SEGURANÇA DA INFORMAÇÃO:

O QUE DEVO SABER PARA SEGUIR UMA CARREIRA DE SUCESSO?

E-BOOK 1 DE 3

EMERSON NASCIMENTO E PAULO TRINDADE

NOSSA MISSÃO COM ESTE E-BOOK

Este é um conteúdo sobre Segurança da informação para iniciantes ou pessoas que desejem ingressar na área, lhes norteando com o único material disponível no mercado brasileiro que trata do dia a dia prático e direto ao ponto, com base nos melhores materiais disponíveis e mais de 40 anos somados de experiência de mercado de seus autores na jornada de Tecnologia.

Esperamos que este material transforme sua carreira lhe trazendo muitos resultados positivos.

Go hard!!!

SOBRE OS AUTORES

Emerson Nascimento

Atualmente com foco em MSS, ISO27k e NIST, possui mais de 20 anos experiência em GSTI, implantação e estruturação de Infraestrutura, Suporte e Service Desk utilizando COBIT/ITIL e Gestão de Projetos utilizando PMI. Gerenciou fábrica de software utilizando práticas de MPS Br e foi professor tutor e conteudísta do curso de pós-graduação EAD da Unisinos/RS em Gestão da Qualidade com ISO 9000 para TI além de escrever para a Revista Service News do HDI Brasil sobre Centros de Suporte.

Paulo Trindade

24 anos no mercado de tecnologia, se especializando em segurança da informação desde 2012. Gerenciou equipes multidisciplinares com mais de 40 pessoas, atuando também na Gestão de NOC e SOC. Em termos de soluções técnicas se especializou em sistemas Unix, Linux, DLP e atualmente trabalha como Consultor de Segurança da Informação.

SUMÁRIO

01

O QUE É A SEGURANÇA DA INFORMAÇÃO?

A segurança da informação iniciou-se pela necessidade do homem de transmitir e proteger informações de forma que fossem acessíveis somente aos seus destinatários, dando assim origem a criptografia, palavra composta por duas outra palavras gregas κρυπτός (kriptós – secreto, escondido) e γράφειν (gráfein – escrita).

Um bom exemplo ocorreu cerca de 100 aC, o Imperador romano Júlio César era conhecido por usar uma forma de criptografia para transmitir mensagens secretas a seus generais do exército postados na frente de guerra. Essa cifra de substituição, conhecida como cifra de César, é a mais mencionada na literatura acadêmica. Falaremos mais no item sobre criptografia.

A Segurança da Informação, InfoSec, Cyber Security ou Segurança Cibernética, sempre evolui de acordo com as necessidades e tendências, onde o centro de tudo não é a tecnologia e sim os negócios de uma empresa e/ou objetivos de um indivíduo.

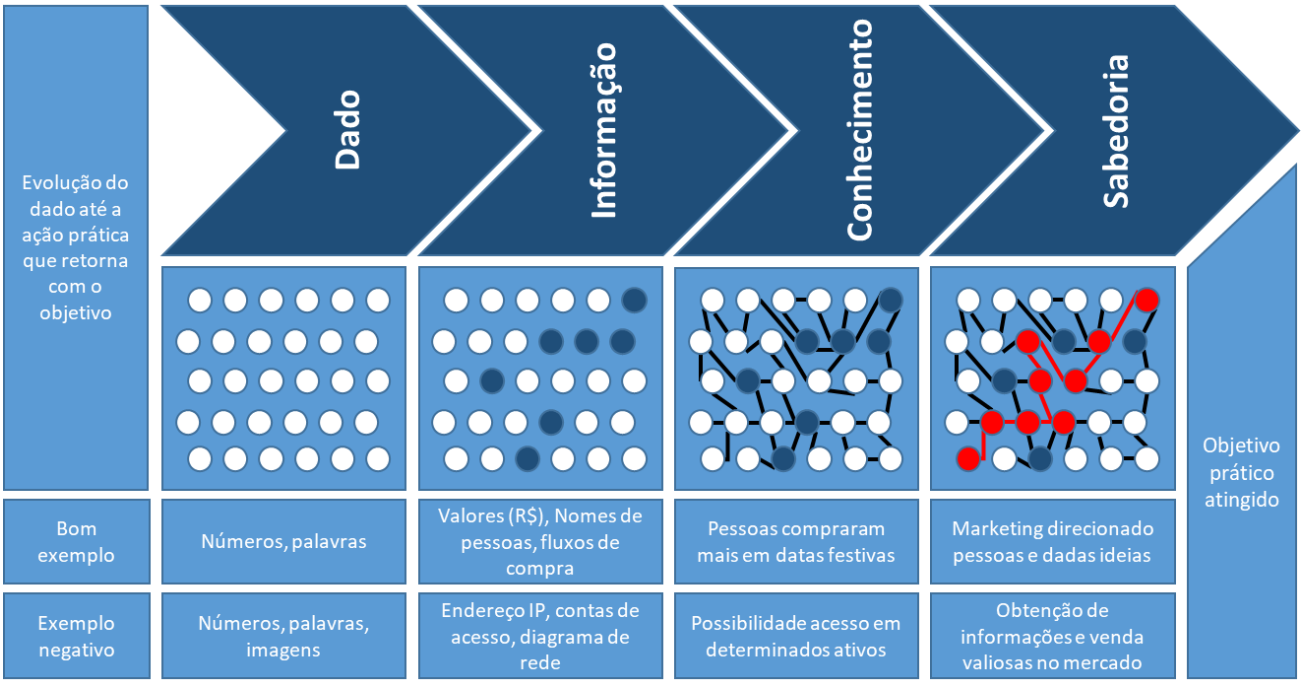
Ou seja, Segurança da Informação se trata de ´proteção, mitigando riscos de forma que os objetivos de um negócio ou indivíduo sejam atingidos.

Como ocorre essa proteção? Para responder a resta pergunta precisamos responder outras questões:

- **O que preciso proteger?**
- **Qual valor do que será protegido?**
- **Quais os riscos envolvidos?**
- **Quais medidas serão tomadas?**
- **Como responder a um incidente?**

Políticas, manuais, padrões, ações e tecnologia devem ser implementadas de acordo com os objetivos do negócio

Você verá ao longo deste material que a Segurança da Informação vai muito além de tecnologias. Imagine um cracker (hacker mal intencionado) ligando para uma pessoa que anunciou seu carro na internet, se passando por "call center do site" e solicitando a sua vítima um código que ele enviou (que na realidade é o código de reconfiguração do WhatsApp). Após isso ele roubará a conta e usará novamente sua lábia (técnica conhecida como engenharia social) para pedir transferências bancárias aos contatos de sua vítima. Qual ferramenta tecnológica ele usou para "invadir" o telefone da vítima? Ele fez uso da "lábia" ou engenharia social. Tais técnicas, sejam Engenharia Social, DDoS, Phishing, DNS Poisoning, SQL Injection etc são chamadas de Vetores de Ataque. Falaremos mais sobre isso.



Para preparar você para a sua evolução tanto em carreira como neste material, você precisa conhecer o conceito DICS ou DIKW (inglês) que é o acrônimo de Dado, Informação, Conhecimento e Sabedoria. Com este conceito você entenderá melhor onde está e poderá entender dentro de sua companhia o que é e em qual estágio está o item mais precioso : A INFORMAÇÃO.

Seguem as descrições de cada um destes níveis do modelo DICS:

DADO – elementos provenientes de uma coleta ou pesquisa. Podem ser classificados em termos de fatos, sinais, ou símbolos e identificados como palavras, números, códigos, tabelas ou base de dados;

INFORMAÇÃO – surge a partir da estruturação ou organização de dados processados para um fim/contexto especifico. Permite identificar o "o que". Se apresenta no formato de sentenças, equações, conceitos e ideias;

CONHECIMENTO – composto por uma mescla de informações contextualizadas, valores, experiências e regras. Permite identificar o "como". Estão na forma de livros, teorias, conceitos e axiomas;

SABEDORIA – ocorre quando há a ressignificação dos outros níveis em combinações metalinguísticas. Permite identificar o "por que". Expressa-se em compêndios, estratégias, paradigmas, sistemas, leis e princípios.

Nosso objetivo nesta breve introdução é lhe mostrar que seu sucesso na área de Segurança da Informação dependerá de sua garra na aquisição de conhecimento e ainda, foco no negócio e objetivo de seus Clientes.

Entenda: você está buscando adquirir ferramentas que possuem um objetivo claro: Garantir os objetivos do negócio. Por mais que fique encantado com as tecnologias que apresentaremos, lembre-se sempre disso. O Cliente é o foco.

02

PRINCIPAIS ÁREAS DA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação, devido sua complexidade, está se ramificando e se especializando em várias outras áreas, por isso é importante que você identifique a área que mais vai ao encontro do seu perfil profissional ou desejo e atuação.

A seguir mostraremos as principais áreas de atuação que podem servir como orientação na escolha de sua carreira.

SECURITY ARCHITECT (arquiteto de segurança): Eles são responsáveis por criar estruturas de segurança complexas e garantir que funcionem corretamente. Eles projetam sistemas de segurança para combater malware, invasões de hackers e ataques DDoS.

SECURITY CONSULTANT (Consultor de Segurança): um especialista que avalia riscos, problemas e soluções de segurança cibernética e fornece orientações;

ETHICAL HACKER (Hacker Ético ou White Hats): procuram por falhas no ambiente usando as mesmas táticas de crackers (hacker criminosos) ou Black Hats, ajudando na identificação das falhas;

CHIEF INFORMATION SECURITY OFFICER (CISO – Diretor de Segurança): Traduz os requisitos de negócio para as medidas de segurança, possui liberdade para construir equipes, supervisionar as ações de segurança além de se reportar ao CEO ou CIO da organização.

SECURITY SOFTWARE DEVELOPER (Analista de Desenvolvimento Seguro): Atua no desenvolvimento de software seguro principalmente em equipes chamadas de DevSecOps (desenvolvimento, segurança e operação), estes profissionais desenvolvem, aplicam segurança e operam a infraestrutura destas aplicações, principalmente em plataformas como Kubernetes, GItlab-CI, Istio entre outras.

03

ALGUNS TERMOS E CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

2FA – 2 FACTOR AUTHENTICATION, ACRÔNIMO PARA AUTENTICAÇÃO DE DOIS FATORES.

AAA – ACRÔNIMO PARA AUTENTICAÇÃO, AUTORIZAÇÃO E AUDITORIA.

ACESSO - ATO DE INGRESSAR, TRANSITAR, CONHECER OU CONSULTAR A INFORMAÇÃO, BEM COMO POSSIBILIDADE DE USAR OS ATIVOS DE INFORMAÇÃO DE UM ÓRGÃO OU ENTIDADE.

AMBIENTE CIBERNÉTICO – INCLUI USUÁRIOS, REDES, DISPOSITIVOS, SOFTWARE, PROCESSOS, INFORMAÇÃO ARMAZENADA OU EM TRÂNSITO, SERVIÇOS E SISTEMAS QUE POSSAM SER CONECTADOS DIRETA OU INDIRETAMENTE A REDES DE COMPUTADORES;

ADWARE - DO INGLÊS ADVERTISING SOFTWARE, É UM TIPO ESPECÍFICO DE SPYWARE PROJETADO ESPECIFICAMENTE PARA APRESENTAR PROPAGANDAS. PODE SER USADO DE FORMA LEGÍTIMA, QUANDO INCORPORADO A PROGRAMAS E SERVIÇOS, COMO FORMA DE PATROCÍNIO OU RETORNO FINANCEIRO PARA QUEM DESENVOLVE PROGRAMAS LIVRES OU PRESTA SERVIÇOS GRATUITOS. TAMBÉM PODE SER USADO PARA FINS MALICIOSOS QUANDO AS PROPAGANDAS APRESENTADAS SÃO DIRECIONADAS DE ACORDO COM A NAVEGAÇÃO DO USUÁRIO E SEM QUE ESTE SAIBA QUE TAL MONITORAMENTO ESTÁ SENDO REALIZADA;

AMBIENTE DE INFORMAÇÃO – AGREGADO DE INDIVÍDUOS, ORGANIZAÇÕES E/OU SISTEMAS QUE COLETAM, PROCESSAM OU DISSEMINAM INFORMAÇÃO;

AMEAÇA – CONJUNTO DE FATORES EXTERNOS OU CAUSA POTENCIAL DE UM INCIDENTE INDESEJADO, QUE PODE RESULTAR EM DANO PARA UM SISTEMA OU ORGANIZAÇÃO;

AMEAÇA PERSISTENTE AVANÇADA (APT) – OPERAÇÕES DE LONGO PRAZO PROJETADAS PARA INFILTRAR OU EXFILTRAR O MÁXIMO POSSÍVEL DE DADOS SEM SEREM DESCOBERTAS, SENDO MAIS CONHECIDAS PELO SEU ACRÔNIMO EM INGLÊS APT – ADVANCED PERSISTENT THREAT. POSSUI CICLO DE VIDA MAIS LONGO E COMPLEXO QUE OUTROS TIPOS DE ATAQUE, SENDO MAIS ELABORADOS E NECESSITANDO DE VOLUME SIGNIFICATIVO DE RECURSOS PARA SUA VIABILIZAÇÃO, O QUE EXIGE FORTE COORDENAÇÃO. EM GERAL, SÃO REALIZADOS POR GRUPOS COM INTENÇÃO DE ESPIONAGEM OU SABOTAGEM;

ANÁLISE DE IMPACTO NOS NEGÓCIOS (AIN) – VISA ESTIMAR OS IMPACTOS RESULTANTES DA INTERRUPÇÃO DE SERVIÇOS E DE CENÁRIOS DE DESASTRES QUE POSSAM AFETAR O DESEMPENHO DAS EMPRESAS, BEM COMO AS TÉCNICAS PARA QUALIFICAR E QUANTIFICAR ESSES IMPACTOS. DEFINE TAMBÉM A CRITICIDADE DOS PROCESSOS DE NEGÓCIO, SUAS PRIORIDADES DE RECUPERAÇÃO, INTERDEPENDÊNCIAS E OS REQUISITOS DE SEGURANÇA DA INFORMAÇÃO PARA QUE OS OBJETIVOS DE RECUPERAÇÃO SEJAM ATENDIDOS NOS PRAZOS ESTABELECIDOS;

ANÁLISE DE INCIDENTES - CONSISTE EM EXAMINAR TODAS AS INFORMAÇÕES DISPONÍVEIS SOBRE O INCIDENTE, INCLUINDO ARTEFATOS E OUTRAS EVIDÊNCIAS RELACIONADAS AO EVENTO. O PROPÓSITO DA ANÁLISE É IDENTIFICAR O ESCOPO DO INCIDENTE, SUA EXTENSÃO, SUA NATUREZA E QUAIS OS PREJUÍZOS CAUSADOS. TAMBÉM FAZ PARTE DA ANÁLISE DO INCIDENTE PROPOR ESTRATÉGIAS DE CONTENÇÃO E RECUPERAÇÃO;.

ANÁLISE DE RISCOS – USO SISTEMÁTICO DE INFORMAÇÕES PARA IDENTIFICAR FONTES E ESTIMAR O RISCO.

COLETA DE EVIDÊNCIAS DE SEGURANÇA - PROCESSO DE OBTENÇÃO DE ITENS FÍSICOS QUE CONTÉM UMA POTENCIAL EVIDÊNCIA, MEDIANTE A UTILIZAÇÃO DE METODOLOGIA E DE FERRAMENTAS ADEQUADAS. ESSE PROCESSO INCLUI A AQUISIÇÃO, OU SEJA, A GERAÇÃO DAS CÓPIAS DAS MÍDIAS, OU A COLEÇÃO DE DADOS QUE CONTENHAM EVIDÊNCIAS DO INCIDENTE.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO - GRUPO DE PESSOAS COM A RESPONSABILIDADE DE ASSESSORAR A IMPLEMENTAÇÃO DAS AÇÕES DE SEGURANÇA DA INFORMAÇÃO.

CONTROLES DE SEGURANÇA – MEDIDAS ADOTADAS PARA EVITAR OU DIMINUIR O RISCO DE UM ATAQUE. EXEMPLOS DE CONTROLES DE SEGURANÇA SÃO: CRIPTOGRAFIA, FUNÇÕES DE "HASH", VALIDAÇÃO DE ENTRADA, BALANCEAMENTO DE CARGA, TRILHAS DE AUDITORIA, CONTROLE DE ACESSO, EXPIRAÇÃO DE SESSÃO E BACKUPS, ENTRE OUTROS.

CREDENCIAL (OU CONTA DE ACESSO) – PERMISSÃO, CONCEDIDA POR AUTORIDADE COMPETENTE APÓS O PROCESSO DE CREDENCIAMENTO, QUE HABILITAM DETERMINADA PESSOA, SISTEMA OU ORGANIZAÇÃO AO ACESSO DE RECURSOS. A CREDENCIAL PODE SER FÍSICA (COMO UM CRACHÁ), OU LÓGICA (COMO A IDENTIFICAÇÃO DE USUÁRIO E SENHA).

CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM) - ACRÔNIMO INTERNACIONAL PARA DESIGNAR UM GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA, RESPONSÁVEL POR TRATAR INCIDENTES DE SEGURANÇA PARA UM PÚBLICO ALVO ESPECÍFICO.

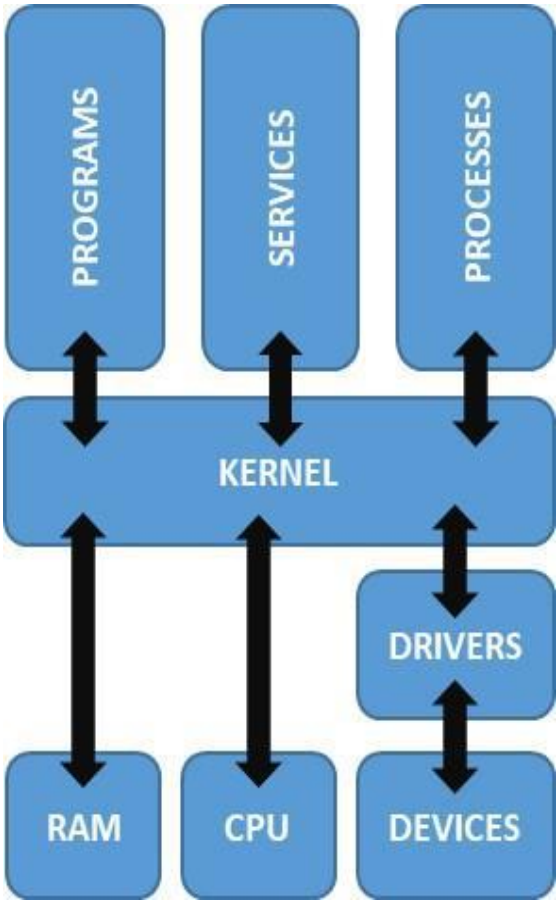
DDOS – ACRÔNIMO DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDA (DISTRIBUTED DENIAL OF SERVICE)

04

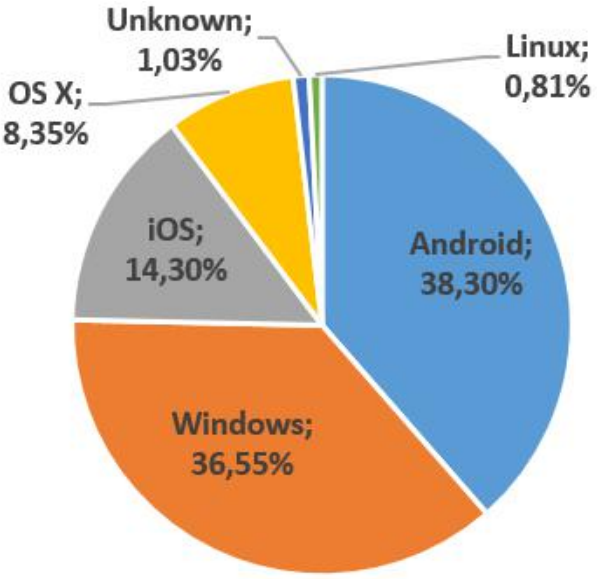
SISTEMAS OPERACIONAIS E SUAS CARACTERÍSTICAS

Vamos ser um pouco mais técnicos? Sim! Vamos lá!

O sistema operacional (OS – Operating System) é comporto por programas, processos e serviços que se comunicam com um núcleo (Kernel) e este se comunica com o hardware. Existem serviços (deamons) que são executados em plano de fundo do OS bem como os aplicativos que fazem interface com o usuário do sistema. Todos possuem um fluxo de comunicação com o hardware e é o que veremos a seguir.



É preciso dominar como cada um destes elementos se comunica entre si, pois uma ameaça pode advir em qualquer uma destas camadas de interação, inclusive advir do próprio hardware devido a falhas no projeto.



Aqui, estamos abordando o conceito dos principais sistemas operacionais de uma forma sintética para possibilitar equalizarmos o conhecimento e podermos mais a frente, ver como aplicar segurança em cada um deles.

Mesmo com estas características básicas que nos ajudam na implementação de segurança, estes sistemas divergem em alguns pontos. A seguir, descreveremos alguns pontos importantes sobre eles.

ANDROID: Android é um sistema baseado no núcleo **LINUX**, desenvolvido por um consorcio de desenvolvedores (Open Handset Alliance). O Google é o principal colaborador. Exige mais hardware que seu concorrente direto, iOS, pois executa uma "camada virtual" que facilita a compatibilidade entre vários hardwares e aplicativos. Open Source.

MICROSOFT WINDOWS: Nasceu em 1985. É Sistema operacional fechado e foi desenvolvido para executar em processadores com arquitetura CISC/x86. Executa binários exclusivos.

APPLE IOS: Sistema baseado no FreeBSD e compilado para executar em processadores de arquitetura RISC/ARM desenhados pela fabricante. Executa binários exclusivos. Sistema fechado.

APPLE OS X: Sistema também baseado no FreeBSD e compilado para executar em processadores CISC/x86. Executa também binários Linux

LINUX: Sistema aberto inspirado no sistema Minix, sistema derivado do UNIX, Linus Torvalds desenvolve em 1991 o primeiro Kernel. Foi ajudado pela comunidade de desenvolvedores que ampliaram sua funcionalidade para diversos processadores além de criarem diversas interfaces e aplicativos.

UNIX: Desenvolvido em 1969 pela AT&T/Bell Labs nos Estados Unidos por Ken Thompson, Dennis Ritchie, Douglas McIlroy, e Joe Ossanna. Lançado pela primeira vez em 1971 escrito inteiramente em linguagem assembly, uma prática comum para a época. Mais tarde, em 1973, o sistema foi reescrito na linguagem de programação C por Dennis Ritchie.

Os sistemas Linux e iOS derivaram do sistema UNIX e compartilham muitas de suas características. Muitos appliances (antes wi-fi, roteadores, firewalls etc) possuem sua base em um Kernel adaptado para certos processadores, mas originalmente um Kernel derivado de versões que se inspiram em um UNIX/Linux. Mais de 60% do mundo usa sistemas com estas características, por isso a importância em aprender um sistema UNIX/Linux.

Existem outros sistemas chamados de RealTime, arquiteturas pequenas com processadores simples que normalmente controlam equipamentos em fábricas. Esteja atento a este ponto!

Nosso objetivo é apresentar algumas diferenças entre os sistemas, mas para a correta aplicação de segurança é necessário que você avance mais no conhecimento dos mesmos. No final deste material indicaremos algumas fontes que lhe ajudarão nesta missão.

05

CONFIDENCIALIDADE INTEGRIDADE E DISPONIBILIDADE

Confidencialidade, Integridade e Disponibilidade! Guarde isso! Essa é a missão!

Também conhecida como CIA Triad (Confidentiality, Integrity and Availability) representa os principais atributos que orientam o planejamento, análise e implementação da Segurança da Informação. Alguns materiais incluem outros atributos, mas que entendemos que estão ligados a estes três. Falaremos mais sobre cada um!

Confidencialidade: Limita o acesso a informação somente às entidades (pessoas, app, hardware etc) autorizadas.

Integridade: garante que a informação manipulada mantenha todas as características originais estabelecidas pelo seu dono, incluindo controle de mudanças e garantia do seu ciclo de vida.

Disponibilidade: propriedade que garante que a informação esteja sempre disponível.

O ciclo de vida da informação segue as três fases de criação, armazenamento, uso, arquivamento e destruição;

Guarde estas características, elas serão a base de tudo que você fará na área. Não dá para algo estar disponível se qualquer um pode acessar, não serve de nada ter a informação, mas ninguém acessar, assim como também é inútil uma informação sem o controle de que pode ter sido corrompida ou alterada.

Veremos a seguir os controles mais comuns em segurança da informação:

<u>Administrativos:</u> Políticas internas, regras, procedimentos e manuais;

<u>Físicos:</u> Travas, cofres, cercas (isso mesmo!), guardas e até cães;

<u>Técnicos</u>: Firewalls, IDS, IPS, EDR, DLP, SIEM, criptografia, CASB, e outros (veremos mais ao longo do material!);

<u>Dissuasivos</u>: Guardas, cães, câmeras, placas de aviso.

Corretivos: Extintor de incêndio, Guardas;

Preventivos: Cercas, Muros.

Recovery (recuperação): Backup, ação legal (justiça),

Compensatórios: não é possível reduzir os riscos a zero, sendo que muitas vezes após a criação de um controle sempre sobre algum risco, para estes casos e quando os custos permitirem aplicamos um controle compensatório, que mitigará o risco residual;

Detectivo: Sensores, cães, câmeras (quando monitoradas) e análise de logs.

RISCO, VULNERABILIDADE E AMEAÇA

Você sabe a diferença entre cada um destes conceitos? Então é a hora de se aprofundar neles, pois para implementar a segurança da informação de forma correta, estes são fundamentais e precisam estar na ponta da língua!

VEJA A FÓRMULA ABAIXO:

$$R = \frac{(V \times A \times I) \times P\%}{M}$$

R = Risco;
V = Vulnerabilidade;
A = Ameaça;
I = Impacto;
P = Percentual de probabilidade;
M = Medidas de Segurança.

Imagine o seguinte cenário: Você possui um carro, possui um risco de prejuízo caso o mesmo seja furtado/roubado, então podemos ficar assim:

R = Prejuízo;

V = Exposição do veículo;

A = Roubo/Furto;

I = Determinado pelo valor do veículo;

P = Determinado pelo local onde o expõe;

M = Seguro (transferir o risco), blindagem (medidas técnicas), escolta (medias dissuasiva), alarmes, monitoração por satélite, não ter carro (evitar o risco), ou aceitar e correr o risco.

Entenda que em Segurança da Informação ocorre da mesma forma, se uma aplicação trata dados de Clientes e existe um risco de prejuízo para imagem em caso de vazamento, medidas devem ser tomadas. Agora faça um exercício mental aplicando a fórmula em outras situações do cotidiano!

É muito importante entender os tipos de resposta que podemos dar ao risco:

<u>Aceitar</u>: decidir aceitar e não faze nada;

<u>Evitar</u>: não ter ou não fazer algo que traga risco;

<u>Transferir</u>: Contratar um seguro, usar proteções (em eletrônica: fusíveis, estabilizadores etc;

<u>Mitigar</u>: Reduzir o risco através de diversas medidas até que o risco seja aceitável.

06

COMO CRIAR SENHAS MAIS SEGURAS

Parece um assunto simples, mas conhecer e saber orientar como criar senhas mais seguras de forma que você não esqueça é sim um desafio!

Com poder computacional de um processador high level atualmente, é possível quebrar senhas em segundos, por isso reservamos aqui algumas dicas fundamentais para criar senhas fortes e não esquece-las nunca mais!

Dica 1: Nunca use palavras simples mesmo que encadeadas, tipo “senhasegura”, neste caso levaria 24h para quebra-la por força bruta ou alguns segundos usando dicionário de senhas;

Dica 2: Use letras maiúsculas, minúsculas, símbolos e números. Você pode usar uma parte de sua canção preferida, usando somente as iniciais das letras de uma frase, por exemplo: “*Moro num país tropical, abençoado por Deus*”, ficaria: MnptApD!91

Dica 3: Cada sistema precisa ter uma senha única. Você pode adicionar duas ou três letras ao início ou ao final da senha, ficando assim para o Instagram: MnptApD!91ins

Segundo o site https://howsecureismypassword.net/ esta senha levaria 2 milhões de anos para ser quebrada com o poder de processamento atual!

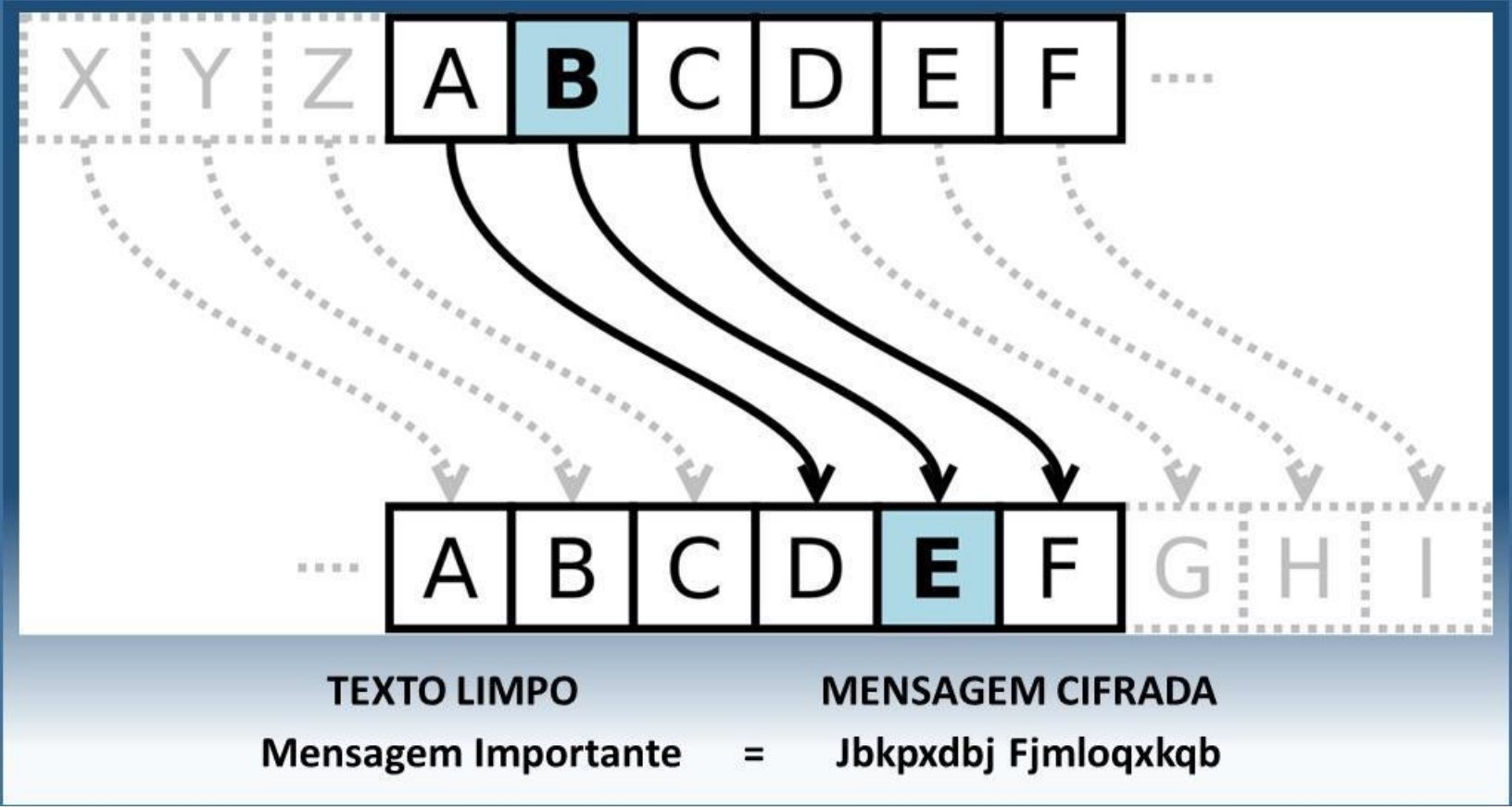
Corporativamente, existem softwares chamados Password Vault (cofre de senhas) onde senhas fortes para acessos administrativos são criadas e guardadas.

Você também pode ter um cofre de senhas, existem vários serviços muito conhecidos, gratuitos e confiáveis na internet, tais como: LastPass, KeePass, 2Password, OneLogin, Duo Security.

Mantenha-se sempre atualizado sobre possíveis eventos de vazamento de senhas dos sistemas que você usa.

07

PRINCÍPIOS DA CRIPTOGRAFIA



Vimos anteriormente que há uma referência no passado sobre criptografia: A Cifra de Cesar.

Ela tinha uma função bem simples, onde eram substituídos os caracteres por outros em 4 posições depois. A criptografia nada mais é que a aplicação de uma regra ou função matemática que fará com que o dado que pode ser lido ou acessado normalmente ficará ilegível para os que não possuem a "regra" ou melhor dizendo, a chave criptográfica.

Criptografia é a aplicação de uma função, exemplo *f(x) = x^2–3*x–7*, cada código ASCII de cada caractere passa pela função transformando-os em outros números.

Veja alguns termos importantes:

Algoritmo: Função matemática usada para criptografia;

Assimétrica: São duas diferentes chaves, uma para criptografar e outra para descriptografar;

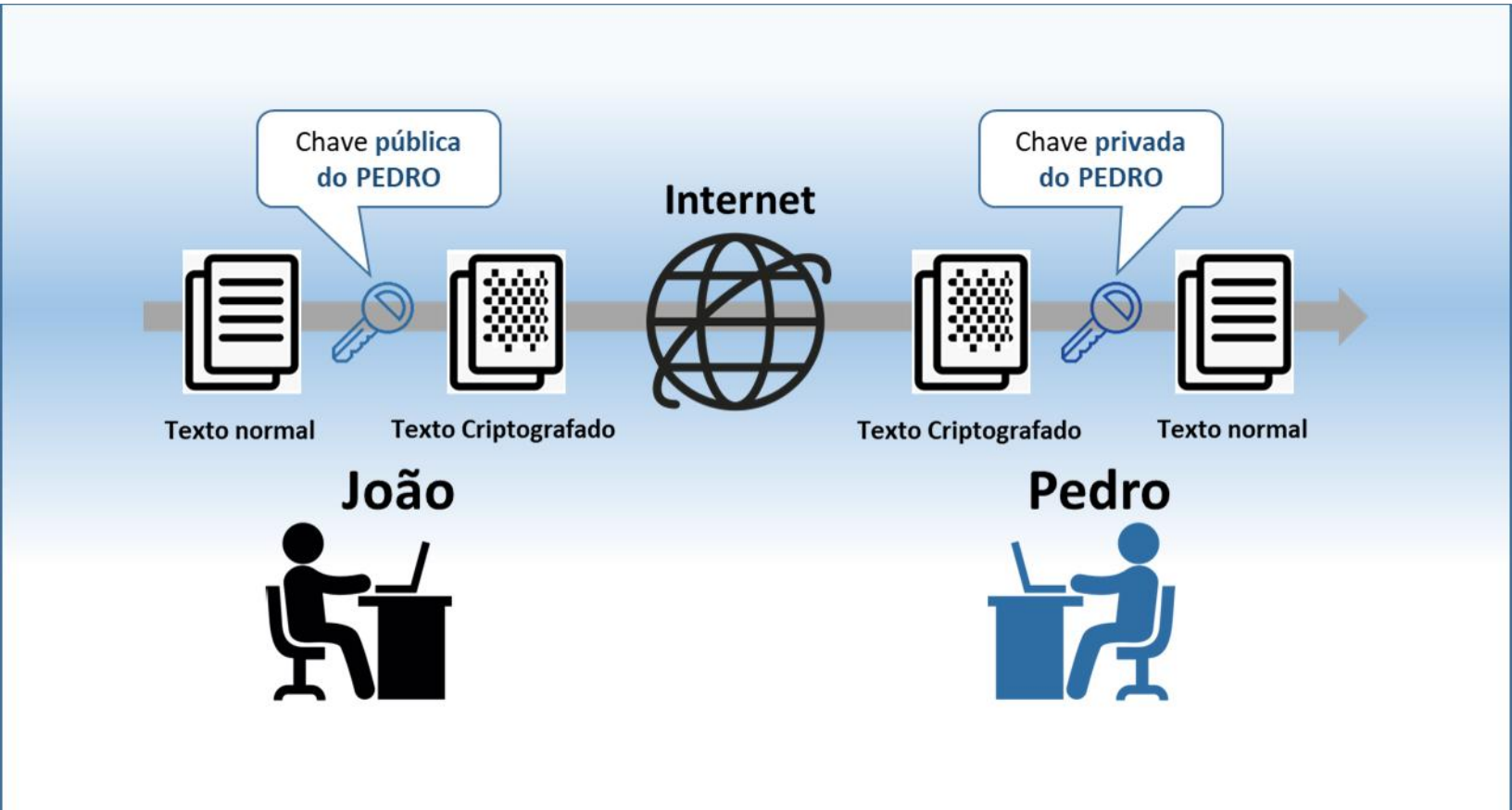
Certificado digital: documento eletrônico emitido por uma empresa certificadora, configurado nos sites HTTPS e que informa para o dispositivo que está acessando que o site é legítimo.

Hash: algoritmo ou função matemática que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo para referências. É utilizado para garantir que a informação não foi modificada na transmissão.

Chave pública: função usada para criptografar. Deve ser enviada a todos que lhe forem enviar documentos criptografados;

Chave Privada: função usada para descriptografia, guardada com a máxima segurança;

Chave única (criptografia simétrica): criptografia e descriptografia são feitos com a mesma chave, neste caso é muito perigoso, pois qualquer um que tiver a chave poderá ter acesso ao dado criptografado.



08

CONCEITOS DE REDE

Conheça e memorize bem o modelo OSI (Open System Interconnection).

Este modelo é abordado em várias certificações, além de lhe dar uma visão de como é a comunicação entre os sistemas que fazem uso da rede.

Tem sete camadas e cada uma representa uma fase na comunicação, com suas devidas características que podem ser exploradas tanto para o ataque, quanto para a defesa de uma rede de comunicações.

Camada	Protocolo	Ataque
7.Aplicação	HTTP, RTP, SMTP, FTP, SSH, Telnet, SIP, RDP, IRC, SNMP, NNTP, POP3, IMAP, BitTorrent, DNS	HTTP Flood, DNS Flood
6.Apresentação	XDR, TLS	SSL Abuse
5.Sessão	NetBIOS	Syn Flood, DDoS, ACK floods
4.Transporte	NetBEUI, TCP, UDP, SCTP, DCCP, RIP ...	Session Hijacking, Port scanning, TCP sequence number prediction
3.Rede	IP (IPv4, IPv6), IPsec, ICMP, ARP, RARP, NAT ...	ARP Spoofing, ARP cache poisoning, ICMP flood
2.Enlace	Subcamada MAC Ethernet, IEEE 802.1Q, HDLC, Token ring, FDDI, PPP, Switch, Frame relay, ATM	MAC Spoofing
1.Física	Cabos, Conectores, 802.11 Wi-Fi RDIS, RS-449, Bluetooth, USB, 10BASE-T, 100BASE-TX, ISDN, DSL	Man in the middle

Cada camada pode se explorada, por isso é necessário desenvolver controles que atendam as necessidades de proteção de toda a rede, estes só serão possíveis com o entendimento da função de cada uma destas camadas

Na imagem acima vemos uma breve referência ao modelo OSI juntamente com alguns protocolos na segunda coluna, bem como algumas modalidades de ataques que são utilizadas se referenciando a cada camada.

1. Física – Função de envio e recebimento de bits, através de um canal de comunicação.

2. Enlace – Fragmentação e transmissão física dos dados recebidos da camada de redes.

3. Rede – Faz entendimento sobre as conexões com outros sistemas computacionais, abertura e fechamento de conexões e já gerencia o congestionamento de redes.

4. Transporte – Gerencia a entrega e recebimento dos dados entre máquinas de envio e recebimento de dados.

5. Sessão – Responsável por iniciar, gerenciar e terminar a conexão entre os chamados hosts.

6. Camada de Apresentação – Formata e apresenta os dados.

7. Aplicação – Funções especializadas como transferência de arquivos, imagens, e-mails com o nosso entendimento e visualização.

A ARPAnet (Advanced Research Projects Agency Network) foi a primeira rede de computadores, construída em 1969 como um meio robusto para transmitir dados militares sigilosos e para interligar os departamentos de pesquisa por todo os Estados Unidos.

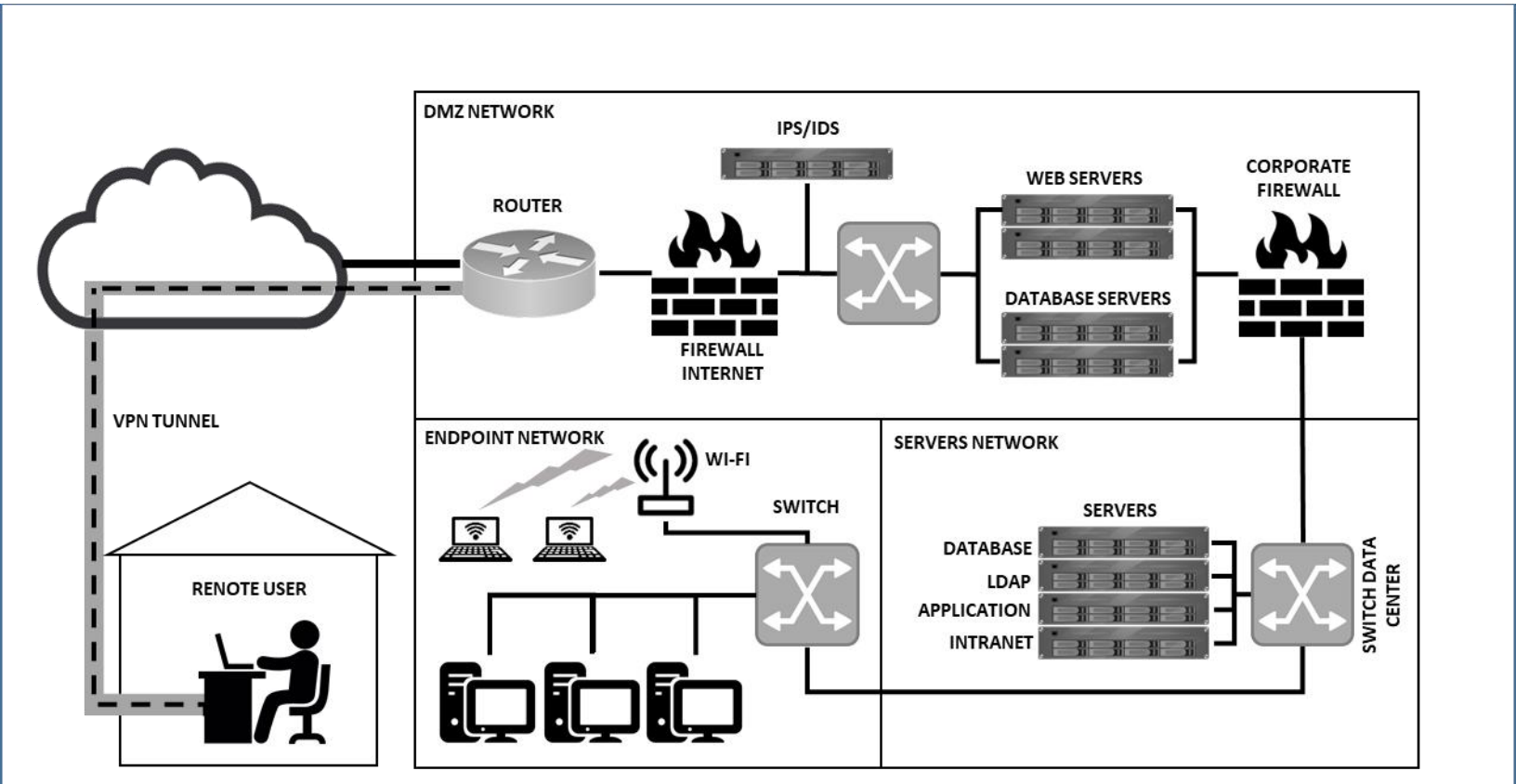
ARPAnet primeiro executou NCP (Network Control Protocol) e posteriormente a primeira versão do conjunto de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol).

A ARPAnet foi o inicio da Internet como conhecemos hoje.

Abaixo vemos um diagrama de rede com várias tecnologias comuns nas empresas. É fundamental que você conheça o conceito de cada um destes dispositivos.

DMZ: zona desmilitarizada ou rede de perímetro, é uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede;

ROUTER: roteador é responsável por encaminhar pacotes de dados entre redes de computadores. Atua nas camadas 2 e 3 do modelo OSI visto anteriormente.



FIREWALL: possui função básica de filtrar o tráfego nocivo recebido. Atua nas camadas 3, 4 e camada 7 atuando nesta como Next Gen Firewall e/ou Proxy;

PROXY: Função de conexão do computador corporativo (Internet), filtrando determinados assuntos bem como conteúdo malicioso;

WEB SERVER: provê serviços de paginas que podem ser acessadas tanto sem criptografia (http) como através de criptografia (https).

DATABASE SERVER: fornece armazenamento de forma relacional dos dados e informações que atendem as aplicações que são executadas nos servidores web.

LDAP: Lightweight Directory Access Protocol, normalmente um Microsoft Active Directory, este fornece um serviço de autenticação para os usuários da rede, contas de serviço, bem como armazena informações sobre os computadores e servidores da rede.

IDS/IPS: Intrusion Detection System e o Intrusion Prevention System são sistemas de detecção e prevenção a Intrusão através da análise dos pacotes através de regras e assinaturas.

WI-FI: é o nome conhecido para o padrão IEEE 802.11 que fornece comunicação via sinal de rádio usando as frequências de 2,4GHz e/ou 5GHz.

Encapsula a comunicação de forma criptografada podendo usar o padrão WPA Wi-Fi Protected Access de 256 bits.

09

SIGLAS FUNDAMENTAIS DE REDE

Nesta parte veremos as principais siglas de serviços de rede que você precisa conhecer.

RFC: Request for Comments são documentos técnicos desenvolvidos e mantidos pelo IETF (Internet Engineering Task Force), que especifica os padrões que serão implementados e utilizados em toda a internet.

Hackers estudam eles em busca de vulnerabilidades ou melhorias.

ARP: Address Resolution Protocol faz o mapeamento de endereço IP para endereço MAC;

LAN: Local Area Network – Rede local.

SFTP: Secure File Transfer Protocol, protocolo criptografado utilizado para a transferência de arquivos;

WAN: Wide Area Network redes que abrangem grandes localidades, frequentemente atribuída a interligação entre redes locais a provedores de acesso ou backbones;

BACKBONES: Redes de grandes operadoras que fornecem acesso a internet;

SNMP: Simple Network Management Protocol é utilizado para monitoração e gerência de rede, sendo compatível com vários tipos de dispositivos;

SMTP: Simple Mail Transfer Protocol pertence a camada de aplicação do correio eletrônico.

TCP: tranmission Control Protocol – está localizado na camada de transporte fazendo o controle da entrega do pacote de dados.

UDP: faz controle de fluxo, controle de erro e sequenciamento, mas não tem reconhecimento dos datagramas (ACK/NACK), ou seja, não controla a entrega de pacotes.

SOCKET: associação entre 2 processos (cliente/servidor) é identificada por um par (socket1, socket2), uma vez estabelecida uma conexão, cada socket corresponde a um ponto final dessa conexão.

DNS: Domain Name System responsável por descodificar os nomes dos domínios dos sites para endereços IP.

DHCP: Dynamic Host Configuration Protocol realiza a configuração automática de dispositivos ligados a uma rede entregando para eles dinamicamente IP, DNS, Gateway, além de outros parâmetros específicos;

IP: Internet Protocol, o principal protocolo de comunicação da Internet, responsável por endereçar e encaminhar pacotes que trafegam pela rede mundial de computadores.

NAT: Network Address Translation, método de remapear endereços IP modificando o mesmo. Utilizado para publicação de servidores na internet, trocando o IP interno para um IP externo (válido na internet);

MAC: Media Access Control, é o endereço físico e único de placas rede (LAN e WLAN). Na rede local, a comunicação ocorre por este endereço utilizando o ARP para identificação.

ICMP: Internet Control Message Protocol é utilizado para fornecer relatórios de erros à fonte original. Os comandos Ping, Tracert, traceroute utilizam este protocolo para comunicação, caso haja algum erro, ele retorna para o dispositivo que originou o comando ou a solicitação.

PORT: porta de comunicação é representada por um número de 1 à 47808 para servidores e de 49152 a 65535 para clientes. Uma porta cliente se conecta a uma porta servidor. Por exemplo o serviço https funciona na porta 443.

VPN: Virtual Private Network túnel criptografado (normalmente IPSec - IP Security Protocol) que encapsula a comunicação tornando-a segura entre um usuário remoto e outras redes.

10

COMANDOS BÁSICOS DO MICROSOFT WINDOWS PARA REDES

Nesta sessão veremos os comandos básicos de rede utilizados no Microsoft Windows, no entanto, muitos destes comandos são aplicáveis a diversos sistemas operacionais: Linux, Unix, AIX, FreeBSD, SunOS e outros. É importante que você conheça o conceito de cada um deles, pois caso o mesmo comando não exista em um outro sistema, existirá outro com a mesma função, sendo que os conceitos dos comandos também se aplicam a equipamentos como Firewall.

PING: testa a conexão com um IP remoto. Usa o protocolo ICMP e envia uma mensagem para um IP de destino e aguarda um retorno. Comando usado para teste de conectividade.

Traceroute: uma conexão passa por diversos caminhos e este comando mostra todos os endereços IP intermediários revelando o caminho percorrido pela comunicação.

Ipconfig: mostra e altera as configurações de rede de um dispositivo, em outros sistemas operacionais você pode usar o ifconfig.

Netstat: comando muito importante, mostra vários aspectos de rede, tais como, falhas, pacotes perdidos, conexões de rede ativas, status das conexões, portas de rede abertas e outros;

Route: um dispositivo possui uma tabela que informa os IPs dos gateways que fazem a ponte para outras redes. Este comando mostra essa tabela.

Arp: em uma rede local as estações se identificam primeiramente pelo IP e depois a comunicação segue via endereço MAC. Este comando mostra essa tabela de IPs relacionados aos MACs em uma rede local.

Telnet: permite a abertura de uma tela caractere, também chamado de terminal, para comandos em servidores com esse suporte. Não é mais utilizado para isso visto que a comunicação acontecia em texto limpo, visível a hackers, mais ainda é muito utilizado para testar portas TCP/IP que estão abertas.

Alguns exemplos de Portas utilizadas:

Protocolo	Porta
FTP (TCP)	21
TELNET (TCP)	23
SMTP (TCP)	25
DNS (TCP/UDP)	53
HTTP (TCP)	80
HTTPS (TCP)	443
MS AD (TCP)	445

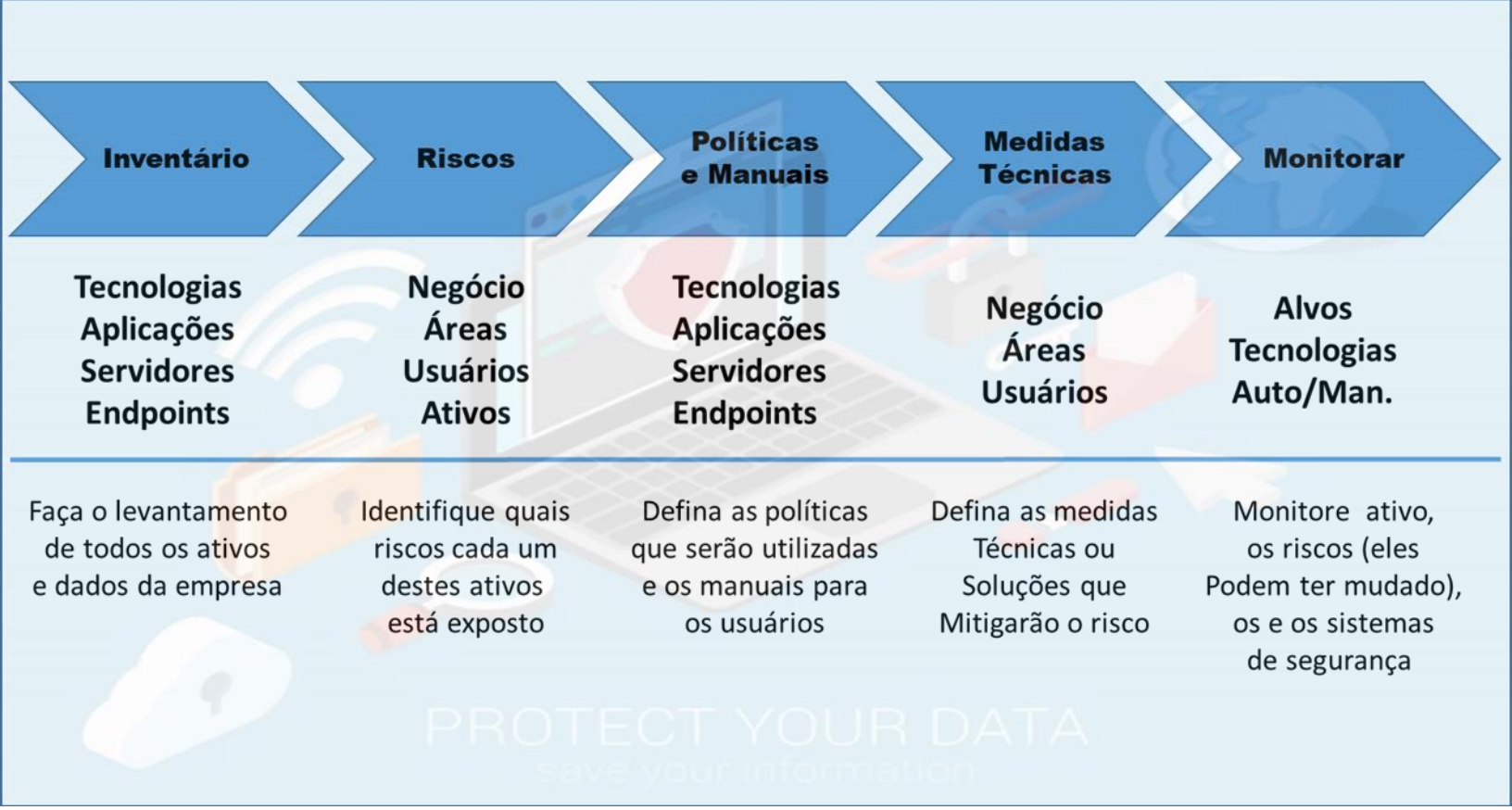
Provavelmente você usará muito este comando para verificar se uma porta de um serviço está aberta e se responde corretamente.

NsLookUp: todo o endereço (ex: www.google.com) é transformado em IP antes da conexão, quem faz este serviço é o servidor de DNS, este processo chama-se Resolução de Nomes. Você pode usar este comando para solicitar uma resolução de nomes de um endereço. No exemplo acima, o servidor chama-se "www" (hostname) e está no domínio "google.com". Se estiver em uma empresa, o nome e endereço de sua estação pode ser algo do tipo: "desktop1.empresa.local"

11

TECNOLOGIAS DE SEGURANÇA

Responda para você mesmo e veja se já conseguiu evoluir ao longo deste material: Como devo implementar segurança da informação? Se ainda não consegue responder com clareza, não tem problema. A seguir, colocamos uma imagem que fará toda a diferença neste entendimento e logo após falaremos de tecnologias mais utilizadas na atualidade para prover a camada tecnológica em segurança da informação.



<u>Inventário:</u> Primeiro – o que se quer proteger? A companhia ou mesmo você precisará saber exatamente o que proteger. Exemplo: Um servidor. Mas um servidor que roda o que? Windows Server 2019. Quais aplicações ele executará? Aplicações Web. Quem fará o acesso? Pessoas na internet;

<u>Riscos:</u> Cada um destes itens possui um risco, inclusive a companhia. Ex.: Windows Server – vulnerabilidades, falta de patches.

Aplicativo Web: acesso indevido, captura de tráfego (man-in-the-middle); Pessoas na internet – terem seus dados roubados, não ter a aplicação disponível quando precisar, preocupação com legislação;

Políticas e manuais: Política de limite do acesso administrativo, política de senhas seguras e troca de senhas, política de atualização dos aplicativos, manuais direcionados aos usuários externos e internos ou mesmo vídeos de como usar a aplicação; Política de sistemas mínimos de segurança, limite de acesso físico;

Medidas técnicas: antivírus, criptografia SHA-2, realização de vulnerability scan e application scan, uso de um WAF, uso de um Next Gen Firewall e uso das versões mais recentes de softwares, implementação de EDR, servidor em cluster, DLP;

Monitoração: Equipe de SOC, Uso de SIEM, desempenho/disponibilidade da aplicação.

VULNERABILITY SCAN: realiza varreduras de redes e dispositivos em busca de vulnerabilidades, opera com uma base de dados atualizável. Emite relatórios.

APPLICATION SCAN: Semelhante ao anterior, mas focado em aplicações web;

NEXT GEN FIREWALL: Firewall que verifica não só a socket, mas também o tipo de dado que está passando, identificando malwares;

WAF: Web Application Firewall: Aplicativo instalado no servidor, atua protegendo aplicações web, também analisando o tráfego

EDR: Endpoint Detection and response – Mais que um antivírus, ele monitora com base no comportamento, alertando o SOC ou tomando as ações de segurança programadas.

CLUSTER: conceito de dois ou mais dispositivos que atuam dividindo a carga de rede e processamento, bem como em casos em que um deles esteja indisponível;

SIEM: Security Information and Event Management) – coleta logs, correlaciona e faz o monitoramento e a análise em tempo real, podem fornecer pistas para os problemas existentes e também futuros bem antes de eles ocorrerem. Existe ainda as necessidades regulatórias (HIPAA, PCI DSS, SOX, GDPR e muitas outras) e que exigem que os Logs de Eventos sejam cuidadosamente monitorados e auditados.

DLP: Data Loss Prevention, prevenção de perda de dados, é utilizado para garantir que dados confidenciais não sejam perdidos, acessados por pessoas não autorizadas, roubados por usuários mal intencionados ou enviados para fora da empresa sem autorização. Monitora usuários e servidores.

SOC: Security Operations Center – equipe de profissionais de segurança que monitora a infra quanto a eventos de segurança bem como administra as ferramentas para tal.

12

ORIENTAÇÕES COM TRILHA DE CERTIFICAÇÕES

Bom, se você já se identificou com alguma área específica, nós organizamos aqui uma trilha que pode ser seguida para ampliar seus conhecimentos e lhe tornar um profissional de referência na área, munindo-o de conhecimento.

Mas a maior virtude de um profissional de segurança é a curiosidade e o auto estudo. As certificações serão boas para o seu currículo, mas na prática, é que você adquire o conhecimento especializado.

ARQUITETO DE SEGURANÇA

INICIANTE:

- Exin ITIL Fountation
- Exin Information Security Foundation/ISO27001
- CompTIA Security+

INTERMEDIÁRIO:

- Certified Ethical Hacker (CEH)

AVANÇADO:

- EC-Council Certified Security Analyst (ECSA)

EXPERT:

- Certified Information Systems Security Professional (CISSP)

CONSULTOR DE SEGURANÇA

INICIANTE:

- Exin ITIL Fountation
- Exin ISF/ISO27001
- Exin Ethical Hacker

INTERMEDIÁRIO:

- Cybersecurity Analyst (CySA+)

AVANÇADO:

- EC-Council Certified Security Analyst (ECSA);
- Certified Information Systems Auditor (CISA);

EXPERT:

Certified Information Systems Security Professional (CISSP)

HACKER ÉTICO

INICIANTE:

- CompTIA Security+
- Exin Ethical Hacker

INTERMEDIÁRIO:

Certified Ethical Hacker (CEH)

AVANÇADO:

- CompTIA Advanced Security Practitioner (CASP)
- EC-Council Certified Security Analyst (ECSA)

EXPERT:

- Certified Information Systems Security Professional (CISSP)

GESTOR DE SEGURANÇA (CISO)

INTERMEDIÁRIO:

- Exin ITIL Fountation
- Exin ISF/ISO27001
- Certified Information Systems Auditor (CISA)

AVANÇADO:

- Certified Information Security Manager (CISM)

EXPERT:

- Certified Information Systems Security Professional (CISSP)

DESENVOLVIMENTO SEGURO

INICIANTE

- EXIN Agile Scrum Foundation
- EXIN Secure Programming Foundation

INTERMEDIÁRIO:

- EXIN DevOps Professional

AVANÇADO:

- EXIN DevOps Master

EXPERT:

- Certified Secure Software Lifecycle Professional (CSSLP)

Aqui estão algumas sugestões de certificações com base no que o mercado tem pedido, no entanto, muitas vezes, a capacidade de auto estudo acaba determinando o sucesso do profissional.

13

SPAM E PHISHING

Phishing é o vetor de ameaça mais utilizado pelos Black Hats, é um misto de engenharia social com algumas tecnologias, seja ela web com páginas falsas ou emails, mensagens de whatsapp ou SMS, tudo com o propósito de roubar informações como número de documentos, contas bancárias, contas e senhas de acesso ou instalar um aplicativo malicioso. Existem várias técnicas, veremos algumas a seguir.

Blind Phishing: mais comum, ocorre via disparo de e-mails em massa, os criminosos contam com o despreparo dos destinatários. O e-mail tem algum link ou anexo malicioso.

Smishing: realizado por meio de disparos de SMS para celulares. Mensagens que induzem a vítima a tomar decisões imediatas, como dizer que ela está endividada ou ganhou um sorteio inesperado.

Clone Phishing: clona um site original para atrair os usuários fazendo-os fornecer informações como: cartões de crédito.

Spear Phishing: ataque direcionado a uma pessoa, muitas vezes contendo informações vazadas sobre a vítima.

Whaling: Em geral, mira empresários e executivos de cargos estratégicos para conseguir dados confidenciais.

SPAM: Essencialmente são mensagem em massa para venda ou marketing de algo.

Veja as características comuns:

“Imperdível! Descontos exclusivos neste Dia da Mães”;

“Seu nome está negativado. Saiba quando isso aconteceu”;

“Seu cadastro foi desativado. Clique aqui para atualizar seus dados”;

“Confirme as informações do seu pedido para recebê-lo em até 5 dias”;

“Você recebeu uma multa. Clique aqui para saber o valor”.

<u>AntiSpam:</u> Solução instalada antes do servidor de email com objetivo de filtrar esses emails indesejados, filtrando por IP, endereço de email, palavras, links e outras características programadas.

A ferramenta mais efetiva contra o phishing é o treinamento. O uso de soluções com campanhas simuladas de phishing tem se tornado uma prática em várias companhias, bem como o treinamento dos usuários mostrando os prejuízos que podem ter.

14

SITES E FERRAMENTAS ÚTEIS PARA SI

Nas próximas páginas compartilharemos com você ótimas dicas de:

- **Sites de informações de segurança;**
- **Repositórios de vulnerabilidades;**
- **Treinamentos gratuitos;**
- **Ferramentas online para segurança.**

- **Pesquise na Enciclopédia de segurança:**
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/

- **Teste a sua senha**
https://howsecureismypassword.net/

- **VPN Gratuita confiável – ProtonVPN**
https://protonvpn.com/

- **Análise de reputação de site ou IP**
https://www.brightcloud.com/tools/url-ip-lookup.php

- **Identifique a quem pertence um IP ou site:**
https://who.is/

- **Veja se uma URL é maliciosa:**
https://www.virustotal.com/

- **Todas as vulnerabilidades conhecidas:**

https://cve.mitre.org/

- **Cursos - análise de vulnerabilidade:**

https://university.tenable.com/partners/learn

- **Dezenas de ferramentas grátis**

https://www.sans.org/free

- **Vários treinamentos de Segurança:**

https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

Este material é o primeiro de alguns passos que, com certeza, te levarão ao sucesso profissional em Segurança da Informação se as informações e dicas aqui contidas forem seguidas com disciplina e aprofundamento!

Fique atento aos nossos canais nas redes sociais, pois estamos produzindo mais conteúdos para você!

Até o próximo!!!

Go Hard!!!