pode ser utilizado para enviar e-mails com trojans e vírus.

A pessoa que envia spam é chamada de spammer. Os spammers violam várias as regras de conduta na web, inclusive a do W3C, consócio de empresas de tecnologia que organismo que regulamentam padrões para a Web.

Phishing Scam trata-se de um tipo de spam que se passa por um presente ou comunicação de uma instituição conhecida, como um banco, empresa ou site popular, induzindo as pessoas a fornecer senhas, dados pessoais e financeiros, que posteriormente podem ser utilizados para roubo de identidade, operações fraudulentas etc.

Inicialmente, os phishings direcionavam as pessoas para páginas fraudulentas na internet, que apresentam formulários onde roubavam os dados pessoais e financeiros. Como essa tática passou a ser muito combatida pelos bancos e fabricantes de softwares, os phishings passaram a instalar Trojans que roubam esses dados ou interceptam uma sessão de Home Banking sem o conhecimento do usuário.

Para proteger os equipamentos da organização, é importante manter softwares de segurança nas estações (hosts), para protegê-las de ameaças como vírus e spams. Podemos ter soluções Antivírus e AntiSpam instaladas nos servidores de arquivos e de correio, assim como nas estações. O importante é certificar-se de que estão sempre ativos e atualizados.

5.3. RootKits, BackDoors e HIDS

Um rootkit é um pacote de programas maliciosos, que substituem os arquivos binários (programas compilados) por um kit de programas que mantém uma porta aberta sem que verdadeiro root (administrador do unix) perceba. Com a porta aberta o invasor pode voltar a qualquer momento e utilizar os privilégios do root (ou do usuário do serviço que ele tenha utilizado, para realizar absolutamente qualquer ação dentro do computador, inclusive roubar, alterar ou destruir qualquer informação.

O nome Rootkit é derivado do usuário root do Unix, ambiente onde essa prática se popularizou, mas existem Rootkit para quase todas as plataformas. Existem Rootkit para Solares, Mac OS, Linux e a maioria das versões do Windows, entre outros. Os Rootkit ganharam publicidade em 2005, quando foi revelado que a gravadora Sony/BMG instalava um Rootkit chamado XCP (*Extended Copy Protection*) em seus CDs de música com o objetivo de instalar um mecanismo anticópia.

Os Rootkit são extremamente difíceis de serem detectados, e infectam o sistema sem que o usuário perceba nada. É difícil garantir a completa remoção dos Rootkit de um sistema, esses programas são especializados em enganar as ferramentas de segurança para ficarem ocultos. A forma mais confiável de reaver seu computador é formatar o disco e reinstalar todo o sistema.

Já o Backdoor é uma possível fonte de vazamento de informações sensível. São os canais secretos de comunicação, ou seja, canais que dos quais os usuários ignoram a existência. Estes canais são chamados de porta de manutenção ou Backdoor, e são comumente utilizados por Trojans para comunicar-se com seu controlador, ou até mesmo fornecer acesso à máquina infectada.

São considerados Backdoor os programas ou partes de códigos escondidos em outros programas, que permitem que um invasor entre ou retorne a um computador comprometido por uma porta dos fundos, sem ter que passar pelo processo normal de autenticação. Nos primórdios da computação, os próprios programadores deixavam alguns Backdoor em seus sistemas e os chamavam de “ganchos de manutenção”.

Nos sistemas Windows, os Backdoor geralmente são Trojans, instalados através de Phishings, ou ainda programas instalados por Worms, que após explorarem uma vulnerabilidade do sistema-alvo infectam arquivos do sistema operacional e criam uma trilha adicional de execução, que mantém essa porta aberta. Esse tipo de Malware também recebe o nome de Rootkit no Windows.

Uma das soluções mais adequadas para detectar a ação de Rootkit é o Host IDS. Estes softwares salvam as informações sobre cada arquivo importante para a

segurança do sistema e de tempos em tempos eles calculam novamente o Hash destes arquivos para verificar se algum deles foi alterado. Além disso, os HIDS são capazes de realizar algumas funções como:

- Análise de logs;
- Correlação de eventos;
- Checagem de integridade;
- Aplicação de políticas de segurança;
- Detecção e alerta para Rootkit;
- Podem detectar variações na configuração do Sistema.

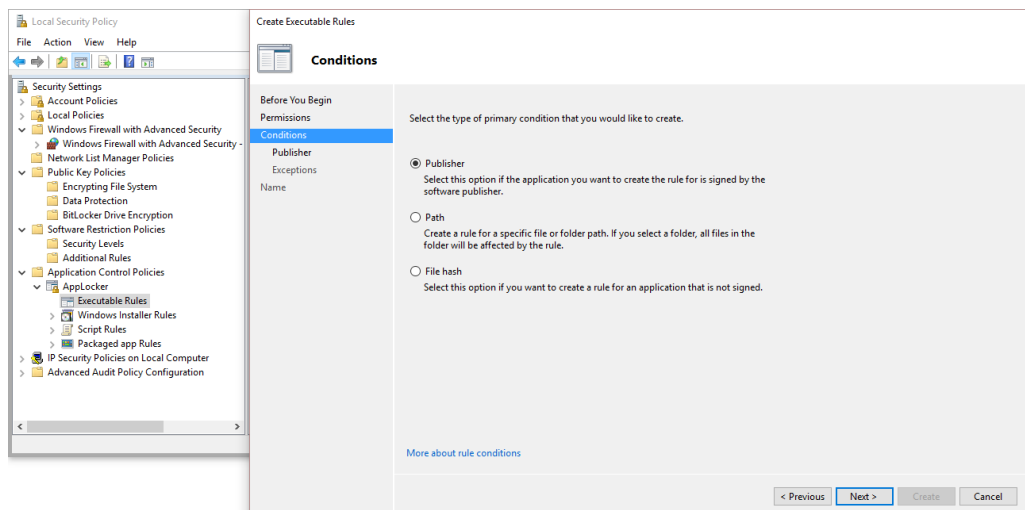
Como exemplo de ferramentas HIDS, citamos: SolarWinds Security Event Manager; Snort; Ossec; Fail2Ban; AIDE; Samhain e Suricata.

5.4. Whitelisting, Blacklist e EndPoint Security

Whitelisting ou lista de permissões, é a prática utilizada pelas equipes de segurança da informação e segurança cibernética para permitir explicitamente a algumas entidades identificadas (hosts) o acesso a um privilégio, serviço, mobilidade, acesso ou reconhecimento específico.

A proteção contra malware em uma infraestrutura de TI, em geral, depende de detecção das suas “assinaturas” por parte de um sistema de anti-malwares ou antivírus. No entanto, identificar um software malicioso é apenas uma das tantas missões que esses sistemas realizam. Na verdade, alguns especialistas diriam até que a detecção baseada em assinaturas – conhecida como Blacklisting – é o lado menos importante do trabalho de um antivírus ou anti-malwares, por exemplo. Por outro lado, existe a tarefa da criação das Whitelisting, que seria a pré-aprovação de softwares inofensivos ao contrário do bloqueio de softwares nocivos – papel da Blacklisting.

Alguns sistemas operacionais possuem funções básicas de Whitelisting. Como exemplo, podemos citar o aplicativo Windows AppLocker, que pode ser configurado para barrar ou permitir a execução de um software baseado no seu fabricante, seu caminho (pasta do executável) ou seu hash.



É possível também em servidores que possuem a função de controladores de domínios como por exemplo o Microsoft Windows Server, realizar a configuração de whitelisting e Blacklisting por meio de GPOs (Group Policies ou Diretivas de Grupo), concedendo ou negando direitos como por exemplo: instalação de programas; acessos a endereços IPs; leitura, escrita ou execução de arquivos, entre outros esquemas que possibilitam aumentar a proteção dos hosts.

Com o aumento exponencial das ameaças em infraestruturas de TI, muitos fabricantes e desenvolvedores de soluções de segurança, perceberam que as empresas necessitavam de soluções integradas de proteção dos seus hosts e passaram a oferecer a seus clientes soluções completas denominadas de soluções Endpoint Security. No geral, as soluções Endpoint Security oferecem em uma única suíte ou console, diversos mecanismos e ferramentas de segurança, a saber:

- Antimalware;
- Antivírus;
- Firewall Pessoais;

- Controle de Listas (Whitelisting);
- Aplicativos de Baseline e Avaliação de Vulnerabilidades;
- Aplicativos de criptografia de arquivos e discos de armazenamento;
- Aplicativos de Backup e Restore
- IPS, IDS e DLP;
- Entre outros.

Como exemplo de soluções Endpoint Security, citamos:

- Sophos Intercept X do fabricante Sophos;
- Kaspersky Endpoint Security do fabricante Kaspersky;
- Symantec Endpoint Security do fabricante Symantec;
- Bitdefender GravityZone Business Security do fabricante BitDefender;
- Entre outras.

Figura 16 - Endpoint Security no quadrante mágico do Gartner Group (Ago 2019).



Capítulo 6. IPS, IDS e VPN

Conforme os estudos realizados até o momento, podemos chegar à conclusão de que existem diversos tipos de ameaças rondando uma infraestrutura de TI. Algumas delas são conhecidas e outras não!

Neste contexto, implementar mecanismos de segurança e proteção que de forma ativa ou passiva realizem o monitoramento constante torna-se uma solução de segurança eficiente e eficaz. Vamos deste ponto em diante conhecer alguma desses mecanismos.

6.1. IPS e IDS (Prevenção ou Detecção de Intrusão)

Com o objetivo de inspecionar dados e verificar a existência de fraudes ou erros, os sistemas financeiros começaram a introduzir, em meados da década de 60, a prática da auditoria. Contudo, surgiram algumas questões pertinentes, sobre o que deveria ser detectado, como realizar uma análise nas descobertas e como proteger os diversos níveis de habilitação de segurança em uma mesma rede sem comprometer a segurança.

Entre 1984 e 1986, então, dois especialistas desenvolveram o primeiro modelo de IDS, chamado IDES (Sistema Especialista em Detecção de Intrusão). Ele é baseado na hipótese de que a base de comportamento de um intruso não é o mesmo de um usuário legítimo. Por isso, o modelo tenta criar um padrão de comportamento de usuários em relação a programas, arquivos e dispositivos, tanto em longo quanto em curto prazo. Depois do IDES, muitos outros sistemas foram desenvolvidos, baseados numa abordagem que combinava estatística e sistemas especialistas.

Conceitualmente, o IDS refere-se a um mecanismo capaz de identificar ou detectar a presença de atividades intrusivas. Em um conceito mais amplo, isto engloba todos os processos utilizados na descoberta de utilizações não autorizadas

de dispositivos de rede ou de computadores. Isto é feito através de um software projetado especificamente para tal propósito.

No entanto, devemos salientar a diferença entre IDS, IPS (Intrusion Prevention System) e IDPS. Enquanto o primeiro é um software que automatiza o processo de detecção de intrusão, o segundo faz a prevenção de intrusão, que tem por objetivo impedir possíveis ataques. Já o IDPS, por fim, é um recurso híbrido de detecção e prevenção acoplado como uma única solução. Mas, por que um sistema de detecção de intrusão é importante em uma infraestrutura de TI?

Então, a cada dia que passa, novas técnicas para comprometer ambientes computacionais são criadas, e é um grande desafio para o mercado de segurança da informação acompanhar esta velocidade, e até mesmo estar à frente para não atuar de forma reativa. O Brasil, por exemplo, é o país que mais sofre com ataques de ransomware na América Latina, com 55% do total.

Por isso, a implementação de uma boa política de IDS é fundamental em uma arquitetura de segurança. Este recurso, se atualizado constantemente, é capaz de manter a infraestrutura distante de ataques oportunistas, seja sob uma perspectiva da rede, ou seja, pelo próprio comprometimento de um computador.

Combinar tantos sistemas de detecção e prevenção de intrusão baseados em rede (NDIS) e em host (HIDS) é essencial para uma boa saúde de segurança. Nenhum dos modelos apresentados é necessariamente excludente. Pelo contrário, eles devem ser tratados como complementares de acordo com a necessidade e criticidade de proteção exigidas por um ambiente corporativo e sua infraestrutura de TI. Os sistemas de detecção de intrusão podem ser categorizados em três grupos, dependendo do tipo de evento que monitoram e a maneira como são implantados. São eles:

1º grupo: IDS baseado em máquina e rede

- **Network Based** – este tipo de IDS monitora o tráfego de rede em um segmento ou dispositivo, e analisa a rede e a atividade dos protocolos para identificar comportamentos suspeitos. Também é capaz de detectar inúmeros tipos de

eventos de interesse, e geralmente é implantado em uma topologia de segurança como fronteira entre duas redes, por onde o tráfego é afunilado. Por causa disso, em muitos casos, o próprio recurso de IDS acaba sendo integrado diretamente no firewall.

- **Host Based** – podemos considerar um computador ou um servidor como host, pois o termo se refere a um equipamento ou ativo propriamente dito. A detecção de intrusão, neste formato, monitora características do dispositivo e os eventos que acontecem com ele em busca de atividades suspeitas. Geralmente, os IDS host based podem ser instalados de maneira individual, tanto para computadores corporativos dentro de uma rede empresarial, quanto para endpoints. Entre as principais características que ele acompanha, destacam-se o tráfego da rede para o dispositivo, os processos em execução, os logs do sistema, e o acesso e alteração em arquivos e aplicações.

2º grupo: IDS baseado em conhecimento e comportamento

- **Conhecimento** – o IDS de conhecimento se baseia em um banco de dados que reconhece a assinatura de vulnerabilidades já identificadas anteriormente. Neste caso, é de suma importância que a estrutura tenha uma política de atualização contínua desse banco de dados, para garantir a continuidade de segurança do ambiente. Aquilo que não é conhecido não pode ser protegido.
- **Comportamento** – este IDS, por outro lado, analisa o comportamento do tráfego e segue uma linha padrão de atividade normal do sistema. Caso haja desvios desse padrão – com a possibilidade de ser uma intrusão –, podem ser tomadas algumas ações, tais como o bloqueio temporário do tráfego ou alarmes para núcleos de operação de rede (NOC/SOC). Dessa forma, a anormalidade pode ser melhor investigada, liberada ou permanentemente bloqueada.

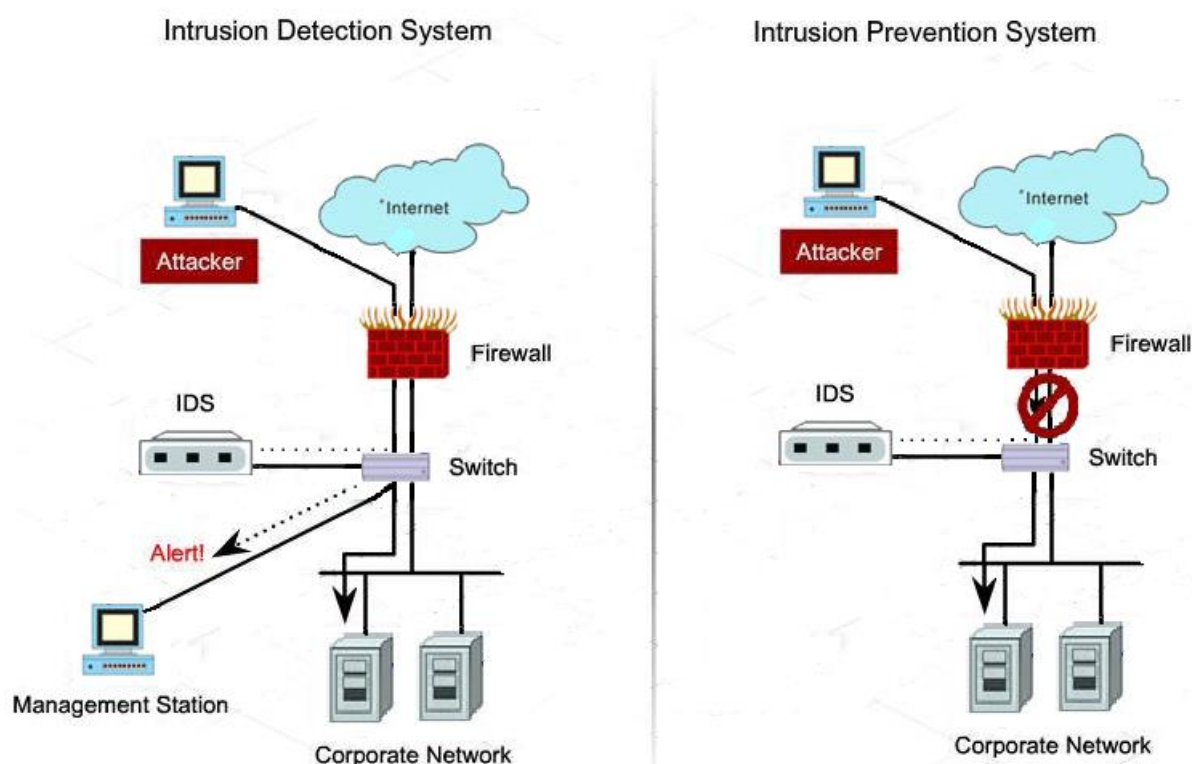
3º grupo: IDS ativo e passivo

- **Ativo** – é definido como um IDS ativo aquele que está programado para bloquear automaticamente ataques ou atividades suspeitas que sejam do seu

conhecimento, sem qualquer necessidade de intervenção humana. Embora seja um modelo extremamente interessante, é importante uma padronização adequada nos ambientes protegidos a fim de minimizar falsos positivos – por exemplo, ao bloquear conexões que são legítimas, assim causando transtornos para a empresa.

- **Passivo** – um IDS passivo, por fim, faz o monitoramento do tráfego que passa através dele e assim identifica potenciais ataques ou anormalidades. Com base nisso, acaba gerando alertas para administradores e times de segurança – sem afetar em nada na comunicação. Trata-se de um modelo bastante interessante em uma arquitetura de segurança e, independente de não atuar diretamente na prevenção, serve como um excelente termômetro de ataques e tentativas de acesso não autorizados a infraestrutura de uma empresa.

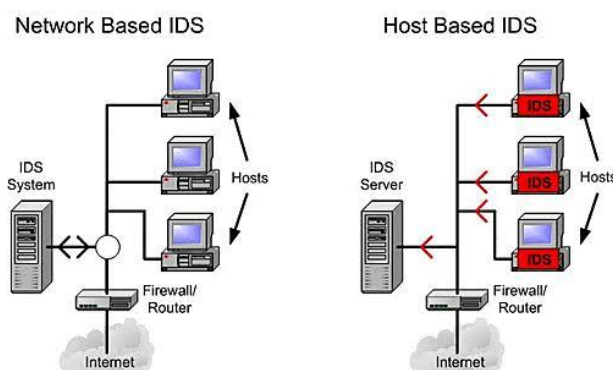
Figura 17 - Diferença entre IDS e IPS.



Conforme podemos observar na figura 17, o IDS apenas executa a função de detectar e alertar as equipes de segurança no caso de uma tentativa de invasão ou

ataque em uma rede. A equipe de segurança por sua vez realiza algum tipo de tratativa para inibir a invasão ou ataque. Ou seja, sua ação é “passiva” que depende de um segundo elemento de resposta. Já no caso do IPS, há uma ação “ativa”. Ou seja, não há a necessidade da ação do elemento de resposta (da equipe de segurança). Esta ação é realizada pelo próprio sistema, mitigando e repelindo a invasão e/ou ataque.

Figura 18 - Tipos IDS



6.2. VPN – Virtual Private Network

À medida que uma empresa cresce, ela pode se expandir para várias localidades em sua cidade, país ou em todo o mundo. Para manter as coisas funcionando de maneira eficiente, as pessoas que trabalham nesses locais precisam de uma maneira rápida, segura e confiável de compartilhar informações nas redes de computadores. Funcionários em viagem, como vendedores, precisam de uma maneira igualmente segura e confiável de se conectar à rede de computadores de seus negócios a partir de locais remotos. Mesmo em lazer, as pessoas desejam manter seus computadores em segurança em uma rede desconhecida ou não segura.

Uma tecnologia popular para atingir esses objetivos é uma VPN (rede privada virtual). Uma VPN é uma rede privada que usa uma rede pública (geralmente a internet) para conectar sites ou usuários remotos. A VPN usa conexões "virtuais" roteadas pela Internet da rede privada da empresa ou de um serviço VPN de terceiros

para o site ou pessoa remota. As VPNs ajudam a garantir a segurança - qualquer pessoa que intercepte os dados criptografados não pode lê-los.

O objetivo de uma VPN é fornecer uma conexão privada segura e confiável entre redes de computadores em uma rede pública existente, geralmente a internet. Entre os benefícios que uma VPN pode oferecer à uma empresa, citamos:

- Conexões estendidas em várias localizações geográficas sem usar uma linha alugada;
- Segurança aprimorada para troca de dados;
- Flexibilidade para escritórios e funcionários remotos usarem a intranet comercial através de uma conexão de Internet existente, como se estivessem diretamente conectados à rede;
- Economia de tempo e despesas para os funcionários comutarem se trabalharem em locais de trabalho virtuais;
- Maior produtividade para funcionários remotos.

Uma empresa pode não exigir todos esses benefícios de sua VPN, mas deve exigir os seguintes recursos essenciais de uma VPN:

- Segurança - a VPN deve proteger os dados enquanto viaja na rede pública. Se os invasores tentarem capturar os dados, eles não poderão lê-los ou usá-los;
- Confiabilidade - Os funcionários e escritórios remotos devem poder se conectar à VPN sem problemas a qualquer momento (a menos que o horário seja restrito), e a VPN deve fornecer a mesma qualidade de conexão para cada usuário, mesmo quando estiver lidando com seu número máximo de simultâneos. Conexões;
- Escalabilidade - À medida que a empresa cresce, deve poder estender seus serviços VPN para lidar com esse crescimento sem substituir completamente a tecnologia VPN.

As equipes de segurança da informação e segurança cibernética, podem realizar a configuração de uma VPN de dois modos:

- VPN site to client: permite que usuários individuais estabeleçam conexões seguras com uma rede de computadores remotos. Esses usuários podem acessar os recursos seguros nessa rede como se estivessem diretamente conectados aos servidores da rede. Um exemplo de empresa que precisa de uma VPN de acesso remoto é uma grande empresa com centenas de vendedores em campo.
- VPN site a site: permite que escritórios em vários locais fixos estabeleçam conexões seguras entre si através de uma rede pública como a Internet. A VPN site a site estende a rede da empresa, disponibilizando recursos de computador de um local para funcionários de outros locais. Um exemplo de empresa que precisa de uma VPN site a site é uma empresa em crescimento, com dezenas de filiais em todo o mundo. As VPNs site a site, podem ser do tipo intranet - se uma empresa tiver um ou mais locais remotos nos quais deseja ingressar em uma única rede privada, poderá criar uma VPN na intranet para conectar cada LAN separada a uma única WAN ou do tipo extranet - quando uma empresa tem um relacionamento próximo com outra empresa (como um parceiro, fornecedor ou cliente), pode criar uma VPN de extranet que conecta as LANs dessas empresas. Essa VPN de extranet permite que as empresas trabalhem juntas em um ambiente de rede compartilhado e seguro, impedindo o acesso às intranets separadas.

Figura 19 - Exemplo de VPN - Site to Client.

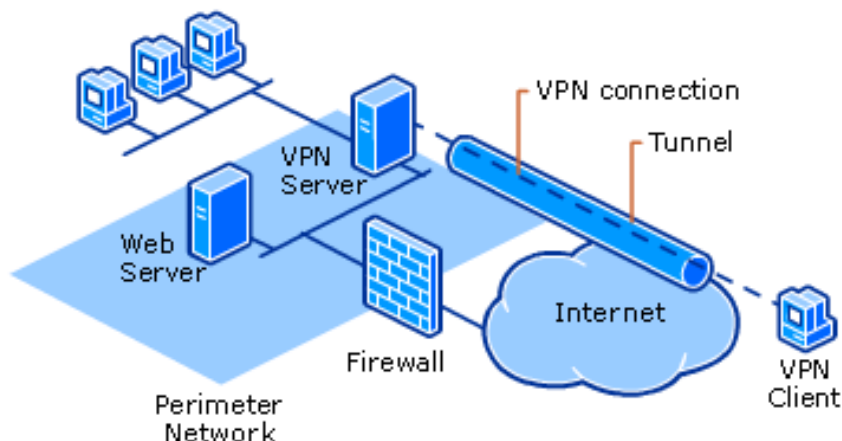
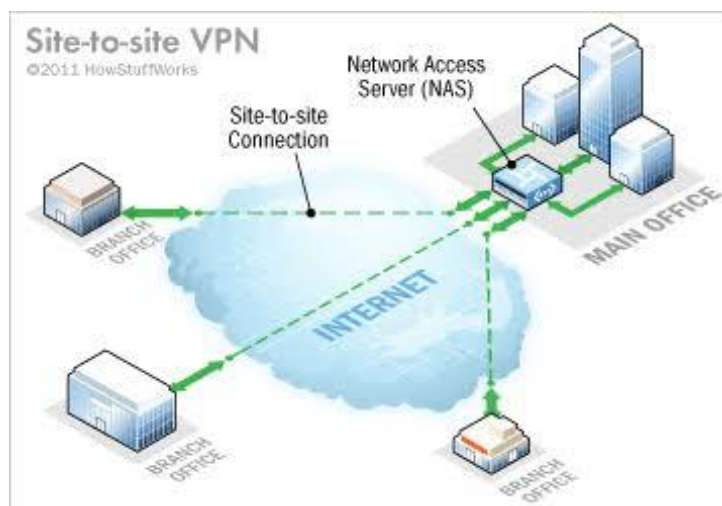


Figura 20 - Exemplo de VPN - Site to Site.



Atualmente as VPNs são consideradas por muitos especialistas de segurança da informação e segurança cibernética, mecanismos confiáveis de proteção para a interligação de infraestruturas de TI distintas e dispostas em regiões físicas diferentes, pois além de prover uma segurança fim a fim de forma segura (criptografada), também fornecem economia. Atualmente os protocolos mais comuns utilizados em uma VPN são: PPTP, L2TP, SSTP, IKEV2 e OpenVPN.

Referências

ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos.

ABNT NBR ISO/IEC 27002:2013. Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação.

BUGS. In: *Wikipédia*, a enciclopédia livre. Flórida: Wikimedia Foudation, 2019. Disponível em: <<https://pt.wikipedia.org/wiki/Bug>>. Acesso em: 31 ago. 2020.

CERT.br. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <<https://www.cert.br/>>. Acesso em: 31 ago. 2020.

COMER, Douglas E. *Redes de Computadores e Internet*. 2. ed. São Paulo: Bookman, 2001.

DANTAS, Mário. *Tecnologia de Redes de Comunicação e Computadores*. Rio de Janeiro: Axcel Books, 2002.

HARRIS, Shon. *CISSP All-in-one*, 3. ed.: Mc Graw Hill, 2004.

INTRUSION DETECTION SYSTEM. In: *Wikipédia*, a enciclopédia livre. Flórida: Wikimedia Foudation, 2020. Disponível em: <https://en.wikipedia.org/wiki/Intrusion_detection_system>. Acesso em: 31 ago. 2020.

KIM, David; SOLOMON, Michael. *Fundamentos de Segurança de Sistemas de Informação*. 1.ed. São Paulo: LTC Exatas Didática, 2014.

MACHADO, Felipe R. Nery. *Segurança da Informação – Princípios e controle de ameaças*. 1.ed. Rio de Janeiro: Editora Érica, 2014.

MICROSOFT. VPN Tunneling Protocols. In: *Microsoft Docs*, 2012. Disponível em: <[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771298(v=ws.10)?redirectedfrom=MSDN)>. Acesso em: 31 ago. 2020.

OUELLET, Eric; LITAN, Avivah; MCSHANE, Ian. *Magic Quadrant for Endpoint Protection Platforms*. Gartner, 2017. Disponível em: <<https://www.gartner.com/en/documents/3588017>>. Acesso em: 31 ago. 2020.

RITTINGHOUSE, John W; RANSOME, F. James. *Cloud Computing: Implementation, Management and Security*. CRC PRESS, 2009.

SCARFONE, Karen; MELL, Peter. *Guide to Intrusion Detection and Prevention Systems*. CSRC, 2007. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-94/final>>. Acesso em: 31 ago. 2020.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*. 2.ed. São Paulo: Gen-LTC, 2013.

SOARES, Luís Fernando; LEMOS, Guido; COLCHER, Sérgio. *Redes de computadores: das LANs, MANs e WANs às redes ATM*. Rio de Janeiro: Campus, 1995.

SPONH, Marco Aurélio. *Desenvolvimento e análise de desempenho de um "Packet Session Filter"*. Porto Alegre – RS: CPGCC/UFRGS, 1997.

STALLINGS, Willian. *Criptografia e Segurança de Redes – Princípios e Práticas*. 6.ed. São Paulo: Pearson, 2016.

STALLINGS, Willian; BROWN, Lawrie. *Segurança de Computadores – Princípios e Práticas*. 2.ed. São Paulo: Elsevier, 2017.

TANENBAUM, Andrew. S. *Redes de Computadores*. 4ª ed. Rio de Janeiro: Editora Campus (Elsevier), 2011.

V., John. *Overview: Forward Proxy vs. Reverse Proxy*. Blog Managed File Transfer and Network Solutions, 2012. Disponível em: <<https://www.jscape.com/blog/bid/87783/Forward-Proxy-vs-Reverse-Proxy>>. Acesso em: 31 ago. 2020.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. Building Internet Firewalls: Internet and Web Security. 2. ed. O'Reilly Media, 2000.