INSTITUTO DE GESTÃO E TECNOLOGIA DA INFORMAÇÃO

Fundamentos em Segurança Cibernética

Bootcamp Online: Analista em Cibersecurity

Paulo Gontijo

2020

Fundamentos em Segurança Cibernética

Paulo Gontijo

© Copyright do Instituto de Gestão e Tecnologia da Informação.
Todos os direitos reservados.

Sumário

Capítulo 1. Introdução a Segurança da Informação e Cibernética

Olá, seja muito bem-vindo a disciplina de Fundamentos em Segurança Cibernética. Esta disciplina é composta de conceitos e práticas, sendo que tanto os conceitos quanto as atividades práticas são demonstradas através dos vídeos gravados disponíveis no Ambiente de Ensino.

Abordaremos nesse material os conceitos da disciplina, pois a prática é melhor demonstrada através dos vídeos. Utilize esta apostila para aprender sobre os temas aqui descritos e também como referência para buscas futuras, afinal é mais rápido e fácil buscar um conteúdo textual do que aquele produzido em vídeos. A organização e divisão dos capítulos reflete o que você encontrará nas aulas práticas, podendo em alguns casos serem agrupados ou separados em prol da didática. A utilização de imagens e gráficos também é encontrada nos slides e nas aulas práticas. Desta forma, a apostila completa o conteúdo oferecido pelos vídeos, estabelecendo links entre os materiais disponibilizados, de forma que você possa aprender como for melhor para você.

A única exceção diz respeito aos capítulos de carreira em Segurança Da Informação e Cibernética, cujo o conteúdo não está presente nesta apostila. O humilde autor entende que tal conteúdo é melhor assimilado ao assistir as aulas gravadas, pois carregam consigo a emoção da voz e dos gestos, num tema cuja pegada central é exatamente essa. Boa leitura!

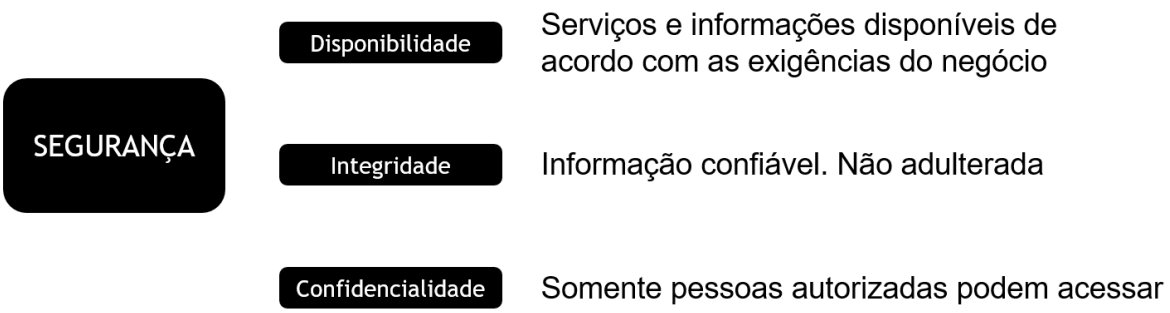
Pilares da Segurança da Informação

Fundamentos devem ser encarados como alicerces de um prédio: dificilmente são alterados. No entanto, podem e devem ser reforçados por conceitos emergentes. Assim, da mesma forma que um prédio construído há décadas, ou que tem novos andares construídos, recebe reforço em seu alicerce, os fundamentos de segurança também são encorpados à medida que novas tecnologias e formas de tratar a informação vão sendo criadas. Isso não significa que os pilares principais deixam de

existir, eles apenas passam a carregar consigo uma carga maior de significado e maneiras inovadoras de implementação de tal fundamento.

Os pilares ou a tríade de segurança da informação é composta por disponibilidade, integridade e confidencialidade. Um exemplo de como um pilar recebe reforço pode ser visto com a assinatura digital. Criada com o propósito de garantir integridade e não repúdio na informação trafegada, tal tecnologia surgiu posteriormente a tríade de segurança, mas não por isso passou a alterar os pilares existentes. Desta forma, tecnologias e controles novos serão criados, mas a associação com os pilares se dará de forma natural no decorrer do desenvolvimento tecnológico.

Figura 1 – Pilares de Segurança da Informação.



É importante entendermos os conceitos de ameaça, vulnerabilidade, ativo e controle de segurança. Uma frase que os conecta pode ser assim exposta: “Uma ameaça explora uma vulnerabilidade presente em um ativo que não é protegido por um controle de segurança”. Poderíamos tomar como exemplo, neste caso, a ameaça como sendo a possibilidade de pane em um HD; como vulnerabilidade a ausência de backup; como ativo o servidor de arquivos e um controle que mitigaria o risco que poderia ser a replicação de discos, por exemplo, através de tecnologia de RAID.

Desta forma, a segurança busca garantir os pilares de segurança da informação através da implantação de controles que protejam ativos de forma que as vulnerabilidades sejam reduzidas ou eliminadas, evitando assim que ameaças causem problemas.

Diferenças entre Segurança da Informação e Cibernética

É comum ouvirmos termos como segurança da informação, segurança cibernética, cybersecurity, segurança do ciberespaço dentre muitos outros. Entender o que há por trás destas diferenças nos leva a direcionar esforços para o local certo. Alguns autores, dentre os quais me identifico, preconizam que a segurança cibernética está contida dentro do que conhecemos como segurança da informação, já outros autores defendem que a segurança cibernética é puramente tecnologia presente no ciberespaço ou Internet, e que a segurança da informação trata de itens como informação falada, escrita e processos de *compliance* e gestão. Fato é que são visões distintas para nomenclaturas distintas.

O conceito com o qual me identifico pode ser interpretado conforme a imagem abaixo. Note que segurança cibernética está contida em segurança da informação, sendo que a lupa está presente naquilo que está contido. Isso quer dizer que estudar, trabalhar ou dissertar a respeito de segurança cibernética não é menor do que estudar, trabalhar ou dissertar sobre segurança da informação; quer dizer apenas que quando nos referimos a segurança cibernética, damos atenção plena, ou seja, foco e lupa para os temas que nos são mais rotineiros e contemporâneos.

Figura 2 – Segurança da Informação e Cibernética.

Proteger do ataque cibernético de hackers é muito mais comum e presente na vida das empresas do Brasil e no mundo do que atender a regras da Sarbanes Oxley, lei americana que se aplica somente a empresas que têm ações negociadas

nos Estados Unidos, motivo pelo qual o termo segurança cibernética ou *cybersecurity* tem ganhado cada vez mais relevância.

Isso não significa, de forma alguma, que quem estuda, trabalha, disserta ou se relaciona de alguma forma com segurança cibernética, deva esquecer os conceitos identificados, majoritariamente, pela ISO 27001, tais como comitês, políticas e controles para garantir uma governança adequada; significa apenas dizer que suas prioridades serão outras, mais conectadas ao ciberespaço.

Governança e Política de Segurança da Informação

Governança pode ser entendida como um conjunto de processos, políticas, leis e regulamentos que definem a maneira como uma empresa é dirigida e operada. Provavelmente já ouvimos falar em conselho de administração, auditoria externa independente, comitês de tomada de decisão, dentre outras. Este conjunto foi aprimorado e continuará sendo ao longo dos anos, sendo que foram construídos sobre erros e acertos, ou seja, no decorrer da história empresas faliram, foram vítimas de fraude e de falsificação informacional. Na contramão, outras tantas empresas tiveram sucesso, foram e continuam sendo transparentes e agradaram os acionistas, a este conjunto de boas práticas que corrige os erros e aprende com os acertos, empacotamos e nomeamos como uma boa governança.

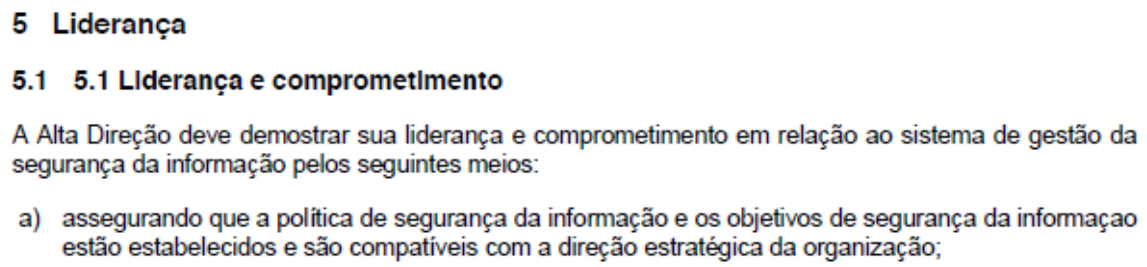
Você, leitor, se questiona: e o que isso tem a ver com segurança? Pois bem, da mesma forma que erros e acertos no ambiento empresarial e corporativo foram sendo acumulados no decorrer dos anos, o mesmo aconteceu com a segurança da informação e ao pacote de boas práticas, que nomeamos de padrões ou *frameworks*.

Tomemos como exemplo a norma ISO 27001, que tem uma longa história baseado em uma norma britânica datada em 1995 e que ao longo do tempo foi se aprimorando, recebendo contribuições de vários países, de empresas privadas de todos os segmentos, de cientistas e estudiosos do tema e de governos. Tal norma continua sendo aprimorada e trata as melhores práticas para implementação, manutenção e melhoria contínua de um sistema de gestão de segurança da

informação, sendo que sistema, neste contexto, pode ser entendido como um conjunto e não como uma aplicação de tecnologia.

A ISO 27001 possui poucas páginas, não mais do que 50 em sua versão em português do Brasil, e muito de nós, após sua leitura, ficamos com o sentimento de que tudo ali contido é muito óbvio e superficial, e de fato é. O objetivo da ISO 27001 é ser um referencial, um norte e não um guia para implantação de segurança nas empresas. Tomemos como exemplo o trecho abaixo, retirado da própria ISO 27001.

Figura 3 – ISO 27001.



5 Liderança

5.1 5.1 Liderança e comprometimento

A Alta Direção deve demostrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a) assegurando que a política de segurança da informação e os objetivos de segurança da informaçao estão estabelecidos e são compatíveis com a direção estratégica da organização;

Fonte: Norma ABNT ISO 27001.

Quantos de nós não gostaríamos de encontrar diretrizes sobre como configurar de forma segurança nossa rede, nossos servidores e quiçá nossos firewalls. Pois bem, sinto muito em informar, caro leitor, que não será nesta norma que encontrará resposta para tais anseios. Embora considere a leitura da ISO 27001 fundamental para qualquer profissional de segurança, os detalhes de implementação estão presentes na ISO 27002 e em outras fontes de referência, como o NIST 800-53, o Cobit, o ITIL e outras publicações.

Antes de passarmos a inspeção da ISO 27002, é fundamental ressaltar que é na ISO 27001 que estão as diretrizes para a certificação de uma empresa, desta forma, uma auditoria externa ao certificar uma empresa ou processo desta, irá, criteriosamente, buscar evidências de que há, por exemplo, conforme trecho acima destacado, política de segurança da informação alinhada aos objetivos da empresa. Há ainda que ressaltar, que a ISO 27001 tem um Anexo A, com uma lista de dezenas, na verdade um pouco mais do que uma centena de controles, também utilizados por

auditores e consultores como referencial para uma boa segurança. Tal anexo é diretamente conectado com os controles da ISO 27002, que veremos a seguir.

Na ISO 27002, encontramos trechos mais alinhados ao mundo dos bits e bytes, passemos ao exemplo:

Figura 4 – ISO 27002 .

Convém que o perímetro de cada domínio seja bem definido. O acesso entre os domínios de rede é permitido, porém é recomendado que seja controlado no perímetro por meio do uso de um *gateway* (por exemplo, *firewall*, roteador de filtro). Convém que o critério para segregação de redes em domínios e o acesso permitido através dos *gateways* seja baseado em uma avaliação dos requisitos de segurança da informação de cada domínio.

Fonte: Norma ABNT ISO 27002.

Uau! Finalmente algo mais técnico, não é verdade? Sim! A ISO 27002, engloba conceitos técnicos, estruturando cada controle com diretrizes de implantação e informações adicionais. O texto acima destacado, está contido no controle do capítulo 13.1.3:

Figura 5 – ISO 27002.

13.1.3 Segregação de redes

Controle

Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

Fonte: Norma ABNT ISO 27002.

Outros frameworks como o Cobit, o ITIL, o PCI DSS e tantos outros, que fruto de uma breve pesquisa no Google podem nos encorajar, ou não, a buscar tais conhecimentos, são também referenciais teóricos e práticos para implantação de segurança da informação e cibernética; no entanto, abordá-los aqui tiraria o nosso foco em seguir forte em aspectos mais conectados à segurança cibernética. O recado importante é: não reinvente a roda. Se precisa implantar segurança da informação, utilize o que o mercado produziu e ajuste apenas a pressão dos parafusos, a calibragem dos pneus para o carro que você guiará adiante.

Se há risco alto de nosso data center pegar fogo, deveríamos rever os nossos controles de segurança, implantando sistemas de combate e brigadistas profissionais, ou eventualmente levando todos os nossos servidores para a nuvem, não é mesmo? Note como a palavra risco nos soa natural e de fato o é, no entanto, poucas empresas aplicam matemática e estatística para que as prioridades definidas sejam aquelas oriundas da matriz de risco e da análise de impacto na continuidade do negócio.

Desta forma, quando estamos falando de definir a prioridade, estamos falando em fazer uma análise quantitativa considerando minimamente a probabilidade e o impacto de uma ameaça explorar uma vulnerabilidade, e com isso termos um risco alto, que precisa ser tratado. Tomemos como exemplo a matriz abaixo:

Figura 6 – ISO 27002.

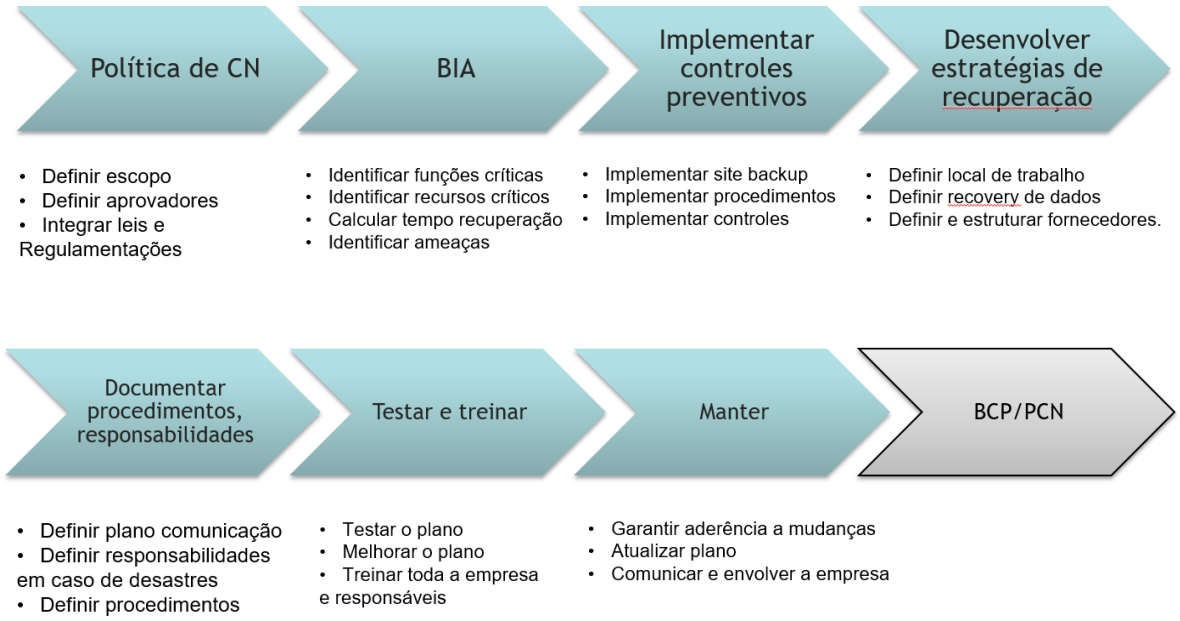
Prioridade definida: Proteger o site de vendas online

Ameaça	Vulnerabilidade	Probabilidade	Impacto	Risco
Acesso mal intencionado e consequente publicação de conteúdo inapropriado	Publicador de conteúdo sem autenticação forte e disponível na internet	3	2	6
Falta de energia	Ausência de site backup	2	2	4
Ataque de DDOS	Link de 100M sem proteção	1	2	2
Roubo de dado de clientes	APIs com acesso a dados de clientes expostas publicamente	3	3	9

Note como a primeira e a última linha possui classificação de risco mais elevadas. O risco é dado pela multiplicação da probabilidade e impacto. Desta forma, após ouvir as pessoas envolvidas o responsável por conduzir os trabalhos de análise de risco deve apresentar a alta direção às prioridades definidas e sugerir controles que reduzam ou eliminem os riscos citados.

De forma análoga, é o plano de continuidade do negócio. Após estabelecido qual o processo de negócio é fundamental para que a empresa continue funcionando, deve-se proceder com as entrevistas envolvendo os responsáveis por operar e manter tal processo. Feito isso, controles devem ser implementados para evitar

paralisações, ainda assim, planos devem ser escritos para que, na falha dos controles, o processo retome seu funcionamento após um período tolerável de paralisação (definido pela alta direção). Há de se destacar ainda, no caso de continuidade do negócio, que é fundamental a realização de testes para atestar que aquilo que foi planejado de fato funciona. O processo completo sugerido pelo livro *All in One* é o que segue, podendo sofrer adaptações em empresas menos regulamentadas.



Privacidade de dados

Considerando o dito por Clive Humby em seu chavão: “Dados são o novo petróleo”, é de se considerar que tal petróleo deva sim ser explorado, mas também protegido, não é mesmo?

É comum termos a certeza que nossos smartphones nos ouvem, nos espiam ou mesmo nos filmam, desta forma, não deveria eu, o proprietário de tal *hardware* e detentor do direito de escolha na instalação dos *softwares* que ali estão embarcados, anuir sobre o uso do que é capturado? Não deveria eu, dono de meus

comportamentos, preferências sexuais, políticas, sociais, determinar quem deveria ter acesso a tais informações? A resposta óbvia é sim!

Fato é que somente recentemente a civilização tem se movido no sentido de criar leis que protejam o cidadão e que entonem a este o direito da escolha e de anuência ao determinar quem pode ter acesso aos seus dados, de que forma (anonimizados ou não) e sobre quais circunstâncias tais dados podem ser compartilhados.

No Brasil a execução de tais direitos está presente na LGPD, Lei Geral De Proteção de Dados. A LGPD conceitua o que são dados pessoais (CPF, nome, e-mail), dados pessoais sensíveis (aqueles que podem gerar discriminação: filiação política, convicção religiosa, saúde, vida sexual etc.) e define claramente os papéis do titular ou dono da informação e de agentes que recebem e manipulam tais informações, cabendo destaque aqui ao controlador, que é quem decide sobre como usar os dados pessoais coletados.

A penalização em caso de vazamento de informações e incidentes envolvendo tais dados pode chegar a 2% do faturamento líquido da empresa (limitado a R$ 50 milhões), possibilidade de tornar público o incidente e a obrigação da empresa em eliminar os dados e não os armazenar novamente.

Segurança de pessoas e engenharia social

A figura abaixo demonstra claramente o elo mais fraco da corrente, feito de carne e osso: nós, seres humanos.

Figura 6 – Elo mais fraco.

Fonte: Artigo de Cibele Sanches, publicado no LinkedIn.

Há de se compreender que este não caiba às máquinas, afinal, se o HD delas pifarem, o erro foi do humano ao não prever um sistema de redundância ou backup, não é mesmo? Sabendo, portanto, que o ônus recai sobre nós e que ainda não temos casos de máquinas sendo presas e privadas de energia elétrica por cometerem crimes e realizações à revelia de seus proprietários, cabe a nós, humanos, nos fortalecer, e este ganho de poder só é possível com treinamento, conscientização e controles complementares. Desta forma, é fundamental que as empresas trabalhem, de forma recorrente, a comunicação com seus funcionários e prestadores de serviço, no sentido de conscientizá-los a respeito da importância deles para a continuidade dos negócios. Tais treinamentos devem ser personalizados por áreas da empresa. Desta forma, desenvolvedores de software precisam de treinamento específico, analista de RH, analista de suporte e tantos outros, incluindo aqui gerentes e diretores. É recomendado que o treinamento envolva situações lúdicas.

Nas aulas gravadas apresento trechos de filmes que melhor representam o quanto uma pessoa mal-intencionada pode obter informações privilegiadas e que posteriormente, ligando as peças, poderá ganhar acesso a sistemas da empresa.

Treinar não é tudo, é preciso estruturar um processo de gestão de segurança voltado para pessoas. Segue abaixo algumas recomendações para melhoria da segurança:

1. Avaliações rigorosas na contratação (especial atenção a ética e cargos técnicos).
2. Concordância expressa com as políticas da empresa.
3. Limitar acessos somente ao necessário.
4. Dentro do possível segregar funções (desenvolvedor não acessa produção).
5. Ter a certeza de remover todos os acessos ao fim do contrato de trabalho.

Capítulo 2. Conceitos básicos de Redes de Computadores e uso de Linux

Neste capítulo veremos os conceitos básicos para o correto entendimento das redes de computador, bem como uma breve introdução ao Linux, sendo que a melhor forma de aprender estes conceitos é acompanhando as práticas (aulas gravadas e disponibilizadas na plataforma de ensino).

Modelo OSI

O modelo OSI (*Open Systems Interconnection*) é composto de sete camadas de comunicação, cada uma com uma finalidade especifica. O objetivo do modelo OSI é permitir a interligação entre equipamentos de diferentes fabricantes. Assim eu posso ter um computador da marca Dell, conectado com um switch da Cisco, que se conecta com um roteador Huawei, que por sua vez está conectado a um firewall Checkpoint. Tudo isso é possível graças a compatibilidade proporcionada por este modelo.

Figura 6 – Modelo OSI.

7	Aplicação	HTTP, SMTP, DNS	Faço o upload de uma imagem para o servidor Web
6	Apresentação	Content-type: ex: jpeg, zip	Adiciono a informação que o content-type é do tipo jpg
5	Sessão	NetBios, SOCKS (rede Tor)	N/A
4	Transporte	TCP, UDP	Enviarei a imagem serializando a comunicação (TCP)
3	Rede	IP, ICMP (ping), BGP	Adiciono IP de origem e destino
2	Ligação de dados	Ethernet, ARP	Adiciono informações de MAC de origem e destino
1	Camada Física	100BaseTX, X.25	Transformo em pulsos elétricos

Modelo de comunicação (simplificado)

1	Camada Física	100BaseTX, X.25	Recebo os pulsos elétricos
2	Ligação de dados	Ethernet, ARP	Verifico se o endereço MAC (Destino é meu)
3	Rede	IP, ICMP (ping), BGP	Verifico se o IP de destino (sou eu)
4	Transporte	TCP, UDP	Respondo como OK ao pedido de conexão e tunelamos
5	Sessão	NetBios, SOCKS (rede Tor)	N/A
6	Apresentação	Content-type: ex: jpeg, zip	Reconheço que preciso receber uma imagem
7	Aplicação	HTTP, SMTP, DNS	Salvo a imagem em disco (se fosse um dado seria no BD)

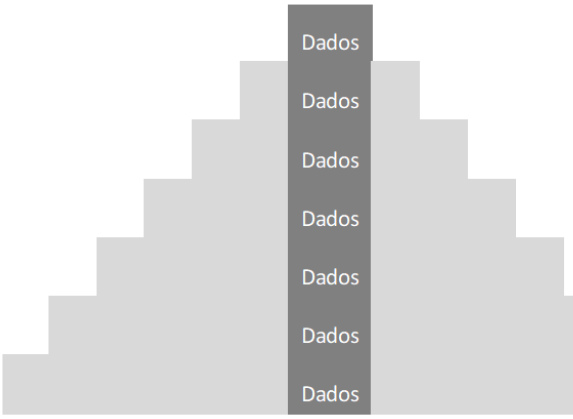
Na imagem acima é descrito na primeira coluna o número da camada, na segunda o seu nome, na terceira o nome do protocolo de exemplo e na quarta um exemplo de fluxo e como cada camada participa do processo. Note como o processo começa no *desktop,* na camada 7, onde o usuário seleciona uma imagem para *upload*

e este pacote vai sendo agregado com informações nas camadas inferiores, até que sai da máquina na camada 1, através da sua transformação em pulsos elétricos. Na outra ponta, temos o servidor, que recebe tais pulsos elétricos e desempacota tais informações, camada a camada até ser interpretada na camada 7, para que a imagem seja salva.

Nem toda comunicação acontece em todas as camadas. O popular comando *ping (echo request)*, por exemplo, começa sua execução na camada 3 e desce o modelo OSI até ser transformado em pulso elétrico. Assim que recebido pelo servidor, ele interpreta tais pulsos elétricos e desempacota o mesmo apenas até a camada 3, respondendo com um *pong (echo reply).*

A figura abaixo demonstra como um pacote recebe agregação de informações à medida que vai descendo as camadas do modelo OSI.

Figura 7 – Pacote no modelo OSI.



Camada 7	Aplicação	HTTP, SMTP, DNS
Camada 6	Apresentação	Content-type: ex: jpeg, zip
Camada 5	Sessão	NetBios, SOCKS (Usado na Rede Tor)
Camada 4	Transporte	TCP, UDP
Camada 3	Rede	IP, ICMP (ping), BGP
Camada 2	Ligação de dados	Ethernet, ARP
Camada 1	Camada Física	100BaseTX, X.25

TCP/IP

O *Transmition Control Protocol/Internet Protocol* é, como o nome diz, o protocolo da internet. Embora carregue apenas o nome TCP, há também o UDP (*User Datagram Protocol*).

O TCP e o UDP atuam na camada 4 do modelo OSI e o IP na camada 3. O TCP fornece conexão com controle de fluxo de sessão, isso significa que há sequenciamento no processamento dos pacotes. Assim, quando executo um comando remotamente, por exemplo: “ps –ax” no caso do Linux, para listar os processos da máquina, eu só devo receber a tela após a tecla ENTER ser pressionada. Já o UDP não prevê este controle de fluxo e por isso é muito utilizado em transmissões de voz e vídeo. Há de se destacar que o TCP possui um tamanho de pacote maior para controles deste fluxo e é por isso mais lento que o UDP.

Em comunicações ao vivo, exemplo, ligação telefônica, o uso de UDP é mais utilizado, pois se eu perco pacotes na comunicação da rede, por exemplo, conduzindo a mensagem falada “estou bem”, não faz sentido eu reproduzir este pacote depois de passado 10 segundos de conversa. No caso de mecanismos de *streaming*, o uso de TCP é mais plausível, motivo pelo qual os principais serviços de streaming o implementam, isso porque garante que a imagem ficará pouco distorcida (perda de pacote). A forma como tais serviços diminuem o efeito da maior lentidão do protocolo TCP é através do *caching* local. Desta forma, a informação que sua televisão recebe agora na verdade vai ser reproduzida dentro de alguns segundos, desta forma, caso alguma informação seja perdida, há tempo para que o TCP corrija as falhas e entregue um conteúdo com melhor qualidade.

Quando falamos de IP, correlacionamos imediatamente com endereços IP, não é mesmo? E esta é a sua função, prover endereçamento para que a comunicação ocorra. Os endereços IPs, na versão mais popular e amplamente usada na internet (IPv4), tem tipicamente um formato análogo a este: 192.168.0.1, ou seja, um conjunto composto de quatro subconjuntos, compostos por até três números.

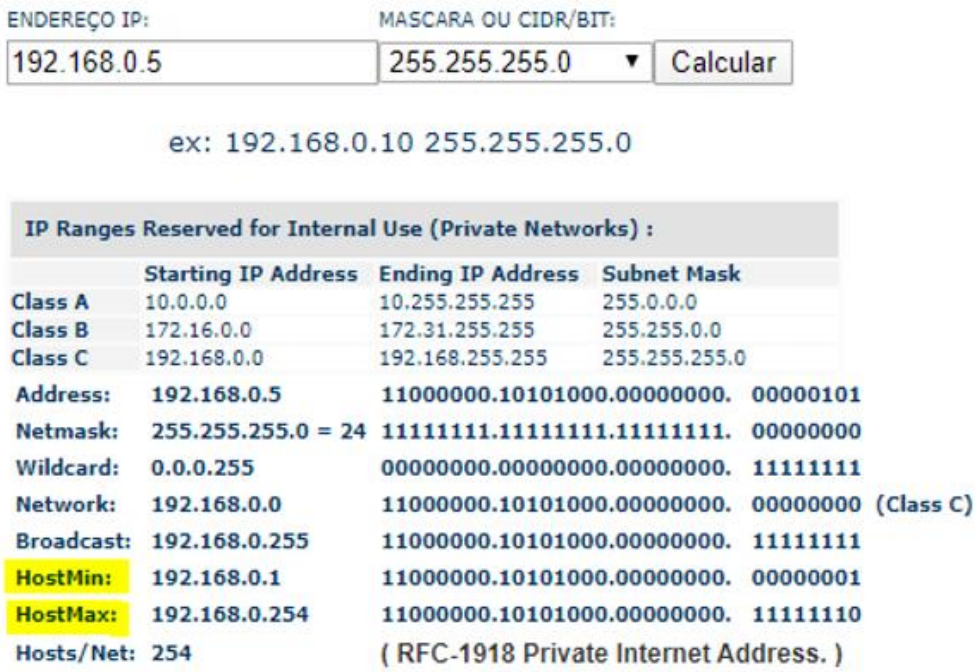
O que é importante reforçarmos, para o nosso conhecimento prático, com relação ao IP, diz respeito a máscara de rede, isso porque é ela quem determina se um pacote vai trafegar na rede local, ou precisará ser encaminhado para que o roteador determine o seu destino.

Considerando que a explicação didática para o entendimento do seu funcionamento é melhor demostrada em sala de aula, não aprofundaremos o seu

conhecimento aqui, até mesmo porque atualmente existem inúmeras opções de calculadoras IP disponíveis na internet. Sorte essa que o autor não teve ao iniciar seus estudos em redes de computadores há muitos anos atrás. ☺

Portanto, mais importante do que investir tempo na compreensão detalhada dos bits e bytes que criam a lógica do comportamento do endereçamento IP, é saber qual a faixa (primeiro e último IP) aquele endereço carrega. Abaixo uma imagem que demonstra tal consulta no site http://calculadoraip.com.br/.

Figura 6 – Calculadora IP.



Fonte: http://calculadoraip.com.br/.

Linux

O sistema operacional utilizado para praticar os conceitos que aprendemos acima e que também aprenderemos nos capítulos posteriores é o Linux, na sua distribuição Ubuntu. O Linux, atualmente já conhecido por todos nós, está presente em servidores, desktops, dispositivos IoT e muito mais. Na minha visão pessoal não

existe entendimento técnico de segurança sem conhecimento de Linux, motivo pelo qual o utilizamos do início ao fim do curso. Isso significa que não é importante conhecer de segurança em Windows ou utilizá-lo para fins de demonstração? De forma alguma.

O fato é que se torna necessário fazer uma escolha para fins didáticos e esta foi a escolha do autor que aqui vos escreve. Ademais, boa parte dos alunos tem contato natural com o Windows no dia a dia, desta forma, utilizar o Linux adiciona conhecimentos para aqueles que ainda não tiveram oportunidade de conhecer o sistema operacional. Caso você nunca tenha usado o sistema operacional do pinguim, como é conhecido, não se assuste. A tela preta, característica principal do seu console de administração, pode espantar no início, mas muito em breve você verá o quão maleável e potente ele é e passará a enxergá-lo como amigo.

Não por menos, nas aulas práticas instalaremos servidores de banco de dados, servidores de e-mail, web, proxy e muitos outros em questões de minutos.

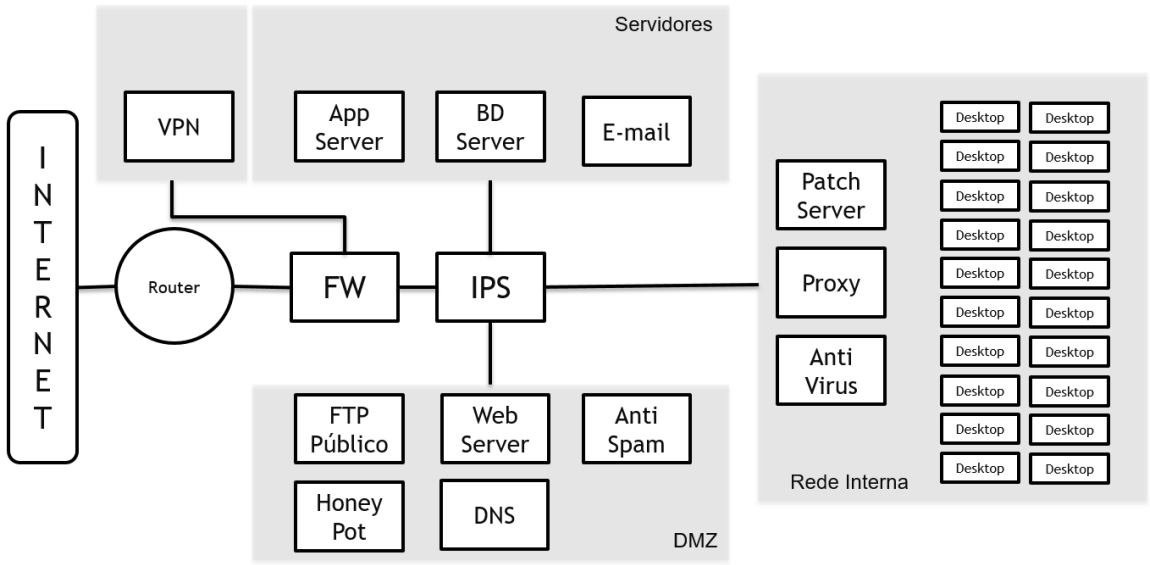
Capítulo 3. Cybersecurity – Infraestrutura e plataformas

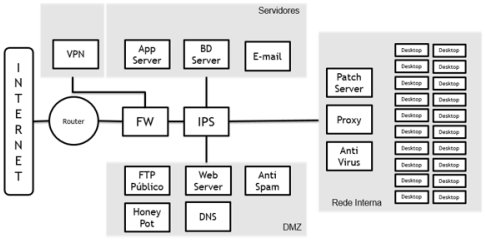
Neste capítulo veremos os ativos que compõe uma infraestrutura de segurança, bem como analisaremos suas fraquezas e ameaças. Você encontrará neste capítulo as mesmas figuras e explicações utilizadas nas aulas gravadas, visto que a explicação do fluxo da comunicação é melhor demonstrada em vídeos.

Ativos de Segurança e Infraestrutura

A topologia abaixo detalhada em uma única figura todos os principais componentes de uma arquitetura de rede que preza pela segurança. Nas imagens seguintes é possível compreender o papel de cada componente.

Figura 7 – Conjunto de images de uma arquitetura segura





Router

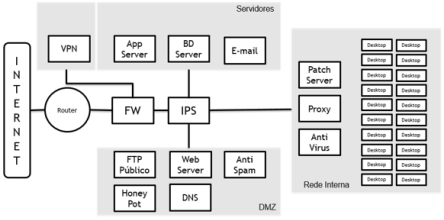
Responsável por rotear o tráfego entre a rede internet e a internet
Fraqueza: Acesso remoto internet
Proteção: ACL, Null Route

FW

Firewall – Responsável por filtrar tráfego na camada de rede
Fraqueza: Regras permissivas
Proteção: Regras firewall, Stateful Inspection

IPS

Intrusion Prevention System – Proteção de Ataque a servidores (assinaturas e heurística)
Fraqueza: Assinaturas desatualizadas
Proteção: Protege vulnerabilidades



VPN

Responsável por criar uma rede virtual Privada através de uma rede pública
Fraqueza: Acesso a rede interna pela internet
Proteção: Criptografia

FTP Server

Servidor utilizado para transferência externa de arquivos.
Fraqueza: Acesso anônimo
Proteção: Evita protocolos inseguros (SMB)

Honey Pot

Utilizado como armadilha para invasores, não possui nenhuma informação confidencial (possui VLAN própria)

Web Server

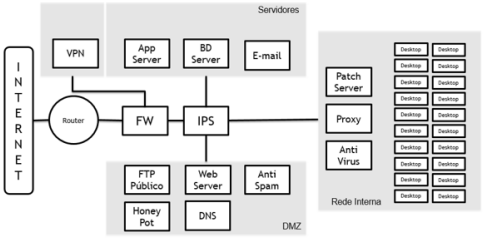
Servidor utilizado para acesso Web. Usualmente não possui aplicação instalada
Fraqueza: Listar conteúdo de diretórios
Proteção: Protege o App Server

DNS

Utilizado para converter Ips em nomes.
Fraqueza: DNS Hijacking
Proteção: Pode usar serviços como Opendns que protegem a rede.

Anti Spam

Servidor utilizado para filtrar conteúdo malicioso oriundo de e-mails.
Fraqueza: Falso positivo
Proteção: Bloqueia o acesso a malwares



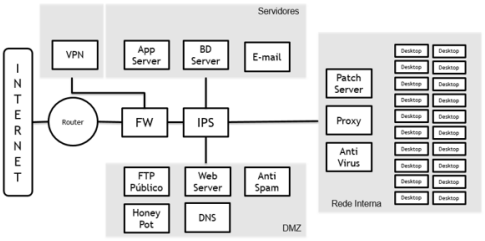
DMZ

Rede desmilitarizada – Agrega serviços que são acessados diretamente pela internet. É uma rede separada e dedicada pois caso um dos serviços/servidores seja invadido são menores as chances de invasão da rede interna.

Servidores são usualmente separados da rede interna (Vlan própria) com o objetivo de segrega-los da rede interna, protegendo-os Por exemplo contra vírus, acesso indevido, etc.

App Server | BD Server | Email

Exemplos:
- App Server – Websphere
- BD Server – Oracle
- E-mail - Exchange



Patch Server

Servidor utilizado para atualização de desktops e servidores.
Fraqueza: Precisa estar atrelado a GMUD
Proteção: Atualização massiva

Proxy

Servidor utilizado para filtrar o acesso Web a internet
Fraqueza: Falso positivo
Proteção: Bloqueia o acesso a sites indevidos

Anti Vírus

Fornece proteção contra vírus e em alguns casos como trojans, malwares, etc.
Fraqueza: Falha de atualização
Proteção: Bloqueia infecção de vírus

Capítulo 4. Ataque a redes de computadores

Entender como os ataques a rede de computadores acontecem é fundamental para entender mecanismos de defesa. Neste capítulo veremos alguns tipos de ataque e praticaremos a fase inicial de um ataque hacker, que é o reconhecimento, onde o atacante busca colher informações sobre o ambiente para utilizar as ferramentas de exploração de vulnerabilidade e posterior manutenção do acesso.

Ataques e defesa a redes de computadores

Cada tipo de ataque a rede de computadores busca explorar um ou mais pilares de segurança da informação, a figura abaixo cita alguns deles:

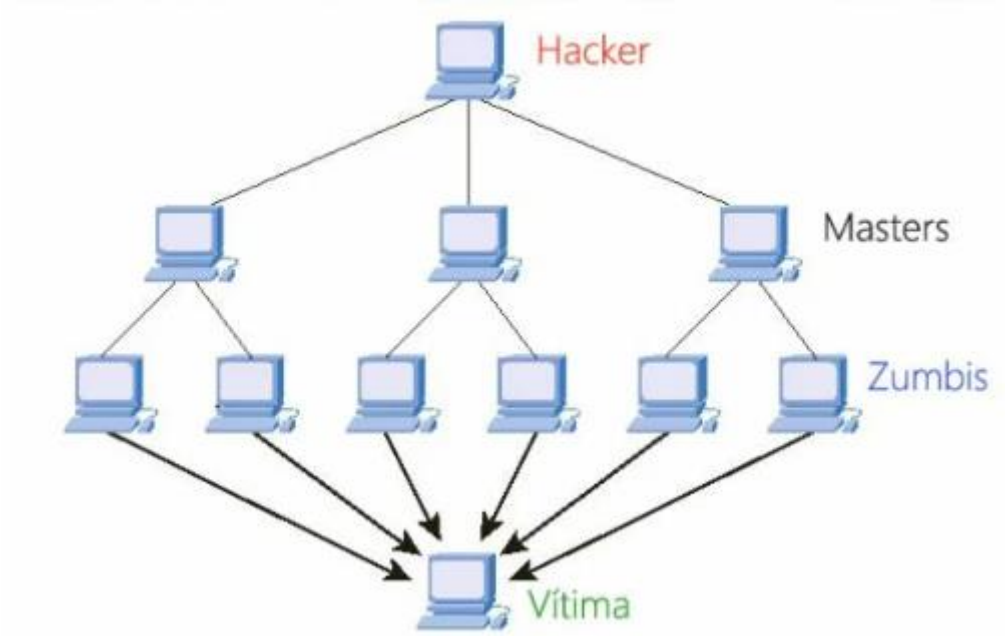
Figura 8 – Exemplos de ataques.

Confidencialidade	Roubo de dados (falha de código)
Integridade	Ransonware
Disponibilidade	DDOS

Um ataque muito famoso na internet é o de DDoS. Vários bancos, empresas de e-commerce e outras tantas já ficaram indisponíveis por ataques como este na internet. Basta fazer uma pesquisa no Google para obter exemplos. O ataque de DDoS tem início com a infecção por *malware* ou software malicioso análogo em dezenas, centenas, as vezes milhares, e há alguns casos raros de milhões de máquinas infectadas. Ao conjunto destas máquinas, denominamos *botnets*. Estas máquinas são então gerenciadas por outras máquinas também invadidas, chamadas máster. O papel da máquina máster é importante, e é necessário que sejam várias, pois a perda de uma delas leva automaticamente a perda de controle de muitas máquinas zumbis. Quando um atacante resolve fazer um ataque, ele envia um comando para que todas estas máquinas façam conexões simultâneas à vítima. Usualmente, a vítima, por mais que seja grande, não está preparada para receber um

número tão gigante de conexões simultâneas, quando este limite é ultrapassado temos então a negação do serviço (*Denial of Service)*.

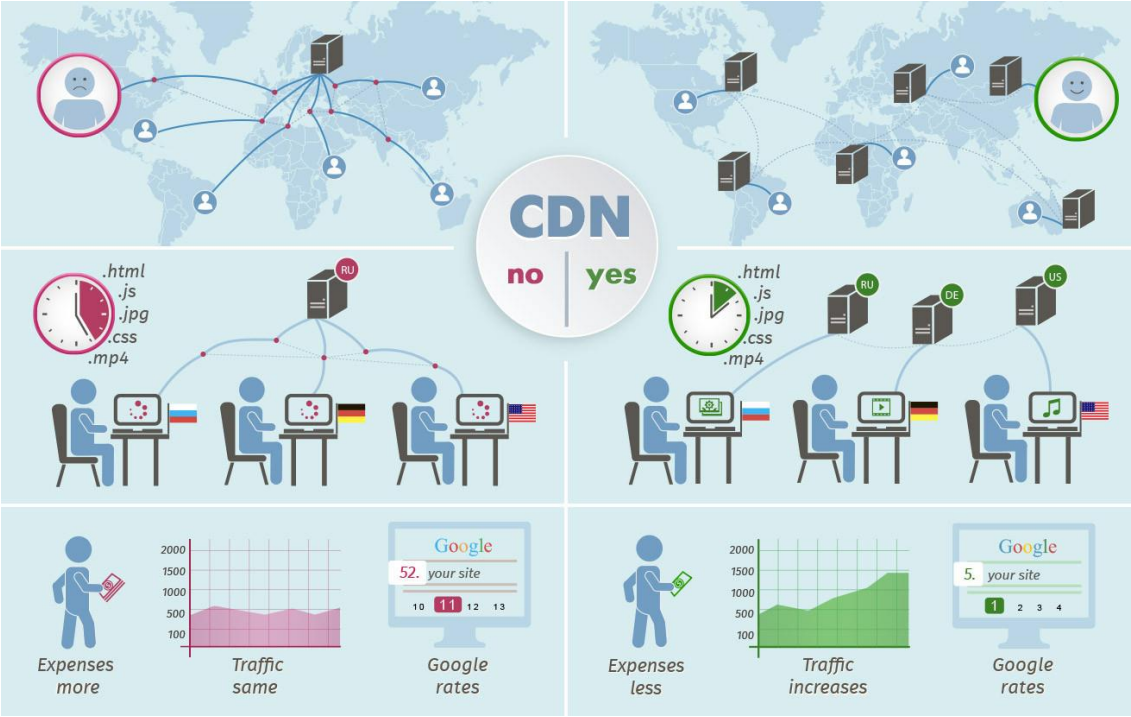
Figura 9 – Ataque DDoS.



Fonte: Canaltech.

Atualmente um serviço muito utilizado para proteção de ataques de DDoS são as chamadas CDNs *(Content Delivery Network)*. O propósito principal destas redes é entregar conteúdos, como imagens, vídeos e páginas web numa velocidade muito mais ágil. Elas fazem isso aproximando o servidor que atende a requisição do *browser* do usuário que acessa o site, no entanto, como tais redes tem uma capacidade de entrega inimaginável em termos de bits por segundo, é comum serem usados também para defesa dos sites de empresas. Abaixo uma figura que compara, do lado esquerdo, um cenário sem CDNs, e do direito a implementação de CDNs.

Figura 9 – Ataque DDoS.



Fonte: Xlab Security.

Outro ataque muito comum em redes de computadores é o sequestre de DNS (Domain Name System). O DNS é responsável por transformar nomes, como www.meusite.com.br para IPs. Desta forma, quando nossos computadores fazem consultas a servidores de DNS, eles recebem como retorno o IP que devem acessar. Se estes DNSs são invadidos, é possível manipular o IP que é acessado, levando o usuário a acessar algo que acredita ser o site correto, quando na verdade, este pode cair em uma armadilha que irá capturar informações relevantes do usuário enganado. Existem algumas formas de se proteger deste tipo de ataque:

1) Utilize diretamente nas máquinas (desktops ou servidores) o IP 8.8.8.8 (Google) ou 1.1.1.1 (Cloudfare).

2) Se o seu servidor de DNS for um roteador de banda larga, mantenha este sempre atualizado e usado sempre como cache de serviços, serviços confiáveis como 8.8.8.8 (Google) e 1.1.1.1 (Cloudfare).

3) Se o seu servidor de DNS está instalado em um servidor interno, garanta que este atue apenas como resolver, ou seja, que ele preste serviços apenas para a rede interna.

Ameaças do cyberspace

Existem uma enormidade de ameaças presentes no cyberspace, o quadro abaixo detalha o tipo de ameaça, como é dado a infecção, os objetivos e a forma de prevenção/remediação. Para fins didáticos, algumas ameaças foram aglutinadas em uma única linha.

Figura 10 – Ameaças do cyberspace.

Ameaça	Como é a infecção	Objetivos	Prevenção/Remediação
Malware / Keylogger	Usualmente via anexo de email	Obter dados como número do cartão de crédito e senhas	Antimalware
Virus / Worms	Falhas em sistemas operacionais ou aplicativos muito usados (ex: pdf reader)	Se replicar e causar danos ao usuário (deletar arquivos, por exemplo)	Antivirus
Ransonware	Falhas em sistemas operacionais ou aplicativos muito usados (ex: pdf reader)	Criptografar arquivos do computador e pedindo resgate em BitCoin para devolução dos dados	Anti-Ransonware Tools
Spywares	Usualmente via anexo de email e instalação de aplicativos baixados da Internet (search bars)	Obter o comportamento e informações pessoais do usuário infectado e direciona-lo para sites de propaganda	Antispyware Tools
Rootkits	Instalado pelo invasor após ter acesso ao sistema (usualmente presente em servidores invadidos)	Permitir o atacante não ser detectado em acessos futuros. Usualmente aplicativos de sistema como "ls", "ps" e outros são substituídos pelos do rootkit	chkrootkit

Criptografia

Criptografia é a arte de tornar inelegível uma mensagem de forma que quem a intercepte não consiga interpretá-la. Abaixo um exemplo de duas palavras, criptografadas da forma mais simples possível. Note que cada letra do alfabeto é substituída pelo caráter do mesmo alfabeto presente cinco posições adiante.

Figura 11 – Exemplo simplificado do uso de criptografia.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	A	B	C	D	E

ATACAR = FYFHFW
AVANTE = FBFSYJ

Atualmente, algoritmos criptográficos com fórmulas matemáticas complexas e sofisticadas tornam o processo de quebra de criptografia um processo bem demorado, de tal forma que havendo a quebra da criptografia, o que por si só exigiria um arsenal gigantesco de processadores, a informação obtida aconteceria depois de anos e, portanto, não seria mais relevante no contexto de sua obtenção.

A criptografia pode ser dívida em simétrica e assimétrica. Cada uma tem seus prós e contras, sendo que o comum em ambas é uma chave; no caso da primeira, chaves iguais compartilhadas entre a origem e o destino, e uma chave diferente (privada e pública) no caso da criptografia assimétrica.

Figura 11 – Criptografia simétrica.

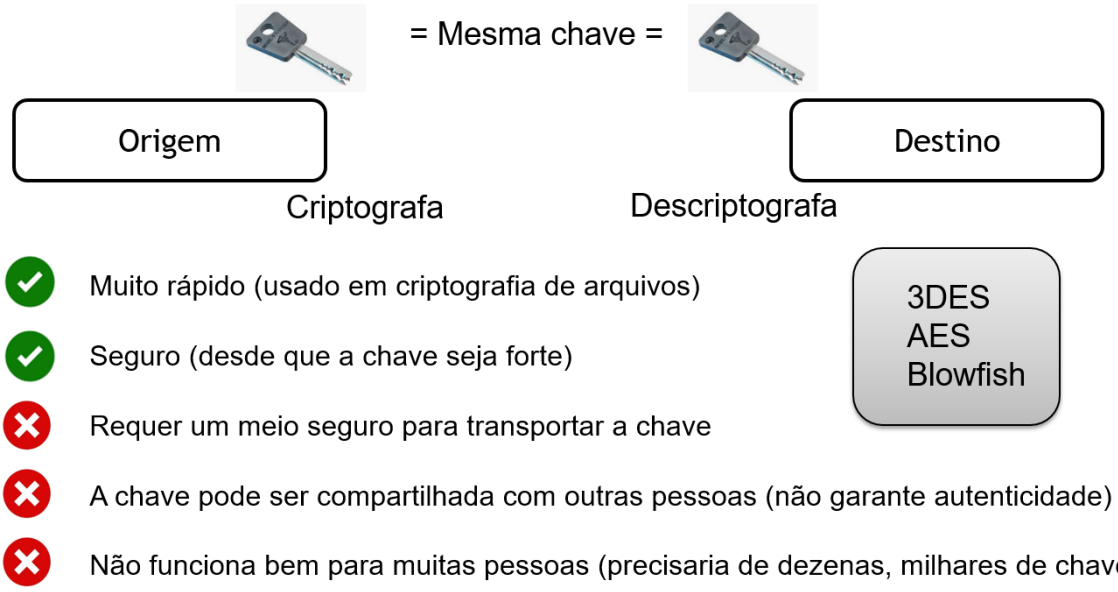
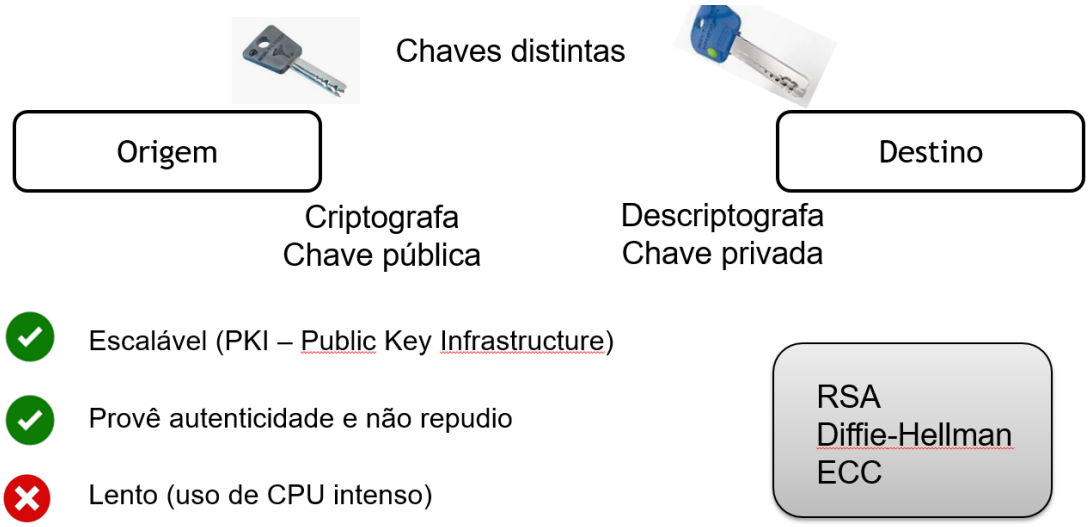


Figura 12 – Criptografia simétrica.



O *hashing* é uma técnica que transforma *strings* de tamanhos variáveis em tamanhos fixos. O objetivo é garantir que uma informação não foi alterada durante seu trânsito. Assim, se eu pretendo enviar uma mensagem ou mesmo um arquivo, eu anexo, usualmente via outro canal de comunicação, o *hash,* e ao receber comparo. Se as *strings* foram iguais, teremos, portanto, que a mensagem não foi alterada durante o trânsito.

Praticidade versus segurança

Quando instalamos sistemas operacionais, desenvolvemos softwares ou entregamos soluções de TI, é nosso desejo que ocorra, na maioria das vezes, de forma mais rápida possível. Esta valorização da entrega rápida acaba despriorizando questões relativas à segurança.

Durante a prática, vocês poderão acompanhar, como que, em nome da praticidade e rapidez, iremos expor serviços desnecessários na internet, acessar com usuários privilegiados, quando a boa prática recomenda que isso não ocorra e outras práticas ruins destacadas durante a apresentação.

Excesso de segurança lega a paralisia e ausência deles leva a incidentes. Encontrar o caminho do meio, assim como todas as esferas da vida, é fator primordial para o sucesso.

Hardening

A tradução de hardening, de acordo com o Google Translator, é endurecimento, e é isso que buscamos ao configurar os sistemas operacionais e banco de dados com regras mais rígidas para evitar acessos não autorizados. Abaixo você encontra as melhores práticas para sistemas operacionais Linux, Windows e sistemas gerenciadores de banco de dados.

Figura 13 – Hardening Linux.

- Utilize SSH sempre!
- Ignore ICMP Broadcast
- Desabilite serviços não usados
- Desinstale pacotes de software desnecessários
- Desabilite o acesso de *root* (use o *sudo)*
- Desabite interfaces Gráficas (KDE, Gnome, etc)
- Gere um CD de *boot*
- Mantenha patches atualizados
- Verifique permissões em arquivos críticos
- Utilize firewall local para filtrar tráfego indevido
- Configure o log para ir para um *syslog*
- Implante antivírus e HIPS

Fonte: SANS.

Figura 14 – Hardening Windows.

- Ignore ICMP Broadcast
- Desabilite serviços não usados
- Microsoft Baseline Security Analyzer
- Defina política de senha
- Defina políticas de auditoria
- Mantenha patches atualizados
- Configure o log para ir para um *syslog*
- Implante antivírus e HIPS

Fonte: CISecurity.

Figura 15 – Hardening Banco de Dados.

- Remova usuários desnecessários (ex: BI, HR, etc)
- Remova a diretrizes que permitem execução de comandos no SO
- Habilite a auditoria de usuários privilegiados
- Habilite auditoria para ações importantes como: "*GRANT*, *CREATE DATABASE*",etc
- Habilite a política de senhas;
- Restrinja o IP de conexão de usuários privilegiados e de aplicações críticas
- Não permita conexões simultâneas (compartilhamento de usuário/senha)
- Remova privilégios excessivos como "*GRANT ANY ROLE*"

Segurança em Cloud

Ao implementarmos a segurança em *cloud computing* é importante entender qual o modelo contratado. No modelo IaaS (Infraestrutura como Serviço) o contratante tem domínio completo do sistema operacional e de todas as camadas instaladas neste (plataformas, aplicações e banco de dados). No modelo PaaS (Plataforma como Serviço), o contratante não consegue operar o sistema operacional, isso reduz sua responsabilidade com relação a manutenção de segurança desta camada, no entanto, mantém a responsabilidade no que tange manter as configurações da

plataforma configuradas de forma segura. Já no modelo de SaaS (Softwares como Serviço), a segurança está diretamente relacionada com a aplicação, neste caso os controles ligados às regras de negócio e autenticação/autorização, devem ser tratados com lupa. O quadro abaixo destaca os itens que devem ser levados em consideração em cada implementação de segurança.

Figura 16 – Segurança em Cloud.

IaaS	PaaS	SaaS
Maior preocupação/esforço é com o SO e a Rede	**Maior preocupação com o desenvolvimento de aplicações,App Server e BD**	**Gerenciamento de acesso e identidade das aplicações**
Provisionar máquinas já com patchs de segurança	Patchs dos App Servers e BDs	Granularidade dos controles da aplicação
Monitorar log em todos os dispositivos	Segurança em banco de dados compartilhados	Criptografia na comunicação
Inibir que outros desabilitem a segurança do sistema	Controle de acesso no gerenciador de conteúdo	Gerenciamento das políticas da aplicação
Isolamento da rede	Criptografia do BD	DLP
Backup e restore	Backup e Restore	Backup e Restore
Gerenciar identidade.	Gerenciar identidade.	Gerenciar identidade. (Federação)

Capítulo 5. Cybersecurity – Aplicações

Segurança em aplicações é um tema vasto e amplo, que abrange várias tecnologias arquiteturas, frameworks e outros. Iremos entender o que torna o desenvolvimento seguro e durante as aulas práticas entender um pouco através do código de uma aplicação real.

Entendendo a causa de aplicações inseguras

O autor que aqui vos escreve, criou carreira iniciando na área de suporte técnico, passou em seguida por áreas de segurança em consultorias e empresas de telecom. Recentemente resolveu inovar e junto com o time de desenvolvedores sentiu na pele o que é desenvolver com segurança.

Desenvolver um código seguro passa por aprender a desenvolver com segurança. Isso abrange não só os desenvolvedores, mas os clientes do produto a ser construído, que precisam ser engajados em ter um pouco menos de velocidade em prol de qualidade, que neste caso é materializado através da segurança.

Mergulhado nesta área, busquei identificar quais práticas melhor alinhariam os desejos das empresas em ter softwares funcionais e desenvolvidos com agilidade, mas com segurança, aos anseios dos desenvolvedores em ter que entregar rápido e com segurança. As lições que aprendi não são uma fórmula mágica para resolver a questão, mas entendo que são um pontapé importante para que tenhamos softwares mais seguros.

1) Tenha **objetivos únicos (OKR)** para as equipes de desenvolvimento, infraestrutura, segurança e **produtos** que envolvam KR de segurança.

2) Dê **voz ativa aos desenvolvedores** para que incluam em suas estimativas de desenvolvimento e requisitos de segurança.

3) Se for necessário **baixar a prioridade** de algum requisito de segurança, o **mantenha no backlog** para a próxima sprint e comunique bem os envolvidos a respeito.

4) **Treine seu time de desenvolvimento** em técnicas de segurança.

5) Avalie se não é melhor **formar desenvolvedores em segurança** em detrimento de profissionais de segurança em desenvolvimento.

6) **Não considere ter controles de segurança máximos** para toda e qualquer aplicação. (Intranet institucional corporativa é certamente menos critica que o e-commerce)

Arquitetura de aplicações

Existem diversas formas de comunicação e funcionamento de aplicações, que são sumarizadas no quadro abaixo.

Figura 17 – Formas de comunicação e funcionamento de aplicações.

Tipo de arquitetura	Principal caracteristica	Exemplos	Ataques mais comuns
Stand alone	Não se comunicam em rede	PDF Readers	PDF que exploram erros e permitem instalação de malwares
Client Server	Comunicação de muitos para poucos Maior parte do processamento no servidor	Microsoft Outlook	Ataques ao servidor de emails Ataques ao cliente Microsoft Outlook
Sistemas distribuídos	Funcionalidades espalhadas em diversos locais (geográficos ou não)	Microserviços	Ataque ao hub central (orquestrador)
Cloud	Não sabemos onde fica	Netflix	Falhas humanas ou bugs de software
Web	Camadas (usualmente MVC)	Aplicações corporativas	DDoS, exploração de vulnerabilidades na aplicação
Mobile	Transito de dados (e não de imagens, sons, etc)	Jogos	Ataques ao servidor

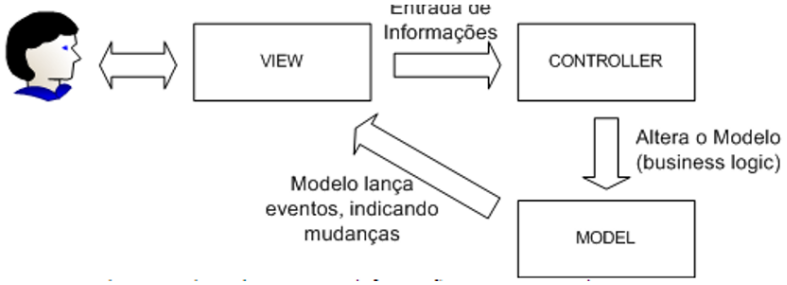
Atualmente as arquiteturas que envolvem Web e APIs (*Application Programming Interface*) são as mais utilizadas, sendo esta última especialmente útil na confecção de aplicações que podem ser rodadas em celulares, televisões, dispositivos diversos como Alexa da Amazon e demais dispositivos de IoT.

As figuras abaixo ilustram o funcionamento destes tipos de aplicação que serão exploradas a seguir, a respeito dos métodos de ataque e defesa.

Na arquitetura MVC, há uma delegação de responsabilidade em cada camada de aplicação. Sendo elas:

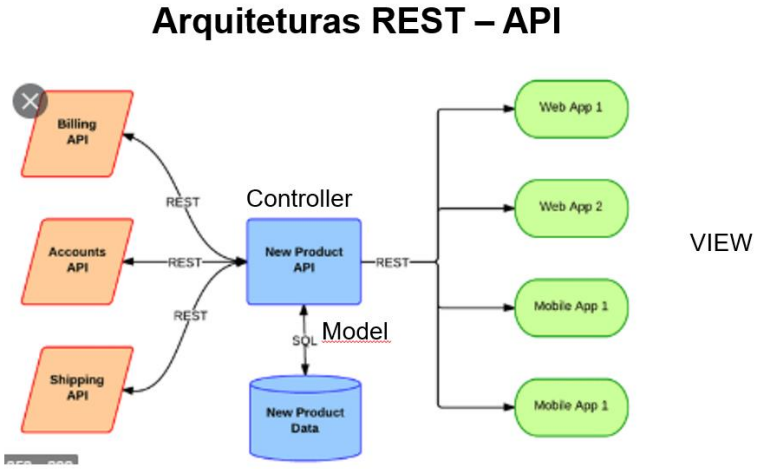
- **View:** responsável por coletar e exibir dados para usuários (veja sobre vulnerabilidades desta camada quando falarmos de Javascript nas aulas práticas).
- **Controller**: responsável por receber as requisições e tratá-las.
- **Model:** responsável por tratamento junto a camada de dados.

Figura 18 – Arquitetura MVC.



Fonte: UFMG

Figura 19 – REST.



Fonte: CXArch.

Na arquitetura de APIs, a View é feita pelo dispositivo remoto, podendo ser uma página Web, um dispositivo móvel ou um dispositivo IoT. Todo o processamento é feito pelo fornecedor de dados. Um bom exemplo disso é a API de consulta de CEP dos Correios, que pode ser consultada por qualquer site de comércio eletrônico, por exemplo.

Ataque e proteção a APIs

O ataque às APIs ocorre quando estas não processam adequadamente as permissões, controles de sessão e outros mecanismos de proteção de segurança ao fornecer as informações devidas.

- Enumeração de dados / Massive attack (DELETE, PUT).
- Falha no controle de sessão.
- Injeção de parâmetros.
- DoS (ausência de paginação).
- Excesso de confiança na camada de apresentação/view (Javascript).

Com relação ao excesso de confiança na camada de apresentação, é importante destacar que o Javascript é processado na camada de *View* e que, portanto, pode ser manipulado por um usuário mal-intencionado. Desta forma, qualquer validação que envolva regra de negócio pode ser facilitada na camada *view*, mas deve ser verificada no *backend* (API).

As proteções para as APIs serão detalhadas a seguir, junto as proteções aplicadas às aplicações Web.

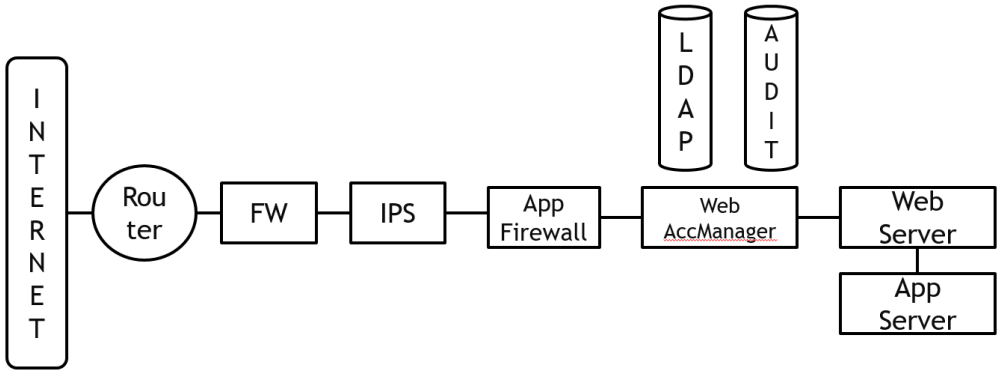
Ataques e proteção a aplicações Web

De acordo com o Owap (Open Web Application Security Project), estes são os ataques mais comuns a aplicações Web:

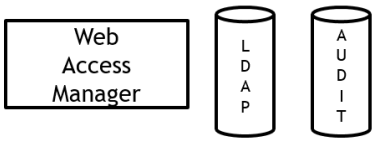
- **Injeção de parâmetros** (SQL Injection, REST Parameters etc.).
- **Falha no controle de acesso** (erro de implementação de sessão, auth etc.).
- **Exposição de informações sensíveis** (disponibilização demasiadamente de infos).
- **Interfaces administrativas expostas.**
- **Falhas de controle de acesso** (usuários autenticados acessam mais do que deveriam).
- **Configuração default** (mensagens verbosas, bibliotecas usadas sem configuração).
- **Cross site scripts** (Injeção de códigos JS em formulários Web).
- **Deserialização insegura** (confiar no que vem do cliente ou é processado por este).
- **Logs / monitoração insuficientes.**

A melhor forma de termos aplicações seguras é tendo código seguro, no entanto, nem sempre isso é possível. Realizar o refatoramento de código legado pode levar anos e o custo seria muito grande. Desta forma, algumas soluções em camada de rede são possíveis e outras são complementares, a seguir listamos estas:

Figura 20 – Coleção de figuras com arquitetura segura de software.



- Adiciona segurança imediata a uma Aplicação que já está em produção
- Implementa a política de segurança em uma camada fora da aplicação.
- Precisa ser corretamente configurado (inputs) para evitar falso positivo (possui módulo learning mode)
- Capaz de proteger contra os ataques do OWASP TOP 10 (Ex: SQL Injection, XSS, etc)
- Pode filtrar informações sensíveis Ex.: nenhum número de cartão de Crédito pode ser trafegado
- Proteção contra brute-force



- Adiciona controle de sessão em toda a aplicação
- Implementa e garante criptografia SSL em todos os acessos
- Garante que todo diretório é privado, a não ser que de forma explicita seja público
- Utiliza-se de autenticação LDAP que é importante para único controle de acesso e política de senha.
- Capaz de auditar de forma assíncrona todos os GETs e POSTs

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos*. Brasil, 2013.

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação*. Brasil, 2013.

JOINT TASK FORCE TRANSFORMATION INICIATIVE. *Managing Information Security Risk*: Organization, Mission, and Information System View. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-39/final>. Acesso em: 14 mai. 2020.

HARRIS, Shon; MAYMI, Fernando. *CISSP All-in-One Exam Guide*. 8. ed. McGraw-Hill Education, 2018.