Síntese de conceitos fundamentais de segurança

CIA/AIC Tríade

- Confidencialidade: Informações só podem ser lidas por quem foi explicitamente autorizado;
- Integridade: Dados são armazenados e transferidos como desejados e que qualquer modificação não é autorizada;
- Disponibilidade: Informações estão prontamente acessíveis à quem pode acessá-las ou modifica-las;

Estrutura de segurança cibernética

- Identificar: Desenvolver políticas e recursos de segurança. Avalie riscos, ameaças e vulnerabilidades e recomende controles de segurança para mitigá-los.
- Proteger: adquirir/desenvolver, instalar, operar e desativar ativos de hardware e software de TI com segurança como requisito incorporado à cada etapa deste ciclo de vida de operações.
- Detectar: Realizar monitoramento contínuo para garantir que controles sejam eficazes e capazes de proteger contra novos tipos de ameaça.
- Responder: Identificar, analisar, conter e erradicar ameaças a sistemas de segurança e dados.
- Recuperar: Implementar resiliência à segurança cibernética para restaurar sistemas e dados se outros controles não conseguirem evitar ataques.

Estrutura de segurança cibernética

- Análise de lacunas: É um processo que identifica como os sistemas de segurança de uma organização se desviam daqueles exigidos ou recomendados por uma estrutura.
    - É realizada ao adotar uma nova estrutura pela primeira vez ou ao atender um novo requisito de conformidade legal.

Competências de Segurança da Informação

- Avaliar riscos e testes;
- Especificar, fornecer, instalar e configurar dispositivos de software seguros;
- Controlar acessos e privilégios do usuário;
- Auditar logs e eventos;
- Relatórios e respostas de incidentes;
- Continuidade de negócios e recuperação de desastres;
- Programas de treinamento e educação em segurança;

Controle de Acesso

- Identificação: Criar uma conta ou ID que represente exclusivamente um dispositivo ou processo na rede;
- Autenticação: Provar que uma entidade é quem ou o que afirma ser ao tentar acessar um recurso;

- Autorização: Determinar quais direitos as entidades devem ter para cada recurso e impor esses direitos;
- Contabilização: Monitorar o uso autorizado de um recurso ou o uso de direitos por uma entidade e alertar quando um uso ou tentativa não autorizada for detectado, para que o usuário não possa negar quer fez algum pedido;

Funções e responsabilidades de Segurança da Informação

- CISO/CSO: A responsabilidade interna geral pela segurança pode ser atribuída a um departamento dedicado, dirigido por um Diretor de segurança (CSO) ou Chief Information Security Officer (CISO);
- Gerentes: Podem ter responsabilidade por um domínio, como controle predial, TIC ou contabilidade;
- Equipe Técnica: Especializada e tem a responsabilidade de implementar, manter e monitorar a política. A segurança pode ser feita uma competência central de sistemas e administradores de rede, ou pode haver administradores de segurança dedicados, como Information Systems Security Officer (ISSO) por exemplo;
- Funcionários não técnicos: Têm a responsabilidade de cumprir a política e com qualquer legislação pertinente;
- A Responsabilidade externa pela segurança recai principalmente sobre os diretores ou proprietários, embora todos os funcionários compartilhem alguma medida da responsabilidade;

Unidades de negócios de Segurança da Informação

- Centro de Operações de Segurança (SOC)
    - Local onde profissionais monitoram e protegem ativos de informações críticas em outras funções de negócios como finanças, operações etc. Difíceis de financiar, são comuns em grandes empresas apenas. Através de SIEM.
- DevSecOps: Desenvolvimento, segurança e operações;
    - Conhecido como Shift Left, que significa que considerações de segurança precisam ser feitas durante as fases de requisitos e planejamentos ao invés de serem inxertadas apenas no final;
- Resposta a incidentes: As equipes atuam como único ponto de contato para notificação de incidentes de segurança. Essa função pode ser tratada pelo SOC ou ser estabelecida como uma unidade de negócios independentes.
    - Equipe de resposta a incidentes cibernéticos (CIRT)
    - Equipe de resposta a incidentes de segurança do computador (CSIRT);
    - Equipe de resposta a emergências do computador (CERT);

Controles de segurança

Controle de segurança: É projetado para oferecer as propriedades de confidencialidade, integridade, disponibilidade e não repúdio a um sistema ou ativo de dados.

- Técnico: O controle é implementado como um sistema (hardware, software ou firmware); Ex: Firewalls, Antivírus.
- Operacional: Controles que dependem de uma pessoa para implementação; Ex: Guardas de segurança e programas de treinamento.

- Gerencial: Controles que dão supervisão do sistema; Ex: Ferramentas que permita avaliação e controle de outros controles.
- Físico: Controles como alarmes, gateways, fechaduras, iluminações, câmeras de segurança que impedem e detectam acessos às instalações e ao hardware;

Tipos funcionais de controles de segurança:

- Preventivo: Restringe física ou logicamente o acesso não autorizado, opera antes de um ataque;
- Detectivo: Não pode impedir o acesso, mas identificará e gravará qualquer tentativa de intrusão bem-sucedida, opera durante um ataque;
- Corretivo: Responde e corrige um incidente e também pode evitar sua ocorrência, opera após um ataque;
- Diretivo: Impõe uma regra de comportamento como uma política, padrão de práticas recomendadas ou procedimento operacional padrão (SOP);
- Dissuasivo: Pode não impedir o acesso de forma física ou lógica, mas desencoraja psicologicamente um invasor de tentar uma invasão;
- Compensação: É um substituto para um controle principal, conforme recomendado por um padrão de segurança e oferece o mesmo nível de proteção (ou melhor), mas usa uma técnica diferente.

NIST Cybersecurity Framework

- Importância dos Frameworks:
  - Declaração objetiva dos recursos atuais;
  - Medição do progresso em direção a uma capacidade de destino;
  - Declaração verificável para relatórios de conformidade regulatória;

NIST:

- Estrutura de Segurança Cibernética (CSF);
- Estrutura de Gerenciamento de Riscos (RMF);
- Normas Federais de Processamento de Informações (FIPS)

- Publicações especiais;

ISO E Cloud Frameworks

International Organization for Standarization (ISO)

- Padrões de segurança da informação 27k;
- Gerenciamento de risco corporativo de 31k (ERM);

Cloud Security Alliance

- Orientação de segurança para provedores de serviços em nuvem (CSPs);
- Arquitetura de referência corporativa;
- Matriz de controle em nuvem;

Statements os Standards for Attestation Engagements (SSAE) Service Organization Control (SOC)

- SOC2 avalia prestador de serviços
    - Relatório tipo 1 avalia o design do sistema;
    - Relatório tipo 2 avalia eficácia contínua;
- Relatório de conformidade pública SOC3;

Benchmarks e Guias de Configuração Segura

Center for Internet Security (CIS)

- The 20 CIS Controls;
- CIS-RAM (Risk Assessment Method)

OS/network plataform/vendor-specific guides and benchmarks

- Vendor guides and templates;
- CIS Benchmarks;
- Department of Defense Cyber Exchange;
- NIST National Checklist Program (NCP);

Application servers and web server applications

- Client/server;
- Multi-tier-front-end, middleware (business logic), and back-end (data);
- Open Web Application Security Project (OWASP)

Regulamentos, Normas e Legislação

- Due Diligence
    - Sarbanes-Oxley Act (SOX);
    - Computer Security Act (1987);
    - Federal Information Security Management Act (FISMA);
- General Data Protection Regulation (GDPR)
- Leis nacionais, territoriais ou estaduais
    - Gramm-Leach-Biley Act (GLBA);
    - Health Insurance Portability and Accountability Act (HIPAA);

    - California Consumer Privacy and Act (CCPA);
- Payment Card Industry Data Security Standard (PCI DSS)

Atores de ameaça e vetores de ataque

Vulnerabilidade, ameaça e risco

Vulnerabilidade: Ponto fraco que pode ser acionado acidentalmente ou explorado de maneira intencional para causar uma violação de segurança. Ex: Hardwares e Softwares instalados incorretamente, desatualizados, uso de senha insegura, falhas de design em softwares ou sistemas operacionais. Fatores como valor do ativo vulnerável e a facilidade de exploração determinam a gravidade das vulnerabilidades.

Ameaça: Potencial de algo ou alguém explorar uma vulnerabilidade e violar a segurança. Pode ser intencional ou não intencional

- Autor ou agente de ameaças são quem causa;
- Caminho e ferramenta usados são chamados de vetor de ataque;

Risco: Nível de perigo representado por vulnerabilidades e ameaças.

Quando uma vulnerabilidade é identificada, o risco é calculado com base na probabilidade de ser explorada e no impacto causado.

Atributos dos Atores de Ameaça

- Ameaças conhecidas contra comportamentos adversários;
- Interno/externo;
- Intenção/motivação
    - Maliciosamente direcionado versus oportunista;
    - Acidental/Não intencional;
- Nível de sofisticação: É a capacidade de um autor de usar técnicas avançadas de exploração;
    - Recursos/Financiamento: Grupos de autores de ameaças precisam de recursos para adquirir ferramentas e mão de obra qualificada. Os mais capazes, recebem financiamento de estados-nação e do crime organizado;
    - Níveis de capacidade do adversário;

Motivações dos Autores de Ameaça

- **Interrupção do serviço**: Impede que uma organização funcione normalmente. Pode envolver ataque à website ou utilização de malware para bloquear acesso à servidores e estações de trabalho de funcionários. DDOS ou cobrar resgate via chantagem.
- **Exfiltração de dados:** Transfere uma cópia de um arquivo ou dado valioso de um computador ou rede sem autorização;

- **Desinformação:** Falsificar websites, manipular mecanismos de pesquisa para injetar sites falsos ou usar bots para publicar fakes em redes sociais.

Hackers, Script Kiddies e Hacktivistas

- **O Hacker Solitário**
  - White hats vs black hats vs grey hats;
  - Autorizados vs não autorizados vs semi-autorizado;
- **Script Kiddies:** Alguém que usa ferramentas hackers sem necessariamente entender como funciona. Geralmente não tem alvo/objetivo específico.
- **Equipes de hackers e hacktivistas: Anonymus, WikiLeaks, Luizsec.**

Hacker: Tem habilidades necessárias para conseguir acesso a sistemas de computador por meios não autorizados ou não aprovados.

Os termos não autorizado e não aprovados (ex black e White) são usados para distinguir a motivação.

White sempre busca autorização para realizar pentest em sistemas privados

Atores estatais e ameaças persistentes avançadas

- **APT: Advanced Persisted Threat**
  - Refere-se à capacidade contínua de um adversário de comprometer a segurança da rede para obter e manter o acesso usando várias ferramentas e técnicas;
  - Atores estatais vem sendo observados como responsáveis por diversos ataques, com o objetivo de espionagem e vantagem estratégica;

Sindicatos e Competidores Criminosos

- **Sindicatos:**
  - Operar em todas as jurisdições legais;
  - Motivado pelo lucro criminal;
  - Podem ser muito bem financiados e ter muitos recursos;
- **Concorrentes:**
  - Espionagem cibernética;
  - Combine com a ameaça interna;

Atores de Ameaças Internas

- **Ameaça Interna Maliciosa:**
  - Tem ou teve acesso autorizado;
  - Empregados, empreiteiros, sócios;
  - Sabotagem, ganho financeiro, vantagem nos negócios;
- **Ameaça Interna Não Intencional:**
  - Políticas e procedimentos fracos;
  - Baixa adesão às políticas e procedimentos;
  - Falta de treinamento/conscientização de segurança;
  - Shadow IT (Existe, mas não se sabe que existe) Ex: Políticas não configuradas 100% nas máquinas;

Superfície de Ataques e Vetores

- **Superfície de ataque:** Pontos onde um invasor pode descobrir/explorar vulnerabilidades em uma rede ou aplicativo, local ou método;
    - Minimizar essa superfície envolve restringir o acesso de modo que apenas endpoints, protocolos/portas, serviços e métodos conhecidos sejam permitidos, todos sendo monitorados para caso haja invasão;
- **Vetores:**
    - **Acesso direto**: Ataque físico ou local (estação de trabalho desbloqueada);
    - **Mídia removível**: Malware em pen drive ou cartão de memória;
    - **Email**: Anexo de arquivo malicioso via email;
    - **Remoto e sem fio**; Obtem credenciais para acessar a rede remotamente ou quebra protocolos de segurança usados para autenticação;
    - **Cadeia de suprimentos**: Ataca fornecedores ao invés de atacar diretamente a empresa;
    - **Web e mídias sociais**: Esconde malwares em arquivos anexados a pastagens ou apresentados como downloads via site ou mídias sociais;
    - **Nuvem**: Obter credenciais para acessar serviços de rede diretamente no fornecedor;
    - **Rede Bluethooth**: Transmitir arquivo malicioso via bluethooth se aproveitando de vulnerabilidade;

Fontes de Pesquisas de Ameaças

- **Fontes de pesquisas de ameaças:** Esforço de coleta da contrainteligência no qual empresas de segurança e pesquisadores tentam descobrir as táticas, técnicas e procedimentos de atacantes cibernéticos modernos;
    - Pesquisa Acadêmica;
    - Análise de ataques a equipamentos de clientes;
    - Honey Pots/Honey Nets;
    - Dark Nets e Dark Web;
        - **Dark Net:** É uma rede estabelecida como uma sobreposição à infraestrutura da internet por software, como o TOR, FreeNet ou I2P que agem para anonimizar o uso e impedir que um terceiro saiba sobre a existência da rede ou analise a atividade.
        - **Dark Web:** Sites, conteúdos e serviços acessíveis apenas através de uma dark-net. Embora existam mecanismos de pesquisa na dark web, muitos sites estão escondidos e seus endereços são divulgados apenas por quadros de aviso boca à boca;
        - **(Dark Net → Rede privada e anônima.**
        - **Dark Web → Conteúdo dentro da Dark Net.)**
    - **Outras fontes de ameaças:**
        - **Pesquisas de ameaças comportamentais:** Comentário narrativo que descreve exemplos de ataques e TTPs coletados por meio de fontes primárias de pesquisas;
        - **Inteligência de ameaças a reputação:** Listas de endereços IP e domínios associados a comportamento malicioso, além de assinaturas de malware conhecido baseado em arquivo.
        - **Dados de ameaça:** Dados do computador que podem correlacionar eventos observados nas próprias redes e registros

do cliente com TTP conhecidos e indicadores de agentes de ameaça; Ex: Virustotal.com

- Esses dados de ameaças podem ser empacotados como feeds que se integram ao SIEM;
- Esses feeds são descritos como Dados de Inteligência de Ameaças Cibernéticas(CTI). Eles por si só não são a solução, porém alinhados à recursos de IA do SIEM, são correlacionados com dados importantes observados da rede do cliente;

Feeds de Ameaça:

- **Fechado/Proprietário:** Pesquisa de ameaças e dados CTI são disponibilizados via assinatura de uma plataforma de inteligência de ameaças comerciais. Provedor de ferramentas de segurança também disponibilizará informações de ataques primeiro aos assinantes dessas plataformas;
  - **Exemplos são: IBM X-Force Exchange, FireEye;**
- **Sites de fornecedores:** Nem sempre a inteligência de ameaças proprietária tem custos, em sites de fornecedores de segurança, hardware e software, enormes quantidades de pesquisa de ameaças são disponibilizadas de graça;
  - **Ex: Blog Security Intelligence da Microsoft;**
- **Centros de compartilhamento de informações públicos/privados:** ISACs (Information Sharing Analysis Centers que foram criados para compartilhas informações sobre ameaças e promover melhores práticas;
- **Inteligência de Código Aberto (OSINT):** Algumas empresas operam serviços de inteligência de ameaças em uma base de código aberto, recebendo por consultoria ao invés de cobrar a plataforma;

Outras Fontes:

- **Revistas acadêmicas;**
- **Conferências;**
- **Solicitação de comentários (RFC):** Novas tecnologias são publicadas como RFC pelo W3C, além de outros RFCS cobrindo considerações sobre outras pesquisas;
- **Mídias Sociais;**

-TTPS e IOCs:

Táticas Técnicas e Procedimentos (TTPs): Declaração Generalizada de comportamento adversário;

- Estratégia e abordagem da campanha (Táticas);
- Vetores de ataques generalizados (Técnicas);
  Ferramentas e métodos específicos de Intrusão (Procedimentos);

Indicador de comprometimento (IOC): Sinal residual de que um ativo ou rede foi atacado

- Evidências específicas de intrusão;
- Pontos de dados individuais;
- Correlação de dados de sistemas e ameaças;

- Análise apoiada por IA;
- Indicador de ataque (IOA);
- Exemplos de IOCs:
    - Softwares e arquivos não autorizados;
    - E-mails suspeitos;
    - Alterações suspeitas do registro e do sistema de arquivos;
    - Uso desconhecido de porta e protocolo;
    - Uso excessivo de largura de banda;
    - Interrupção de serviço;
    - Uso de conta suspeito ou não autorizado;
        - Ias são utilizadas pois detectar esses IOCs e conectar com outros sinais de ataques pode levar muito tempo dos analistas, além de falsos positivos;

Feeds: Quando se usa plataformas de Inteligência de ameaças cibernéticas (CTI), se recebe um feed de dados de ameaças, essas informações podem ser combinadas com eventos da sua própria rede e então uma plataforma de análise realiza a correlação para detectar se algum IOC está presente. Existem várias maneiras que um feed de dados pode ser implementado, como:

- **Structured Threat Information eXpression (STIX):** Descreve terminologia padrão padrão para IOCs e formas de indicar relações entre eles; (Sintaxe, como isso é escrito)
- **Trusted Automed eXchange of Indicator Information (TAXII):** Fornece um meio para transmitir dados CTI entre servidores e clientes; (protocolo para transmissão de feeds) (Angélica)

Automated Indicator Sharing (AIS): É um serviço oferecido pelo Departamento de Segurança Interna (DHS) para que as empresas participem do compartilhamento de inteligência de ameaças; (Especialmente voltado para ISACs, mas empresas privadas também podem aderir.

Threat Maps: Mapas animados que mostram a origem, o alvo e o tipo de ataques detectados por uma plataforma CTI. Provedores de soluções de segurança publicam esses mapas mostrando ataques globais aos sistemas de seus clientes;

File/Code Repositories: Repositório de arquivos/códigos como o virustotal.com que contém assinaturas de códigos malware conhecidos;

BugBounty: Recompensas por achar bugs e brechas em empresas que disponibilizam URLs pra isso.

Algoritmos criptográficos

Criptografia significa “escrita secreta”, é tornar as informações seguras codificando-as. Somente quem detém a chave ou que sabe como decodificar, pode acessar a informação. Garantem confidencialidade., apenas.

Conceitos criptográficos:

- **Texto simples ou cleartext:** É uma mensagem não criptografada.
- **Texto Cifrado:** É uma mensagem criptografada.
- **Algoritmo ou cifra:** Processo usado para criptografar ou descriptografar uma mensagem.
- **Criptoanálise:** É a arte de decifrar sistemas criptográficos.

Criptografia Simétrica (Uma chave): Usar uma chave com cifra garante que a descriptografia só possa ser realizada por uma pessoa autorizada. Esse tipo de criptografia é muito rápida e geralmente usada para criptografia em massa de grandes quantidades de dados. O grande problema é: Como essa chave será transmitida?

Algoritmos de substituição e transposição:

- **Substituição:** Ex: ROT13, em que as letras são alternadas em 13 posições do alfabeto, com "A" se tornando "N".
- **Transposição:** A ordem é alternada, com as letras sendo escritas como colunas e depois são concatenadas. Ex: H L O O L
  E L W R D

Criptografia Assimétrica (Duas Chaves): Possui um par de chaves, uma pública e uma privada, ambas diferentes entre si. A chave pública é usada para criptografar e a privada para descriptografar. Ambas são geradas de forma que seja impossível extrair a chave privada a partir da pública.

HASH: Garante Integridade. Um algoritmo de hash produz uma cadeia de bits de tamanho fixo a partir de um texto simples de entrada, que pode ser de qualquer tamanho. A saída é o chamado HASH. Essa função é projetada para que seja impossível descobrir o texto à partir do HASH e para que dois textos diferentes dificilmente possam gerar o mesmo HASH, embora há uma chance remota de que isso aconteça.

Duas implementações populares de hash são:

Secure HASH Algorithm (SHA): Considerado o mais forte, existem variantes que produzem saídas diferentes, com resumos mais longos e considerados mais seguros. A variante mais popular é a SHA256, que produz um resumo de 256 bits.

Message Digest Algorithm #5 (MD5): Produz um resumo de 128 bits. Não é considerado tão seguro quanto o SHA256, mas pode ser necessário para a compatibilidade entre os produtos de segurança.

Infraestrutura de chave pública

Public Key Infraestructure (PKI): É a infraestrutura que ajuda a estabelecer a confiança no uso da criptografia de chave pública para assinar e criptografar mensagens por meio de certificados digitais. Um certificado digital é uma afirmação pública de identidade, validada por uma entidade de certificação (CA).

Autoridades Certificadoras: A PKI visa comprovar que os proprietários de chaves públicas são quem eles dizem ser. De acordo com a PKI, todo mundo que emitir uma chave pública deve publicá-la em um certificado digital, que tem sua validade garantida pelas CAs. A PKI pode usar CAs privadas ou de terceiros. Uma CA privada pode ser configurada dentro de uma organização para comunicações internas. Para comunicações públicas ou entre empresas, uma CA de terceiros pode ser usada para estabelecer uma relação de confiança entre servidores e clientes. Ex de CAs de terceiros: Comodo, DIgiCert, GeoTrust, IdenTrust e Let's Encrypt.

Certificados Autoassinados: Já que o uso de PKIs pode ser caro as vezes, Certificados Autoassinados servem para aplicações internas e ambientes de desenvolvimento e homologação. Pode ser aplicado em máquinas, servidores web ou códigos de programa. Os sistemas operacionais e navegadores notificam, mas isso pode ser ignorado. Porém, não é aconselhado usar esse tipo de certificados em aplicações críticas.

Revogação de certificados:

- Um certificado revogado por uma CA, não é mais válido e não pode mais ser des-revogado;
- Um certificado suspenso pode ser reativado;
- CAs devem manter uma lista de certificados revogados (CRL) contendo todos os certificados revogados ou suspensos;

Soluções criptográficas

Criptografia em apoio à confidencialidade: Ao implantar um sistema criptográfico para proteger os ativos de dados, deve-se considerar todas as maneiras pelas quais as informações podem ser potencialmente interceptadas. Os dados podem ser descritos em 3 estados:

- **Dados em Repouso:** É quando os dados estão em algum tipo de mídia de armazenamento persistente;
- **Dados em trânsito:** É o estado em que os dados são transmitidos por uma rede;
- **Dados em uso:** É o estado em que os dados estão presentes em uma memória volátil como registros e cache de RAM e CPU do sistema.

Criptografia de transporte e troca de chaves: A criptografia de transporte/comunicação protege os dados em movimento. Vários produtos de criptografia de transporte foram desenvolvidos para diferentes soluções de rede.

- **Wi-Fi Protected Access (WPA):** O acesso ao Wi-Fi protegido protege o tráfego enviado por uma rede wireless;
- **Internet Protocol Security (IPsec):** O protocolo de segurança IP protege o tráfego enviado entre dois pontos de extremidade por meio de uma rede de transporte púbica ou não confiável. Isto é chamado de rede virtual privada (VPN);
- **Transport Layern Security (TLS):** A segurança de camada de transporte protege os dados da aplicação, como dados da Web ou de e-mail, enviados por meio de uma rede pública ou não confiável;

SALT: É um valor aleatório que é usado junto da senha na hora da criação do HASH, o tornando ainda mais imprevisível e diferente.

(SALT + Senha) X SHA = HASH

Ofuscação: É a arte de tornar uma mensagem ou dados difíceis de encontrar. Trata-se de segurança por obscuridade, que é uma técnica obsoleta. No entanto existem algumas aplicações para tecnologias de ofuscação:

- Esteganografia: Incorpora informações em uma fonte inesperada, como mensagem ou imagem. Um arquivo que detém essas informações é chamado de cover text.
- Mascaramento de Dados: Pode significar a ocultação de parte ou de todo o contéudo de um campo de banco de dados, substituindo todas as sequencias de caracteres por \”x\” por exemplo
- Tokenização: Significa a substituição de todo o valor de um campo de banco de dados ou de parte dele por um token gerado aleatoriamente.

Implementar o gerenciamento de identidade e acesso

Autenticação

Autenticação: É realizada quando um solicitante ou requerente apresenta credenciais a um servidor de autenticação. O servidor compara o que foi apresentado com a cópia das credenciais armazenadas. Se corresponderem, a conta será autenticada.

Design em autenticação:

- **Confidencialidade:** Em termos de autenticação, é essencial. Pois se os dados de autenticação vazarem, os autores de ameaças podem se passar pelo titular da conta e agir com os direitos que isto tiver;
- **Integridade:** Refere-se à confiabilidade do mecanismo de autenticação e se é difícil que autores de ameaça o contornem;
- **Disponibilidade:** Significa que o tempo necessário para autenticar não prejudica os fluxos de trabalho e é fácil o suficiente para os usuários operarem.

Fatores de autenticação: O mais antigo, é algo que você sabe, como por ex **Personal Identification Number (PIN):** Algo que você sabe.

Conceitos de senha:

O gerenciamento inadequado de senhas continua sendo um dos maiores vetores de ataque para empresas. Se uma organização for depender de credenciais baseadas em senha, seu uso preciso ser regido por políticas e treinamentos sólidos.

Uma política de melhores práticas de senha instrui os usuários sobre a escolha e manutenção de senhas.

Para complementar isso, políticas impostas pelo sistema podem ajudar a reforçar os princípios do gerenciamento de credenciais e estipular requisitos para senhas determinadas por usuários.

Principais Conceitos:

- Comprimento da senha: Impõe um comprimento mínimo para senhas. Pode haver um máximo;
- Complexidade: Impões regras de complexidade, como não pode incluir nome do usuário na senha, conter maiúsculas, minúsculas, caracteres especiais e etc.
- Idade da senha: Reforça que a senha seja trocada após um número definido de dias;
- Reutilização de senhas e histórico: Não permitir que senhas usadas anteriormente sejam repetidas no futuro; O atributo de histórico define quantas senhas antigas são bloqueadas;

Autenticação Multifator (MFA): Combina o uso de mais um tipo de fator, como por ex: Senha + token de acesso recebido via e-mail ou sms.

- **Fator algo que você tem:** É um fator de propriedade. Isso significa que o titular da conta possui algo que ninguém mais possui, como Smartcard, Smartphone que pode receber um código ou gerar token criptográfico;
- **Fator algo que você é:** Fator biométrico ou inerente. Usa fatores biológicos, como impressão digital, reconhecimento facial, etc.
- **Fator algum lugar que você está:** Sistema aplica um fator baseado em localização a uma decisão de autenticação. Pode ser usando localização geográfica do dispositivo ou seu endereço de rede do Protocolo IP, a rede Wi-Fi, a LAN Virtual.

Taxa de Rejeição Falsa (FRR): É quando um usuário legitimo não é reconhecido. Também chamado de TIPO I ou Taxa de não correspondência falsa (FNMR). A FRR é medida em porcentagem.

Taxa de Aceitação Falsa (FAR): É quando um intruso é aceito (Erro tipo II ou taxa de correspondência falsa (FMR). A FAR é medida em porcentagem.

Taxa de Erro de Cruzamento (CER): O ponto em que a FRR e a FAR se encontram. Quanto mais baixo o CER, mais eficiente e confiável é a tecnologia.

Taxa de Transferência (velocidade): É o tempo necessário para criar um modelo para cada usuário e o tempo necessário para se autenticar.

Taxa de Falha no Registro (FER): São incidentes nos quais não é possível criar e relacionar um modelo à um usuário durante o registro. Qualidade/custo dos sensores.

Tokens de Autenticação Físicos: Fator de propriedade. Autenticador é capaz de gerar ou receber um token que identifica e autentica o usuário.

- **Autenticação baseada em certificado:** É quando o requerente controla uma chave privada que pode gerar um token assinado exclusivo. Provedor pode verificar a assinatura por meio de chave pública.
- **Senha de Uso Único (OTP):** É quando um token é gerado usando uma função HASH em um valor de segredo compartilhado, além de uma semente de sincronização, como uma marca de Data/Hora (TOTP) ou um HMAC (HOTP). O token só pode ser usado uma vez.
- **Fast Identity Online (FIDO) Universal 2nd Factor (U2F):** Usa um par de chaves pública/privada para registrar cada conta, evitando a necessidade de comunicar um segredo compartilhado, que é o ponto fraco do HOTP e do TOTP. A chave privada fica protegida no dispositivo U2F e assina o token. A chave pública é registrada no servidor de autenticação e verifica o token. Como não há certificados, não depende da PKI.
  (TOTP é por quanto tempo o token é válido)

Autorização

Autorização é a parte do gerenciamento de identidade e acesso que rege a distribuição de privilégios a usuários e serviços da rede. Um modelo de controle de acesso ajuda as organizações a gerenciar as implicações das atribuições de privilégios.

Controle de Acesso Discricionário: O DAC baseia-se na primazia do proprietário do recurso. Em um modelo DAC, cada recurso tem um proprietário, que tem controle total sobre o recurso e pode modificar sua lista de controle de acesso (ACL) para conceder direitos a terceiros.

Controle de Acesso Obrigatório: O modelo MAC expõe informações à ameaça de comprometimento através das contas de proprietários privilegiados. O controle de acesso obrigatório (MAC) baseia-se em níveis de autorização de segurança.

Controle de Acesso baseado em Função: No RBAC a organização define seus requisitos de permissão com base nas tarefas que um funcionário ou serviço deve ser capaz de executar. Cada conjunto de permissões é uma nova função e usuário ou conta de serviço é alocada em uma ou mais funções.

- Torna mais fácil distribuir privilégios em empresas grandes, pois aloca funcionários em poucos grupos, repassando os privilégios de um pro outro.

Controle de Acesso Baseado em Atributos: O ABAC é o tipo mais refinado do modelo de controle de acesso. Ele toma decisões com base em uma combinação de atributos de indivíduo e objeto, além de quaisquer atributos de sistema ou sensíveis ao contexto. Além da associação a grupos/função, esses atributos podem incluir informações sobre o sistema operacional, endereço IP ou presença de patches atualizados e antimalware.

Ex: Cada conta de serviço de cada servidor diferente, deve alertar o SIEM caso tente logar em um sistema que não é o dele.

Atribuições de privilégio mínimo: Significa que uma entidade principal recebe o mínimo possível de direitos, somente para concluir uma tarefa que está autorizada a executar.

Provisionamento: É o processo de configuração de um serviço de acordo com um procedimento padrão ou lista de práticas recomendadas.

Desprovisionamento: É o processo de remoção dos direitos de acesso e permissão alocados a um funcionário, quando ele deixa a empresa, ou de um terceirizado, quando o projeto é concluído.

Restrições de conta:

- **Política baseada em localização:** Sistema aplica um fator baseado em localização a uma decisão de autenticação. Pode ser usando localização geográfica do dispositivo ou seu endereço de rede do Protocolo IP, a rede Wi-Fi, a LAN Virtual ou unidade organizacional.
- **Localização Geográfica:** Por endereço IP ou Serviços de Localização(GPS)
- **Restrições Temporais: Restrições de acordo com a hora do dia**, **Política de Login baseada na duração**(tempo máximo que uma conta pode ficar logada), **Política de tempo de viagem impossível**(Utilizando a localização dos eventos de login durante o tempo), **Política de Permissões** temporárias(remove uma conta após um período).

Gestão de Acesso Privilegiado (PAM): Refere-se à políticas, procedimentos e controles técnicos para evitar que contas privilegiadas sejam comprometidas. Eles identificam e documentam contas privilegiadas, dando visibilidade ao seu uso, além de gerenciar as credenciais usadas para acessá-las.

Gestão de Identidade

Autenticação Local:

- **No Windows(LSASS:** É o Local Security Authority Subsystem Service que compara a credencial enviada à um hash armazenado no banco de dados do Security Accounts Manager (SAM), que faz parte do registro.

Entrada na rede do Windows: É o LSASS que pode passar as credenciais de autenticação a um controlador de domínio do Active Directory (AD). O sistema padrão para autenticação de rede é baseado no Kerberos, mas aplicativos Legados podem usar autenticação NT LAN Manager (NTLM)**.**

Autenticação Remota:

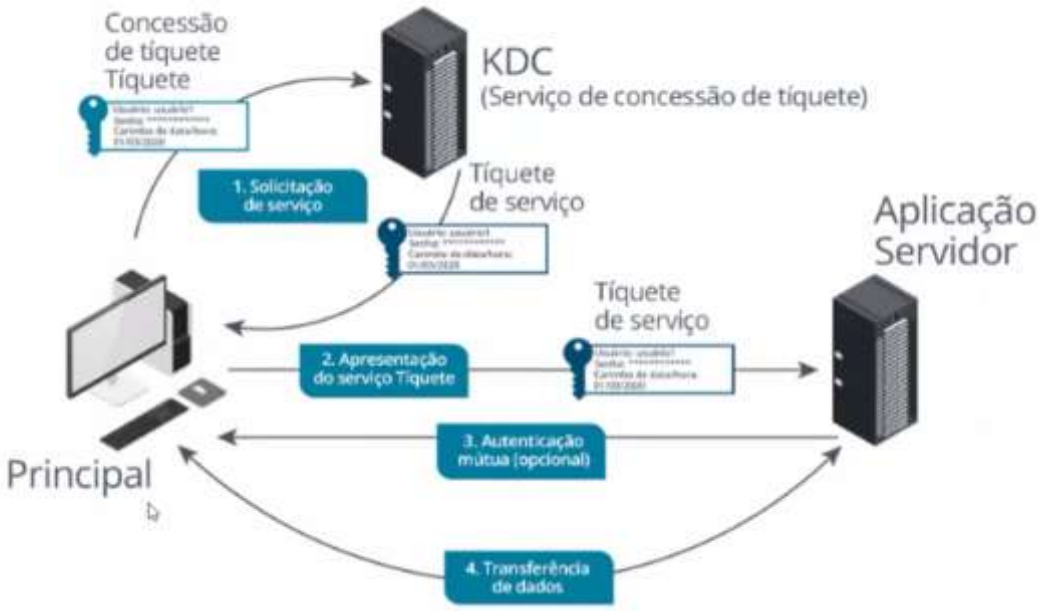
- **No Windows:** Se o dispositivo do usuário não estiver conectado diretamente à rede local, a autenticação poderá acontecer em uma VPN, Wi-Fi Corporativo ou portal web. Eles usam protocolos para criar uma conexão segura entre a máquina do cliente, o dispositivo de acesso remoto e o servidor de autenticação.
- **No Linux:** Os nomes das contas do usuário local são armazenados em /etc/passwd. Quando um usuário faz login em um shell interativo local, a senha é contastrada com um HASH armazenado em /etc/shadow.

Geralmente, o login interativo em uma rede é feito usando o Secure Shell (SSH) e com o SSH o usuário pode fazer o login usando chaves criptográficas ao invés de uma senha.

Serviços de Diretório: Armazena informações sobre usuários, computadores, grupos/funções de segurança e serviços. Cada objeto no sistema possui uma série de atributos. O esquema de diretório descreve os tipos de atributos, as informações que eles contem e se eles são opcionais ou necessários. Para que produtos de diferentes fornecedores sejam interoperáveis, a maioria dos serviços de diretório baseia-se no Lightweight Directory Access Control (LDAP).

Autenticação de Login Único:

- **Single Sign-On (SSO):** Permite que o usuário se autentique uma vez e em seguida receba autorizações em servidores de aplicativos compatíveis, sem precisar se autenticar novamente.
- **Kerberos:** É um protocolo de autenticação e autorização de rede de login único usado em muitas redes, com destaque para a sua implementação pelo serviço Active Directory (AD) da Microsoft.
- **Key Distribution Center (KDC):** Para comprovar suas identidades. Dois serviços compõem um KDC, o serviço de autenticação e o serviço de concessão de tíquetes.



Federação: É a noção de que uma rede precisa estar acessível a mais pessoas do que apenas a um grupo determinado de funcionários. Significa que uma empresa confia em contas criadas e gerenciadas por uma rede diferente. Como fazer login em outros sites via Google ou Linkedin.

Proteger a arquitetura de rede corporativa

Conceito de arquitetura e infraestrutura:

- Arquitetura de rede significa a seleção e posicionamento de meios, dispositivos e protocolos/serviços e ativos de dados;

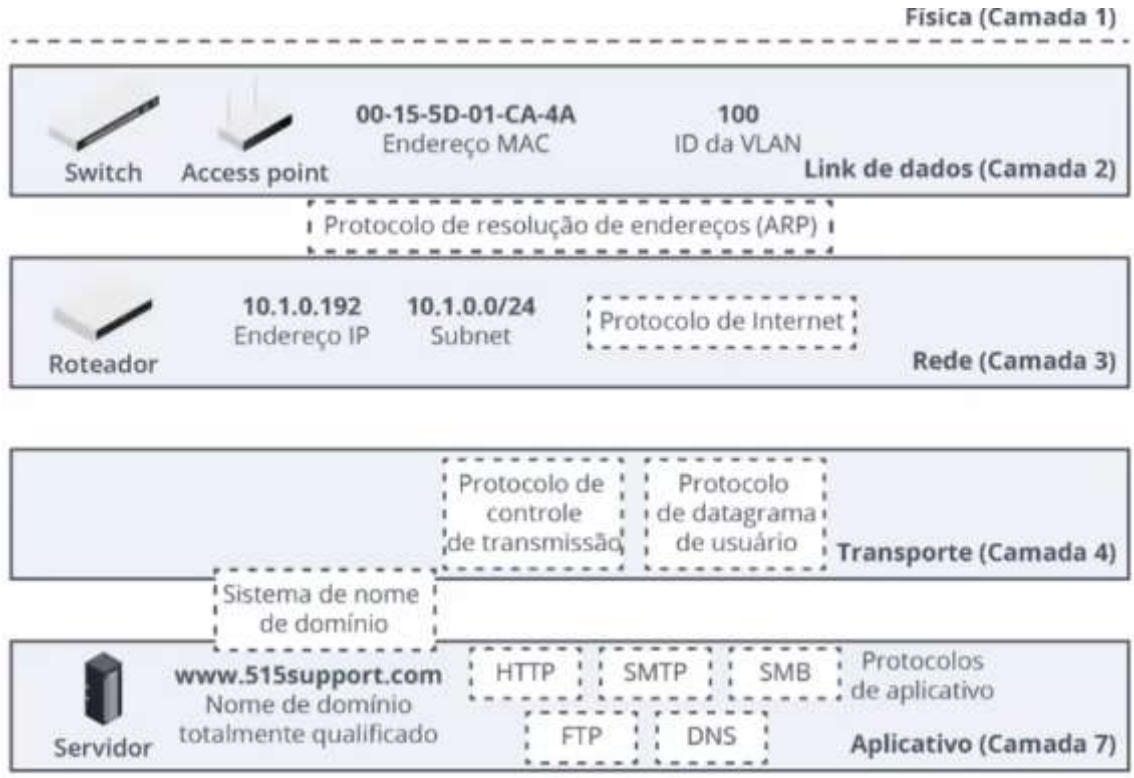
- Infraestrutura de rede são os meios, dispositivos e protocolos de endereçamento/encaminhamento que suportam a conectividade básica;
- Aplicativos de rede são os serviços executados na infraestrutura para sustentar as atividades do negócio, como o processamento de faturas ou envio de e-mails.
- Ativos de dados são as informações criadas, armazenadas e transferidas como resultado da atividade de negócios.

Infraestrutura de rede:

É útil empregar um modelo de camadas para analisar a infraestrutura e os serviços de rede. O modelo OSI, é um exemplo amplamente citado de como definir camadas de funções de rede.

A rede é composta de nós e links. Na camada Física ou camada 1 do modelo OSI, os switches encaminham quadros entre os nós de uma rede cabeada. Os switches funcionam na camada 2 do modelo OSI. Um endereço MAC é um valor de 48 bits escrito em notação hexadecimal, como 00-15-5D-01-CA-4A

O modelo OSI possui 7 camadas, e o modelo TCP/IP possui 4 camadas.



Access Point funciona na Camada 2

- Eles fornecem uma ponte entre uma rede com fio e hosts ou estações sem fio.

Roteadores na Camada 3

- Enviam pacotes por uma rede da internet, tomando decisões de encaminhamento com base em endereços IP.

Os protocolos de transporte TCP e UDP na Camada 4

- Permitem que os clientes troquem dados com os servidores de aplicativos. O protocolo TCP estabelece conexões confiáveis e o UDP permite transferências não confiáveis e sem conexão.

Protocolos de aplicativos atuam na Camada 7

- Possibilitam a funcionalidade cliente/servidor para serviços ao nível do usuário, como navegação web, e-mail e transferência de arquivos.

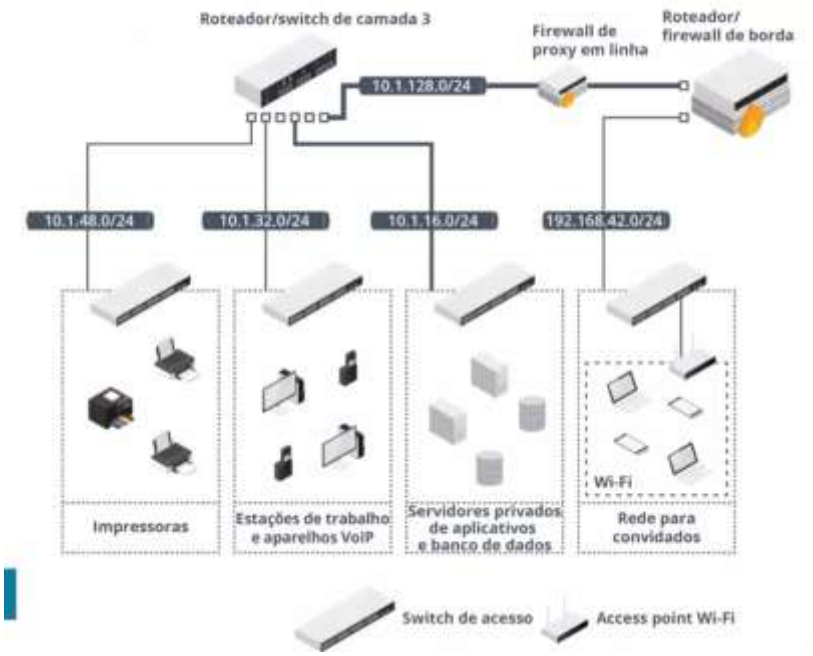
DNS atua na camada 7

- São servidores do sistema de nomes de domínio. Eles hospedam registros de nomes e executam a resolução de nomes para permitir que aplicativos e usuários abordem hosts e serviços usando nomes de domínio ao invés do endereço IP.

Outras considerações sobre infraestrutura de roteamento:

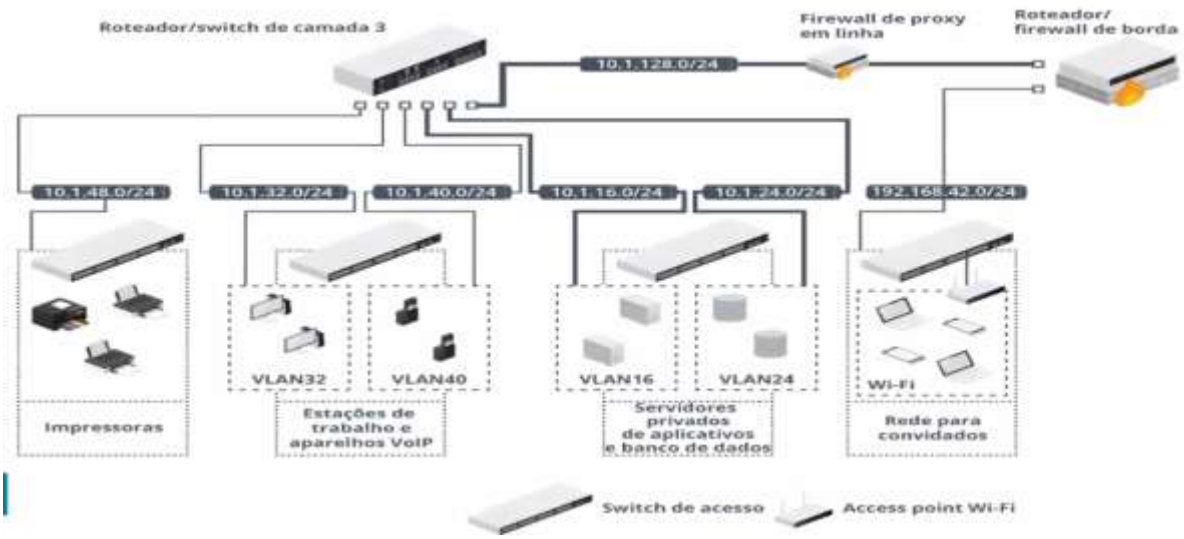
Protocolo IP: Fornece mecanismo de endereçamento para redes e sub-redes lógicas.

IPV4 possui 32 bits em notação decimal, IPV6 possui 128 bits em notação hexadecimal



VLANs: É um recurso compatível com a maioria dos switches e atua de forma que todos os switches conectados juntos na mesma rede local podem ser configurados com um conjunto coerente de Ids de VLAN, que vão de 2 a 4.094.

Cada VLAN é um domínio de transmissão separado. Todo tráfego de uma VLAN pra outra deve ser roteado.



Demilitarized Zone (DMZ) > Screened subnet:

A Zona Desmilitarizada (DMZ) em TI é uma rede intermediária entre a rede interna de uma organização e a internet. Ela é usada para hospedar serviços acessíveis externamente, como servidores web ou de e-mail, garantindo que, mesmo se invadidos, os atacantes não tenham acesso direto à rede interna.

Superfície de Ataque:

Pontos fracos:

- **Pontos Únicos de Falha (SPOF):** Um ponto crítico que depende de um único servidor de hardware, dispositivo ou canal de rede;
- **Dependências Complexas:** Serviços que requerem a disponibilidade de diversos sistemas;
- **Disponibilidade acima da confidencialidade e integridade:** Usar atalhos para colocar um serviço em operação, sem testes e análises prévias;
- **Falta de Documentação:** Segmentos de rede, dispositivos e serviços podem ser adicionados sem procedimentos adequados de controle de mudanças, levando a uma falta de visibilidade sobre a composição de rede;

Segurança da Porta: Cada porta de parede e de switch é uma oportunidade para um invasor conectar um dispositivo à rede. Como proteger:

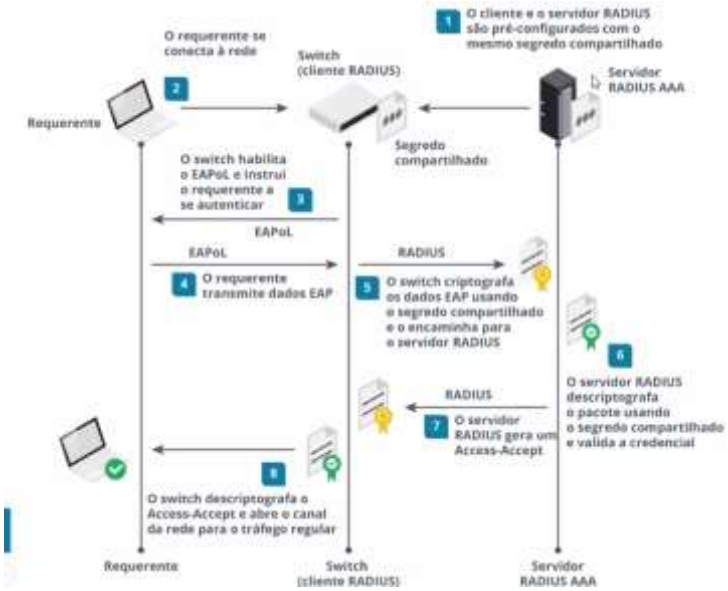
- Filtragem MAC e limitações MAC: Cada computador possui um endereço MAC, configurar uma filtragem MAC, significa que apenas MACs autorizados podem se conectar ao switch.
- Protocolo 802.1x: O padrão IEEE 802.1x Port Based Network Access Control (PNAC) permite que um switch exija autenticação quando um host se conecta a uma das suas portas. O 802.1x usa arquitetura AAA, autenticação, autorização e accountability.

O padrão 802.1x é implementado por dois protocolos:

- EAP: Fornece uma estrutura para implantar vários tipos de métodos de autenticação. Frequentemente usado com ceritficados digitais para estabelecer uma relação de confiança e estabelecer um túnel seguro para

transmissão de credenciais do usuário ou para realizar a autenticação de smart-card sem uma senha.

- RADIUS: Permite que o autenticador e o servidor de autenticação comuniquem as decisões de autenticação e autorização. O autenticador é um cliente RADIUS e o servidor de autenticação é um servidor RADIUS.



Isolamento Físico: Isolar hosts essenciais a qualquer tipo de rede. Um host que não está conectado a nenhuma rede é chamado de Air-gapped(isolado/vedado).

Considerações sobre arquitetura:

- **Custos:** Mudanças, aquisição e atualização demanda um alto investimento inicial, que não possui retorno e tende a se depreciar com o passar do tempo.
- **Computação e responsividade:** Minimizam o tempo de processamento das cargas de trabalho.
- **Escalabilidade e Facilidade de Implantação:** Minimizam os custos quando as cargas de trabalho aumentam ou diminuem.
- **Disponibilidade:** Minimiza tempo de inatividade e maximiza o tempo de atividade.
- **Energia:** A instalação consegue atender a demanda de energia dos dispositivos e cargas de trabalho?

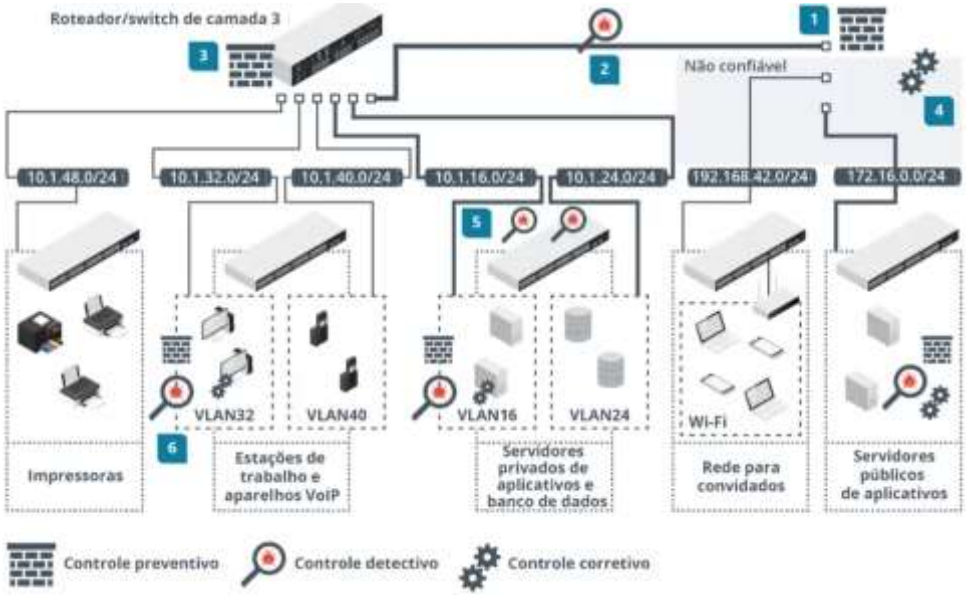
Dispositivos de segurança para redes

Posicionamento do Dispositivo:

- **Seleção de controles eficazes:** É o processo de escolher o tipo e o posicionamento de dispositivos de software de segurança. O objetivo é reforçar a segmentação, aplicar controles de acesso e monitorar o tráfego em busca de violações da política.
    - A seleção de controles eficazes é regida pelo princípio da defesa em profundidade. Na Defesa em Profundidade, as zonas críticas de segurança são protegidas por diversos controles preventivos, de detecção

e corretivos que operam em cada camada do modelo OSI. Essa defesa é assegurada por uma escolha cuidadosa do posicionamento do dispositivo dentro da topologia de rede.

- **Posicionamento do Dispositivo:**
  - **Controles preventivos:** São firewalls, que são colocados na borda de um segmento ou zona de rede. Eles controlam o que entra e sai do segmento, assegurando a integridade e a confidencialidade;
  - **Controles de Detecção:** Podem ser colocados dentro do perímetro para monitorar tráfego trocado entre os hosts no segmento e com isso são gerados alertas de tráfego malicioso que tenha escapado do controle de perímetro;



Atributos do Dispositivo: Eles determinam a maneira precisa para posicionar um ativo na topologia de rede.

- **Ativo x Passivo**: Um controle de segurança passivo não requer nenhum tipo de configuração de cliente ou agente nem transferência de dados de host para operar. Por ex: o tráfego de rede pode ser direcionado ou copiado para um sensor e verificado por um mecanismo de análise. Esse controle é completamente passivo e os hosts da rede não teriam conhecimento de sua operação.
- **Ativo x Passivo**: Um controle de segurança ativo que realiza varredura deve ser configurado com credenciais e permissões de acesso e trocar dados com hosts de destino. Um controle ativo que realiza filtragem exige que os hosts sejam explicitamente configurados para usar controle e isso pode implicar na instalação de um software agente no host.

Ao ocorrer uma falha o dispositivo pode estar configurado como Fail-Open ou Fail-Closed

- **Fail-Open:** Significa que o acesso à rede ou ao host é preservado, se possível. Este modo prioriza a disponibilidade em vez da confidencialidade ou integridade.

O risco desse tipo de controle é que um agente pode criar um cenário de falha para contornar o controle.

- **Fail-Closed:** Significa que o acesso é bloqueado ou o sistema entra no estado mais seguro disponível, seja qual for a falha ocorrida. Este modo prioriza a confidencialidade e a integridade em vez da disponibilidade. Seu maior risco é o período de inatividade do sistema após uma falha.

Firewalls: É um controle preventivo projetado para aplicar políticas ao tráfego que entra e sai de uma zona de rede.

- **Filtragem de Pacotes:** Um firewall de filtragem de pacotes é configurado especificando um grupo de regras chamado Access Control List (ACL). Cada regra um tipo especifico de pacote de dados e a ação a ser realizada quando um pacote corresponder à regra. Ele pode inspecionar os cabeçalhos dos pacotes IP e as regras são baseadas nas informações encontradas nesses cabeçalhos:
    - **Filtragem de IP:** Aceita ou nega o tráfego com base nos nos bits do endreço IP de origem e/ou destino. A maioria dos firewalls pode filtrar por endereços MAC.
    - **Protocol ID/Type:** É um pacote IP que carrega um protocolo identificado, sendo os mais comuns o TCP ou UDP. Outros tipos menos comuns incluem o ICMP e protocolos que facilitam o roteamento.
    - **Filtragem de portas/segurança:** Aceita ou nega um pacote com base nos números da porta TCP ou UDP de origem e destino.

Tipos de Firewall:

- **Firewall do aparelho:** É um firewall de hardware autônomo implantado para monitorar o tráfego que entra e sai de uma zona de rede .

Firewalls Camada 4 e Camada 7:

- Um firewall de filtragem de pacotes básicos é stateless, ou seja, não tem monitoração de estado. Isso significa que não preserva informações sobre sessões de rede. Cada pacote é analisado de maneira independente sem nenhum registro de qualquer pacote analisado anteriormente. Esse tipo de firewall requer esforço mínimo de processamento, mas é vulnerável a ataques espalhados por uma sequência de pacotes.
- Um Firewall de inspeção stateful rastreia informações sobre a sessão estabelecida entre dois hosts. Todos os firewalls agora **incorporam algum nível de capacidade de inspeção de estado**. Os dados das sessões são armazenados em uma tabela de estado. Quando um pacote chega o firewall verifica para confirmar se ele pertence a uma conexão existente, em caso negativo, as regras comuns de filtragem de pacotes para determinar se deve permitir. Depois que a conexão é autorizada, o firewall geralmente permite a passagem do tráfego sem monitoramento para poupar esforço de processamento.

Firewall de Camada 4: Essa é a camada de transporte do modelo OSI. Um firewall de camada 4 examina o handshake de três vias do TCP para distinguir as conexões novas já estabelecidas. Uma conexão TCP legítima deve seguir uma sequência **SYN > SYN/ACK > ACK**, o que divergir disso, pode ser descartado.

Firewall de Camada 7: Um firewall de camada 7 pode inspecionar os cabeçalhos e o payload de pacotes de camada de aplicativo. Um recurso importante é verificar se o protocolo do aplicativo corresponde à porta, pois o malware pode tentar enviar dados TCP brutos pela porta 80 apenas por ela estar aberta, por exemplo. Os firewalls com reconhecimento de aplicativos têm muitos nomes diferentes, incluindo Gateway de camada de aplicativo, inspeção stateful multicamada e inspeção profunda de pacotes.

Servidor Proxy: O proxy que atua junto com firewall desconstrói cada pacote, analisa e se estiver em conformidade com as regras, ele reconstrói e o encaminha.

- **Servidor Proxy de Encaminhamento:** Atua no tráfego de saída de um protocolo específico.
- **Proxy não transparente:** Significa que o cliente precisa ser configurado com o endereço do servidor proxy e o número da porta para usá-lo. Por convenção, a porta na qual o servidor proxy aceita conexões de cliente é a TCP/8080.
- **Um servidor proxy transparente:** Intercepta o tráfego do cliente sem que o cliente tenha que ser reconfigurado. Deve ser implementado como um roteador ou um dispositivo em linha.

Sistemas de Detecção de Intrusos: São um controle que realiza análises em tempo real do tráfego de rede ou registros do sistema e do aplicativo.

- **Sensores:** Sistemas de detecção de intrusão capturam o tráfego por meio de um sniffer(detector) de pacotes, chamado de sensor. O sensor pode usar um SPAN/porta espelhada ou um TAP em linha.

O tráfego capturado pelos sensores é enviado para o IDS, como **Snort**, **Suricata** ou **Zeek/Bro**. Quando é detectada uma correspondência do tráfego com uma assinatura de ameaça, o IDS emite um alerta ou gera um entrada de log, mas não bloqueia o host de origem.

Um IDS é usado para identificar e registrar hosts e aplicativos e para detectar tentativas de descoberta de senhas, varreduras de portas, Worms, aplicativos de Backdoors, pacotes ou sessões inválidas, além de outros tipos de violações de políticas.

IPS: Verifica o tráfego em busca por correspondências a assinaturas de ameaças e pode ser configurado para atuar automaticamente para interromper um ataque. Essas são respostas comuns:

- Bloquear de forma temporária ou permanente a origem do tráfego em desacordo;
- Redefinir a conexão, mas não bloquear o endereço de origem;
- Redirecionar o tráfego para um honeypot ou honeynet para análise adicional de ameaça;

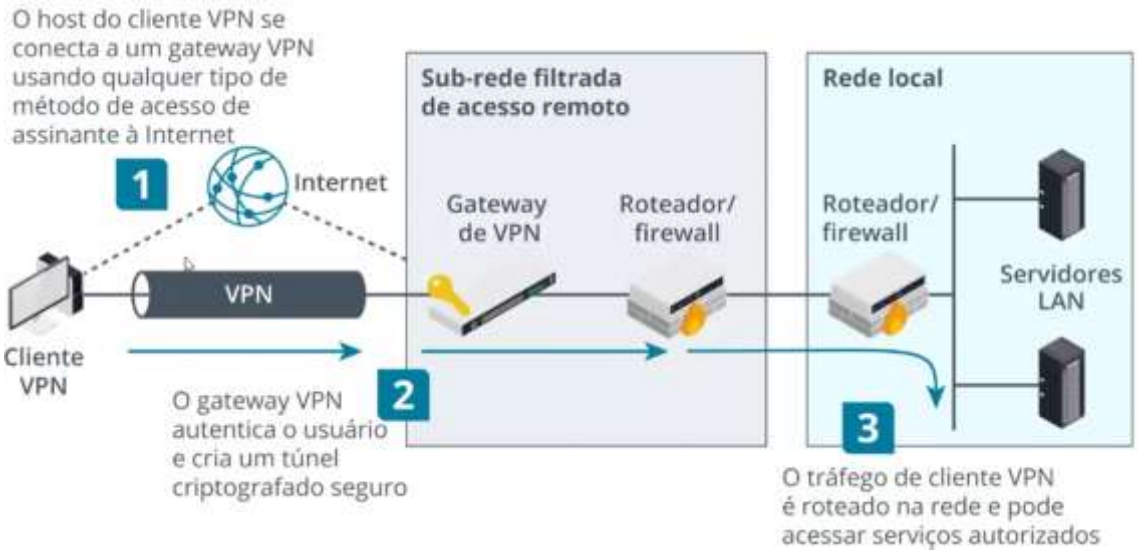
Firewall de Última Geração (NGFW): Geralmente possui as seguintes funções:

- Filtragem com reconhecimento de aplicativos da Camada 7, incluindo a inspeção do tráfego criptografado de segurança da camada de transporte (TLS);
- Integração com diretórios de rede, facilitando políticas de filtragem baseadas em tempo e conteúdo por usuário ou por função e proporcionando maior proteção contra uma ameaça interna.

Gerenciamento Unificado de Ameaças (UTM): É um produto de segurança que centraliza em um único dispositivo vários tipos de controle de segurança: firewall, antimalware, prevenção de intrusão de rede, filtragem de spam, filtragem de conteúdo, prevenção contra perda de dados, VPN, gateway de acesso à nuvem e proteção de endpoint/verificação de malware.

Comunicações Seguras

Arquitetura de Acesso Remoto:



Protocolos de VPN:

Protocolos legados como PPTP, foram descontinuados por não oferecerem a segurança adequada. Atualmente os mais comuns são TLS e IPsec.

Secure Shell: É o principal meio de obter acesso remoto seguro a um terminal de linha de comando. É usado principalmente para administração remote e transferência de arquivos (SFTP). O mais utilizado é o SSH.

Os servidores SSH são identificados por um par de chaves pública/privada denominado chave host. O SSH permite que o cliente use vários métodos para autenticar no servidor e esses métodos podem ser ativado ou desativado conforme necessário no arquivo /etc/ssh/sshd_config.

Servidores Jump:

Um servidor jump (ou jump server) é um servidor intermediário usado para acessar redes seguras de forma controlada. Ele funciona como uma ponte entre redes externas e servidores internos, aumentando a segurança ao restringir acessos diretos.

Principais funções:

- Controle de acesso: Apenas usuários autorizados podem passar pelo jump server.
- Registro de atividades: Registra acessos e comandos executados.
- Segurança aprimorada: Reduz a exposição direta de servidores críticos.

Geralmente, é usado em conexões SSH ou RDP para administração de servidores internos.

Arquitetura de rede em nuvem segura

Modelos de implantação em nuvem: Um modelo de implantação em nuvem classifica a posse e o provisionamento do serviço. É importante reconhecer que os modelos de implantação têm impactos diferentes em ameaças e vulnerabilidades.

- **Público (Multilocatário):** É um serviço oferecido na internet por provedores de serviços em nuvem (CSPs) para consumidores na nuvem; (CSPs: AWS, Azure)
- **Hospedagem Privada:** É hospedada por terceiros para uso exclusivo da organização. Isso é mais seguro e pode garantir melhor desempenho, mas é igualmente mais caro.
    - Infraestrutura em nuvem completamente privada e de propriedade da organização. Esse tipo de entrega é mais voltado para serviços bancários e governamentais que exigem um controle de acesso mais rigoroso nas suas operações.

Tipos de modelos de serviço de nuvem:

- **Saas:** Aplicativos de Software como serviço, como Office 365 ou Google G Suite ou Salesforce;
- **Paas:** A plataforma como serviço fornece recursos que ficam entre Saas e Iaas. Uma solução típica de Paas fornece servidores e infraestrutura de rede de armazenamento (como no Iaas), mas também uma plataforma de ativo/banco de dados da Web de várias camadas. Alguns exemplos são: Oracle Database, Microsoft Azure SQL Database e Google App Engine.
- **Iaas:** Infraestrutura como serviço é um meio de provisionar recursos de TI, como componentes de servidores, balanceadores de carga e rede de área de armazenamento (SAN) rapidamente. Em vez de comprar esses componentes e os links que eles necessitam, você os aluga conforme necessário no datacenter do provedor de serviços. Ex: Amazon Elastic Compute Cloud, Microsoft Azure Virtual Machines, Oracle Cloud e Open Stack. (Ambiente para testes para subir instancias)

Matriz de Responsabilidade: Ao usar a infraestrutura de nuvem, os riscos de segurança são compartilhados e não transferidos entre o provedor de nuvem e o cliente. **O provedor da nuvem é responsável por proteger a infraestrutura subjacente, enquanto o cliente é responsável por proteger seus aplicativos de dados.**

Responsabilidade	Local	IaaS	PaaS	SaaS	FaaS	Guia da nuvem de controles do CIS	Benchmarks dos fundamentos do CIS
Classificação e contabilização dos dados	●	●	●	●	●	✓	✓
Proteção de end-point e cliente	●	●	●	◪	◪	✓	✓
Gerenciamento de identidade e acesso	●	●	◪	◪	◪	✓	✓
Controles no âmbito dos aplicativos	●	●	◪	◪	◪	✓	✓
Controles de rede	●	◪	●	●	●	✓	✓
Infraestrutura do host	●	◪	●	●	●	✓	
Segurança física	●	●	●	●	●		

● Cliente na nuvem ● Provedor de nuvem

Computação Centralizada e Descentralizada

- **Centralizada:** Todo o processamento e armazenamento de dados é realizado em um único local, tipicamente um servidor central. Todos os usuários e dispositivos dependem do servidor central para acessar e processar dados e para segurança desses dados. Ex: Computadores Mainframe e arquiteturas cliente-servidor.
- **Descentralizada:** É um modelo no qual o processamento e armazenamento dos dados são distribuídos em diversos locais ou dispositivos. Ex: Blockchain, Redes Peer to Peer(P2P) que sã projetadas para distribuir processamento e armazenamento de dados entre nós participantes sem depender de um servidor central, CDNs, Dispositivos IOT, TOR.

Arquitetura resiliente em nuvem: É o potencial de fornecer serviços resilientes em diferentes níveis, como componentes, servidores, redes locais, sites, datacenters e redes de longa distância. Alta disponibilidade (HA) refere-se ao armazenamento provisionado com garantia de 99,99% ou mais de tempo de atividade.

- **Replicação:** Permite que as empresas copiem dados para um lugar onde possam ser utilizados de forma mais eficaz. A nuvem é usada como uma área de armazenamento central, disponibilizando dados a todas as unidades de negócio.
    - **Cold Storage e Hot Storage:** Diz respeito à rapidez com que dados podem ser recuperados. O Hot recupera mais rápido que o Cold, porém, quanto mais rápido, maior o custo
    - **Alta disponibilidade em todas as zonas:** As CSPs dividem o mundo em regiões, cada região é independente das outras. As regiões são divididas em zonas de disponibilidade que têm datacenters independentes, com sua própria energia, resfriamento, conectividade e riscos. A escolha é baseada na latência.
- **Modalidades de Replicação:**
    - **Replicação Local:** Replica seus dados em um único datacenter na região em que você criou sua conta de armazenamento. As réplicas estão frequentemente em rodízios de falhas e domínios de upgrade separados.
    - **Replicação Regional:** Replica seus dados em vários datacenters em uma ou duas regiões.

- **Armazenamento georredundante (GRS):** Replica seus dados para uma região secundária distante da região primária. O que protege os dados em caso de interrupção ou desastre regional.

Virtualização de aplicativos e containers: É um tipo mais limitado de VDI, onde ao invés de executar toda a área de trabalho do cliente como uma plataforma virtual, o cliente acessa um aplicativo hospedado em um servidor ou transmite o aplicativo do servidor para o cliente para processamento local. Ex: Citrix XenApp, Microsoft App-V e VMware ThinApp.

Computação sem servidor: Provedor gerencia e aloca recursos automaticamente conforme necessário, cobrando apenas pelo uso real do aplicativo. Um exemplo de aplicativo sem servidor são Chatbots.

Sistemas Integrados: São usados em vários aplicativos especializados, incluindo eletrônicos de consumo, automação industrial, sistemas automotivos, dispositivos médicos e etc.

- **Sistemas operacionais em tempo real (RTOS):** Projetado para usos em aplicativos que exigem processamento e resposta em tempo real. Trata-se de sistemas operacionais com fins específicos, projetados para altos níveis de estabilidade e velocidade de processamento.

Sistemas de Controle Industrial (ICS): Sistemas de automação de processos e fluxos de trabalho. Controlam máquinas usadas em infraestruturas críticas, como de serviços de fornecimento de energia e água, serviços de sáude, telecomunicação de segurança nacional.

- **Controle de supervisão e aquisição de dados (SCADA):** Assume o lugar de ICSs de grande escala multilocal. O sistema SCADA geralmente é executado como software em computadores comuns, coletando dados e gerenciando dispositivos, e equipamentos industriais como PLCs incorporados, denominados dispositivos de campo.

Internet das Coisas: Refere-se a rede de dispositivos físicos, veículos, aparelhos e outros objetos com sensores, software e conectividade incorporados, possibilitando coleta e troca de dados.

Zero Trust: Definida pelo NIST SP 800-207 como paradigmas de segurança cibernética que movem as defesas de perímetros estáticos baseados em rede para se concentrar em usuários, ativos e recursos. Uma arquitetura Zero Trust consegue proteger melhor dados, aplicativos, redes e sistemas contra ataques mal intencionados e acesso não autorizado do que arquiteturas tradicionais, o que garante que apenas os serviços necessários e de fontes apropriadas sejam permitidos. Seus principais benefícios são:

- **Maior Segurança:** Todos os usuários, dispositivos e aplicativos devem ser autenticados antes do acesso à rede;
- **Melhores Controles de Acesso:** Limites mais rigorosos sobre quem ou o que pode acessar recursos e de quais localizações;
- **Governança e Conformidade aprimoradas:** Limita o acesso dos dados e fornece maior visibilidade operacional sobre atividade do usuário e do dispositivo;

- **Maior granularidade:** Concede o acesso necessário, quando necessário ao usuário;
- **Exemplos:** Google BeyondCorp, JEDI, Cisco Zero Trust Architeture, Palo Alto Networks Prisma Access;

Gestão de Ativos

Rastreamento de ativos: Um processo de ativos rastreia todos os sistemas, componentes, dispositivos e outros objetos de valor críticos à organização em um inventário.

- **Atribuição de Ativos/Contabilização:** A atribuição/contabilização de propriedade de ativos e a classificação são componentes essenciais de um processo de gestão de ativos bem estruturado, garantindo que as organizações gerenciem e protejam efetivamente seus recursos ao passo que elas mantem a responsabilidade.
- **Monitoramento/Rastreamento:** Incluem tarefas de inventário e enumeração, que envolvem a criação e manutenção de **uma lista abrangente de todos os ativos dentro da organização**, seja **hardware**, **software**, **dados** e **equipamentos de rede**.
    - **Inventário Manual:** Em organizações menores ou para tipos de ativos específicos, a criação e manutenção manual de ativos pode ser viável;
    - **Inventário de Rede:** Ferramentas de varredura de rede como Nmap, Nessus ou OpenVAS conseguem detectar e enumerar automaticamente dispositivos em rede, como switches, servidores, roteadores e estações de trabalho.
- **Software de Gestão de Ativos:** As soluções como Lansweeper, ManageEngine ou SolarWinds conseguem descobrir, rastrear e catalogar automaticamente vários tipos de ativo, como hardware, software e licenças;
- **Banco de dados de gerenciamento de configurações (CMDB):** Um repositório centralizado de informações relacionas à infraestrutura de TI de uma organização, que inclui ativos, configurações e relacionamentos. Ferramentas como ServiceNow ou BMC Remedy podem ajudar a criar e manter um CMDB;
- **Soluções de gerenciamento de dispositivos móveis (MDM):** Soluções como Microsoft Intune, VMware Workspace ONE ou MobileIron podem ajudar a enumerar e proteger os dispositivos;
- **Descoberta de ativos em nuvem:** Ferramentas nativas em nuvem como AWS Config e Azure Resource Graph, ou de terceiros como CloudAware e CloudCheckr podem ajudar a descobrir e catalogar ativos implantados em nuvem;

Conceitos de Proteção de Ativos:

- **Convenções de nomenclatura padrão e identificação de ativos:** Ativos tangíveis podem ser identificados por etiquetas de código de barras ou identificação por radiofrequencia (RFID) que é um chip programado com dados do ativo. Uma convenção de nomenclatura padrão torna o ambiente mais consistente para ativos digitais e de hardware.
- **Gerenciamento das configurações:** Garante que cada elemento configurável não tenha se afastado de sua configuração aprovada;

- **Controle e Gerenciamento de Mudanças:** Reduzem o risco de que alterações nestes componentes possam causar interrupção nas operações da organização.

ITIL é uma popular estrutura de documentação de atividades e processos de boas práticas para prestação de serviços de TI

Backups de Dados: Desempenham um papel essencial na proteção de ativos, garantindo disponibilidade e integridade dos dados e sistemas críticos.

- **Frequência de Backups;**
- **Backups Locais:** Envolvem o armazenamento de dados localmente (no mesmo local que os sistemas protegidos) em discos rígidos ou fitas para fornecer acesso e recuperação rápidos em caso de corrupção ou perda de dados ou falhas de sistemas;
- **Backups Externos:** Envolvem transferência de dados para um local remoto, a fim de garantir a proteção contra desastres naturais, roubo e outras ameaças físicas;

SnapShots: Captam o estado de um sistema em um ponto específico no tempo. Possui três tipos, de máquina virtual (VM), filesystem e rede de área de armazenamento (SAN) cada um tem como alvo um tipo diferente de hierarquia.

- **De VM:** Criados por VMware vSphere ou Microsoft Hyper-V, capturam o estado da máquina virtual, o que inclui sua memória, armazenamento e configurações, o que permite que os administradores revertam a VM para um estado anterior à falhas ou corrupção de dados durante um teste por exemplo.

Destruição Segura de Dados: O Regulamento Geral sobre a Proteção de Dados (RGPD) ou à Lei de Portabilidade e Responsabilidade de Seguros de Saúde(HIPAA) exigem a exclusão ou destruição de dados específicos quando não forem mais necessários ou se solicitado pelo titular dos dados.

Descarte de Ativos: O descarte/desativação de ativos enfocam no manuseio seguro e em conformidade de dados e dispositivos de armazenamento no fim do seu ciclo de vida ou quando não são mais necessários. Alguns conceitos importantes são:

- **Limpeza:** Processo de remoção de informações confidenciais de uma mídia de armazenamento. Geralmente usa técnicas especializadas como apagamento de dados, desmagnetização ou criptografia para garantir que os dados sejam irrecuperáveis;
- **Certificação:** Documentação e verificação do processo de limpeza ou destruição de dados. Geralmente envolve a obtenção de um certificado de destruição ou limpeza emitido por um prestador de serviços terceirizado respeitável, garantindo que tudo foi feito de acordo com padrões e regulamentos do setor;

Continuidade das Operações (COOP): Refere-se ao processo de garantir que uma organização possa manter ou retomar rapidamente os processos críticos em caso de interrupção, desastre ou crise. Seus conceitos visam minimizar o tempo de inatividade, proteger recursos essenciais e manter a resiliência dos negócios;

Escalabilidade e Elasticidade:

Escalabilidade é a capacidade de aumentar os recursos para atender à demanda em uma proporção de custo semelhante, ou seja, se o uso dobrar, será cobrado menos que o dobro; Possui dois tipos: Horizontal: adicionar recursos em paralelo com os existentes e Vertical: Aumentar a potência dos recursos existentes.

Tolerância a falhas e redundância: Um sistema que sofre falhas, mas continua fornecendo o mesmo nível de serviço é chamado de tolerante. Essa tolerância normalmente é obtida provisionando redundância para componentes essenciais e pontos únicos de falha.

A resiliência do site pode ser Hot, Warm e Cold

- Um site Hot: Pode fazer failover quase imediatamente, Pode ser um prédio com equipamentos mantido atualizado com um conjunto de dados ao vivo;
- Um site Warm: Pode ser semelhante, mas exige que um conjunto de dados mais recente seja carregado;
- Um site Cold: Leva mais tempo para configurar. Pode ser um prédio vazio com um contrato de arrendamento em vigor para instalar qualquer equipamento quando necessário;

Redundância de Energias:

- **Fontes de Alimentação Duplas;**
- **Backups de baterias e fontes de alimentação ininterruptas (UPSs);**
- **Geradores;**

Tecnologias de Engano: São ferramentas e técnicas de resiliência de segurança cibernética para aumentar o custo do planejamento de ataques para o agente de ameaças. Honeypots, Honeynets, Honeyfiles e Honeytokens são ferramentas de segurança usadas para detectar e se defender de ataques.

Honeypots são sistemas de chamariz que imitam sistemas e aplicações reais e são projetados para permitir que as equipes de segurança monitorem as atividades dos invasores e coletem informações sobre suas táticas e ferramentas;

Controles de Segurança Física

- **Barricadas e pontos de entrada/saída:** Servem para canalizar o fluxo de pessoas por meio de pontos de entrada e saída definidos. Cada ponto de entrada deve ter um me de autenticação para que apenas pessoas autorizadas possam passar.
- **Cercas;**
- **Iluminação;**
- **Bollards:** Postes verticais curtos feitos de aço, concreto e etc e instalados em intervalos ao redor de um perímetro ou entrada.

Portões e Fechaduras:

- **Física, eletrônica ou Biométrica;**
- **Travas de cabo;**
- **Crachás de Acesso;**

Seguranças e Câmeras (vídeovigilância):

- **Reconhecimento de movimento;**
- **Detecção de objetos;**
- **Drones/UAV;**

Sistemas e Sensores de Alarme:

- **Circuitos;**
- **Detecção de Movimentos;**
- **Detecção de Ruídos;**
- **Proximidade;**
- **Pânico/sob coação;**
- **Infravermelhos;**

Vulnerabilidades de dispositivos e sistemas operacionais:

Vulnerabilidades do Sistem Operacional (SO): Os SOs são o componente mais crítico de qualquer infraestrutura, portanto suas vulnerabilidades podem levar a problemas significativos quando exploradas;

- **Windows:** Vulnerabilidade mais notória foi MS08-067 no serviço Windows Server. Já o MS17-010 representou uma atualização de segurança significativa e críticas lançada pela Microsoft em março de 2017.
- **Android:** Stagefright de 2015, que permitia que invasores executassem códigos maliciosos em um dispositivo Android enviando uma mensagem MMS criadas especialemente.
- **IOS:** Em 2019 diversas vulnerabilidades no IOS foram descobertas pelo time Project Zero do Google. Elas permitiam ataques de watering hole se aproveitavam de diversas vulnerabilidades para obter acesso total a um dispositivo após fazer a vitima visitar um site mal-intencionado;
- **Linux:** HeartBleed de 2014 foi um bug na biblioteca de software criptográfico de OpenSSL. Ela permitia que invasores lessem a memória dos sistemas que executavam as versões vulneráveis do software OpenSSL, comprometendo as chaves secretas usadas para proteger dados;

Vulnerabilidades de Sistemas Legados e em fim de vida (EOL): Apresentam desafios consideráveis para organizações, pois seus patches ou correções de segurança não estão mais disponíveis ou são difíceis de aplicar. Tanto os Sistemas Legados quanto os EOL tem algo em comum: Ambos são desatualizados

Vulnerabilidades de Firmware: O firmware é o software fundamental que controla o hardware e pode conter vulnerabilidades significativas, como Meltdown e Spectre, de 2018, que afetaram quase todos os computadores e dispositivos móveis. Elas estavam ligadas aos processadores disponíveis dentro das máquinas e permitia que programas maliciosos roubassem dados durante o processamento. Outra vulnerabilidade, o LoJax, também de 2018, permitia que um invasor permanecesse no sistema mesmo após substituição completa do disco rígido ou reinstalação do SO.

Vulnerabilidade de virtualização: Uma vulnerabilidade significativa é o conceito VM escape, que acontece quando um invasor com acesso a uma máquina virtual força a

saída desse ambiente isolado e obtém acesso ao sistema host ou à outras VMs em execução no mesmo Host. Ela pode permitir que um invasor obtenha controle de todas as máquias virtuais em execução em um único servidor físico, levando à uma violação de segurança potencialmente devastadora; Um exemplo famoso é Cloudburst.

Vulnerabilidades de Zero Day: É uma falha de segurança em software ou hardware que ainda não foi descoberta ou corrigida pelo desenvolvedor. Como os fabricantes não têm conhecimento do problema, não há uma correção disponível, tornando o sistema vulnerável a ataques. Hackers podem explorar essas falhas para roubo de dados, invasão de sistemas ou instalação de malware antes que uma solução seja implementada. Podem ser exploradas antes de que seja tomado o conhecimento delas ou que tenham chance de corrigir.

Vulnerabilidades de Configuração Incorreta: A vulnerabilidade de configuração incorreta ocorre quando um sistema, aplicativo ou serviço é mal configurado, deixando brechas de segurança. Isso pode incluir permissões excessivas, senhas fracas, serviços desnecessários ativados ou falta de atualizações. Essas falhas podem ser exploradas por invasores para obter acesso não autorizado, roubar dados ou comprometer o sistema.

SideLoad, Root e Jailbreak: Dispositivos Móveis

Root e Jailbreaks são métodos usados para obter privilégios elevados e acesso à arquivos de sistemas em dispositivos móveis, o que permite que usuários contornem certas restrições impostas por fabricantes do dispositivo ou do SO.

Root: Envolve obter acesso root ou privilégios administrativos em um dispositivo Android para modificar arquivos de sistema, instalar ROMs personalizadas e acessar recursos e configurações indisponíveis a usuários comuns.

Jailbreak: Ato de obter acesso total a um dispositivo IOS após remover limitações impostas pelo sistema operacional.

Sideload: Consiste na instalação de aplicativos de fontes de fora da loja de aplicativos oficial da plataforma.

Vulnerabilidades de Aplicativos e Nuvem

Condição de Corrida e TOCTOU: Vulnerabilidade de condição de corrida refere-se à falhas de software associadas ao momento ou à ordem dos eventos de um programa de software, que podem ser manipulados, causando resultados indesejáveis ou imprevisíveis. Uma condição de corrida descreve quando duas ou mais operações devem ser executadas na ordem correta. Quando a lógica do software não verifica ou não impõe essa ordem, problemas de segurança podem ocorrer, como corrupção de dados, acesso não autorizado, ou violações de segurança semelhantes. Essa vulnerabilidade se manifesta de várias maneiras, como em vulnerabilidades time-of-check to time-of-use (TOCTOU), em que um estado do sistema muda entre o estágio de verificação(time-of-check) e o estágio de uso(time-of-use).

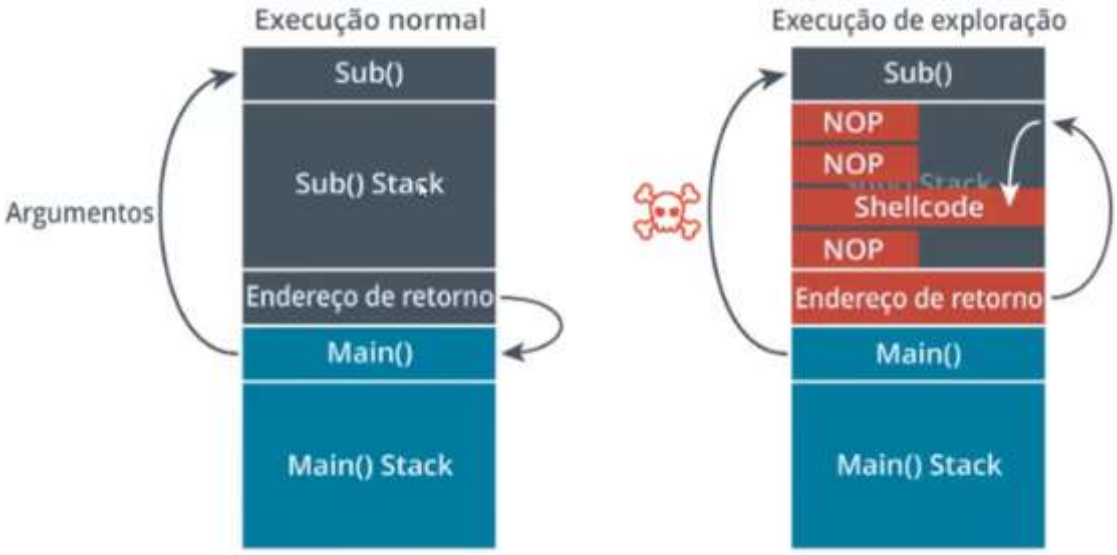
Injeção de memória: São um tipo de falha de segurança em que um invasor pode introduzir um código malicioso na memória de processos de um aplicativo em execução. Um invasor geralmente projeta o código injetado para alterar o comportamento de um

aplicativo para que ele forneça controle ou acesso não autorizado sobre o sistema. Ex: SQL Injection.

Buffer Overflow: Um Buffer é uma área de memória que o aplicativo reserva para armazenar dados esperados. Para explorar essa vulnerabilidade, o invasor propositalmente envia dados que deliberadamente preenchem de mais o buffer.

Uma das vulnerabilidades mais comuns é um Stack overflow. Um Stack é uma área da memória usada por uma sub-rotina de programa. Inclui um endereço de retorno, que é o local do programa que chamou a sub-rotina. Um invasor pode usar um buffer overflow para alterar o endereço de retorno, o que lhe permitirá executar um código arbitrário no sistema.

Os ataques de Buffer Overflow são mitigados em hardwares e SOs operacionais modernos por meio de controles sobre a aleatoriedade do layout do espaço do endereço (Address Space Layout Randomization, ASLR) e de prevenção contra a execução de dados (Data Execution Prevention, DEP).



Ataques a Aplicativos WEB:

- **Cross-Site Scripting(XSS):** O Cross-Site Scripting (XSS) é um tipo de vulnerabilidade em aplicações web que permite a injeção de scripts maliciosos em páginas vistas por outros usuários. Esses scripts podem roubar cookies, redirecionar vítimas para sites falsos, ou realizar ações em nome do usuário sem seu consentimento. O XSS ocorre quando a aplicação não valida ou sanitiza corretamente entradas de usuários antes de exibi-las.
- **SQL Injection:** O SQL Injection é uma vulnerabilidade que permite a um atacante injetar comandos SQL maliciosos em consultas de um banco de dados. Isso acontece quando a aplicação não valida ou sanitiza corretamente as entradas do usuário. Com essa técnica, um invasor pode obter, modificar ou até deletar dados sensíveis, comprometendo a segurança do sistema.

Comandos SQL:

- **SELECT: Selecionar dados;**

- **INSERT: Inserir dados;**
- **DELETE: Deletar dados;**
- **UPDATE: Atualizar dados;**

Considerando um formulário Web que deve receber um nome como entrada, ao usuário digitar o nome Bob, o aplicativo realizará a seguinte consulta:

SELECT*FROM tbl_user WHERE username='Bob'

SELECT*FROM tbl_user WHERE username= " or 1=1#

Ataques a aplicativos baseados em nuvem:

Nuvem como plataforma de ataque: Invasores podem usar plataformas em nuvem para espalhar phishing e malware. Podem usar serviços em nuvem para hospedar arquivos maliciosos e destribuí-los através de e-mails de phishing.

Cloud Access Security Brokers (CASB): É um software de gerenciamento corporativo projetado para mediar o acesso de usuários a serviços em nuvem em todos os tipos de dispositivos.

Dentre os fornecedores CASB estão:

Blue Coat, Skyhigh Security, Forcepoint, Microsoft Cloud App Security, Cisco Cloudclock.

Os CASBs fornecem visibilidade sobre como os clientes e outros nós da rede estão usando serviços em nuvem.

Cadeia de suprimentos: As vulnerabilidades da cadeia de suprimentos de software referem-se aos possíveis **riscos** e **fragilidades** introduzidos nos produtos de software durante o ciclo de vida de desenvolvimento, distribuição e manutenção. Essa cadeia apresenta vários estágios desde a codificação inicial até a implantação para o usuário final, e inclui diversos fornecedores de serviços, hardware e de software.

- **Lista de Materiais de software (SBOM):** É um inventário completo de todos os componentes de um produto de software. O OWASP Dependency-Check é uma ferramenta de análise de composição de software (SCA) que identifica as dependências do projeto e verifica se há alguma vulnerabilidade conhecida e divulgada publicamente associada a elas.

Métodos de identificação de vulnerabilidades física

Varredura de vulnerabilidades: Ferramentas de varredura de vulnerabilidades como OpenVAS e Nessus são instrumentos populares que oferecem uma ampla gama de recursos desenvolvidos para analisar equipamentos de rede, Sos, bancos de dados, conformidade com patches, configuração e muitos outros sistemas.

Varredura credenciada e não credenciada:

- **Varredura não credenciada:** É feita direcionando pacotes de teste a um host sem estar conectado ao aplicativo ou sistema operacional. A visualização é aquela que o host expões a um user sem privilégios na rede.
- **Varredura credenciada:** Recebe uma conta de usuário com direitos de acesso a vários hosts, além de outras permissões necessárias para as rotinas de teste.

Esse tipo de teste permite uma análise muito mais aprofundada, principalmente para detectar quando aplicativos ou definições de segurança estiverem configurados incorretamente.

Scanners de aplicativos para computador e web: A varredura de vulnerabilidades de aplicativos apresenta um método especializado de varredura de vulnerabilidades para identificar pontos fracos de aplicativos de software. Isso inclui análise estática (Revisando códigos do aplicativo sem executá-lo) e análise dinâmica (testando aplicativos em execução), que podem identificar problemas como entradas não validadas, falhas nos controles de acesso e vulnerabilidades de injeção de SQL.

Scanners de aplicativos para computador e web:

- **Monitoramento de pacotes:** Está associado à identificação de vulnerabilidades por rastrear e avaliar a segurança de pacotes de software, bibliotecas e dependências de terceiros usados em uma organização para garantir que estejam atualizados e livres de vulnerabilidades conhecidas que agentes mal-intencionados possam explorar.

Outros métodos de avaliação de vulnerabilidades:

- **Testes de penetração:** São uma abordagem mais agressiva para o gerenciamento de vulnerabilidades. Hackers éticos tentam violar a segurança de uma organização, explorando vulnerabilidades para demonstrar seu impacto potencial. Podendo ser **de ambiente desconhecido, parcialmente conhecido ou conhecido. (Black, Grey, White Box).**

Vulnerabilidades e exposições comuns: Um scanner automatizado precisar ser mantido atualizado com informações sobre vulnerabilidades conhecidas. Essas informações são geralmente chamadas de feed de vulnerabilidades, embora a ferramenta Nessus se refira a eles como Plug-ins, e o OpenVAS se refira como testes de vulnerabilidade de rede (NVTs). Esse feed muitas vezes é um elemento importante dos modelos comerciais dos fornecedores de ferramentas de varredura, pois as atualizações mais recentes exigem uma assinatura válida.

Os feeds usam identificadores comuns para facilitar o compartilhamento de dados de inteligência em diferentes plataformas. Muitos Scanners de vulnerabilidade usam o Security Content Automation Protocol (SCAP) para obter atualizações de feed ou de plug-ins.

CVE: É um dicionário de vulnerabilidades em sistemas operacionais e softwares de aplicativos publicados (cve.mitre.org).

VULNERABILIDADES E EXPOSIÇÕES COMUNS

O dicionário CVE é a principal fonte de dados do National Vulnerability Database (NVD) do NIST (nvd.nist.gov).

O NVD complementa as descrições de CVE com análises adicionais, uma métrica de criticidade calculada usando o Sistema de Pontuação de Vulnerabilidade Comum (CVSS), além de informações de correção.

Pontuação	Descrição
0,1+	Baixo
4.0+	Médio
7,0+	Alto
9.0+	Crítico

Falso Positivo: Refere-se a uma instancia em que um programa de varredura ou outra ferramenta de avaliação identificam incorretamente uma vulnerabilidade.

Por exemplo, uma verificação de vulnerabilidades pode sinalizar uma **porta aberta no firewall** como um risco de segurança com base no seu uso conhecido por um determinado malware. No entanto, se essa porta não estiver aberta no sistema, serão desperdiçados tempo e esforço ao investigar o problema. Se uma varredura de vulnerabilidades gerar demasiados falsos-positivos, corre-se o risco de se desconsiderar as varreduras no geral, podendo ocasionar problemas maiores.

Falso Negativo: São quando possíveis vulnerabilidades não são detectadas em uma verificação. Esse risco pode ser evitado executando varreduras periodicamente e utilizando programas de varredura de diferentes fornecedores.

Resposta e correção de vulnerabilidades:

- **Validação:** Validar a correção de vulnerabilidades garante que as ações de correção tenham sido implementadas corretamente e funcionem como planejado.
- **Geração de Relatórios:** É um aspecto essencial do gerenciamento de vulnerabilidades e fundamental para manter a postura de segurança cibernética de uma organização. Um relatório destaca as vulnerabilidades e as classifica de acordo com sua gravidade e impacto potencial nos ativos da organização.

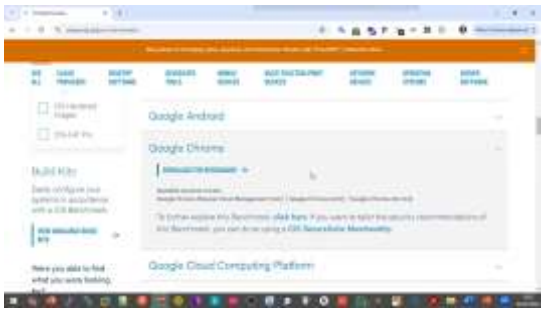
Linhas de base de segurança da rede

Guias de configuração segura e benchmarks

Uma linha de base segura é uma coleção de configurações padrão para dispositivos de rede, softwares, patches e atualizações, controles de acesso, registros em log, monitoramento, políticas de senha, criptografia, proteção de endpoint e muitos outros. As linhas de base seguras melhoram a segurança, a capacidade de gerenciamento e a eficiência operacional da tecnologia da informação, estabelecendo regras e

procedimentos uniformes e centralizados em relação à configuração e proteção do ambiente.

Os benchmarks do CIS são um recurso importante para as práticas recomendadas de configuração segura.



Ferramentas de gerenciamento de configuração como Puppet, Chef, Ansible e Group Policy da Microsoft permitem que as organizações automatizem a implantação de configurações de linha de base seguras em diversos sistemas.

Para monitorar a conformidade, ferramentas que atendem ao SCAP, como **OpenSCAP**, podem avaliar e verificar a adesão do sistema à linha de base.

O verificador de Conformidade com o **SCAP (SCC)** é uma ferramenta mantida pelo **DISA** que é usada para medir a conformidade com as linhas de base do **STIG**.

Conceitos de hardening: Hardening descreve os métodos para aumentar a segurança de um dispositivo alterando sua configuração padrão, geralmente implementando as recomendações nas linhas de base seguras publicadas.

Considerações sobre instalação de rede wireless: Referem-se aos fatores que garantem a boa disponibilidade de access points Wi-Fi autorizados.

- **Posicionamento de Wireless Access Points (WAP):** Uma rede sem fio baseada em infraestrutura compreende um ou mais wireless access points, cada um conectado a uma rede com fio. Os access points encaminham o trafego de ida e volta da rede comutada com fio. Cada **WAP** é identificado por seu endereço **MAC**, também conhecido como seu Basic Service Set Identifier, **BSSID**. Cada rede wireless é identificada por seu nome ou identificador de conjunto de serviço (Service Set Identifier, SSID).
- **Interferencia de co-canal (CCI) –** Quando dois WAPs próximos usam o mesmo canal, eles competem pela largura de banda dentro desse canal, Á medida que os sinais colidem e têm que ser retransmitidos.
- **Interferência de canal adjacente (ACI):** Os canais tem apenas ~5 MHz de espaçamento, mas o Wi-Fi requer 20 MHz de espaço no canal. Quando os canais selecionados para WAPs não são espaçados de forma limpa, o padrão de interferência cria um número significativo de erros e perde de largura de banda.

Por exemplo, se dois pontos de acesso dentro do intervalo um do outro forem configurados na faixa de 2,4 GHz com os canais 1 e 6, eles não se sobrepõem. Se um terceiro ponto de acesso for adicionado usando o canal 3, ele usará parte do espectro usado pelos outros WAPs, e todas as três redes sofrerão interferência

Criptografia Wireless: Uma rede wireless deve ser configurara com definições de segurança. Sem criptografia qualquer um pode interceptar e ler pacotes que passam pela rede wireless. A primeira versão do acesso Wi-Fi protegido (Wi-Fi Protected Acces, WPA) foi projetada para corrigir vulnerabilidades críticas no padrão de privacidade equivalente com fio (WEP) predecessor. Assim como o **WEP**, a versão 1 do WPA usa cifra de fluxo RC4, mas adiciona um mecanismo chamados protocolo de integridade de chave temporal (TKIP) para torná-la mais forte.

Configuração Wi-FI protegida (WPS) (WPA2): Laçados para facilitar a vida para clientes residenciais. Em geral os dispositivos terão um botão. Pressionalos simultaneamente no access point e no adaptador asscociará os dispositivos usando um **PIN** e, em seguida, associará o adaptador ao ponto de acesso usando **WPA2**.

Acesso Wi-Fi protegido 3 (WPA3): Nem o WEP nem a versão 1 do WPA são considerados seguros o suficiente para uso contínuo. O WPA2 usa a cifra AES com chaves de 128bits, no lugar do RC4 e o CCMP substitui o TKIP. O CCMP fornece criptografia autenticada, que é projetada para dificultar os replay attacks.

Métodos de Autenticação de Wi-Fi:

- **Autenticação pessoal no WPA3:** Embora o **WPA3** ainda use uma senha para autenticar estações no modo pessoal, ele altera o método que esse segredo usa para combinar com as chaves de sessão. O esquema usado é chamado de troca de chaves autenticada por senha (PAKE). No WPA3, o protocolo de autenticação simultânea de iguais (SAE) substitui o handshake de 4 vias, que foi considerado vulnerável a vários ataques.
- **Serviço RADIUS (Remote Authentication Dial-in User Service):** Esse padrão é publicado como um padrão da Internet. Existem vários produtos RADIUS para servidor e cliente.
  O dispositivo NAS (cliente RADIUS) é configurado com o endereço IP do servidor RADIUS e com um segredo compartilhado. Isso permite que o cliente seja autenticado no servidor. Lembre-se de que o cliente é o dispositivo de acesso(Switch, access point ou gateway VPN), não o computador ou notebook do usuário. Opcionalmente o NAS pode usar o RADIUS para contabilidade (registro). A contabilidade usa a porta 1813. O servidor de contabilidade pode ser diferente do servidor de autenticação.

Rogue Access Points and Evil Twins: Um ponto de acesso desonesto é aquele que foi instalado na rede sem autorização com intenção maliciosa ou não. **É vital pesquisar periodicamente o site para detectar WAPs desonestos**. Um usuário mal-intencionado pode configurar tal ponto de acesso com algo tão básico como um smartphone com recursos de amarração, e um usuário não-malicioso poderia habilitar tal ponto de acesso por acidente. Se conectado a uma LAN sem segurança, um WAP não autorizado cria um backdoor através do qual atacar a rede.

Um WAP Rogue também pode ser usado para capturar tentativas de login do usuário, permitir ataques man-in-the-middle e permitir acesso a informações privadas. **Um WAP desonesto disfarçado de legítimos é chamado de Evil Twin.**

Desassociação e replay de ataques: O uso de um WAP desonesto pode ser associado a um ataque de desautenticação. Isso envia um fluxo de quadros falsificados para fazer com que um cliente desautentique de um WAP.

Controle de acesso à rede (NAC): Não apenas autentica usuários e dispositivos antes de lhes permitir acesso à rede, mas também verifica e impõe conformidade com as políticas de segurança estabelecidas. Ele avalia a versão do SO, o nível do patch, status do antivírus ou a presença de software de segurança específico. Ele garante que os dispositivos atendam um conjunto mínimo de padrões de segurança antes de receber acesso à rede.

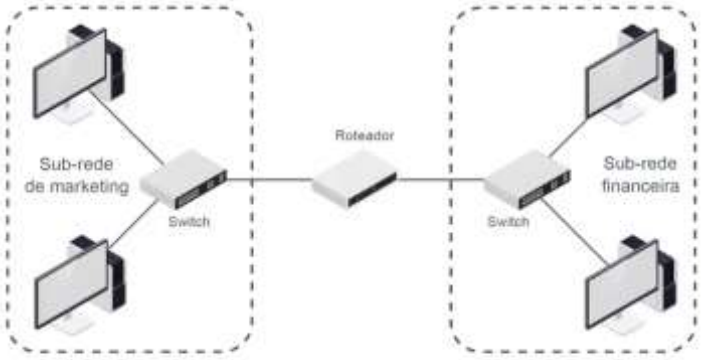
Avaliar os recursos de segurança do endpoint (computadores)

Implementar a segurança do endpoint

Hardening de Endpoints: Descreve a alteração de um SO ou aplicativo para que ele funcione com segurança. Os parâmetros de práticas recomendadas desempenham um papel crítico no hardening de dispositivos: eles fornecem um conjunto padrão de diretrizes ou listas de conferência para configurar dispositivos com segurança.

Proteção de Endpoints: O objetivo do hardening de dispositivos é aprimorar a segurança de um sistema, reduzindo as possíveis vulnerabilidades que uma entidade mal-intencionada pode explorar.

- **Segmentação:** Reduz o impacto potencial de um incidente de segurança cibernética, isolando os sistemas e limitando a disseminação de um ataque ou infecção por malware. Além disso, a segmentação permite um controle mais detalhado sobre o acesso aos dados para garantir que usuários, dispositivos e aplicativos tenham acesso apenas às informações necessárias para suas tarefas específicas, o que aumenta a proteção e a privacidade dos dados.



Uma rede segmentada que mostra as sub-redes de marketing e finanças e o posicionamento dos dispositivos da rede. O tráfego entre as duas redes é controlado pelo roteador. (Imagens © 123RF.com.)

- **Isolamento:** Refere-se à segregação de dispositivos individuais dentro de uma rede para limitar sua interação com outros dispositivos e sistemas. Isso visa aprimorar a proteção dos endpoints impedindo a disseminação lateral de ameaças, caso um dispositivo seja comprometido.
  Essa abordagem é particularmente útil para ameaças como worms ou ransomware, que se propagam rapidamente pelas redes.

- **Antivírus e Antimalware:** A primeira geração de softwares antivírus e caracterizada pela detecção e prevenção baseadas em **assinatura** de vírus conhecidos. Um antivírus agora executa a detecção generalizada de malware, não apenas vírus e worm, mas também cavalos de troia, spyware, PUPs, cryptjackers etc. Embora os antivírus continuem sendo importantes, a detecção baseada em assinatura é amplamente reconhecida como insuficiente para a **prevenção de violações de dados.**
- **Criptografia de Disco:** Criptografia completa do disco (FDE) significa que todo o conteúdo da unidade (ou volume), incluindo arquivos do sistema e pastas, é criptografado. A criptografia de disco pode ser aplicada em HDDs e SSDs. Uma das suas desvantagens é o **desempenho reduzido**.
- **Gerenciamento de patches:** No Windows esse processo é feito por meio do **Windows Update** e no Linux pode ser configurado via **yum-cron** ou **apt unattended-upgrades**. O processo pode ser facilitado por pacotes como System Center Configuration Manager (**SSCM**)/**Endpoint Manager** da Microsoft.

Proteção Avançada de Endpoints:

- **Detecção e resposta de endpoint (EDR) e detecção e resposta estendidas (XDR):** Um EDR busca fornecer visibilidade em tempo real e histórica do comprometimento, conter o malware em um único host e facilitar a remediação do host para seu estado original. O XDR **amplia** o EDR, fornecendo recursos mais amplos de visibilidade e resposta, pois estende a proteção para além dos endpoints, incorporando dados da rede, plataformas de nuvem, gateway de e-mail, firewall e etc.
- **Detecção/prevenção de intrusão baseada em host (HIDS/HIPS):** A detecção de intrusão baseada em host (HIDS) e a prevenção de intrusão baseada em host (HIPS) descrevem ferramentas de software que monitoram e protegem hosts individuais, como computadores ou servidores, contra o acesso não autorizado e atividades mal-intencionadas. Os sistemas de HIDS e HIPS usam detecção baseada em assinatura, detecção de anomalias e análise de comportamento para identificar atividades suspeitas.
  Um dos principais recursos do HIDS é o monitoramento de integridade de aplicativos (FIM). Ele audita os principais arquivos do sistema para garantir que correspondam às versões autorizadas.
  - Tripwire e o OSSEC são exemplos de ferramentas multiplataforma com opções pra proteger uma ampla gama de aplicativos.
- **Análise de comportamento do usuário (UBA)/Análise de comportamento do usuário e da entidade (UEBA):** A UBA, também conhecida como UEBA, é uma abordagem de segurança cibernética baseada no monitoramento e na análise do comportamento dos usuários dentro de uma organização para detectar anomalias indicativas de possíveis ameaças, como ameaças internas, contas comprometidas ou fraude. A UBA utiliza **machine learning, ciência de dados e técnica de análise estatística** para estabelecer um perfil de linha de base para os usuários e entidades de uma organização.

Configuração de Endpoints:

- **Controle de acesso:** Refere-se à regulamentação e ao gerenciamento das permissões concedidas a indivíduos, softwares, sistemas e redes para acesso a recursos ou informações. Os controles de acesso garantem que apenas entidades autorizadas (usuários, dispositivos ou software) possam executar ações especificas ou acessar determinados dados, enquanto o acesso a entidades não autorizadas é negado.
- **Princípio do privilégio mínimo (PoLP):** É fundamental para melhorar a proteção de endpoints e minimizar o risco de problemas de segurança.
  Por exemplo, no Linux existem 3 permissões básicas:
  - Read: Capacidade de acessar e visualizar conteúdo de arquivos ou listar conteúdo no diretório;
  - Write: Capacidade de salvar alterações em um arquivo, ou criar, renomear e excluir arquivos em um diretório.
  - Execute: Capacidade de executar um script, programa ou a capacidade de acessar um diretório, executar um arquivo a partir desse diretório ou executar uma tarefa nesse diretório, como pesquisa de arquivos.
  - 
  - d rwx r-x r-x home é a mesma coisa que chmod g+w, o-x home (adicionar permissão de w ao group (+) e remover execução de outros users (-))
  - chmod u=rwx,g=rx,o=rx home é igual chmod 755 home (u tem as 3 permissões(7), group tem r e x (5) e outros users tbm 5)
- **SELinux:** Permite um controle de permissão mais granular sobre cada processo e objeto do sistema dentro de um sistema operacional, limitando estritamente os recursos que um processo pode acessar e quais operações podem executar. Opera com base em um principio de que se um processo ou usuário não precisa de acesso a recursos para operar, ele será bloqueado para isolar melhor os aplicativos.

Hardening de dispositivos móveis a segurança do endpoint

Técnincas de hardening de dispositivos móveis: A proteção de hardening é fundamental para a segurança cibernética e inclui várias práticas essenciais para proteger os dispositivos contra ameaças e vulnerabilidades, o que inclui controles como atualizações regulares, restrições de acesso, configurações seguras criptografia, bloqueio de tela, controles de acesso à rede e aproveitamento de soluções de gerenciamento de dispositivos móveis (**MDM**) para centralizar o gerenciamento e garantir a conformidade do dispositivo.

- **Modelos de implantação:** São fundamentais pra definir como uma organização usa, gerencia e protege os dispositivos. Ele afeta tudo, desde a experiencia do usuário até o nível de controle da organização sobre o dispositivo.

    - **Bring your own device (BYOD):** Significa que o dispositivo móvel pertence ao funcionário.
    - **Corporate owned, business Only (COBO)** Significa que o dispositivo pertence à organização e só pode ser usado para negócios da empresa.
    - **Corporate owned, personally enabled (COPE):** SIgnifica que o dispositivo é escolhido e fornecido pela organização e permanece sua propriedade. O usuário pode usá-o ara acessar contas pessoais de email, redes sociais e navegação pessoal na web.
    - **Choose your own device (CYOD):** Semelhante ao COPE, exceto que o funcionário tem a opção de escolher os dispositivos de uma lista preestabelecida.

Criptografia completa do dispositivo e mídia externa: Todas as versões de SO para smartphones e tablets, exceto as mais antigas, oferecem criptografia completa de dispositivo.

- IOS e Android: No IOS, a criptografia de proteção de dados é ativada automaticamente quando você configura um bloqueio por senha no dispositivo. No Android há grandes diferenças de uma versão para outra. A partir do Android 10, não há criptografia de disco completa, pois é considerada prejudicial ao desempenho.

Serviços de Localização:

- **Delimitação Geográfica e aplicação de restrições a câmeras e microfones: Geofencing** é a prática de criar um limite virtual com base na geografia real. Ela pode ser uma ferramenta útil no que diz respeito ao uso de funções como câmera ou vídeo ou à aplicação de autenticação com reconhecimento de contexto.

Métodos de conexão Wi-Fi e tethering: Os dispositivos móveis geralmente são configurados para usar uma conexão Wi-Fi para dados, se disponível. Se o usuário estabelecer uma conexão com uma rede corporativa que usa uma forte segurança WPA3, há um risco bastante baixo de espionagem ou ataques de invasores intermediários.

- **Redes de área pessoal (PANs):** Elas permitem a conectividade entre um dispositivo móvel e periféricos. Também é possível estabelecer redes ad hoc (ou ponto a ponto) entre dispositivos móveis ou entre disp móveis e outros dispositivos de computação.
- **Tethering e access points:** Um smartphone pode compartilhar sua conexão web com outro dispositivo, como um pc. Quando essa conexão é compartilhada por Wi-Fi com vários outros dispositivos, o smartphone é descrito como um access point (hotspot). Quando a conexão é compartilhada ao conectar o smartphone a um PC com um cabo USB ou com um único PC via Bluetooth, também é conhecido como tethering.

Ameaças de conexão Bluetooth:

- **Bluejacking:** Um tipo de spam em que alguém envia uma mensagem de texto, ou imagem ou vídeo não solicitada ou um vCard(detalhes de contato). Também pode ser vetor de malware, como cavalo de troia.

- **Bluesnarfing:** Refere-se ao uso de uma vulnerabilidade no Bluetooth para roubar informações do telefone de outra pessoa.

Riscos do NFC: Não possibilita criptografia, portanto, espionagem e os ataques intermediários On-Path são possíveis se o invasor conseguir encontrar alguma maneira de interceptar a comunicação e os serviços de software. Tres principais ex: Apple Pay, Google Pay, Samsung Pay.

Aprimorar recursos de segurança de aplicativos

Parâmetros de referência para a segurança dos protocolos de aplicativos

Protocolos Seguros:

- **HTTPS:** Para tráfego seguro na WEB.
- **SMTPS e IMAPS:** Proteger protocolos de email tradicionais.
- **SFTP ou FTPS:** Proteger transferência de arquivos.
- **LDAPS:** Para acesso seguro a diretórios.
- **DNSSEC:** Para consultas DNS seguras.

Esses protocolos garantem que as mensagens confidenciais sejam transmitidas com segurança.

Protocolos **inseguros**, como **HTTP** e **Telnet**, transmitem informações em formato de **texto não criptografado,** o que significa que qualquer pessoa que acesse os pacotes de dados pode ler quaisquer dados interceptados em uma rede. Por outro lado, os seguros, como **HTTPS** e **SSH** usam criptografia para proteger os dados transmitidos e melhorar a segurança. Uso do HTTPS é crucial para impedir que informações confidenciais do usuário, como credenciais de login e dados inseridos em campos de formulário, sejam roubadas ao usar páginas Web.

A camada de soquetes seguros (SSL) foi desenvolvida pela Netscape para resolver a falta de segurança em HTTP. Provou ser muito popular e logo adotada como um padrão chamado de TLS. Ela é normalmente usada com o HTTP, mas pode ser usada com outros protocolos, como a VPN.

Pra implementar o TLS, um servidor recebe um certificado digital assinado por uma autoridade de certificação (CA) confiável.

Segurança da Camada de Transporte (TLS):

- **Versões de SSL/TLS:** Embora a sigla SSL ainda seja usada, as versões de segurança da TLS são as únicas seguras de usar. Um servidor pode fornecer suporte para clientes legados, mas isso é menos seguro. Por exemplo, um servidor TLS 1.2 pode ser configurado para permitir que clientes façam downgrade para TLS 1.1 ou 1.0 ou mesmo SSL 3.0 se não suportarem TLS 1.2.

Um ataque de **Downgrade** é quando um ataque on-path tenta forçar o uso de um conjunto de cifras e versão SSL/TLS fracas. A versão 1.3 do TLS foi aprovada em 2018 e combate o ataque de downgrade, impedindo o uso de versões anteriores.

Serviços de diretório seguro: Um diretório de rede lista os sujeitos e objetos (como diretórios e arquivos) disponíveis na rede, além das permissões que os sujeitos tem sobre os objetos. Um diretório facilita a autenticação e a autorização, e é fundamental que ele seja mantido como um serviço altamente seguro. A maioria dos serviços de diretório é baseada no Lightweight Directory Access Protocol (**LDAP**), executado na **porta 389**.

A autenticação, conhecida como associação ao servidor, pode ser implementada das seguintes maneiras:

- **Sem autenticação:** É concedido acesso anônimo ao diretório.
- **Simple Bind (associação simples):** O cliente deve fornecer nome diferenciado (Distinguished Name, DN) e senha, que são passados como simples.
- **Simple Authentication and Security Layer, SASL (autenticação simples e camada de segurança):** O cliente e o servidor negociam o uso de um mecanismo de autenticação suportado por ambos, como **Kerberos**. O **comando STARTTLS** pode ser usado para exigir criptografia e integridade da mensagem. Este é o mecanismo preferencial para implementação do LDAP pelo AD da Microsoft.
- **LDAP Secure (LDAPS):** Significa que o servidor é instalado com um certificado digital, que é usado para configurar um túnel seguro para a troca de credenciais do usuário. O **LDAPS usa a porta 636.**

Segurança com protocolo de gerenciamento de rede simples (SNMP): É uma estrutura amplamente utilizada para gerenciamento e monitoramento. O SNMP consiste em um monitor SNMP e agentes.

- O agente é um processo (software ou firmware) em execução em um switch, roteador, servidor ou outro dispositivo de rede compatível com SNMP.
- Esse agente mantem um banco de dados chamado de base de informação de gerenciamento (MIB), que mantem estatísticas em relação a atividade do dispositivo.
- Consultas do dispositivo ocorrem pela **porta 161 (UDP)**; as interceptações são comunicadas pela porta **162 (também UDP).**

Serviços de transferência de arquivos: Um servidor de **FTP** é configurado normalmente com vários diretórios públicos, hospedando arquivos e contas de usuário.

- **SSH FTP (SFTP) e FTP sobre SSL (FTPS):** O Secure File Transfer Protocol (SFTP) resolve os problemas de privacidade e integridade do FTP criptografando a autenticação e a transferência de dados entre cliente e servidor. No SFTP, um link seguro é criado entre o cliente e o servidor usando o SSH na porta **TCP 22**.
  Outro meio de proteger o FTP é usar o protocolo de segurança da conexão SSL/TLS. Há dois modos de fazer isso:
- **TLS explícito (FTPES):** Usa o **comando AUTH TLS** para atualizar uma conexão estabelecida na **porta 21** de não segura para segura. Isso protege as credenciais de autenticação.
- **TLS implícito (FTPS):** Negocia um túnel **SSL/TLS**. Este modo usa a porta segura 990 para a conexão de controle.

Serviços de email: Usam dois tipos de protocolos:

- O SMTP que especifica como o email é enviado de um sistema para outro
- Um protocolo de caixa de correio armazena mensagens para os usuários e permite que eles baixem para computadores clientes ou as gerenciem no servidor.

Secure SMTP (SMTPS): Para entregar uma mensagem, o servidor SMTP do remetente descobre o endereço IP do servidor SMTP do destinatário com base no nome de domínio contido no endereço de email.

As comunicações SMTP podem ser protegidas usando TLS e seu funcionamento é muito parecido com o HTTPS com um certificado no servidor SMTP. O SMTO usa a TLS de duas maneiras:

- **STARTTLS**: Este comando atualiza uma conexão insegura existente para usar o TLS. Também é denominado TLS explícito ou TLS oportunista.
- **SMTPS**: Estabelece uma conexão segura antes de quaisquer comandos SMTP (HELO, por exemplo) sejam trocados. Também denominado TLS implícito.

  O método **STARTTLS** é mais **amplamente implementado** do que **SMTPS**. As configurações típicas de SMTP usam as seguintes portas e serviços seguros:
- Porta 25: Usada para retransmissão de mensagem a servidores SMTP ou agentes de transferência de mensagens (MTA): Message Transfer Agents;
- Porta 587: Usada por clientes de email (MTA) para enviar mensagens de entrega por um servidor SMTP;
- Porta 465: Usada por alguns provedores e clientes de email para envio de mensagens por TLS implícito (SMTPS), embora esse uso agora seja obsoleto pela documentação padronizada.

Secure POP (POP3S): O Post Office Protocol(POP3) é um protocolo de caixa de correio projetado para **armazenar as mensagens entregues pelo SMTP** em um servidor. Quando o cliente se conecta à caixa de correio, o POP3 baixa as mensagens para o cliente de email do destinatário. Um aplicativo cliente que usa o POP3, como o Microsoft Outlook ou Mozilla Thunderbird, estabelece uma conexão TCP com o servidor POP3 pela **porta 110.**

Secure IMAP (IMAPS): Em comparação com o POP3, ele aceita conexões permanentes a um servidor e conecta vários clientes à mesma caixa de correio simultaneamente. Os clientes se **conectam ao IMAP pela porta TCP 143**. No **IMAPS (IMAP com camada SSL/TLS), a porta é a TCP 993**.

Três tecnologias se destacaram como essenciais para verificar autenticidade dos emails e evitar phishing e spam. **Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) e Domain-based Message Authentication, Reporting & Conformance (DMARC).**

- **SPF:** É um método de autenticação de email que ajuda a **detectar** e **evitar** falsificações do endereço do remetente comumente usadas em email de phishing e spam. O SPF funciona verificando o endereço IP do remetente em relação a uma

lista de endereços IP de envio autorizado publicados nos registros TXT do DNS do domínio de remetente do email.

- **A DomainKeys Identified Mail (DKIM):** Utiliza recursos de criptografia para habilitar a verificação de email, permitindo que o remetente assine emails usando uma assinatura digital. O servidor de email de recebimento usa um resgitro DKIM no registro DNS do remetente para verificar a assinatura e a integridade do email.
- **A Domain-based Message Authenticatio, Reporting & Conformance (DMARC):** Usa os resultados das verificações SPF e DKIM para definir regras para lidar com mensagens, como mover mensagens para quarentena ou spam, rejeitá-las imediatamente ou marcá-las com tags. O DMARC também fornece recursos de relatório, dando ao proprietário de um domínio visibilidade sobre quais sistemas estão enviando emails em seu nome, incluindo quaisquer atividades não autorizadas.
  O uso combinado de SPF, DKIM e DMARC aumenta significativamente a segurança dos emails, tornando muito mais difícil para os invasores se passarem por domínios confiáveis, o que é uma das táticas mais comuns usadas em **ataques** de **phishing** e **spam**.

Prevenção contra perda de dados por email: Regulamentos como **GDPR**, **HIPAA** e **PCI DSS** impõem requisitos rigorosos para proteger tipos de dados específicos, com a DLP servindo como um mecanismo fundamental para garantir a conformidade e evitar a transmissão não autorizada de dados.

As tecnologias DLP (Data Loss Prevention) **impedem o compartilhamento ou a divulgação não autorizada de informações confidenciais**. As políticas DLP são essenciais para monitorar e controlar o conteúdo usado em plataformas de comunicação, como o email.

Filtragem de DNS: É uma técnica que bloqueia ou permite o acesso a sites específicos controlando a resolução de nomes de domínio em endereços IP.

Implementação da filtragem DNS: OpenDNS da Cisco, Quad9 ou CleanBrowsing.

Alguns softwares de **código aberto** como **Pi-hole** e **Adguard**.

Segurança de DNS: Para garantir sua segurança em uma rede privada, os servidores DNS locais devem aceitar apenas consultas recursivas de hosts locais e não da internet.

Muitos serviços de DNS são executados no **BIND** (Berkley Internet Name Domain), distribuído pelo Internet Systems Consortium (isc.org). O mesmo conselho geral se aplica a outros softwares de servidor de **DNS**, como o programa da Microsoft.

Filtragem de DNS: O rastreamento de DNS consiste em obter informações sobre uma rede privada usando o servidor de DNS dela para, em seguida, executar uma transferência de zona para um DNS mal-intencionado. Opcionalmente, o rastreamento obtém essas informações simplesmente consultando o serviço de DNS por meio de uma ferramenta como o **nslookup** ou **dig**.

- **As extensões de segurança do DNS (DNSSEC):** ajudam a atenuar ataques de falsificação e adulteração por meio de um processo de validação para respostas de DNS.

Técnicas de codificação seguras:

Validação de entrada: É uma técnica de proteção essencial usada no desenvolvimento de softwares e da web que trata da questão da entrada não confiável. Através da entrada não confiável, o atacante pode fornecer dados especificamente criados para um aplicativo a fim de manipular seu comportamento. (Ataques de injeção)

Cookies Seguros: Cookies são pequenos fragmentos de dados armazenados em um computador por um navegador web ao acessar um site. Eles mantem os estados da sessão, lembram as preferencias do usuário e rastreiam o comportamento do usuário e outras configurações. Os cookies podem ficar vulneráveis se não forem devidamente protegidos, levando a ataques como sequestro de sessão e cross-site-scripting.

Para implementar cookies seguros, os devs devem seguir certos princípios bem documentados: por exemplo, usar o atributo "**Secure**" para todos os cookies, de modo a garantir que eles sejam enviados apenas por conxões HTTPS e protegidos contra interceptações; Usar atributo "**HttpOnly**" para impedir que os scripts do lado do cliente acessem cookies e proteger contra ataques de scripts entre sites; e usar atributo "**SameSite**" para limitar quando os cookies são enviados a fim de mitigar ataques de falsificação de solicitações entre sites.

Análise do código estático: É uma prática essencial de desenvolvimento de software. Envolve examinar o código-fonte para identificar possíveis vulnerabilidades, erros e práticas de codificação irregulares antes que o programa seja finalizado. Ao examinar o código em um estado "estático", os devs conseguem detectar e corrigir problemas no incio do ciclo de vida do desenvolvimento. As práticas de segurança da aplicativos também exigem testes de segurança de aplicativos estáticos e dinâmicos (SAST).

Ferramentas de análise de código estático:

SonarQube;

Coverity;

Fortify;

Proteção para aplicativos:

- **Tratamento de erros:** Um aplicativo bem elaborado deve ser capaz de lidar com erros e exceções sem problemas. Isso significa que ele funcionará de forma controlada se algo imprevisível acontecer. O ideal é que o programador tenha escrito um gerenciador de execuções estruturado (Structured exception handler SEH) para determinar o que o aplicativo deve fazer.
  Um exemplo de um gerenciador de exceções mal feito é o bug **Apple GoTo**.

Criação de Sandbox para software: É um mecanismo de segurança usado no desenvolvimento e operação de softwares para isolar os processos em execução ou impedi-los de acessar o sistema em que estão sendo executados. **É um recurso de proteção criado para controlar um programa de modo que ele funcione com acesso altamente restrito.** Essa estratégia de contenção reduz o impacto em potencial de softwares mal-intencionados ou com mau funcionamento.

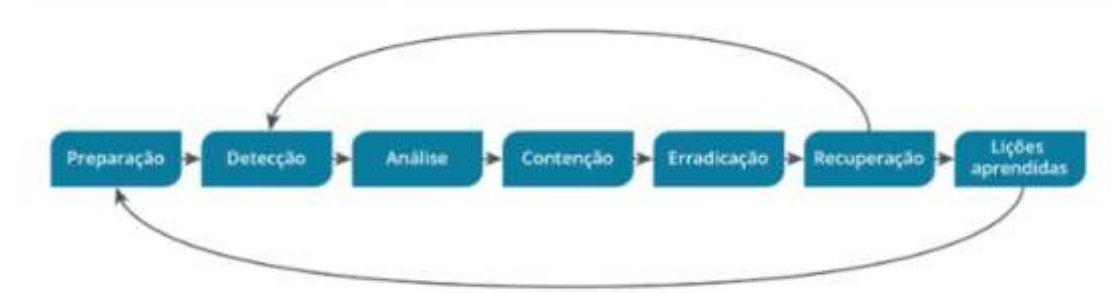
Explicar os conceitos de monitoramento e resposta a incidentes

Resposta a incidentes

Uma resposta eficaz a incidentes é regida por políticas e procedimentos formais, estabelecendo funções e responsabilidades para uma equipe de respostas de incidentes.

Processos de resposta a incidentes: Um incidente de cibersegurança se refere a uma tentativa de violação (Bem-sucedida ou não) das propriedades de segurança de um ativo, comprometendo sua **confidencialidade**, **integridade** ou **disponibilidade**. A política de resposta a incidentes (IR) define os **recursos**, **processos** e **diretrizes** para **lidar com incidentes de cibersegurança**. O ciclo de vida de resposta da CompTIA é um processo de sete etapas:

- **1. Preparação:** Em primeiro lugar, torna o sistema resiliente a ataques. Isso inclui o Hardening para fortalecer sistemas, elaborar políticas e procedimentos e configurar linhas de comunicação confidenciais. Isso implica também em criar recursos e procedimentos de resposta a incidentes.
- **2. Detecção:** Descobre indícios de atividade do autor de ameaça e indicadores da possível ocorrência de um incidente podem ser gerados a partir de um sistema de intrusão automatizado. Ou então os incidentes podem ser detectados manualmente, por meio de operações de threat hunting, ou relatados por funcionários, clientes ou autoridades policiais.
- **3. Análise:** Determina se um incidente ocorreu e faz uma triagem para avaliar a gravidade com base nos dados relatados como indícios.
- **4. Contenção:** Limita o escopo e a magnitude do incidente. O principal objetivo da resposta a incidentes é proteger os dados, limitando o impacto imediato sobre clientes e parceiros de negócios. Também necessário notificar partes interessadas e identificar outros requisitos da denúncia.
- **5. Erradicação:** Remove a causa e restaura o sistema afetado para um estado seguro ao aplicar definições de configuração seguras e instalar patches após a contenção do incidente.
- **6. Recuperação:** Reintegra o sistema ao processo de negócios original com a causa do incidente erradicada. Esta fase de recuperação pode envolver a restauração de dados a partir do backup e testes de segurança. Os sistemas devem ser monitorados de perto por um determinado período para detectar e evitar qualquer recorrência do ataque. O processo de respotar pode ter que iterar por meio de várias fases de identificação, contenção, erradicação e recuperação para efetuar uma resolução completa.
- **7. Lições Aprendidas:** Analisa o incidente e as respostas para identificar se os procedimentos ou sistemas podem ser melhorados. Também é fundamental documentar o incidente. Os resultados desta fase retroalimentam uma nova fase de preparação no ciclo.



▶ Description

Preparação: É o processo que **estabelece** e **atualiza** as **políticas e os procedimentos** para lidar com violações de segurança. Isso inclui provisionar a equipe e os recursos para implementar essas políticas. Ferramentas como gerenciamento de eventos e informações de segurança (**SIEM**) e orquestração de segurança, automação e resposta (**SOAR**) fornecem painéis de **alerta** e **monitoramento** para gerenciar totalmente as etapas de resposta a incidentes.

- **Plano de Comunicação:** As políticas de resposta a incidentes devem também estabelecer linhas claras de comunicação para relatar incidentes e notificar as partes afetadas à medida que o gerenciamento de um incidente avança.
- **Gerenciamento de partes interessadas:** As partes com informações privilegiadas não devem divulgar nada a partes não confiáveis, intencionalmente ou inadvertidamente.
- **Plano de resposta a incidentes:** O resultado da atividade de preparação é um plano formal de respostas a incidentes (IRP). Ele deve listar os procedimentos, contatos e recursos disponíveis para os agentes de respostas, abrangendo várias categorias de incidentes.

Detecção: É o processo de **correlacionar eventos** de fontes de dados de rede e sistema e determinar se eles são um indicador de um incidente.

Existem vários canais pelos quais os indicadores podem ser registrados:

- Correlacionar eventos em arquivos de log, mensagens de erro, alertas de IDS, alertas de firewall e outras fontes de dados e padrões de comportamento de ameaça conhecidos.
- Identificar desvios das métricas de referência do sistema.
- Inspecionar Manual ou fisicamente o local, as instalações, redes e hosts. A busca proativa de sinais de intrusão é chamada de threat hunting.
- Fazer uma notificação por meio de um funcionário, cliente ou fornecedor.
- Relatar publicamente novas vulnerabilidades ou ameaças por meio de um provedor de sistemas, de um regulador, da mídia ou outra parte externa.

Quando um evento suspeito é detectado, é fundamental que a pessoa apropriada no **CIRT seja notificada**, para que possa lidar com a situação e formular a resposta apropriada. Essa pessoa é chamada de **primeiro agente de resposta**.

Análise: Após o processo de detecção relatar um ou mais indicadores de processo análise, o primeiro agente de resposta investiga os dados para determinar se um incidente genuíno foi identificado e qual o nível de prioridade deve ser atribuído a ele. Por

outro lado, o relatório pode ser categorizado como falso positivo e descartado. A classificação um evento de incidente como true positive geralmente depende da correlação de vários indicadores. Quando um incidente é verificado como um true positive, o próximo objetivo é identificar o tipo de incidente e os dados ou recursos afetados. Isso estabelece a categoria e o impacto do incidente e permite a atribuição de um nível de prioridade.

- **Impacto:** Vários fatores afetam o processo de determinação do impacto:
    - **Integridade dos dados:** O fator mais importante na priorização de incidentes geralmente é o valor dos dados em risco.
    - **Tempo de inatividade:** É o grau em que um incidente interrompe os processos de negócios. Um incidente pode degradar (reduzir desempenho) ou interromper (parar completamente) a disponibilidade de um ativo, sistema ou processo de negócios.
    - **Economia/publicidade:** Tanto a integridade dos dados quanto o tempo de inatividade têm efeitos econômicos importantes de curto e longo prazo. Os custos no curto prazo envolvem resposta a incidentes e oportunidades de negócios perdidas. No longo prazo, danos à reputação e à posição no mercado.
    - **Escopo:** Refere-se ao número de sistemas impactados.
    - **Tempo de detecção:** Pesquisas mostram que mais da metade das violações de dados não são detectadas por semanas ou meses após a invasão, e uma invasão bem-sucedida geralmente consegue violar os dados em poucos minutos. Os sistemas usados para procurar intrusões devem ser minuciosos e a resposta à detecção deve ser rápida.
    - **Tempo de recuperação:** Em alguns incidentes, é necessária uma correção longa, pois as alterações necessárias no sistema são complexas de implementar. Este período de recuperação prolongado deve desencadear um estado de alerta elevado para identificar ataques contínuos ou novos.
- **Categoria:** As categorias e definições de incidentes garantem que todos os membros da equipe de resposta e outros funcionários da organização tenham a mesma compreensão dos significados dos termos, conceitos e descrições. A análise eficaz de incidentes depende da threat intelligence. Essa pesquisa fornece informações sobre táticas, técnicas e procedimentos (TTPs) do invasor. Uma ferramenta fundamental para a pesquisa contra ameaças é a estrutura usada para descrever as etapas de um ataque. Essas etapas são muitas vezes chamadas de **cyber kill chain**.

Análise: Um playbook (manual) é um procedimento operacional padrão orientado por dados para ajudar os analistas a detectar e responder a cenários específicos de ciberameaças. O manual começa com um relatório de um painel de alertas. Em seguida, ele leva o analista a percorrer as etapas de análise, contenção, erradicação, recuperação e lições aprendidas.

Contenção: Após a detecção e a análise, o banco de dados de gerenciamento de incidentes deve ter um registro dos indícios do evento, a natureza do incidente, seu impacto e o investigador responsável pelo gerenciamento do caso. A próxima fase do

gerenciamento de incidentes é determinar uma resposta adequada. Estes são alguns dos problemas complexos enfrentados pelo CIRT:

- Quais danos ou roubos já ocorreram? Quanto mais dano poderia ser causado? Em quanto tempo (controle de perdas)?
- Quais medidas de remediação estão disponíveis? Quais são seus custos e implicações?

As técnicas de contenção podem ser classificadas como estratégias de **isolamento** ou de **segmentação**.

- **Contenção baseada em isolamento:** O isolamento envolve a remoção de um componente afetado de um qualquer ambiente maior que ele se integre: desde a remoção de um servidor da rede depois de ter sido alvo de um ataque de negação de serviço até transferência de um aplicativo para uma sandbox fora dos ambientes do host em que ele geralmente é executado. O isolamento remove qualquer interface entre o sistema afetado e a rede de produção ou a internet.
- **Contenção baseada em segmentação:** É um meio de alcançar o isolamento de um host ou grupo de hosts usando tecnologias e arquitetura de rede. A segmentação usa VLANs, roteamento/sub-redes e listas de controle de acesso (ACLs) de firewall para impedir que um host se comunique fora do segmento protegido. Em vez de isolar completamente os hosts, você pode configurar o segmento protegido como um honeynet ou skinhole e permitir que o invasor continue a receber uma saída filtrada para leva-lo a crer que o ataque está tendo sucesso. Isso facilita a análise dos TTPs do autor das ameaças e, potencialmente, da sua identidade. A atrivuição do ataque a um grupo específico permitirá uma estimativa de capacidade do autor das ameaças.

Erradicação e Recuperação: Após a contenção de um incidente, o processo de erradicação de técnicas e controles de mitigação para remover as ferramentas de intrusão e as alterações não autorizadas de configurações dos sistemas. Quando vestígios de malware, backdoors e contas comprometidas são eliminados, o processo de recuperação garante a restauração de recursos e serviços. Isso significa que os hosts serão totalmente reconfigurados para voltar a operar o fluxo de trabalho de antes do incidente. Uma parte essencial da recuperação é o processo de garantir que o sistema não possa ser comprometido por meio do mesmo vetor de ataque, ou que pelo menos, o mesmo vetor seja monitorado para fornecer aviso prévio de outro ataque.

A erradicação de malwares ou outros mecanismos de intrusão e a recuperação do ataque envolvem várias etapas:

- **1. Reconstituição dos sistemas afetados:** Remover os arquivos ou ferramentas mal intencionadas dos sistemas afetados ou restaurar os sistemas a partir de backups/imagens seguros.
- **2. Reavaliação dos controles de segurança:** Garantir que eles não sejam vulneráveis a outro ataque, sendo o mesmo ou um novo que o invasor pode iniciar por meio das informações obtidas sobre a rede.

- **3. Garanta que as partes afetadas sejam notificadas** e tenham os meios necessários para remediar seus próprios sistemas. Por ex, se as senhas dos clientes forem roubadas, eles devem ser aconselhados a alterar as credenciais de todas as outras.

Lições Aprendidas: O processo de lições aprendidas analisa incidentes de segurança para determinar a causa raiz, se podiam ter sido evitados e como evita-los no futuro. Essa atividade começa com uma reunião em que a equipe analisa o incidente e as respostas. A reunião deve incluir a equipe diretamente envolvida, bem como outros responsáveis por lidar com incidentes não envolvidos no caso, mas que podem fornecer perspectivas externas objetivas. Todos devem contribuir livre e abertamente para a discussão. Essas reuniões devem evitar apontar culpados e se concentrar em melhorar os procedimentos. A liderança deve gerenciar as preocupações disciplinares relacionadas à falha da equipe em seguir os procedimentos estabelecidos separadamente.

Após a reunião deve ser compilado um relatório de lições aprendidas **(lessons learned report – LLR) ou relatório pós-ação (after-action report – AAR).**

O processo de lições aprendidas deve invocar a análise da causa raiz ou o esforço para determinar como o incidente pôde ocorrer. Muitps modelos foram desenvolvidos para estruturar a análise de causa raiz. Um deles é o modelo dos "**Cinco Porquês"**, que começa com uma declaração do problema e em seguida apresenta sucessivas perguntas para detalhar causas raiz.

Teste e treinamento: Eles validam o processo de preparação que a organização como um todo está pronta para executar a resposta a incidentes. Por outro lado, as lições aprendidas podem mostrar que isso não é verdade e identificar uma necessidade de testes e programas de treinamentos adicionais.

Teste: Os procedimentos e ferramentas usados na resposta a incidentes são difíceis de dominar e executar de forma eficaz. Os analistas não devem utilizá-los pela primeira vez no contexto de alta pressão de um incidente real. Os exercícios de teste ajudam a equipe a desenvolver competências e podem ajudar a identificar deficiências nos procedimentos e ferramentas. Testes de cenários específicos de resposta a incidentes podem usar três formatos:

- **Exercício tabletop:** Este é o tipo de teste menos dispendioso, um facilitador apresenta um cenário e os agentes de resposta explicam as medidas que tomariam para identificar, conter e erradicar a ameaça.
- **Passo a passo:** Neste modelo, um facilitador apresenta o cenário como num tabletop, mas os agentes de resposta demonstram na prática as ações que tomariam. Ao contrario de um tabletop, os agentes de resposta realizam ações como executar varreduras e analisar arquivos de amostra, geralmente em versões de sandbox.
- **Simulações:** Trata-se de um exercício coletivo no qual a Red Team tenta realizar uma intrusão, a Blue Team opera os controles de resposta e recuperação e a White Team modera e avalia o exercício. Esse tipo requer investimento e planejamento consideráveis.

Threat Hunting: Utiliza **insights** obtidos na **threat intelligence** para descobrir de forma proativa se há evidências de **TTPs** já presentes na rede ou no sistema. É diferente de um

processo reativo, que só é acionado quando as condições de alerta são relatadas por meio de um sistema de gerenciamento de incidentes. A threat hunting pode fornecer informações úteis para o processo de preparação da resposta a incidentes.

Análise forense digital

Devido processo legal (Due Proccess) e Guarda Legal de Documentos (Legal Hold): Análise forense digital é a prática de **coletar** evidências de sistemas de computadores utilizando um padrão que será aceito em um tribunal. As investigações forenses costumam ser utilizadas para processar crimes decorrentes de ameaças internas, principalmente fraude ou uso de equipamentos.

Devido processo legal: É um termo usado no direito comum dos EUA e do Reino Unido para exigir que as pessoas só sejam condenadas por crimes após a aplicação justa das leis do país. De forma geral, ele pode ser entendido como um conjunto de proteções processuais para garantir um desfecho justo. Este princípio é fundamental para a investigação forense. Se uma investigação de perícia forense for iniciada, é importante que os técnicos e gerentes estejam cientes dos processos que ele usará. Em um julgamento, a defesa tentará explorar qualquer incerteza ou erro relativo à integridade da evidência ou do processo de coleta.

Guarda legal de documentos: Refere-se ao fato de que as informações que podem ser relevantes para um processo judicial devem ser preservadas. As informações sujeitas a guarda legal podem ser definidas pelos órgãos reguladores e isso implica que os sistemas de computador podem ser apreendidos como evidência, o que tem um impacto obvio na rede. Uma empresa sujeita a guarda legal geralmente precisa suspender qualquer exclusão/destruição rotineira de logs e registros eletrônicos.

Aquisição: É o processo de obtenção de uma cópia limpa de dados de um dispositivo apreendido como evidência. Se o sistema de computador ou dispositivo não for de propriedade da empresa, resta a dúvida sobre a validade legal da busca ou apreensão. Isso impacta as políticas de BYOD. Por exemplo, se um funcionário for acusado de fraude, você deve verificar se o equipamento e os dados dele podem ser legalmente retidos em uma busca e apreensão. Qualquer erro pode tornar inadmissível a evidencia obtida a partir da busca.

Ela geralmente é feita usando uma ferramenta para criar uma imagem a partir dos dados mantidos no dispositivo alvo. Uma imagem pode ser adquirida de um armazenamento **volátil** ou **não volátil**. O princípio geral é capturar evidências na ordem de volatilidade, de mais volátil pra menos volátil. O guia de práticas recomendadas da ISOC para coleta e arquivamento de evidências, define a ordem geral da seguinte forma:

1. Registros de CPU e memória em cache;
2. Conteúdo da memória RAM, incluindo tabela de roteamento, cache ARP, tabela de processos, estatísticas do kernel.
3. Dados em dispositivos de armazenamento em massa (HDDs, SSDs e dispositivos de memória flash).
   Caches de memória do sistema, como arquivos de hibernação e espaço de troca/memória virtual.
   Caches de arquivos temporários, como cache do navegador.
   Arquivos e diretórios de usuários, aplicativos e SO.

4. Dados de log e monitoramento remotos.
5. Configuração física e topologia de rede.
6. Mídias de arquivo e documentos impressos.

Aquisição de memória do sistema: A memória do sistema consiste em dados voláteis mantidos em módulos de memória RAM. Volátil significa que os dados são perdidos quando se interrompe a alimentação elétrica. Uma extração de memória do sistema cria um arquivo de imagem que pode ser analisado para identificar os processos em execução, o conteúdo de sistemas de arquivos temporários, dados de registro, conexões de rede, chaves criptográficas, entre outros.

Há vários Ex de ferramentas comerciais para aquisição de memória do sistema para Windows. No Linux, O **Volatility Framework** inclui uma ferramenta para instalar um driver de kernel.

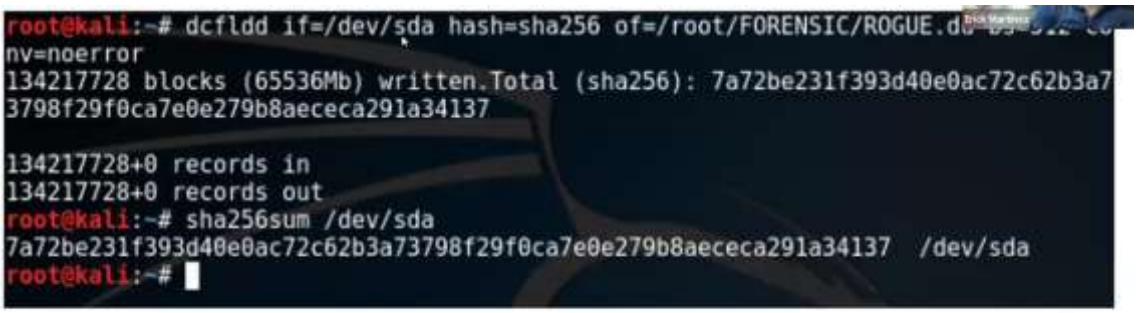
Aquisição de imagem de disco: Refere-se à aquisição de dados de armazenamento não volátil. O armazenamento não volátil inclui HDDs, SSDs, firmware, outros tipos de memória flash (pen drives USB e cartões de memória) e mídia óptica (CD, DVD). A aquisição de disco também captura a instalação do SO se o volume de inicialização for incluído. Existem três estados de dispositivo para aquisição de armazenamento persistente:

- **Aquisição ao vivo:** copiar os dados enquanto o host ainda está em execução. Os dados nos discos reais terão mudado, portanto esse método pode não produzir evidencias legalmente aceitas, além de poder alertar o invasor e dar tempo para que ele realize ações contra a análise forense.
- **Aquisição estática desligando o host:** ao fazer isso, há o risco de o malware detectar o processo de desligamento e executar ações contra a análise forense para tentar remover os vestígios que deixou.
- **Aquisição estática tirando o plugue da tomada:** Interromper a alimentação diretamente na tomada. É mais provável que isso preserve os dispositivos de armazenamento em um estado de limpeza forense, mas há risco de corromper os dados.

Há muitos utilitários de criação de imagens GUI, incluindo alguns pacotes de Ferramentas Forenses. Se nenhuma ferramenta especializada estiver disponível, em um host Linux, o comando dd cria uma cópia de um arquivo de entrada (if=) em um aquivo de saída (of=). No exemplo a seguir, o sda é a unidade fixa:

dd if=/dev/das of=/mnt/usbstick/backup.img

Um fork mais recente do **dd** é o **dcfldd**, que fornece recursos adicionais, como vários arquivos de saída e verificação de correspondência exata.



Uso do dcfldd (uma versão do dd com mais funcionalidades de análise forense criada pelo Departamento de Defesa dos EUA — DoD) e geração de um hash dos dados do disco de origem (sda).

Preservação: É vital que a evidencia coletada na cena do crime esteja em conformidade com uma linha cronológica válida. Informações digitais são suscetíveis à violação, portanto, o acesso à evidencia deve ser rigorosamente controlado. A gravação em vídeo de todo o processo de aquisição de evidencias estabelece a proveniência da evidencia, comprovando que vieram diretamente da cena do crime.

Para obter uma imagem forense válida de um armazenamento não volátil, a ferramenta de captura não pode alterar dados ou metadados (propriedades) no disco ou sistema de arquivos de origem. Um bloqueador de gravação filtra os comandos de gravação no nível do driver e do SO para impedir que quaisquer dados no disco ou volume sejam alterados.

- **Integridade de evidências e não repúdio:** Depois que o disco em questão estiver conectado com segurança à estação de trabalho forense, a aquisição de dados ocorre da seguinte forma:
- 1. É feito um hash criptográfico da mídia do disco usando a função de hash MD5 ou SHA.
- 2. Uma cópia bit a bit da mídia é feita usando um utilitário de geração de imagens.
- 3. Um segundo hash de imagem é feito. Ele deve ser igual ao hash original da mídia.
- 4. Uma cópia da imagem de referência é feita e validada novamente pela soma de verificação. A análise é realizada na cópia.

Cadeia de custódia: Os dispositivos de host e mídia retirados de uma cena de crime devem ser rotulados, ensacados e selados usando sacos capazes de apresentar evidência de violação. Cada evidencia deve ser documentada por um formulário de cadeia de custódia. Cadeia de custódia registra onde, quando e quem coletou as evidências, quem posteriormente as manuseou e onde foram armazenadas. O que estabelece a integridade das evidências.

Fontes de Dados, Painéis e Relatórios: É algo que pode ser submetido a perícia para descobrir indícios. Investigações de análise de forense digital e de resposta a incidentes usam diversas fontes de dados:

- Dados e metadados do sistema de arquivos de dispositivos de mídia e memória do sistema.
- Arquivos de log gerados por dispositivos de rede.
- Tráfego de rede capturado por sensores e/ou quaisquer condições alertáveis ou registráveis indicadas por sistemas de detecção de intrusão.

- Arquivos de log e alertas gerados por scanners de vulnerabilidades baseados em rede.

Painéis (Dashboards): Fornece um console onde é possível atuar para resposta diária a incidentes. Apresenta um resumo das informações extraídas das fontes de dados pertinentes. O painel de um manipulador de incidentes conterá eventos não categorizados que foram atribuídos à sua conta, além de gráficos e tabelas mostrando as principais métricas de status.

Dados de log: São um recurso crítico para investigar incidentes de segurança. Além do formato do log, você também deve considerar a variedade de fontes dos arquivos de log e saber como determinar qual tipo de arquivo oferecerá melhor suporte a qualquer cenário de investigação.

Os hosts de aplicativos do **Windows** podem usar o **Event Viewer** para registrar logs no devido formato do sistema. O **syslog** (**UNIX ou Linux**) fornece um formato aberto, protocolo e software para criação de logs de mensagens de eventos.

- **Logs do Linux:** O registro em log no Linux pode ser implementado de forma diferente para cada distribuição. Algumas usam o syslog ao direcionar mensagens relacionadas a um subsistema específico para um arquivo de texto plano. Outras distribuições usam o Journald como um sistema de registro em log unificado com um formato de arquivo binário ao invés de texto simples. As mensagens do Journald são lidas usando o comando **journalctl**, mas ele pode ser configurado para exportar algumas mensagens para arquivos de texto via syslog.

Alguns dos principais arquivos de log são:

- **/var/log/messages** ou **/var/log/syslog:** armazenam todos os eventos gerados pelo sistema.
- **/var/log/auth.log** (Debian/Ubuntu) ou **/var/log/secure** (RedHat/CentOS/Fedora): registram tentativas de login, uso de privilégios sudo e outros dados de autenticação e autorização.
- **O log do gerenciador de pacotes** (apt, yum ou dnf, dpendendo da distribuição) armazena informações sobre qual software foi instalado e atualizado.

Ferramentas de alerta e monitoramento:

Gerenciamento de eventos e informações de segurança: Softwares projetados para auxiliar no gerenciamento de entradas de dados de segurança e fornecer relatório e alertas são muitas vezes descritos como gerenciamento de eventos e informações de segurança (SIEM). A função principal de uma ferramenta SIEM é coletar e correlacionar dados de sensores de rede e logs de dispositivos/hosts/aplicativos. Ex: Wazuh(de graça).

- **Coleta com e sem agente:** A coleta é como o SIEM ingere dados de eventos de segurança de várias fontes. Existem três tipos principais de coleta de dados de segurança:
    - **Baseada em agente:** Ela demanda instalar um serviço de agente em cada host. À medida que os eventos ocorrem no host, os dados de log são filtrados, agregados e normalizados no host.
    - **Listener/collector:** Em vez de instalar um agente, os hosts podem ser configurados para enviar alterações de log para o servidor SIEM. Um

processo é executado no servidor de gerenciamento para analisar e normalizar cada fonte de log/monitoramento. Esse método geralmente é usado para coletar logs de switches, roteadores e firewalls, pois é improvável que eles estejam compatíveis com agentes.

- **Sensor:** Além dos dados de log, o SIEM pode coletar capturas de pacotes e dados de fluxo de tráfego de detectores. Um sniffer consegue gravar dados de rede usando a funcionalidade de porta espelhada de um switch ou algum tipo de toque na mídia da rede.

Agregação de logs: Diferentemente da coleta, a agregação de logs refere-se à normalização de dados de diferentes fontes para que se tornem consistentes e pesquisáveis. No SIEM, cada fonte de dados de agente, coletor ou sensor precisará do seu próprio analisador para identificar atributos e conteúdos que podem ser mapeados em campos padrão nas ferramentas de relatório e análise do SIEM. Outra função importante é normalizar as diferenças de data/fuso horário em uma única linha do tempo.

Infraestrutura de monitoramento:

- **Monitores de rede:** Diferentemente do monitoramento de tráfego da rede, um monitor de rede coleta dados sobre dispositivos de infraestrutura da rede, como switches, access points, roteadores e firewalls. Isso é usado para **monitorar** o status de carda da CPU/memória, tabelas de estados, capacidade do disco, velocidades/temperatura do ventilador, estatísticas de erro/utilização dos elos da rede e assim por diante. Outra função importante é uma mensagem de heartbeat para indicar a **disponibilidade**. Esses dados podem ser coletados usando o Protocolo de Gerenciamento de Rede Simples (**SNMP**).

Analisar indicadores de atividades mal-intencionadas

Indicadores de ataques de malware

Classificação de Malware:

- **Vírus e worms:** Representam alguns dos primeiros tipos de malware e se espalham sem qualquer autorização do usuário, sendo ocultados dentro do código executável de outro processo. Esses processos são descritos como infectados por malware.
- **Cavalos de troia:** São malwares escondidos dentro de um pacote instalador de software que parece legítimo. Esse tipo de malware não busca nenhum tipo de consentimento para instalação e opera secretamente.
- **Programas potencialmente indesejados: (PuPs/PUAs):** São softwares instalados com um pacote selecionado pelo usuário ou talvez empacotados como um novo sistema de computador. Esse tipo de software as vezes é descrito como grayware em vez de malware. Também pode ser chamado de bloatware.

Vírus de computador: É um tipo de malware projetado para se replicar e se espalhar de computador para computador, geralmente infectando aplicativos exe ou código de programas. Suas classificações são:

- **Não residente/infectador de arquivos:** O vírus está dentro de um arquivo executável do host e é executado com o processo do host. Ele tentará infectar outras imagens de processo no armazenamento persistente e executar outras ações de payload. Em seguida, ele passa o controle de volta para o programa host.
- **Inicialização:** O código do vírus é gravado no setor de inicialização do disco ou na tabela de partição de um disco fixo ou mídia USB e é executado como um processo residente na memória quando o SO é iniciado ou a mídia é conectada no computador.
- **Vírus de macro:** O malware usa os recursos de programação disponíveis nos mecanismos de script locais para o SO e/ou navegador, como PowerShell, Windows Management Instrumentation (WMI), JavaScript, documentos do Microsoft Office com código VBA ativado ou documentos PDF com JavaScript ativado.

Worms de computador e Malware Fileless: Um worm é um malware que reside na memória e pode ser executado sem a intervenção do usuário e ser reproduzido nos recursos da rede. Ao contrário do vírus que só é executado após alguma ação, como executável, pen drive ou até ao abrir um arquivo infectado, o worm é executado ao explorar uma vulnerabilidade em um processo quando o usuário navega em um site, executa um aplicativo de servidor vulnerável ou está conectado a um a um compartilhamento de arquivo infectado.

Spyware e Keyloggers: Os primeiros Worms e vírus se concentravam no potencial destrutivo da autorreplicação. À medida que os usos lucrativos desse tipo de software se tornaram aparentes, no entanto, eles começaram a ser codificados com payloads projetados para facilitar invasões, fraudes e roubo de dados. Os bloatwares e malwares podem ser usados para diferentes níveis de monitoramento:

- **Adware:** É uma classe de bloatware/PUP que reconfigura o navegador, por exemplo, permitindo cookies de rastreamento, alterando provedores de pesquisa padrão, abrindo páginas do patrocinador na inicialização, adicionando favoritos e etc. Eles podem ser instalados como extensão do navegador.
- **Spyware:** é um tipo de software malicioso que coleta informações do dispositivo de um usuário sem seu consentimento. Ele pode monitorar atividades online, capturar senhas, registrar pressionamentos de tecla e até ativar câmeras e microfones. Normalmente, é usado para espionagem, publicidade invasiva ou roubo de dados.
- **Keylogger**: é um tipo de spyware ou hardware que registra todas as teclas digitadas em um dispositivo, muitas vezes sem o conhecimento do usuário. Ele é usado para capturar senhas, dados bancários e outras informações sensíveis, podendo ser uma ferramenta de espionagem ou cibercrime.

Cavalos de troia por acesso remoto e backdoors: Qualquer tipo de método de acesso a um host que dribla o método de autenticação padrão e fornece controle administrativo ao usuário remoto pode chamar-se de backdoor. Um cavalo de troia por acesso remoto (**RAT**) é um malware de backdoor que **imita a funcionalidade de programas legítimos** de controle remoto, mas é projetado

especificamente para operar secretamente. Depois que o RAT é instalado, permite que o autor da invasão acesse o host, envie arquivos, instale softwares e etc.

Ransomware, crypto-malware e bombas lógicas: Ransomware é um tipo de malware que tenta **extorquir** a vítima tornando o computador e/ou arquivos de dados indisponíveis e **exigindo pagamento**.

- **Malware de cryptojacking:** Assume o controle dos recursos do host para **minerar criptomoedas**. O malware comete esse ato de forma mal-intencionada e é classificado como **cryptojacking**.
- **Bombas Lógicas:** Após infectar um sistema, eles esperam por uma hora ou data pré-configurada (bomba-relógio) ou, então, por um evento do sistema ou do usuário (bomba-lógica). As bombas lógicas também não precisam ser códigos de malware. Um exemplo típico é um administrador de sistemas descontente que deixa o script de uma armadilha que é executada caso sua conta seja excluída ou desativada. É improvável que um software antivírus detecte esse tipo de script ou programa mal-intencionado. Esse tipo de armadilha é chamado de **mina**.

Ataques físicos: É aquele direcionado contra a infraestrutura de cabeamento, os dispositivos de hardware ou o ambiente das instalações que hospedam a rede.

- **Força Bruta**: Pode assumir várias formas diferentes, como por ex:
  - **Smashing** – Destruição física de um dispositivo de hardware para executar a negação de serviço física.
  - Invasão de instalações ou armários forçando uma fechadura ou portão de acesso. É provável que seja um indicio de roubo ou adulteração.
- **RFID Cloning (clonagem RFID):** É um ataque em que os dados de um cartão ou dispositivo RFID (como cartões de acesso ou pagamentos por aproximação) são copiados sem contato físico direto. Isso é feito usando um leitor RFID não autorizado para capturar as informações da vítima e transferi-las para um clone, permitindo acesso ou transações fraudulentas.

Ataques à rede: É uma categoria geral que abrange uma série de estratégias e técnicas que os autores de ameaças usam para interromper ou obter acesso a sistemas por meio de um vetor de rede. A análise de ataques à rede geralmente se dá considerando o lugar que cada tipo de ataque pode ter dentro de um ciclo de vida geral do ataque cibernético:

- **Reconhecimento:** É quando um autor de ameaças usa ferramentas de varredura para obter informações sobre a rede. A descoberta do host identifica quais endereços IP estão sendo usados.

- A **coleta de credenciais** é um tipo de reconhecimento em que o autor da ameaça tenta descobrir senhas ou segredos criptográficos que lhe permitirão obter acesso autenticado a sistemas de rede.
- **Armamento:** Entrega e violação referem-se a técnicas que permitem ao autor da ameaça obter acesso sem precisar de autenticação. Isso normalmente envolve vários tipos de código malicioso, que é direcionado a um host ou serviço de aplicativo vulnerável por meio da rede ou, então, o envio de código oculto em anexos de arquivos e enganar um usuário para executá-lo.
    - **Comando e controle (C2 ou C&C):** Beaconing e persistência referem-se a técnicas e códigos maliciosos que permitem que um autor de ameaças opere um host comprometido remotamente e mantenha o acesso a ele por um tempo.
    - **Movimento lateral, pivoting e escalação de privilégios:** Referem-se a técnicas de permitem ao autor da ameaça mover-se de um host para outro dentro de uma rede ou de um segmento de rede para outro e obter permissões cada vez mais elevadas em sistemas e serviços em toda a rede. Esses tipos de ataques são detectados por meio de anomalias em logins de conta e uso de privilégios, mas a detecção geralmente depende de software com aprendizagem de máquina, pois normalmente é difícil diferenciar o comportamento anômalo do comportamento normal.
    - **Exfiltração de dados:** Refere-se à obtenção de um ativo de informação e à sua cópia para a máquina remota do invasor. Transferências anômalas de dados volumosos podem ser um indicador de exfiltração, mas um autor de ameaças pode executar o ataque furtivamente, movendo apenas pequenas quantidades de dados em certos momentos.

Ataques distribuídos de negação de serviço: Os ataques Dos contra hosts e gateways de rede normalmente pertencem a um tipo chamado de **Dos distribuídos (DDoS)**. DDoS significa que o ataque é iniciado a partir de **vários hosts simultaneamente**. Normalmente, um autor de ameaças comprometerá as máquinas para usar como manipuladores em uma rede de comando e controle. Os manipuladores são usados para comprometer milhares ou milhões de hosts com ferramentas de bot DDoS, formando uma **botnet**.

Alguns tipos de ataques DDoS simplesmente visam consumir a largura da banda de rede, negando-a aos hosts legítimos.

Outros causam esgotamento de recursos no host alvo bombardeando-o com solicitações, que consomem ciclos de CPU e memória. Isso atrasa o processamento do tráfego legítimo e pode travar o sistema host completamente. Por exemplo, um ataque de **SYN flood** funciona retendo o pacote **ACK** do cliente durante o handshake de três vias do TCP. Um servidor, roteador ou firewall pode manter uma fila de conexões pendentes, registradas em sua tabela de estados. Quando não recebe um pacote ACK do cliente, ele reenvia o pacote SYN/ACK o

número de vezes definido antes de expirar a conexão. O problema é que um servidor só consegue gerenciar um número limitado de conexões pendentes, que o ataque DDoS rapidamente preenche.

Ataques refletidos: Em um ataque de **DoS refletido distribuídos (DRDoS)**, o autor da ameaça falsifica o endereço IP da vítima e tenta abrir conexões com vários servidores externos. Esses servidores direcionam suas respostas SYN/ACK para o host da vítima. Isso consome rapidamente a largura de banda disponível da vitima.

Ataques On-Path: É quando o autor da ameaça ganha uma (algo faltando) entre dois hosts e captura, monitora e retransmite de maneira transparente toda a comunicação entre eles. Como o autor da ameaça retransmite as comunicações interceptadas, os hosts podem não ser capazes de detectar a presença do autor da ameaça.

Um ataque on-path também pode ser usado para **modificar secretamente o tráfego**. Por exemplo, um host on-path pode apresentar uma estação de trabalho com um formulário de site falsificado para tentar capturar a credencial do usuário. Esse ataque também é chamado de ataque **on-path** ou de **ataque avdversary-in-the-middle (AitM)**.

Os ataques on-path podem ser lançados em qualquer camada da rede

Um exemplo infame ataca a forma como o encaminhamento na camada 2 funciona em segmentos locais. O protocolo de **resolução de endereços (ARP)** identifica o endereço MAC de um host no segmento local que possui um endereço IPv4. Um ataque **ARP poisoning** usa um gerador de pacotes, como o Ettercap, para transmitir pacotes de resposta ARP não solicitados. Como o ARP não tem mecanismo de segurança, os dispositivos de recebimento confiam nessa comunicação e atualizam sua tabela de cache de endereõs MAC:IP com endereço falsificado.

Ataques ao sistema de DNS: O sistema de nomes de domínio (**DNS**) resolve solicitações de serviços nomeados para endereços IP. A resolução de nomes é um método de endereçamento crítico na internet e em redes privadas. Há muitos ataques potenciais contra o DNS.

Na internet pública, os ataques podem usar técnicas de **typosquatting** para fazer com que as vítimas confundam sites maliciosos com sites legítimos. O DNS pode ser explorado em um ataque DRDoS. Os autores de ameaças também podem alvejar diretamente os serviços de DNS público como um meio de realizar DoS contra um site ou recurso de nuvem. Por fim, um autor de ameaças pode conseguir desviar um servidor DNS público e inserir registros falsificados, direcionando as vítimas para sites mal-intencionados.

- **Ataques on-path baseados em DNS:** Se o autor tiver acesso á mesma rede local da vítima, ele pode usar o envenenamento de ARP para

responder a consulta DNS da vítima com respostas falsas. Isso pode ser combinado com um ataque de negação de serviço no servidor DNS legítimo da vítima. Um DHCP falso pode ser usado para configurar clientes com o endereço de um resolvedor de DNS controlado pelo autor da ameaça.

- **Envenenamento de cache do cliente DNS:** O arquivo HOSTS requer acesso de administrador para sua modificação. Nos sistemas **UNIX** e **Linux**, ele é armazenado como **/etc/hosts**, e no **Windows** é colocado em **%SystemRoot%\System32\Drivers\etc\hosts**.

Ataques de senha: Visa explorar os pontos fracos inerentes à seleção e gerenciamento de senhas para recuperar o texto simples e usá-lo na tentativa de comprometer uma conta.

- **Ataques online:** É quando o autor interage diretamente com o serviço de autenticação, como um formulário de login na web ou gateway VPN, por ex. Esse ataque pode aparecer nos registros de auditoria como logins com falha repetida e, em seguida, um login bem-sucedido, ou logins bem-sucedidos em horários e locais incomuns.
- **Ataques offline:** Significa que um invasor obteve um banco de dados de hashes de senha, como o **%SystemRoot%\System32\config\SAM**, **%SystemRoot\NTDS\NTDS.DIT** (o armazenamento de credenciais do AD) ou o **/etc/shadow**.
- **Ataques de força bruta**
- **Ataques híbridos e de dicionário:** Um ataque de dicionário é usado quando há boa chance de adivinhar o valor do texto simples, como uma senha não complexa. O software gera valores de hash a partir de um dicionário de texto simples para tentar corresponder a um hash capturado. Um ataque de **senha híbrida** combina com ataques de **dicionário** e de **força bruta**. Ele é direcionado principalmente contra senhas ingênuas com complexidade inadequada, como james1.
- **Password spraying (pulverização de senhas):** É um ataque online de força bruta horizontal, onde o invasor escolhe uma ou mais senhas comuns e tenta essas senhas em conjunto com vários nomes de usuário.

Ataques criptográficos: Visam sistemas de autenticação geralmente de do sistema que usa criptografia fraca.

- **Ataques de downgrade:** Faz com que um servidor ou cliente use um protocolo de especificação inferior com cifras mais fracos e chaves mais curtas. Por exemplo, uma combinação de um ataque on-path e downgrade no HTTPS pode tentar forçar o cliente a usar uma versão fraca de TLS. Isso torna mais fácil para um autor de ameaças forçar o uso de conjuntos de cifras fracas e falsificar a assinatura de uma autoridade de certificação na qual o cliente confia.
- **Ataques Birthday:** Um ataque de colisão depende da capacidade de criar um documento malicioso que gera o mesmo hash que o documento

inofensivo. Um ataque birthday é um meio de explorar colisões em funções hash por meio de forma bruta.

Indicadores de ataques a aplicativos

Ataques a aplicativos: É direcionado a uma vulnerabilidade no SO ou no software do aplicativo. Uma vulnerabilidade no aplicativo é uma falha de design que pode abrir lacunas no sistema de segurança do aplicativo ou que leve o aplicativo a falhar. Existem dois cenários principais para ataques a aplicativos:

- **Comprometer o sistema operacional ou aplicativos externos** em um host de rede explorando cavalos de tróia, anexos maliciosos ou vulnerabilidades do navegador. Isso permite que o autor da ameaça obtenha uma base de apoio em uma rede local.
- **Comprometer a segurança de um site ou aplicativo web:** Isso permite que um autor de ameaças obtenha o controle de um host web e roube dados dele ou use-o para tentar penetrar ainda mais na rede.

Escalação de privilégios:

- **Vertical:** É quando um usuário ou aplicativo conseguem acessar funcionalidades ou dados que não deveriam estar disponíveis para eles. Por exemplo, um processo pode ser executado com privilégios de adm local, mas uma vulnerabilidade permite que o código arbitrário seja executado com privilégios SYSTEM mais elevados.
- **Horizontal:** É quando um usuário acessa funcionalidades ou dados destinados a outro usuário. Por exemplo, por meio de um processo em execução com privilégios de adm local em uma estação de trabalho do cliente, o código arbitrário pode ser executado como uma conta de domínio em um servidor de aplicativos.

Ataques de injeção de comando e diretório transversal: Directory transversal é outro tipo de ataque de injeção realizado contra um servidor Web. O invasor solicita um arquivo fora do diretório principal (../). Esse ataque pode ser bem-sucedido se a entrada não for filtrada corretamente, e as permissões de acesso ao arquivo permitirem que o processo do servidor Web o leia, grave ou execute. O autor da ameaça pode usar um **ataque de canonicalization** para disfarçar a natureza da entrada maliciosa. Por exemplo, para executar um ataque de diretório transversal, o invasor pode enviar um URL como o seguinte:
http://victim.foo/?show=../../../etc/config

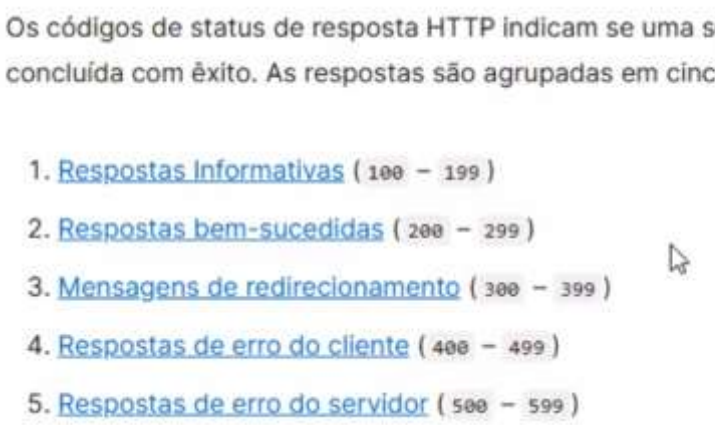
Análise de URL: Uma solicitação normalmente compreende um método, um recurso (como um caminho de URL), número da versão, cabeçalhos e corpo. Os principais métodos são os seguintes:

- GET (obter): recuperar um recurso.

- POST (enviar): enviar dados para o servidor para processamento pelo recurso solicitado.
- PUT (colocar): criar ou substituir recurso.

Codificação por cento: Um URL pode conter apenas caracteres não reservados e reservados do mesmo padrão. Os caracteres reservados são usados como delimitadores dentro da sintaxe do URL e só devem ser usados de forma não codificada para esses fins. Os caracteres reservados são: : / ? # [ ] @ ! $ & * + , ; =

Logs do servidor web: O código de status de uma resposta pode revelar bastante sobre a solicitação e o comportamento do servidor. Códigos na faixa de **400** indicam erros baseados no cliente, os códigos na faixa de **500**, indicam erros baseados no servidor.


Os códigos de status de resposta HTTP indicam se uma solicitação HTTP específica foi concluída com êxito. As respostas são agrupadas em cinco classes:

1. Respostas Informativas (100 – 199)
2. Respostas bem-sucedidas (200 – 299)
3. Mensagens de redirecionamento (300 – 399)
4. Respostas de erro do cliente (400 – 499)
5. Respostas de erro do servidor (500 – 599)

Erros de aplicações web. Igual o 404 not found

Resumir conceitos de governança de segurança

Políticas, normas e procedimentos

Políticas, normas e procedimentos: São três componentes essenciais que formam a base do programa de segurança de uma organização. As políticas são documentos oficiais de **alto nível** que definem o compromisso de segurança da organização.

As normas são mais específicas do que as políticas e **detalham os métodos** usados para implementar os requisitos técnicos e processuais.

Os procedimentos são instruções detalhadas, passo a passo, que descrevem como concluir tarefas específicas e se alinhar aos requisitos estabelecidos nas normas. Os procedimentos fornecem **instruções** claras para que os indivíduos desempenhem suas funções de forma consistente, segura e eficiente.

Políticas:

- **Políticas organizacionais comuns**
  - **Política de uso aceitável (AUP):** Descreve as maneiras aceitáveis de usar a rede e os sistemas de computação, definindo o que constitui um comportamento aceitável por parte dos usuários. Geralmente abordam

comportamento de navegação, o conteúdo apropriado, os downloads de software e o manuseio de informações sensíveis. O objetivo de uma AUP é garantir que os usuários não se envolvam em atividades que possam prejudicar a organização ou seus recursos. Ela deve também especificar as consequências da não conformidade e requerer que os funcionários reconheçam conhecimento das regras via assinatura.
    - **Políticas de segurança informação:** São políticas criadas por uma organização para garantir que todos os usuários de TI cumpram as regras e diretrizes relacionadas à segurança das informações armazenadas no ambiente ou na esfera de autoridade da organização.
    - **Planos de continuidade dos negócios e continuidade das operações (COOP):** Estas políticas se concentram nos processos críticos que devem permanecer operacionais durante e após uma interrupção substancial, como um desastre natural ou ciberataque.
    - **Ciclo de vida de desenvolvimento de software (SDLC):** Regem o desenvolvimento de software dentro de uma organização. Elas fornecem um plano estruturado detalhando os estágios de desenvolvimento, desde a análise inicial de requisitos até a mudança após a implantação. Isso garante que todos os programas de software produzidos atendam às normas de eficiência, confiabilidade e segurança da organização.
    - **Gerenciamento de mudanças:** Descrevem como as modificações nos sistemas e software de TI são solicitadas, revisadas, aprovadas e implementadas, incluindo todos os requisitos de documentação.
- **Diretrizes:** Referem-se as recomendações que orientam as ações em uma função ou departamento específico. Elas são mais flexíveis do que as políticas e permitem maior autonomia para indivíduos que as implementam. As diretrizes fornecem as práticas recomendadas e sugestões para atingir as metas e concluir as tarefas de forma eficaz. Elas ajudam as pessoas a **entender** as **etapas** necessárias para cumprir uma política ou melhorar a eficácia.

Procedimentos: Definem instruções passo a passo e listas de verificação para garantir que uma tarefa seja concluída de forma a manter a conformidade com a política.

- **Gerenciamento de pessoal:** O gerenciamento de identidade e acesso (IAM) envolve procedimentos e tecnologias de TI/segurança e políticas de RH. As políticas de gerenciamento de pessoal são aplicadas em três fases:
    - **Recrutamento (contratação):** Localizar e selecionar pessoas para trabalharam em cargos específicos. Aqui, questões de segurança incluem avaliar candidatos e realizar verificação de antecedentes.
    - **Operação (trabalho):** Geralmente é o departamento de RH que gerencia a comunicação de políticas e treinamentos aos funcionários. Por isso é crucial que os gerentes de RH elaborem programas de treinamento que transmitam a importância da segurança aos funcionários.
    - **Rescisão ou separação (demissão ou aposentadoria):** Quando funcionários deixam a empresa, a rescisão é um processo difícil, com inúmeras implicações de segurança.
- **Verificação de antecedentes:** Uma verificação de antecedentes determina basicamente se uma pessoa é quem diz ser e se ela nunca se envolveu com

atividades criminosas. Funcionários que trabalharão em ambientes de alta confidencialidade devem ser melhor analisados.

- **Integração:** É o processo de receber um novo funcionário na organização. Cuidados devem ser tomados na criação de contas de clientes e convidados.
- **Transmissão segura de credenciais:** Criar e enviar uma senha inicial. O processo precisa de proteção contra funcionários administrativos desonestos. Contas recém-criadas com senhas simples ou padrão são um backdoor facilmente explorado.
- **Alocação de ativos:** Fornecer computadores ou dispositivos móveis para o usuário ou concordar que o usuário possa trazer seus próprios dispositivos.
- **Treinamento/políticas:** Agendar treinamento e certificação de segurança relevantes à função.
- **Playbooks:** São manuais essenciais para estabelecer e manter os procedimentos organizacionais, pois estabelecem um repositório central de estratégias e táticas bem definidas e padronizadas. Eles orientam o pessoal para garantir a consistência nas operações e melhorar a qualidade e a eficácia.
- **Gerenciamento de mudanças:** A implementação de mudanças deve ser planejada com cuidado, considerando como a alteração afetará componentes dependentes. Em relação à maioria das mudanças grandes ou significativas, as organizações devem tentar primeiro testar a mudança. Toda mudança deve ser acompanhada por um plano de reversão, caso tenha consequências imprevistas ou prejudiciais.
- **Desligamento:** Uma entrevista de saída é o processo de garantir que um funcionário deixa uma empresa de maneira apropriada. Também é usado quando um projeto com contratados terceirizados termina. Em termos de segurança, existem vários processos que precisam ser concluídos:
    - **Gerenciamento de contas:** Desativar contas e privilégios do usuário.
    - **Ativos da empresa:** Recuperar dispositivos móveis, chaves, mídia USB e etc. O funcionário precisará provar que não reteve cópias em alguns casos.
    - **Ativos pessoais:** Eliminar dados e aplicativos da empresa nos dispositivos de propriedade do funcionário.

Normas: Definem o resultado esperado de uma tarefa, como um estado de configuração específico para um servidor ou a linha de base de desempenho para um serviço. Elas se concentram em vários elementos dinâmicos, como requisitos regulamentares, necessidades específicas do negócio, estratégias de gerenciamento de riscos, práticas do setor e expectativas das partes interessadas

- **Normas do setor:** As normas comuns do setor usadas por organizações públicas e privadas incluem:
- **ISO/IEC 27001:**
- **ISO/IEC 27002:**
- **ISO/IEC 27017:**
- **ISO/IEC 27018:**

- **ISO/IEC 27001** — uma norma internacional que fornece uma estrutura de sistema de gerenciamento de segurança de informações (ISMS) para garantir que controles de segurança adequados e proporcionais estejam em vigor.
- **ISO/IEC 27002** — esta é uma norma complementar à ISO 27001 e fornece orientação detalhada sobre controles específicos a serem incluídos em um ISMS.
- **ISO/IEC 27017** — uma extensão da ISO 27001 específica para serviços em nuvem.
- **ISO/IEC 27018** — outra adição à ISO 27001, específica para proteger informações de identificação pessoal (PII) em nuvens públicas.

- **NIST 800-63**
- **PCI DSS**
- **FIPS**

- **Publicação especial 800-63 do NIST (National Institute of Standards and Technology)** — uma norma do governo dos EUA para diretrizes de identidade digital, incluindo requisitos de senha e controle de acesso.
- **PCI DSS (Payment Card Industry Data Security Standard)** — norma para organizações que lidam com cartões de crédito das principais bandeiras, incluindo requisitos para proteger os dados do titular do cartão.
- **FIPS (Federal Information Processing Standards)** — normas e diretrizes desenvolvidas pelo NIST para sistemas de computadores federais nos Estados Unidos. Elas especificam requisitos para criptografia.

Ambiente jurídico: Comitês de segurança garantem que as organizações cumpram todas as leis e regulamentos de cibersegurança aplicáveis para protege-las contra reponsabilidade legal.

- **Dados pessoais e Regulamento Geral sobre a Proteção de Dados (RGPD):** Quando alguns tipos de legislações abordam o dever de diligencia de cibersegurança, outros se concentram total ou parcialmente na segurança da informação, pois afeta a privacidade ou os dados pessoais. A privacidade é um conceito diferenciado e exige que a coleta e o processamento de informações estejam seguros e justos.
  A justiça e o direito á privacidade promulgados pelo RGPD da EU, implicam que dados pessoais não pode ser coletados, processados ou retidos sem o consentimento informado do indivíduo. **Consentimento informado** significa que os dados devem ser coletados e processados apenas para a finalidade declarada, e essa finalidade deve ser claramente descrita ao usuário em linguagem simples, não em jargão jurídico.

- **Lei de Privacidade do Consumidor da California (CCPA):** Concede aos residentes da Califórnia o direito de saber quais informações pessoais as empresas coletam sobre eles, a finalidade e com quem são compartilhados. A CCPA se aplica á qualquer organização, independente da sua localização.
- **Regulamentações e leis nacionais, locais, regionais e setoriais:** Muitos países têm leis nacionais para apoiar práticas eficazes de segurança cibernética e proteger os dados dos cidadãos. O escopo e os pormenores dessas leis variam de um país para o outro, mas as organizações devem cumprir as leis em todas as jurisdições onde funcionam.
  As leis e regulamentos de segurança cibernética específicos da indústria regem como os dados devem ser tratados e protegidos. Vejamos alguns exemplos importantes para mostrar a importância da segurança cibernética em todos os setores da indústria e que é protegida por uma complexa matriz de leis a serem observadas pelas operações de segurança cibernética e governança organizacional:

Governança e responsabilidade: As práticas de governança asseguram que as organizações cumpram todas as leis e regulamentações de segurança cibernética aplicáveis para protege-las contra responsabilidade legal. A governança e a supervisão organizacional devem administrar muitos riscos legais, como requisitos de conformidade regulatório, obrigações contratuais, leis de privacidade, proteção de propriedade intelectual e contratos de licenciamento, e interpretar e traduzir esses requisitos legais em controles operacionais para evitar problemas legais.

- **Conselhos de governança:** São fundamentais para garantir a governança e a supervisão de segurança eficazes de uma organização, pois são responsáveis por definir os objetivos estratégicos, as políticas e as diretrizes para as práticas de segurança e gestão de riscos.
- **Funções da governança de dados**: A governança de segurança depende muito de funções especialmente desenvolvidas e interdependentes, denominadas proprietário, controlador, processador e guardião. Cada função carrega responsabilidades únicas que contribuem para manter uma supervisão e controle de seguranças eficazes.
    - **Proprietário**: Identifica o nível de classificação e confidencialidade dos dados, decide quem deve ter acesso a eles e qual nível de segurança deve ser aplicado.
    - **Controlador:** Garante que as atividades de processamento de dados cumpram todos os requisitos legais.
    - **Guardião:** É responsável pela guarda segura, transporte, armazenamento dos dados e implementação de regras de negócios.

Gestão de mudanças

Automação e Scripts: Tornaram-se ferramentas essenciais nas operações modernas de TI, ajudando as organizações a otimizar processos, fortalecer a segurança e aumentar a eficiência. A automação serve para aprimorar tanto a governança de segurança quanto a gestão de mudanças. Em termos de governança, a automação pode ajudar a impor políticas de segurança de forma mais consistente e eficiente, além de auxiliar no monitoramento e na geração de relatórios para fornecer informações valiosas às equipes de liderança e aos gestores de risco. Na gestão de mudanças, a automação pode reduzir o risco do erro humano, diminuir o tempo de implementação e fornecer trilhas de auditoria claras.

Explicar processos de gestão de riscos

Processos e conceitos de gestão de riscos

Gestão de risco: Envolve **identificar** possíveis problemas, **avaliar** seu **impacto** potencial na organização e **implementar** controles para mitiga-los. Os principais conceitos incluem a identificação de riscos, a avaliação de risco, a mitigação e o monitoramento. O **apetite** e a **tolerância** ao risco são importantes para **determinar** o nível de risco aceitável para uma organização.

Identificação e avaliação de riscos: É fundamental à gestão dos riscos relacionados à segurança cibernética. Envolve o reconhecimento de riscos **técnicos**, como ataques de **malware**, tentativas de **phishing, ameaças internas**, **falhas de equipamentos** e **vulnerabilidades de software**, e **riscos não técnicos**, como **políticas** ou **treinamento** inadequados. Os métodos para identificação de riscos incluem vulnerabilidades, testes de penetração, auditorias de segurança. Threat intelligence e etc.

Análise de risco vs avaliação de riscos: Análise de risco refere-se ao processo de identificação e avaliação de riscos potenciais e suas características. Seu objetivo é **entender** a natureza e o **escopo** dos riscos examinando suas causas, **consequências** e **preocupações**.

A **avaliação de riscos** é uma abordagem sistemática projetada para estimar os níveis potenciais de risco e sua relevância através da interpretação dos dados coletados durante a análise de risco. Ela considera a **probabilidade de um evento ocorrer** e a

gravidade de suas consequências. Também pode **envolver a priorização de riscos** com base em seu **impacto potencial** e a definição de estratégias de gestão de riscos.

- **Análise quantitativa:** Busca **atribuir valores concretos** a cada fator de risco.
    - **Expectativa de perna única (Single Loss Expectancy, SLE):** O valor que seria perdido em uma única ocorrência do fator de risco. É determinado multiplicando o valor do ativo por um fator de exposição (Exposure Factor, EF). EF é a porcentagem do valor do ativo que seria perdida. Por exemplo, pode ser determinado que um tornado danificaria 40% de um edifício. Nesse caso, o fator de exposição é de 40% porque apenas parte do ativo é perdida. Se o valor do edifício for de US$ 200k, a SLE desse evento é de 200.000*0,4 ou US$ 80.000.
    - **Expectativa de perda anualizada (Annualized Loss Expectancy, ALE):** O valor que seria perdido ao longo de um ano. É determinado multiplicando a SLE pela taxa anualizada de ocorrência (Annualized Rate of Ocurrance, ARO). A ARO é o numero de vezes que um evento ocorre em um ano. No nosso exemplo anteriro (muito simplificado), se for previsto que um tornado causará um impacto duas vezes por ano, então ARO será 2. A ALE é o custo do evento (SLE) multiplicado pelo número de ocorrências em um ano. No exemplo do tornado, a SLE é de US$80k e a ARO é de 2, portanto ALE é de US$160k. Esse valor pode ser útil ao ser usado para considerar diferentes maneiras de proteger o prédio de tornados, sendo o valor máximo para implementar proteções.
- **Análise qualitativa:** É um método usado na gestão de riscos para avaliá-los com base em julgamento subjetivo e fatores qualitativos, em vez de dados e números precisos. Seu objetivo é proporcionar uma compreensão qualitativa dos riscos, o impacto potencial e a probabilidade de ocorrência.
- **Risco inerente:** É o nível de risco antes de qualquer tentativa de mitigação.
- **Mapa de calor (heat map):** Para cada risco, é atribuída uma cor (vermelho, amarelo ou verde) a cada coluna para representar sua gravidade, probabilidade, custo das medidas de controle e assim por diante. A publicação **FIPS 199** explica como aplicar categorizações de segurança (Security Categorizations, SC) a sistemas de informação com base no impacto que uma violação de confidencialidade, integridade ou disponibilidade teria na organização.

Os possíveis impactos podem ser classificados da seguinte forma:

- **Baixo:** Danos ou perdas menores a um ativo ou perda de desempenho.
- **Moderado:** Danos ou perdas significativas a ativos ou perda de desempenho.
- **Alto:** Grandes danos ou perdas, ou incapacidade de executar uma ou mais funções essenciais.

Estratégias de gestão de riscos: Definem abordagens proativas e sistemáticas para identificar, avaliar, priorizar e mitigar riscos com o objetivo de minimizar seus impactos negativos.

- **Mitigação:** É o processo geral de redução da exposição aos fatores de risco ou dos seus possíveis efeitos. Uma contramedida que reduz a exposição a uma ameaça ou vulnerabilidade é denominada dissuasão (ou redução) de riscos. A

redução de riscos se refere a **controles** que podem **diminuir** as chances de um incidente de risco **acontecer** ou **atenuar** os custos caso aconteçam.

- **Transferência de risco**: Significa **atribuir** o risco a um **terceiro**, como uma **seguradora**. Não é possível eliminar os riscos por completo, portanto, um dos principais objetivos de fazer sua gestão é determinar um nível adequado de **risco admissível**, que varia de acordo com o setor, estilo de liderança, ambiente jurídico etc.
- **Aceitação de riscos:** Significa que nenhuma contramedida é implementada porque o nível de risco não a justifica. Uma exceção de risco é uma situação em que, devido a condições financeiras, técnicas ou operacionais, não é possível mitigar um risco usando práticas padrão de gestão de riscos ou dentro de um prazo especificado. Uma exceção de risco reconhece formalmente o risco e busca identificar controles de mitigação alternativos, se possível. Elas devem ser **temporárias** e **reavaliadas** a intervalos estabelecidos para verificar se os níveis de risco mudaram ou se a exceção foi removida.

Risco residual e apetite ao risco: Enquanto o risco inerente é o risco antes da mitigação, o risco residual representa a **probabilidade** e o **impacto após** a aplicação de medidas específicas de mitigação, **transferência** ou **aceitação**. O apetite ao risco é uma **avaliação estratégica do nível tolerável** de risco residual. Enquanto a aceitação de riscos se limita a um único sistema, o **apetite ao risco abrange todo um projeto ou instituição**. O apetite ao risco é limitado pela regulamentação e conformidade.

Registro de riscos: É um documento que apresenta os resultados das avaliações de risco de forma compreensível e inclui informações sobre riscos, a gravidade, o responsável pelo risco e todas as estratégias de mitigação identificadas. O registro pode incluir uma matriz de riscos no formato de mapa de calor para classificações de impacto e probabilidade, data de identificação, descrição, contramedidas, status e responsável ou caminho de escalonamento.

Limite de risco: Define os limites ou níveis de risco aceitáveis para uma organização. Dentro dessa delimitação, os riscos são considerados aceitáveis e administráveis. Eles se baseiam em vários fatores, como requisitos regulamentares, objetivos organizacionais, expectativas das partes interessadas e o apetite ao risco da organização.

Indicadores-chave de risco: Key Risk Indicators, KRIs são indicadores preditivos críticos que as organizações usam para monitorar e prever possíveis riscos. Essas métricas fornecem um **indício inicial do aumento de exposições ao risco** em diferentes áreas da organização. Os **KRIs** avaliam o impacto potencial e a probabilidade de diversos riscos para que as equipes de liderança possam tomar medidas proativas e geri-los de forma eficaz.

Um responsável pelo risco é o indivíduo **encarregado de gerir um risco específico**, o que inclui: **identificar e avaliar o risco, implementar medidas para mitigá-lo, monitorar a eficácia das medidas e realizar ações corretivas conforme necessário.**

Relatório de riscos: Descreve os métodos usados para comunicar o perfil de risco de uma organização e a eficácia do seu programa de gestão de riscos. Ele auxilia na tomada de decisões, evidencia preocupações e assegura que as partes interessadas entendam os riscos da organização. Os relatórios de riscos operacionais devem incluir detalhes específicos sobre os fatores que contribuem para o risco e são apropriados para gerentes ou funcionários técnicos. Os relatórios de riscos também **devem informar claramente as recomendações de resposta ao risco, como aceitar, mitigar, transferir ou evitar o risco.**

Análise de impacto nos negócios (BIA):

- **Identificação de sistemas críticos:**
  - **Pessoas:** (funcionários, visitantes e fornecedores).
  - **Ativos tangíveis:** (Edifícios, móveis, equipamentos e maquinário fabril, equipamentos de informática e telecomunicação, arquivos de dados eletrônicos e documentos em papel).
  - **Ativos intangíveis:** (ideias, reputação comercial, marca)
  - **Procedimentos:** (cadeias de suprimentos, procedimentos críticos e operacionais)

Análise de impacto nos negócios: A Business Impact Analysis (BIA), é um processo que ajuda as empresas a entenderem os possíveis efeitos das interrupções em suas operações.

Isso envolve identificar e avaliar o impacto de diversos cenários de ameaça não previstos nos negócios, como acidentes, emergências e desastres.

Ao realizar uma BIA, as empresas podem **criar**, de forma **proativa**, **estratégias** de **recuperação** para **minimizar** o **impacto** das **interrupções e garantir a resiliência operacional**.

- **Funções essenciais (MEF): Mission Essential Function**, é aquela que não pode ser adiada. Isso significa que a organização deve ser capaz de executar a função do modo mais contínuo possível. Além disso, em caso de interrupção no serviço, as funções essenciais devem ser restauradas primeiro. A análise das funções essenciais geralmente é regida por quatro métricas principais:
  - **Tempo máximo tolerável de inatividade (Maximum Tolerable Downtime, MTD)** é o período mais longo pelo qual uma função de negócios pode ser interrompida sem causar falha irreversível para a empresa. Cada processo de negócios pode ter seu próprio MTD, por exemplo: um intervalo de minutos a horas para funções críticas, 24 horas para funções urgentes, sete dias para funções normais e assim por diante. Os MTDs variam de acordo com a empresa e o evento. **(MTD É RTO + WRT)**
  - **Objetivo de tempo de recuperação (Recovery Time Objective, RTO)** é o período após um desastre em que um sistema de TI pode permanecer off-

line. Isso representa o tempo necessário para identificar se há um problema e executar a recuperação (por exemplo, restaurar do backup ou mudar para um sistema alternativo).

- **Tempo de recuperação do trabalho (Work Recovery Time, WRT)** Após a recuperação dos sistemas, pode haver trabalho adicional para reintegrar os diferentes sistemas, testar a funcionalidade geral e informar os usuários do sistema sobre quaisquer alterações ou práticas de trabalho diferentes para que a função de negócios volte a ter total suporte.
- **Objetivo de ponto de recuperação (Recovery Point Objective, RPO)** É a quantidade de perda de dados que um sistema pode suportar, medida em tempo. Ou seja, se um banco de dados for destruído por um vírus, um RPO de 24 horas significa que poderão ser recuperados dados de uma cópia de backup que foram salvos até 24 horas antes de o bd ter sido infectado.

O tempo médio de reparo (Mean Time To Repair, MTTR) o tempo médio entre falhas (Mean Time Between Failures, MTBF) são indicadores-chave de desempenho (KPIs) usados para medir a confiabilidade e a eficiência de sistemas, processos e equipamentos.

- **MTBF** representa a vida útil estimada de um produto. É calculado dividindo o tempo operacional total pelo número de falhas. Por exemplo, se você tem 10 dispositivos que funcionam por 50 horas e dois deles falham, o MTBF é de 250 horas/falha (10*50)/2.
- **MTTR** é uma medida do tempo gasto para corrigir uma falha até que o sistema retorne à plena operação. Também pode ser descrito como tempo médio para substituir ou recuperar. É calculador dividindo o número total de horas de manutenção não prevista pelo número de incidentes de falha.

Conceitos de gestão de fornecedores:

Seleção de fornecedores: As práticas de seleção de fornecedores devem avaliar e analisar sistematicamente possíveis fornecedores para minimizar os riscos associados à terceirização ou aquisição. O **objetivo** é selecionar fornecedores que estejam alinhados com a tolerância ao risco da organização e demonstrem capacidade de gerir os riscos de forma eficaz.

- **Conflito de interesses;**
  - Interesses financeiros
  - Relações pessoais
  - Relacionamentos competitivos
  - Informações privilegiadas

Acordos legais:

- **Memorandum of Understanding (MOU):** um acordo não vinculativo que descreve as intenções, as metas em comum e os termos gerais da cooperação entre as partes. Os MOUs servem como uma etapa preliminar para estabelecer um entendimento comum antes de prosseguir com um acordo mais formal.
- **Nondisclosure Agreement (NDA):** Garante o sigilo e a proteção de informações confidenciais compartilhadas durante relacionamento. Um NDA é um acordo vinculativo e provavelmente será assinado juntamente de um MOU.
- **Memorandum of Agreement (MOA):** Um acordo formal que define os termos, condições e responsabilidades específicos das partes. Os MOAs estabelecem uma relação juridicamente vinculativa que abrange objetivos, funções, recursos e obrigações. Eles proporcionam uma estrutura confiável para a colaboração.
- **Business Partnership Agreement (BPA):** Governa parcerias estratégicas de longo prazo entre organizações. Os BPAs abrangem vários objetivos, incluindo **metas**, **acordos financeitos**, **processos** de tomada de decisão, **direitos** de **propriedade intelectual**, **confidencialidade** e **mecanismos** de **resolução** de **disputas**. Os BPAs fornecem um meio para governar relacionamentos colaborativos e mutuamento benéficos.
- **Master Service Agreement (MSA):** Descreve os termos e condições gerais de um contrato específico, como provisionamento de recursos em nuvem ou suporte de tíquetes/help desk. Um MSA inclui escopo, preços, entregas e direitos de propriedade intelectual.
- **Acordos detalhados:** Enquanto os acordos inciais estabelecem uma estrutura para colaboração ou prestação de serviços, outros acordos podem ser implementados para especificar os termos dos detalhes operacionais. Isso ajuda a administrar as relações com os fornecedores de forma eficaz.
    - **SLA (Service-level Agreement):** define as métricas de desempenho específicas, os padrões de qualidade e os níveis de serviço esperados do fornecedor.
    - **Statement of Work (SOW)/Work Order (WO):** Detalha o escopo, os entregáveis os cronogramas e as responsabilidades de um projeto ou compromisso de um fornecedor. São cruciais para garantir alinhamento entre a organização e o fornecedor, descrevendo as tarefas do fornecedor, as expectativas da organização e as entregas acordadas**.**
- **Regras de compromisso:**
    - **Rules of Engagement (ROE):** definem os parâmetros e as expectativas para os relacionamentos com os fornecedores. Descrevem as **responsabilidades, os métodos de comunicação, mecanismos de apresentação de relatórios, os requisitos de segurança e as obrigações de conformidade que os fornecedores devem cumprir**. Estabelecem diretrizes claras para o comportamento, as atividades e o acesso do fornecedor a informações confidenciais.

Auditorias e avaliações

Atestações e avaliações: Refere-se à verificação e validação da precisão, confiabilidade e eficácia dos controles, sistemas e processos de segurança implementados em uma organização. Envolve um exame independente e objetivo por uma entidade qualificada e

confiável, como um auditor ou avaliador. O atestado é uma **declaração** ou **confirmação formal** de que os controles e práticas de segurança de uma organização estão em conformidade com padrões, regulamentos ou práticas recomendadas específicas e proporciona uma garantia às partes interessadas, como à gerência, clientes e parceiros de negócios e reguladores, de que as medidas de segurança de uma organização são adequadas e eficazes à proteção de informações confidenciais, mitigação de riscos e manutenção de CIA.

Testes de penetração: Pode envolver as seguintes etapas:

- **Verificar a existência de uma ameaça:** usar vigilância, engenharia social, scanners de rede e ferramentas de avaliação de vulnerabilidades para identificar vetores pelos quais as vulnerabilidades possam ser exploradas.
- **Contornar os controles de segurança:** procurar maneiras fáceis de atacar o sistema. Por exemplo, se a rede é fortemente protegida por um firewall, é possível obter acesso físico a um computador no prédio e executar malware a partir de um pendrive?
- **Testar ativamente os controles de segurança:** investigar os controles procurando por fraquezas e erros de configuração, como senhas fracas ou vulnerabilidades de softwares.
- **Explorar vulnerabilidades:** provar que uma vulnerabilidade é de alto risco explorando-a para obter acesso a dados ou instalar backdoors.
- **Sondagem ativa:** consiste em sondar e interagir ativamente com os sistemas e redes-alvo para coletar informações. Visa descobrir e obter informações sobre a infraestrutura, os serviços e as vulnerabilidades potenciais do alvo. Técnicas comumente usadas são:
    - Varredura de portas
    - Enumeração de serviços
    - Fingerprint do SO
    - Enumeração de DNS
    - Rastreamento de aplicativos da Web.
- **Sondagem passiva:** consiste em coletar informações sobre os sistemas e redes-alvo sem interagir diretamente com eles, concentrando-se na coleta de dados disponíveis publicamente e na observação passiva do tráfego de rede. Técnicas comumente usadas são:
    - Levantamento de inteligência de código aberto
    - Análise de tráfego de rede
    - Engenharia Social

  Ela ajuda testadores de penetração a coletar informações iniciais sobre a pegada digital de um alvo. É menos intrusiva e carrega um risco de detecção menor do que as técnicas de sondagem ativa.

Tipos de Testes de Penetração:

- **Ofensiva e defensiva:** O teste de penetração ofensiva, **Red Teaming** é uma abordagem proativa e controlada para simular ataques cibernéticos reais aos sistemas, redes e aplicativos de uma organização. Seu principal objetivo é identificar vulnerabilidades, fragilidades e possíveis vetores de ataque e são feitos imitando os TTPs de possíveis invasores. O **Blue Teaming**, avalia as medidas de

segurança defensiva de uma organização, os recursos de detecção, os procedimentos de resposta a incidentes e a resiliência geral contra ameaças cibernéticas. E visa avaliar a eficácia dos controles de segurança existentes e identificar áreas de melhoria.

Resumir conceitos de proteção de dados e conformidade

Classificação e conformidade de dados

Tipos de dados: Refere-se a categorizar ou classificar os dados com base em suas características inerentes, estrutura e uso pretendido. Os tipos de dados fornecem uma maneira de **organizar** e **entender** os diferentes formulários de dados em um sistema ou conjunto de dados. A **classificação de dados** em tipos específicos facilita a **análise**, o **processamento**, a **interpretação** e a **proteção** de informações.

- **Segredos comerciais:** São informações valiosas e confidencias que dão a uma empresa uma vantagem competitiva. Os segredos comerciais abrangem muitas informações privativas/proprietárias e sigilosas, incluindo formulas, processos, métodos, técnicas, listas de clientes, informações de preços, estratégias de marketing e outros dados críticos para os negócios. As empresas geralmente exigem que funcionários assinem NDAs (arquivos de não divulgação para proteger confidencialidade dos segredos comerciais.
- **Dados legíveis por humandos:** São informações que os humanos podem entender e interpretar facilmente sem processamento ou conversão adicionais. Formato acessível e legível, como texto, imagens ou conteúdo multimidia. Ex são documentos, relatórios, e-mails, páginas web, apresentações.
- **Dados não legíveis por humanos**: São aqueles que não são facilmente compreendidos ou interpretados pelos humanos em sua forma bruta. Podem estar em código binário, dados criptografados ou em uma estrutura ou codificação complexa que requer software ou algoritmos especializados para interpretar e decifrar.

Classificação de dados: Classificação de dados e esquemas de categorização marcam ativos de dados com tags para que os dados sejam gerenciados ao longo do ciclo de vida das informações. Um esquema de classificação de dados é uma arvore de decisão que se usa para aplicar uma ou mais tags ou rótulos a cada ativo de dados. Muitos são baseados no grau de confidencialidade necessário:

- **Público:** Não há restrições para a visualização dos dados.
- **Confidencial:** Informações são altamente sensíveis e devem ser vistas apenas por pessoas aprovadas dentro da organização.
- **Crítico:** As informações são valiosas demais para se permitir qualquer risco de captura. A visualização é muito restrita.

Outro tipo de esquema de classificação identifica o tipo de ativo de informação:

- **Privativo:** Informações privativas ou propriedade intelectual (PI) são informações criadas pela empresa e de posse dela.
- **Dados privados/pessoais:** estas informações estão relacionadas a uma identidade individual.

- **Sensível:** este rótulo é geralmente usado no contexto de dados pessoais e informações sensíveis que tratem de um assunto que poderia prejudicar um indivíduo se for divulgado.
- **Restrito:** Informações sensíveis que exigem controles rigorosos e acesso limitado devido a sua natureza altamente confidencial.

Soberania de dados e considerações geográficas:

Soberania de dados: Soberania de dados refere-se a uma jurisdição que impede ou restringe o processamento e o armazenamento em sistemas que não residem fisicamente nessa jurisdição.

Considerações geográficas: Os requisitos geográficos se encaixam em dois cenários diferentes:

- Os locais de armazenamento podem ter que ser cuidadosamente selecionados para mitigar problemas de soberania de dados.
- Funcionários que precisam de acesso a partir de várias localizações geográficas.

Dados de privacidade: São informações sensíveis ou de identificação pessoal associadas à identidade pessoal, financeira ou social de um indivíduo, incluindo dados que, se expostos ou tratados incorretamente, podem infringir os direitos de privacidade de um indivíduo. Exs de dados de privacidade incluem **nomes, endereços, informações de contato, números de previdência social, prontuários médicos, transações financeiras** e geralmente, quaisquer outros dados que possam identificar uma pessoa específica.

- **Funções e responsabilidades:** Controlador de dados e o processador de dados são duas funções definidas pelos regulamentos de proteção de dados, como o RGPD. Embora ambos lidem com os dados pessoais, essas funções tem semelhanças e diferenças importantes.
    - Controlador e o processador de dados estão envolvidos no tratamento de dados pessoais, O controlador de dados é a entidade ou organização que determina os propósitos e meios de processamento de dados pessoais.
    - O processador é aquele que processa os dados pessoais em nome do controlador de dados, atuando sob a autoridade e instruções do controlador de dados. Os processadores não têm poder de decisão independentes sobre os dados pessoais.
- **Direito ao esquecimento:** É um princípio fundamental da LGPD que concede aos titulares o direito de solicitar a exclusão ou remoção dos seus dados pessoais sob certas circunstâncias.

Violações de privacidade e violações de dados: a violação de dados ocorre quando as informações são lidas, modificadas ou excluídas sem autorização. Neste sentido, “lidas” pode significar tanto “vistas por uma pessoa” como “transferidas para uma rede ou mídia de armazenamento”. A violação de dados é a perda de qualquer tipo de dados, enquanto a violação de privacidade se refere especificamente à perda ou divulgação de dados pessoais e confidenciais.

- **Consequências organizacionais:**
    - Danos à reputação.

- Roubo de identidade.
- Multas.
- Roubo de propriedade intelectual

Notificação de violações: São definidas em lei ou regulamentos quem deve ser notificado.

- **Notificação e divulgação públicas:** Além da parte reguladora, pode ser necessário notificar às autoridades de cumprimento da lei, indivíduos e empresas externas afetadas pela violação, e ao público por meio da imprensa ou redes sociais. As obrigações também descrevem cronogramas para quando as partes devem ser notificadas. Por exemplo, no âmbito RGPD, a notificação deve ser feita dentro de **72 horas após tomar conhecimento de uma violação de dados pessoais**.

Protação de dados: A classificação dos dados como "em repouso", "em movimento" e "em uso" é essencial para medidas eficazes de proteção e segurança de dados. Ao analisar os dados com base em seu estado, as organizações conseguem adaptar medidas e controles de segurança para lidar com os riscos e requisitos específicos associados a cada estado de dados. Isso facilita a organização a proteger os dados em todo o seu ciclo de vida.

- **Dados em repouso:** Nesse estado os dados estão em algum tipo de mídia de armazenamento persistente. Exemplos de tipos de dados que podem estar em repouso são informações financeiras armazenadas em bancos de dados, mídia audiovisual arquivada, políticas operacionais e outros documentos administrativos. Nesse estado é possível criptografar os dados por técnicas como criptografia de disco inteiro, criptografia de banco de dados e criptografia da pasta ou do arquivo.
- **Dados em transito:** Nesse estado os dados são transmitidos por uma rede. Exemplos são tráfego de sites, tráfego de acesso remoto e etc. Nesse estado eles podem ser protegidos por um protocolo de criptografia de transporte, como TLS ou IPSec.
- **Dados em uso:** Nesse estado estão presentes na memória volátil, como registros e cache de RAM ou CPU do sistema. Exemplos de tipos de dados que podem estar em uso são documentos abertos em um aplicativo de processamento de texto, dados de banco de dados que estão sendo modificados no momento, registros de eventos sendo gerados enquanto um SO está em execução e outros. Quando os dados passam de "em repouso" para "em uso" eles são descriptografados e isso pode durar durante toda a sessão, o que os coloca em risco.

Políticas de pessoal

Políticas de Pessoal: Desempenham um papel essencial no estabelecimento de diretrizes, expectativas e padrões claros para funcionários. Elas fornecem uma estrutura para a gestão eficaz dos recursos humanos e mantem um ambiente de trabalho justo, legalizado e produtivo. As políticas de pessoal promovem uniformidade, comunicação clara, desenvolvimento dos funcionários, resolução de conflitos e gerenciamento de riscos. Ao implementar essas políticas eficazmente, as organizações podem aumentar a

satisfação dos funcionários, atrair e reter talentos, além de mitigar riscos legais e operacionais.

Políticas de conduta: As políticas operacionais incluem o gerenciamento de privilégios/credenciais, o processamento de dados e a resposta a incidentes.

- **Política de uso aceitável:** Ao aplicar uma política de uso aceitável (AUP), é importante proteger a organização contra as implicações **legais** e de **segurança** do possível mau uso que os **funcionários** fizerem de seus equipamentos.
- **Uso de dispositivos particulares no local de trabalho:** Dispositivos portáteis, dispositivos USB e reprodutores de mídia, podem representar uma ameaça considerável à segurança dos dados, pois eles facilitam a cópia de arquivos. Recursos de gravação de voz e vídeo são outras questões obvias de segurança. É importante também levar em conta o uso particular não autorizado de software pessoal ou de softwares ou serviços que não foram sancionados para um projeto (**shadow IT**).
- **Política de mesa limpa:** Impede que os funcionários mantenham arquivos na área de trabalho.

Treinamento baseado em usuários e funções: funcionários destreinados são uma vulnerabilidade enorme e é necessário que sejam treinados e capacitados independente do seu nível de hierarquia. Alguns tópicos gerais que precisam ser abordados:

- Visão geral das políticas de segurança da organização e das penalidades por não conformidade.
- Procedimentos de identificação e notificação de incidentes.
- Procedimentos, restrições e orientações de segurança no local, incluindo simulações de segurança, acompanhamento de convidados, uso de áreas seguras e dispositivos pessoais.
- Tratamento de dados, incluindo confidencialidade de documentos, backup, criptografia e assim por diante.
- Gerenciamento de senhas e contas, além de recursos de segurança de PCs e dispositivos móveis.
- Conscientização sobre ameaças de engenharia social e malware, como phishinig, explorações de sites e spam.

Tópicos e Técnicas de capacitação:

- **Treinamento baseado em computador e gamificação:** O treinamento baseado em computador (CBT) permite que um aluno adquira habilidades e experiencia ao concluir vários tipos de atividades práticas, tais como:
    - **Simulações:** Recriar interfaces de sistema ou usar emuladores para que os alunos possam praticar as tarefas de configuração.
    - **Cenários de ramificação:** Fazer com que os alunos escolham quais são as melhores opções para resolver um incidente de segurança cibernética.
- **Campanhas de phishing:**
- **Comportamento anômalo:** O reconhecimento de comportamento anômalo se refere à identificação de ações ou padrões que se desviam significativamente das expectativas. Isso inclui tráfego de rede incomum, anomalias na atividade na

conta do usuário, ações de ameaça interna, eventos anormais no sistema e transações fraudulentas.