1.2

Ativos - qualquer coisa de valor para uma organização que deva ser protegida, incluindo servidores, dispositivos de infraestrutura, dispositivos finais e o maior ativo, dados.

Há quatro etapas para identificação e classificação de ativos: 1. Determinar uma categoria de identificação de ativos adequada. Estabeleça a responsabilização, identificando o proprietário de todos os ativos de informações e de softwares de aplicativos. Determinar os critérios de classificação. e 4 Implemente um esquema de classificação.

Vulnerabilidades - Uma fraqueza em um sistema ou em seu design que pode ser explorada por um agente ameaçador.

Ameaças - Qualquer perigo potencial para um ativo.

O gerenciamento de ativos consiste em inventários de todos os ativos e, em seguida, desenvolver e implementar políticas e procedimentos para cobri-los.

Ciclos de um ativo

Aquisição

Implementação

Utilização

Manutenção

Eliminação

Defesas em profundidade

Uma analogia comumente usada para descrever uma abordagem de defesa em profundidade é chamada de “cebola de segurança”. Como ilustrado na figura, um ator de ameaça teria que descascar as defesas de uma rede camada por camada de uma maneira semelhante a descascar uma cebola. Só depois de penetrar cada camada, o ator da ameaça alcançaria os dados ou o sistema de destino.

O cenário em mudança da rede, como a evolução das redes sem fronteiras, mudou essa analogia para a “alcachofra de segurança”, que beneficia o ator de ameaça.

Conforme ilustrado na figura, os atores da ameaça não precisam mais descascar cada camada. Eles só precisam remover certas “folhas de alcachofra”. O bônus é que cada “folha” da rede pode revelar dados eventuais que não estejam bem protegidos.

Por exemplo, é mais fácil para um agente ameaçador comprometer um dispositivo móvel do que comprometer um computador ou servidor interno protegido por camadas de defesa. Cada dispositivo móvel é uma folha. E folha após folha, tudo leva o hacker a mais dados. O coração da alcachofra é onde os dados mais convenientes são encontrados. Cada folha fornece uma camada de proteção enquanto fornece simultaneamente um caminho para o ataque.

Nem todas as folhas precisam ser removidas para chegar ao coração da alcachofra. O hacker arrancou uma armadura de segurança ao longo do perímetro para chegar à “coração” da empresa.

estratégia de defesa

Sobreposição

Para garantir que as informações e os dados permaneçam disponíveis, uma empresa precisa criar diferentes camadas de proteção. Um bom exemplo de camadas é uma empresa que armazena seus documentos ultra-secretos em um servidor protegido por senha em um prédio trancado e cercado por uma cerca elétrica.

Uma abordagem em camadas oferece a proteção mais abrangente porque, mesmo que os crimes cibernéticos penetrem em uma camada, eles ainda precisam enfrentar várias outras defesas. Idealmente, cada camada deve ser mais complicada de superar!

A defesa em profundidade não fornecerá um escudo cibernético impenetrável, mas ajudará a empresa a minimizar riscos, mantendo-se um passo à frente das violações virtuais.

[17:23, 19/03/2025] Eduardo: Limitação

Limitar o acesso aos dados e às informações reduz a possibilidade de uma ameaça. Uma empresa deve restringir o acesso para que os usuários tenham apenas o nível de acesso necessário para fazer o seu trabalho.

Uma empresa deve ter ferramentas e configurações certas, como permissões de arquivo, para limitar o acesso, bem como medidas processuais certas, que definem etapas específicas para fazer qualquer coisa que possa afetar a segurança. Por exemplo, um procedimento de restrições que exige que os funcionários sempre consultem documentos provisórios em uma sala com CCTV garante que eles nunca removam esses documentos das instalações.

[17:23, 19/03/2025] Eduardo: Diversidade

Se todas as camadas protegidas fossem as mesmas, não seria muito difícil, para os crimes virtuais, realizar um ataque bem-sucedido. As camadas devem ser diferentes para que, se uma camada for penetrada, a mesma técnica não funcione em todas as outras, o que comprometeria todo o sistema. Uma empresa pode usar diferentes algoritmos de criptografia ou sistemas de autenticação para proteger os dados em diferentes estados.

Para atingir o objetivo de diversidade nas defesas, as empresas podem usar produtos de segurança de diferentes empresas como diferentes fatores de autenticação, como um cartão de furto de uma empresa e um leitor de impressão digital fabricado por uma empresa diferente, bem como medidas de segurança variadas, como bloqueios de tempo nos armários e supervisão por um membro da equipe de segurança ao desbloqueá-lo.

[17:24, 19/03/2025] Eduardo: Ofuscação

A ofuscação de informações também pode proteger dados e informações. Uma empresa não deve revelar informações que as infrações virtuais podem usar para descobrir a versão do sistema operacional em execução em um servidor ou o tipo de equipamento que ele usa.

Por exemplo, as mensagens de erro não devem conter nenhum detalhe que os crimes virtuais possam usar para determinar as vulnerabilidades que estão presentes. Ocultar certos tipos de informação dificulta ataques de crimes virtuais a um sistema.

[17:24, 19/03/2025] Eduardo: Simplicidade

A complexidade não garante, necessariamente, a segurança. Se uma empresa implementa sistemas complexos que são difíceis de entender e solucionar problemas, o “tiro pode sair pela culatra”. Se os funcionários não entendem como configurar uma solução complexa corretamente, pode ser tão fácil quando em uma solução mais simples para os crimes virtuais comprometerem esses sistemas.

Para manter a disponibilidade, uma solução de segurança deve ser simples, do ponto de vista de dentro da empresa, mas complexa do ponto de vista externo.

[17:32, 19/03/2025] Eduardo: 1.2

O gerenciamento de configuração refere-se à identificação, controle e auditoria de melhorias e de quaisquer alterações feitas na linha de base exigidas de um sistema.

A configuração da linha de base inclui todas as definições definidas para um sistema que fornece uma base para todos os sistemas semelhantes, como um tipo de modelo.

[17:33, 19/03/2025] Eduardo: Um log registra todos os eventos que ocorrem. As entradas de log contêm um arquivo de log e uma entrada de log contém todas as informações relacionadas a um evento específico. Registros precisos e completos são muito importantes na segurança digital.

[17:33, 19/03/2025] Eduardo: O gerenciamento de dados do log de segurança do computador deve determinar os procedimentos para o seguinte:

Gerando arquivos de log

Transmissão de arquivos de log

Armazenamento de arquivos de log

Análise de dados

Baixando dados de log

[17:37, 19/03/2025] Eduardo: O analisador de pacotes captura cada pacote, mostra os valores de vários campos no pacote e analisa o conteúdo. Um sniffer pode capturar o tráfego em redes com e sem fio.

Os analisadores de pacotes executam as seguintes funções:

Log de tráfego

Análise de problemas de rede

Detecção de uso indevido da rede

Detecção de tentativa de invasão da rede

Isolamento do sistema explorado

[17:38, 19/03/2025] Eduardo: Logs do sistema operacional

O sistema operacional registra eventos de registro que estão vinculados às ações relacionadas ao sistema operacional. Os eventos do sistema incluem o seguinte:

Solicitações de cliente e respostas do servidor, como autenticações de usuário bem-sucedidas

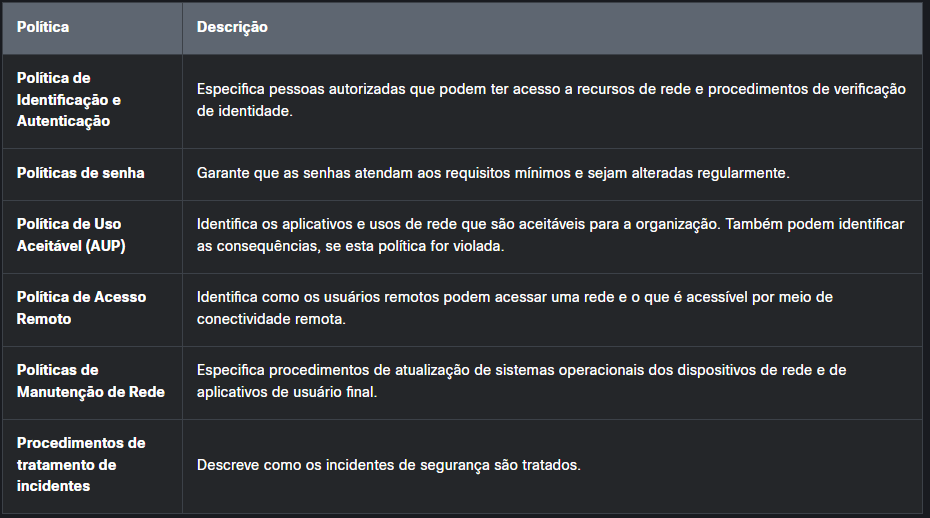
Informações de uso que contêm o número e o tamanho das transações em um determinado período de tempo

[17:38, 19/03/2025] Eduardo: Segurança de aplicações

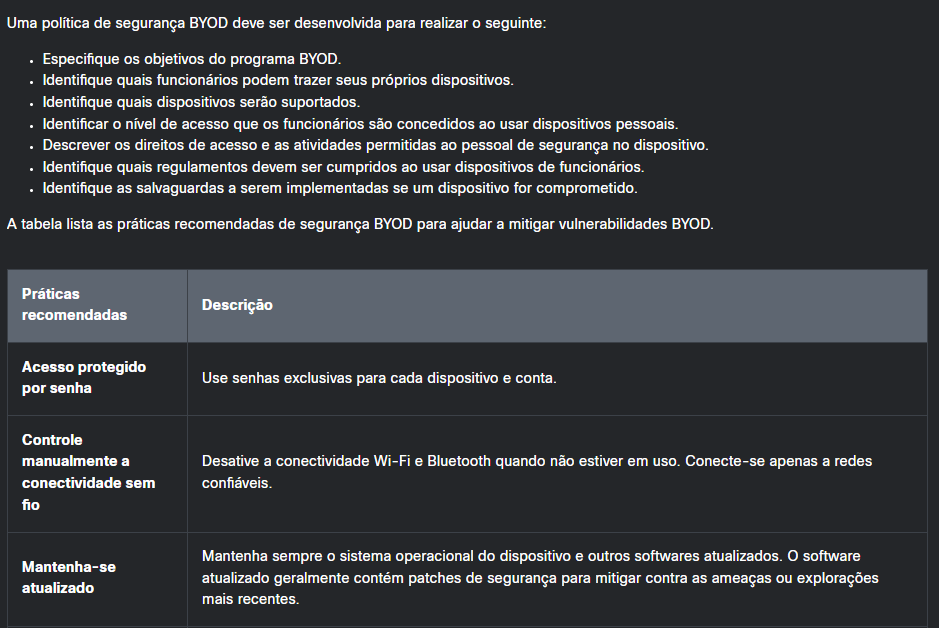
As empresas utilizam software de segurança pela rede ou pelo sistema para detectar atividades mal-intencionadas.

Esse software gera um log de segurança para fornecer dados de segurança do computador. Os logs são úteis para a realização de análise de auditorias e para a identificação de tendências e de problemas no longo prazo. Os registros também permitem que uma empresa forneça documentação que mostre que está em conformidade com as leis e os requisitos regulamentares.

1.3

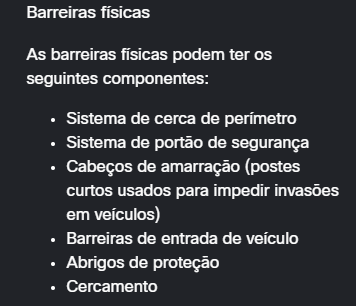


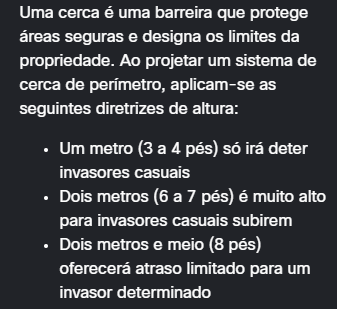
1.3.1



2.1

**Cercas e barreiras físicas**





Sistemas de autenticação de biometria incluem medições da face, impressão digital, geometria da mão, íris, retina, assinatura e voz.

Ao selecionar sistemas biométricos, há vários fatores importantes a serem considerados, incluindo:

* Precisão
* taxa de transferência
* Aceitação para usuários
* Exclusividade do órgão biométrico e ação
* Resistência à falsificação
* Confiabilidade
* Requisitos de armazenamento de dados
* Tempo de inscrição
* Intrusão na verificação

O mais importante desses fatores é a precisão, que é expressa em tipos de erro e taxas.

A primeira taxa de erro é erros de tipo I ou rejeições falsas. Um erro de tipo I rejeita uma pessoa que se registra e é um usuário autorizado. No controle de acesso, em que o objetivo principal é afastar os criminosos digitais, a falsa rejeição é o erro menos importante. Isso significa que alguém que deve obter acesso não tem acesso.

Aceitação falsa é um erro Tipo II. Os erros de tipo II permitem a entrada de pessoas que não deveriam ter acesso, o que significa que um criminoso digital pode obter acesso. Erros de tipo II permitem a entrada de invasores e, portanto, são considerados o erro mais importante em um sistema de controle de acesso de biometria.

A taxa de aceitação também é um conceito importante aqui. A taxa de aceitação é indicada como uma percentagem e é a taxa na qual um sistema aceita indivíduos que cancelaram a inscrição ou impostores como usuários autênticos.

**2.1.5 Vigilância**

Guardas e escoltas

Vigilância eletrônica e por vídeo

Vigilância sem fio e RFID - RFID (Radio Frequency Identification, Identificação por radiofrequência)

**2.2.2 Desenvolvimento de Aplicativos**

Desenvolvimento e teste

pode ser desenvolvido, testado e depurado antes de ser implantado.  A garantia de qualidade (QA) pode encontrar falhas no software.

Preparo e produção

Provisionamento e desprovisionamento

normalização

A normalização é usada para organizar dados em um banco de dados e ajudar a manter a integridade dos dados. A normalização converte uma sequência de entrada em sua forma mais simples conhecida para garantir que todas as sequências tenham representações binárias exclusivas e que qualquer entrada mal-intencionada seja identificada.

 procedimento armazenado

Um procedimento armazenado é um grupo de instruções SQL pré-compiladas armazenadas em um banco de dados que executa uma tarefa. Se você usar um procedimento armazenado para aceitar parâmetros de entrada de clientes que usam dados de entrada diferentes, reduzirá o tráfego de rede e obterá resultados mais rápidos.

ofuscação e a camuflagem

Um desenvolvedor pode usar a ofuscação e a camuflagem para impedir que o software seja reprojetado. A ofuscação oculta dados originais com caracteres ou dados aleatórios. A camuflagem substitui os dados confidenciais por dados fictícios realistas.

reutilização de código

A reutilização de código significa usar o software atual para criar um novo software, economizando tempo e custos de desenvolvimento. É preciso ter cuidado, no entanto, para evitar a introdução de vulnerabilidades.

Kits de desenvolvimento de software e bibliotecas de terceiros (SDKs)

Kits de desenvolvimento de software e bibliotecas de terceiros (SDKs) fornecem um repositório de códigos úteis para tornar o desenvolvimento de aplicativos mais rápido e mais barato. A desvantagem é que qualquer vulnerabilidade em SDKs ou bibliotecas de terceiros pode afetar muitos aplicativos.

2.2.6 Regras de Validação

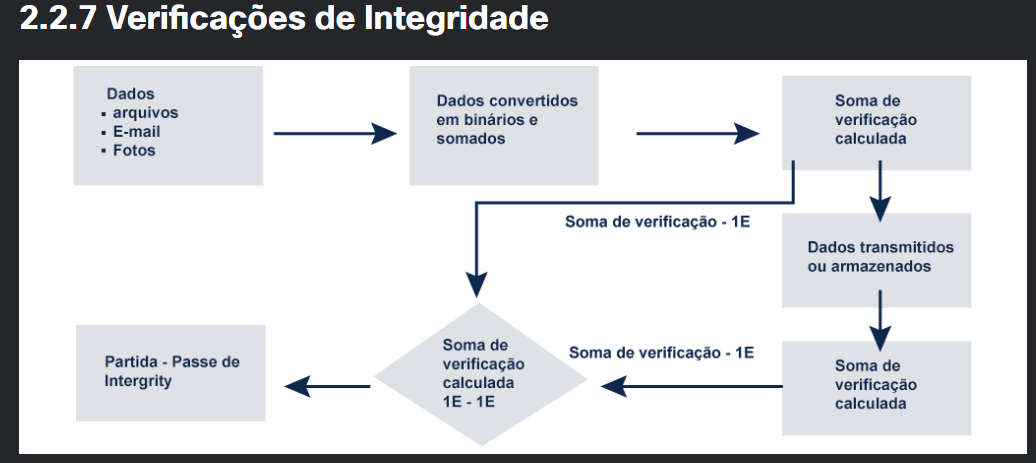
Uma regra de validação verifica se os dados estão nos parâmetros definidos pelo projetista de banco de dados. Uma regra de validação ajuda a garantir a integridade, a precisão e a consistência dos dados. Os critérios usados na regra de validação incluem o seguinte:

* Tamanho – verifica o número de caracteres em um item de dados
* Formato – verifica se os dados estão de acordo com um formato especificado
* Consistência – verifica a consistência dos códigos nos itens de dados relacionados
* Intervalo – verifica se os dados estão dentro de valores mínimo e máximo
* Dígito de verificação – efetua um cálculo extra para gerar um dígito de verificação para detecção de erros

**dígito de verificação.**

**Multiplique o primeiro dígito do ISBN por 10, o segundo dígito por 9,...o nono dígito por 2. Somar todos os números.**

**O dígito de verificação é o número necessário para obter o total a ser adicionado a um múltiplo de 11.**



 A verificação de integridade executa uma **função hash** para obter um instantâneo de dados e, em seguida, usa esse instantâneo para garantir que os dados permaneçam inalterados. Um **checksum** é um exemplo de uma função hash.

Como funciona um checksum

Uma checksum verifica a integridade de arquivos, ou de strings de caracteres, antes e depois de serem transferidos de um dispositivo para outro por uma rede local ou pela Internet. As checksum simplesmente convertem cada conjunto de informações para um valor e soma o total. Para testar a integridade de dados, um sistema de recebimento apenas repete o processo. Se as duas somas forem iguais, os dados são válidos. Caso contrário, uma alteração ocorreu em algum lugar ao longo do caminho.

Funções hash

Funções hash comuns incluem MD5, SHA-1, SHA-256 e SHA-512. Eles usam algoritmos matemáticos complexos para comparar dados com um valor de hash. Por exemplo, depois de baixar um arquivo, o usuário pode verificar a integridade do arquivo, comparando os valores de hash da fonte com o valor gerado por qualquer calculadora de hash.

Controle de versão

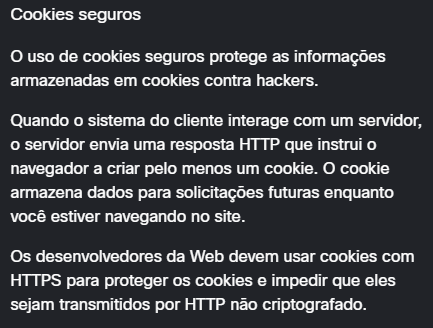
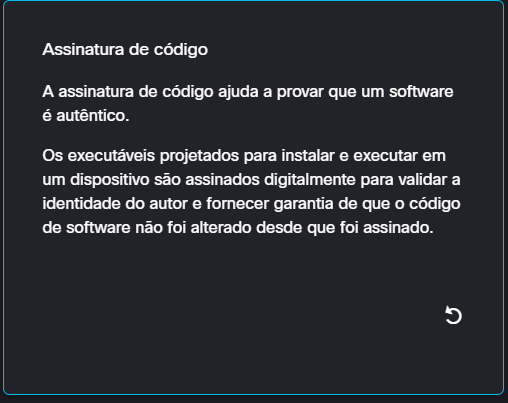
As empresas usam controle de versão para evitar alterações acidentais por usuários autorizados. O controle de versão significa que dois usuários não podem atualizar o mesmo objeto, como um arquivo, registro de banco de dados ou transação, ao mesmo tempo. Por exemplo, o primeiro usuário a abrir um documento tem a permissão para alterar esse documento. A segunda pessoa tem uma versão somente leitura.

Backups

Backups precisos ajudam a manter a integridade de dados, se os dados forem corrompidos. Uma empresa precisa verificar o seu processo para garantir a integridade do backup, antes que ocorra perda de dados.

Autorização

A autorização determina quem tem acesso aos recursos da empresa, de acordo com a necessidade de cada um. Por exemplo, controles de acesso de usuário e permissões de arquivo garantem que apenas determinados usuários possam modificar os dados. Um administrador pode definir as permissões de um arquivo como somente leitura. Como resultado, um usuário que acessa esse arquivo não pode fazer nenhuma alteração.

**2.2.8 Outras práticas de segurança de aplicativos**

**2.2.10 Controle de ameaças a aplicativos**

Acesso não autorizado a data centers, salas de computador e armário de cabos

 Período de inatividade do sistema

* Desenvolver um plano de continuidade de negócios para aplicativos essenciais para manter a disponibilidade das operações.
* Desenvolver um plano de recuperação de desastres para aplicativos e dados essenciais.

Vulnerabilidade de software do sistema operacional de rede

* Desenvolver uma política para lidar com atualizações de software de aplicativo e do sistema operacional.
* Instale correções e atualizações regularmente.

Acesso não autorizado a sistemas

* Use a autenticação multifatorial.
* Monitorar arquivos de log

Perda de dados

* Implementar padrões de classificação de dados.
* Implementar procedimentos de backup.

Vulnerabilidades de desenvolvimento de software

* Realizar testes antes do lançamento do software.

**2.3.2 Serviços de rede e de roteamento**

Para verificar os serviços de rede não protegidos, verifique se um dispositivo tem portas abertas usando um scanner de porta. Um scanner de porta envia uma mensagem para cada porta e espera por uma resposta, indicando como a porta é usada e se está aberta.

Protocolo de Configuração Dinâmica de Host (DHCP)

O DHCP usa um servidor para atribuir um endereço IP e outras informações de configuração automaticamente aos dispositivos de rede. Na realidade, o dispositivo está obtendo uma permissão do servidor DHCP para usar a rede. Os invasores podem direcionar servidores DHCP para negar o acesso a dispositivos na rede, mas medidas de segurança como rastreamento de DHCP impedem que servidores DHCP invasores forneçam endereços IP para clientes ao validar mensagens de fontes que não são confiáveis.

A Figura 1 fornece uma lista de verificação de segurança para DHCP:

* Proteja fisicamente o servidor DHCP.
* Aplique as correções de software.
* Localize o servidor DHCP atrás de um firewall.
* Monitore a atividade do DHCP analisando os registros do DHCP.
* Mantenha uma solução antivírus forte.
* Desinstale qualquer serviço e aplicação não utilizado.
* Feche as portas não utilizadas.

Domain Name System (DNS)

O DNS converte um URL ou endereço de site, como www.cisco.com, em um endereço IP numérico. Quando os usuários digitam um endereço da Web na barra de endereços, o servidor DNS reconhece o endereço IP. Os invasores podem direcionar os servidores DNS para negar o acesso aos recursos da rede ou redirecionar o tráfego para sites falsos. Use serviço e autenticação seguros entre servidores DNS para protegê-los contra esses ataques.

As DNS Security Extensions (DNSSEC) usam assinaturas digitais para fortalecer a autenticação e proteger contra ameaças ao DNS.

Uma checklist de segurança para DNS:

* Manter softwares DNS atualizados.
* Impeça que a string de versão revele informações.
* Separe os servidores DNS internos e externos.
* Restrinja as transações permitidas pelo endereço IP do cliente.
* Use assinaturas de transação para autenticar transações.
* Desative ou restrinja as transferências de zona e as atualizações dinâmicas o máximo possível.
* Habilitar o log e analisar logs.
* Use Domain Name System Security Extensions (DNSSEC).
* Assine zonas.
* Protocolo de mensagens de controle da Internet (ICMP)
* Dispositivos de rede usam ICMP para enviar mensagens de erro como quando um serviço solicitado não está disponível ou se o host não pode acessar o roteador.
* O comando ping é um utilitário de rede que usa o ICMP para testar a acessibilidade de um host em uma rede. O ping envia mensagens ICMP para o host e aguarda uma resposta. Os criminosos digitais podem alterar o uso do ICMP para executar ataques de canal secreto e reconhecimento, negação de serviço (DoS). Muitas redes filtram solicitações de ICMP para evitar esses ataques.
* Routing Information Protocol (RIP)
* O RIP limita o número de saltos permitidos em um caminho em uma rede do dispositivo de origem para o destino. O número máximo de saltos permitidos para o RIP é 15. O RIP é um protocolo de roteamento usado para trocar informações de roteamento sobre quais redes cada roteador pode acessar e a que distância estão essas redes.
* O RIP calcula a melhor rota com base na contagem de saltos, mas os criminosos digitais também podem direcionar roteadores e o protocolo RIP. Esses ataques a serviços de roteamento podem afetar o desempenho e a disponibilidade; alguns ataques podem até resultar em redirecionamento de tráfego. Use os serviços seguros com autenticação e implemente patches e atualizações de sistema para proteger serviços de roteamento como o RIP.
* Network Time Protocol (NTP)
* Ter o tempo correto nas redes é importante. Carimbos de data e hora corretos são necessários para rastrear com precisão os eventos da rede, como as violações de segurança. Além disso, a sincronização do relógio é fundamental para a interpretação correta dos eventos nos arquivos de dados syslog, bem como para os certificados digitais.
* O NTP (Network Time Protocol, Protocolo de tempo de rede) é um protocolo que sincroniza os relógios de sistemas de computadores em redes de dados. O NTP permite que os dispositivos de rede sincronizem as configurações de hora com um servidor NTP. Os criminosos virtuais atacam servidores de tempo para interromper a comunicação segura que depende de certificados digitais e esconder informações do ataque, como carimbos de data e hora. Use a autenticação NTP para verificar se o servidor é confiável.

2.3.3 Telnet, SSH e SCP

**O Secure Shell (SSH)** é um protocolo que fornece uma conexão com um dispositivo remoto de natureza segura (criptografada) e baseada em uma linha de comando. **O Telnet** é um protocolo mais antigo que usa transmissão de texto não criptografado, não protegido, tanto para autenticação de logon (nome de usuário e senha) quanto para dados transmitidos entre os dispositivos de comunicação. O SSH deve ser usado em vez do Telnet para gerenciar conexões, pois ele oferece criptografia forte. O SSH usa a porta TCP 22. Já o Telnet usa a porta 23.

**A SCP (Secure Copy, cópia segura)** , transfere, com segurança, arquivos de computador entre dois sistemas remotos. O SCP usa o SSH para a transferência de dados (incluindo o elemento de autenticação), para que o SCP garanta a autenticidade e a confidencialidade dos dados em trânsito.

**2.3.4 Protocolos seguros**

Protocolo de Gerenciamento Simples de Rede (SNMP)

O SNMP coleta estatísticas de dispositivos TCP / IP para monitorar a rede e equipamentos de computador. O SNMPv3 é o padrão atual - ele usa criptografia para evitar a espionagem e garantir que os dados não tenham sido violados durante o trânsito.

HTTP

O Hypertext Transfer Protocol (HTTP) fornece conectividade básica da Web e usa a porta 80. O HTTP contém segurança interna limitada e é aberto ao monitoramento de tráfego durante a transmissão de conteúdo, deixando o computador do usuário aberto para ataques. Vamos ver como outros protocolos fornecem uma conexão mais segura:

* A Secure Sockets Layer (SSL) gerencia a criptografia usando um handshake de SSL no início de uma sessão para fornecer confidencialidade e evitar a interceptação e a violação.
* O Transport Layer Security (TLS) é um substituto atualizado e mais seguro para SSL.
* O SSL / TLS criptografa a comunicação entre o cliente e o servidor. Onde for usado, o usuário verá HTTPS no campo de URL de um navegador em vez de HTTP.
* FTP
* O File Transfer Protocol (FTP) oferece a capacidade de transferir arquivos entre um cliente e um servidor. No FTP, o cliente usa um nome de usuário e uma senha de texto sem formatação para se conectar. O File Transfer Protocol Secure (FTPS) é mais seguro - ele adiciona suporte a TLS e SSL para evitar a interceptação, a violação e a falsificação de mensagens trocadas.
* POP, IMAP e MIME
* O e-mail usa Post Office Protocol (POP), IMAP (Internet Message Access Protocol) e MIME (Multipurpose Internet Mail Extensions) para anexar dados sem texto, como imagens ou vídeos, a uma mensagem de e-mail.
* Para proteger o POP (porta 110) ou IMAP (porta 143), use SSL / TLS para criptografar e-mails durante a transmissão. O protocolo Secure / Multipurpose Internet Mail Extensions (S / MIME) oferece um método seguro de transmissão. Ele envia mensagens digitalmente assinadas e criptografadas que fornecem autenticação, integridade de mensagem e não-repudiação.

**2.4.2 Redes da área local virtuais (VLANs)**

As VLANs fornecem uma forma de agrupar dispositivos em uma LAN e em switches individuais. VLANs não são iguais a LANs: LANs virtuais são baseadas em conexões lógicas, enquanto LANs são baseadas em conexões físicas. Portas individuais de um switch podem ser atribuídas a uma VLAN específica. Outras portas podem ser usadas para interconectar fisicamente os switches e permitir o tráfego de várias VLANs entre os switches. Essas portas são chamadas Trunks (troncos).

**2.4.3 Zona Desmilitarizada (DMZ)**

Uma zona desmilitarizada (DMZ) é uma pequena rede entre uma rede privada confiável e a Internet.

Acesso a redes não confiáveis

Os servidores Web e de correio geralmente são colocados na DMZ para permitir que os usuários acessem uma rede não confiável, como a Internet, sem comprometer a rede interna.

Zonas de risco

A maioria das redes tem de duas a quatro zonas de risco: a LAN privada confiável, a DMZ, a Internet e uma extranet.

* Na zona de LAN, o nível de risco é baixo e o nível de confiança é alto.
* Na zona da extranet, o nível de risco é médio-baixo e o nível de confiança médio-alto.
* Na DMZ, o nível de risco é médio-alto e o nível de confiança é médio-baixo.
* Na zona da Internet, o nível de risco é alto e o nível de confiança é baixo.
* Modelo zero-trust
* Os firewalls gerenciam o tráfego de ponta a ponta (tráfego que vai entre os servidores no data center da empresa) e o tráfego de ponta a ponta (dados que entram e saem da rede da empresa).
* Para proteger sua rede, uma empresa pode implementar um **modelo de confiança zero**. Confiar em usuários e endpoints automaticamente na empresa pode colocar qualquer rede em risco, já que usuários confiáveis podem se mover por toda a rede para acessar dados. A rede Zero Trust monitora constantemente todos os usuários na rede, independentemente de status ou função.

2.5.2 Segurança de dispositivos sem fio

A Wired Equivalent Privacy (WEP) foi o primeiro protocolo de segurança usado para redes sem fio. Isso foi substituído pelo Wi-Fi Protected Access (WPA), que melhorou a segurança das conexões sem fio.

Configuração de WPA

O Wi-Fi Protected Access (WPA) foi a resposta do setor de computadores para enfraquecer a utilização do padrão WEP. A configuração mais comum de WPA é WPA-PSK (Pre-Shared Key, Chave pré-compartilhada). As chaves usadas pelo WPA são 256 bits, um aumento significativo sobre as chaves de 64 bits e 128 bits usadas no sistema WEP.

Recursos do WPA

O padrão WPA forneceu várias melhorias de segurança. Primeiro, o WPA fornecia verificações de integridade da mensagem (Message Integrity Checks - MIC) que poderiam detectar se um invasor tinha capturado e alterado os dados transmitidos entre o ponto de acesso sem fio e um cliente sem fio. Outra melhoria importante de segurança foi o protocolo TKIP (Temporal Key Integrity Protocol, Protocolo de integridade da chave temporal). O padrão TKIP proporcionou a capacidade de tratar, proteger e alterar melhor as chaves de criptografia. O AES (Advanced Encryption Standard, Padrão de criptografia avançada) substituiu o TKIP por um melhor gerenciamento de chaves e proteção de criptografia.

WPA2 - Wi-Fi Protected Access II

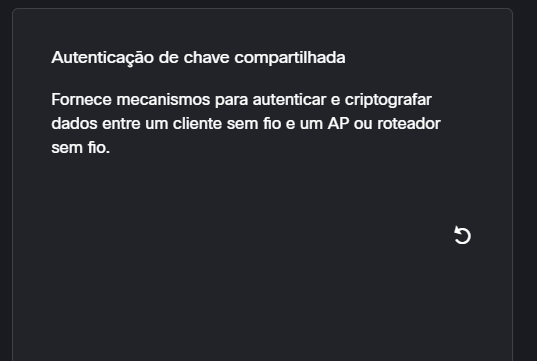
Como resultado, o lançamento do padrão WPA2 (Wi-Fi Protected Access II, Acesso protegido por Wi-Fi II) aconteceu em 2006. Isso introduziu o uso obrigatório de algoritmos AES e substituiu o TKIP pelo modo de cifra de contador pelo protocolo de código de autenticação de mensagens de cadeia de bloco (CCMP).

WPA3 - Wi-Fi Protected Access III

O WPA3 adicionou mais recursos ao WPA2, como a manutenção de algoritmos criptográficos robustos e a melhoria da troca de chaves.

Como utilizar o Wi-Fi Protected Setup (WPS)

A Configuração protegida por Wi-Fi (WPS) pode ser usada para configurar uma rede doméstica sem fio segura. Conectar dispositivos de IoT à rede sem fio No entanto, o WPS apresenta uma grande vulnerabilidade de segurança, pois o PIN do usuário pode ser descoberto através de um ataque de força bruta. Por isso, o WPS não deve ser usado e deve ser desativado por completo.

**2.5.5 Autenticação2.5.6 Protocolos de autenticação**

**O protocolo de autenticação extensível (EAP) é uma estrutura de autenticação usada em redes sem fio. Vamos descobrir como isso funciona.**

1. **O usuário solicita a conexão à rede sem fio através de um access point.**
2. **O access point solicita dados de identificação (nome de usuário) do usuário, que é então enviado para um servidor de autenticação.**
3. **O servidor de autenticação solicita a prova de que a ID é válida.**
4. **O access point solicita prova de que a ID é válida do usuário, na forma de uma senha.**
5. **O usuário fornece a senha ao access point. O access point envia de volta para o servidor de autenticação.**
6. **O servidor confirma que o nome de usuário e a senha estão corretos e passa essas informações para o access point e o usuário.**
7. **Conecte-se à rede sem fio.**
8. EAP-TLS
9. Requer certificado de cliente: Sim  
   Requer certificado de servidor: Sim  
   Implantável facilmente: Dificuldade  
   de segurança : alta
10. PEAP
11. Requer certificado de cliente: Não  
    Requer certificado de servidor: Sim  
    Implantável facilmente: Dificuldade  
    de segurança: média
12. EAP-TTLS
13. Requer certificado de cliente: Não  
    Requer certificado de servidor: Sim  
    Implantável facilmente: Dificuldade  
    de segurança: média
14. EAP-FAST
15. Requer certificado de cliente: Não  
    Requer certificado de servidor: Não  
    Implantável facilmente: Dificuldade  
    de segurança: média

**2.5.8 Autenticação mútua**

Access points não autorizados

Um access point é qualquer dispositivo de hardware que permite que outros dispositivos sem fio se conectem a uma rede com fio. Qualquer dispositivo que tenha uma interface transmissora sem fio e cabeada ligada a uma rede pode, possivelmente, agir como access point não autorizado.

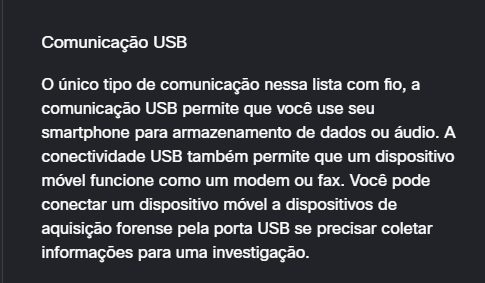
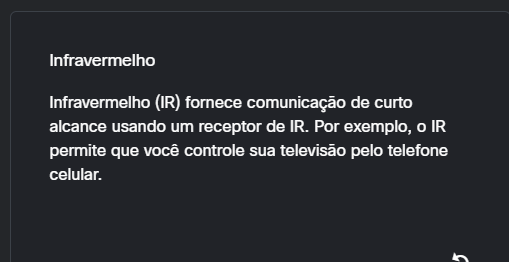
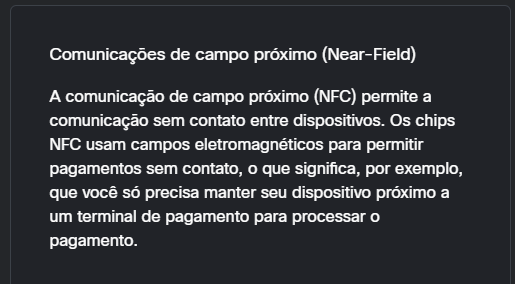
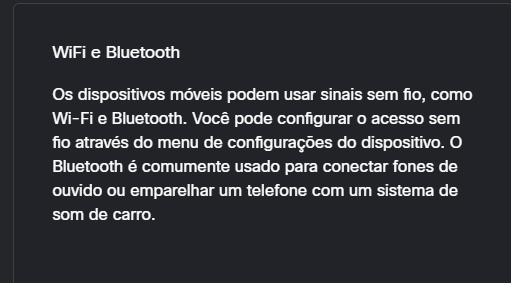
Como evitar ataques

Quando você se conecta a um access point não autorizado, o impostor que o configura pode solicitar e copiar dados do seu dispositivo. Esse tipo de ataque man in the middle é muito difícil de detectar e pode resultar em credenciais de logon roubadas e dados lidos.

A autenticação mútua é a autenticação de duas vias que pode impedir access points não autorizados. É um processo no qual as duas entidades em um link de comunicação se autenticam antes de se conectarem. Isso permite que os clientes detectem access points não autorizados e evitem esses ataques MitM.

**2.5.10 Métodos de comunicação**

Os dispositivos móveis usam comunicações por celular para se conectar a um provedor de serviços. Provedores sem fio usam redes LTE 5G IP para acessar a Internet e outros serviços de dados, por exemplo.



2.5.11 Gerenciamento de dispositivos móveis

Um dispositivo móvel emitido por uma empresa pode conter dados pessoais e organizacionais; ele pode ser de propriedade da corporação ou habilitado pessoalmente (COPE).

**Segmentação e conteinerização do armazenamento**

A segmentação do armazenamento e a conteinerização permitem separar o conteúdo pessoal e do trabalho em um dispositivo. Ele fornece uma área autenticada e criptografada que separa as informações confidenciais da empresa dos dados pessoais do usuário.

A conteinerização também nos permite:

* Isolar os aplicativos.
* Controle as funções do aplicativo.
* Exclua as informações do container.
* Bloqueie ou limpe o dispositivo remotamente.
* **Gerenciamento de conteúdo**
* Uma empresa precisa considerar os riscos de segurança envolvidos no uso de aplicativos que compartilham dados, por exemplo, Dropbox, Box, Google Drive e iCloud. Um sistema de segurança de gerenciamento de identidades pode ser usado para controlar quais dados um usuário pode acessar.
* **Gerenciamento de aplicativos**
* A lista de permissão permite que você **assine digitalmente** as aplicações para que você possa autorizar as aplicações que os usuários podem instalar. Isso ajuda a garantir que as aplicações instaladas sejam provenientes de fontes confiáveis.
* A autenticação usando senhas fortes é uma prática recomendada para os aplicativos que exigem credenciais de usuário.

**2.5.12 Proteções de dispositivo móvel**

**Jailbreaking, root e sideloading**

**Jailbreaking, root e sideload são formas de contornar as limitações de um dispositivo para fazer coisas que o dispositivo está impedido de fazer. Os usuários podem tentar fazer o jailbreak (dispositivos da Apple) ou root (dispositivos Android) para executar um aplicativo que não está autorizado ou não está disponível na loja.**

**O jailbreak remove a restrição de que apenas aplicativos autorizados pela Apple podem ser executados no dispositivo. O enraizamento ignora a arquitetura de segurança do Android para permitir acesso administrativo completo ao dispositivo. Ambos representam um risco para a empresa.**

**Há soluções disponíveis que podem detectar um dispositivo com "jailbroken" ou "rooteado". Um dispositivo é então marcado como não compatível e removido da rede ou tem o acesso negado a aplicativos organizacionais.**

**As lojas de aplicativos de terceiros também podem representar um risco para as empresas porque os aplicativos aos quais elas fornecem acesso não foram avaliados corretamente. O sideloading (carregamento lateral) ocorre quando o usuário percorre as configurações de aplicativo aprovado para instalar aplicativos não aprovados. Isso é menos invasivo do que fazer jailbreaking ou rooting, mas ainda é um risco.**

Quais são as proteções?

As proteções contra ameaças a dispositivos móveis incluem:

* Os **bloqueios de tela** exigem uma senha, um PIN ou um padrão para acessar o dispositivo.
* A **autenticação biométrica** usa uma característica física exclusiva (impressão digital, face, íris ou voz).
* A **autenticação com reconhecimento de contexto** usa aprendizado de máquina para determinar o acesso com base no comportamento normal do usuário.
* A **limpeza remota** exclui os dados do dispositivo, caso ele seja roubado ou perdido.
* A **criptografia completa** do dispositivo pode criptografar todos os dados em um dispositivo móvel.

**2.5.13 Rastreamento de GPS**

O GPS (Global Positioning System, Sistema de posicionamento Global) usa satélites e computadores para determinar a localização de um dispositivo. A tecnologia de GPS é um recurso padrão em smartphones e oferece rastreamento de posição em tempo real que normalmente pode localizar um local a aproximadamente 5 metros.

Alguns aplicativos usam a delimitação geográfica ou geolocalização, que usa a identificação por radiofrequência (RFID) para determinar uma área geográfica.

**2.6.2 Alta disponibilidade**

Sistemas de alta disponibilidade normalmente incluem estes três princípios de projeto.

**Eliminar pontos únicos de falha**

O primeiro princípio que define os sistemas de alta disponibilidade começa com a identificação de todos os dispositivos e componentes do sistema cuja falha resultaria em falha em todo o sistema. Os métodos para eliminação de pontos únicos de falhas incluem dispositivos de hot standby, componentes redundantes e várias conexões ou caminhos.

**Fornecer transição confiável**

Fontes de alimentação redundantes, sistemas de energia de backup e sistemas de comunicação de backup proporcionam transição confiável.

**Detectar falhas à medida que ocorrem**

O monitoramento ativo do dispositivo e do sistema detecta vários tipos de eventos, incluindo falhas do dispositivo e do sistema. Os sistemas de monitoramento podem até acionar o sistema de backup em caso de falha.

2.6.3 Os Cinco Noves

Toda empresa quer poder operar ininterruptamente, mesmo em condições extremas, como durante um ataque.

Dentre as práticas mais populares de alta disponibilidade estão os cinco noves. Ela recebe esse nome do objetivo de atingir uma taxa de disponibilidade de 99,999%, ou seja, cinco noves em seguida. Isso significa que o período de inatividade é menos de 5,26 minutos por ano.

Sistemas padronizados

A padronização dos sistemas propicia que os sistemas usem os mesmos componentes. Os inventários de peças são mais fáceis de manter, e é possível trocar componentes durante uma emergência.

Clustering

Clusters de vários dispositivos agrupados proporcionam um serviço que parece ser uma única entidade para um usuário. Se um dispositivo falhar, os outros dispositivos permanecem disponíveis.

Sistemas de componente compartilhado

Os sistemas são criados para que um sistema completo possa substituir um que falhou.

2.6.4 pontos únicos de falha

Únicos pontos de falha são links fracos na cadeia que podem provocar interrupção das operações da empresa. Um único ponto de falha é qualquer parte da operação da empresa cuja falha significa falha completa de todo o sistema - em outras palavras, se falhar, o sistema inteiro falhará.

2.6.6 Redundância N + 1

A redundância N+1 garante a disponibilidade do sistema, no caso de falha de um componente. Os componentes (N) precisam ter, no mínimo, um componente de backup (+1).

**2.6.7 RAID**

**O RAID obtém os dados normalmente armazenados em um único disco e os espalha entre várias unidades. Se qualquer disco único RAID0 for perdido, o usuário poderá recuperar os dados de outros discos que também hospedam os dados.**

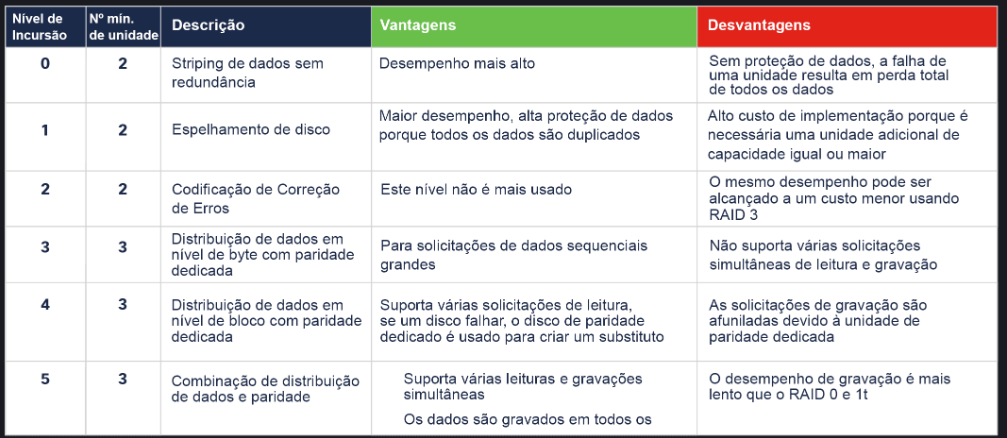
**O RAID também pode aumentar a velocidade da recuperação de dados, já que várias unidades recuperarão os dados solicitados mais rapidamente do que um disco fazendo o mesmo.**

**Uma solução RAID pode ser baseada em software ou hardware. Uma solução baseada em hardware requer um controlador de hardware especializado, no sistema que contenha as unidades RAID.**

**Os termos a seguir descrevem as várias maneiras pelas quais o RAID pode armazenar dados na matriz de discos.**

* **Espelhamento - Armazena dados duplicados em uma segunda unidade.**
* **Distribuição - Grava dados em várias unidades para que segmentos consecutivos sejam armazenados em unidades diferentes.**
* **Paridade - mais precisamente, tirar a paridade. Após a distribuição, as somas de verificação são geradas para verificar se não há erros nos dados distribuídos. Essas somas de verificação são armazenadas em uma terceira unidade.**

**Existem outras arquiteturas RAID, que combinam principalmente os elementos acima.**



**2.6.8 Spanning Tree**

**O Spanning Tree Protocol (STP) soluciona esses problemas. A função básica do STP é prevenir loops em uma rede, quando os switches se interconectarem por vários caminhos. O STP garante que os links físicos redundantes estejam livres de loop e que apenas um caminho lógico seja executado entre todos os destinos na rede. O STP bloqueia intencionalmente os caminhos redundantes que poderiam provocar um loop.**

**2.6.9 Redundância de roteador**

**o roteador de encaminhamento e o roteador standby usam um protocolo de redundância para determinar qual roteador deve assumir o papel ativo na redundância. Cada roteador está configurado com um endereço IP físico e um endereço IP do roteador virtual. Dispositivos finais usam o endereço IP virtual como o gateway padrão.**

**O roteador de encaminhamento e o roteador standby usam seus endereços IP físicos para trocar mensagens periódicas. O objetivo dessas mensagens é ter certeza de que os dois ainda estão on-line e disponíveis.**

A capacidade de uma rede de se recuperar dinamicamente da falha de um dispositivo que atua como um gateway padrão é conhecida como **redundância de primeiro salto**.

**2.6.10 Redundância de local**

Replicação síncrona

* Sincroniza os dois locais em tempo real
* Requer alta largura de banda
* Os locais devem ser próximos um do outro, para reduzir a latência

Replicação assíncrona

* Não sincronizados em tempo real, mas muito próximo disso
* Requer menos largura de banda
* Os sites podem estar mais distantes, pois a latência é o menor dos problemas

Point-in-time-Replication (Replicação de um ponto no tempo)

* Atualiza periodicamente a localização dos dados de backup
* Mais conservador em termos de largura de banda, pois não exige uma conexão constante

O equilíbrio correto entre custo e disponibilidade determinará a escolha correta para uma empresa.

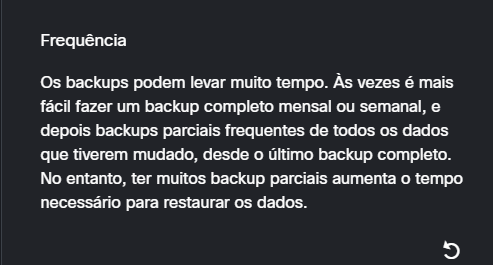
2.6.11 Design resiliente

Resiliência representa os métodos e configurações usados para tornarem um sistema ou rede tolerante a falhas.

Como visto nos exemplos acima, o design resiliente é mais do que apenas adicionar redundância. É fundamental entender as necessidades comerciais da empresa e, em seguida, incorporar a redundância para criar uma rede resiliente.

**Resiliência de aplicativo**

* **Hardware tolerante a falhas** (mais complexo e mais caro) é um sistema projetado com a colocação de múltiplos componentes essenciais em um mesmo computador.
* **Arquitetura de cluster**é um grupo de servidores que funcionam como se fossem um único sistema.
* **Backup e restauração** Cópias de backup de arquivos com a finalidade de poder restaurá-los se ocorrer perda de dados (menos complexo e menos caro).
* **Resiliência do IOS**
* O IOS (Interwork Operating System, Sistema operacional Interwork) para roteadores e switches Cisco incluem um atributo resiliente de configuração. Permite recuperação mais rápida se alguém, intencionalmente ou não, reformatar a memória flash ou apagar o arquivo de configuração de inicialização. Este atributo mantém uma cópia de trabalho segura do arquivo de imagem do IOS do roteador e uma cópia do arquivo de configuração de execução. O usuário não pode remover esses arquivos seguros, também conhecidos como o bootset primário.

**2.6.12 Sistema e backups de dados**

**2.6.14 Potência**

* Data centers devem estar em uma fonte de alimentação diferente do resto do edifício.
* Fontes de alimentação redundantes: dois ou mais feeds (fontes de alimentação) provenientes de duas ou mais subestações elétricas.
* Condições de alimentação.
* Backup de sistemas de energia são, muitas vezes, necessários.
* Uma UPS deve estar disponível para sistemas de desligamento normais.

**termos padrão vinculados a eventos do sistema de energia elétrica.**

**Excesso de energia**

* Pico: alta tensão momentânea.
* Sobrecarga: alta tensão prolongada.

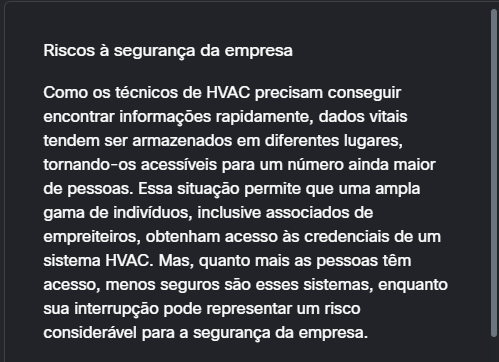
**Perda de energia**

* Falha: perda momentânea de energia.
* Blackout: Perda completa de energia.

**Degradação de energia**

* Sag/dip: baixa tensão momentânea.
* Queda de energia: baixa tensão prolongada.
* Corrente de Inrush (Pico de Corrente): sobrecarga inicial de energia.

**2.6.15 Aquecimento, ventilação e ar-condicionado (HVAC)**



2.7.2 Ameaças a setores importantes de indústrias

Ao longo da última década, ataques cibernéticos como Stuxnet provaram que um ataque cibernético pode destruir ou interromper infraestruturas essenciais. O ataque Stuxnet, especificamente, foi direcionado ao sistema SCADA (Supervisory Control and Data Acquisition, Controle de supervisão e aquisição de dados) e foi usado para controlar e monitorar processos industriais. O SCADA e outros sistemas de controle industrial (ICSs) são usados nos sistemas de manufatura, produção, energia e comunicação.

**Sistemas integrados**

Por que os sistemas integrados estão vulneráveis a ataques?

Os ataques contra sistemas integrados exploram vulnerabilidades de segurança nos componentes de software e hardware. Eles são suscetíveis a ataques de tempo, em que os invasores descobrem vulnerabilidades estudando quanto tempo o sistema leva para responder a diferentes entradas. Um ataque de tempo é considerado um ataque de canal lateral.

Esse tipo de ataque se baseia nas informações obtidas com a implementação de um sistema, e não nos pontos fracos do software. Informações de tempo, consumo de energia, vazamentos eletromagnéticos ou até mesmo som podem ser essa fonte de informações.

Como os sistemas integrados podem ser protegidos?

Uma técnica é usar a tecnologia **System on Chip (SoC)**. A tecnologia SoC é um módulo de hardware "Small Form Factor" (SFF). Exemplos de clientes incluem dispositivos como Raspberry Pi e Arduino. Esses dispositivos são computadores de placa única que podem ser implementados usando um "Field-Programmable Gate Array" (FGPA), um circuito integrado que pode ser programado ou modificado em campo. Isso significa que o usuário pode fazer alterações após a implantação do dispositivo.

O SoC integra um microcontrolador, uma aplicação ou microprocessador e periféricos como uma GPU, um módulo de Wi-Fi ou um coprocessador. O processador pode executar um sistema operacional como Windows, Linux ou Android.

Muitos desses dispositivos de SoC têm autenticação ruim e / ou não podem ser atualizados ou corrigidos. Devido à natureza desses dispositivos, um nível de confiança implícita é necessário, pois não há nenhum programa formal para verificar os controles de segurança.

**2.7.5 Internet das Coisas (IoT)**

**Usam um sistema operacional em tempo real(RTOS) um pequeno sistema operacional que permite a troca rápida em tarefas que se concentram no tempo e não na taxa de transferência. Esses aplicativos são executados com tempo preciso e alta confiabilidade**

**As vulnerabilidades associadas ao RTOS são injeção de código, ataques de Ddos e inversão de propriedade (onde uma tarefa de alta prioridade e trocada por uma de prioridade mais baixa)**

**Usar um scanner de IoT, como a Shodan, é uma maneira fácil de saber se um dispositivo de automação residencial está vulnerável a ataques. Os dispositivos de IoT se comunicam usando métodos de curto, médio ou longo alcance e incluem celular (4G, 5G), rádio e Zigbee. O Zigbee é um conjunto sem fio de protocolos para redes pessoais de área (WPANs).**

**2.7.8 Equipamento VoIP**

**Voz sobre IP (VoIP) usa redes como a Internet para fazer e receber chamadas de telefone.**

**De que equipamento você precisa?**

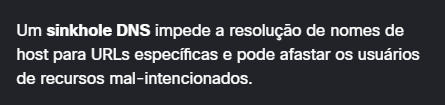
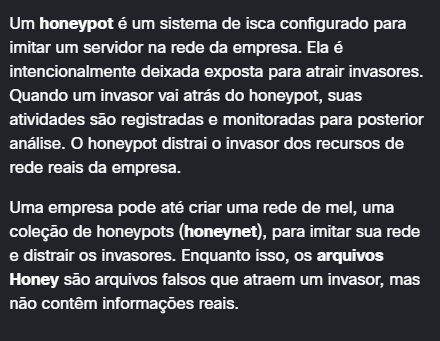
**Você precisa de uma conexão com a Internet e um telefone para VoIP. Várias opções estão disponíveis como configuração do telefone:**

* **Um telefone tradicional, com um adaptador (o adaptador atua como uma interface de hardware entre um telefone tradicional, analógico e uma linha digital VoIP)**
* **Um telefone ativado para VoIP**
* **Software VoIP instalado em um computador**

**Como você pode proteger seu serviço de VoIP?**

**Implemente as seguintes contramedidas para proteger o VoIP:**

* **Criptografe os pacotes de mensagens de voz para proteger contra espionagem.**
* **Use o SSH para proteger gateways e switches.**
* **Altere todas as senhas padrão.**
* **Use um sistema de detecção de invasão para detectar ataques, como envenenamento ARP.**
* **Use autenticação forte para mitigar o spoofing de registro (os criminosos virtuais roteiam todas as chamadas recebidas da vítima para eles), representação de proxy (engana a vítima para se comunicar com um proxy falso configurado pelos criminosos virtuais) e sequestro de chamadas (a chamada é interceptada e reencaminhada para um caminho diferente, antes de chegar ao destino).**
* **Implemente firewalls que reconhecem VoIP para monitorar os streams e filtrar sinais anormais.**

**2.7.11 Tecnologias de enganação**

**3.1 Controles de acesso**

**exploraremos exemplos de controles físicos, lógicos e administrativos antes de analisar de perto como o acesso é controlado por 'AAA' - autorização, autenticação e contabilidade.**

**3.1.2 Controles de acesso físico**

**3.1.3 Controles de acesso lógicos**

**Controles de acesso lógico são as soluções de hardware e software usadas para gerenciar o acesso aos recursos e sistemas. Essas soluções baseadas em tecnologia incluem ferramentas e protocolos que os sistemas de computador usam para identificação, autenticação, autorização e auditoria.**

**Exemplos de controle de acesso lógico incluem:**

* **A criptografia é o processo de pegar o texto claro e criar o texto codificado.**
* **Os cartões inteligentes possuem um microchip integrado.**
* **As senhas são strings de caracteres protegidos.**
* **A biometria se refere às características físicas dos usuários.**
* **As listas de controle de acesso (ACLs) definem o tipo de tráfego permitido em uma rede.**
* **Os protocolos são conjuntos de regras que regem a troca de dados entre os dispositivos.**
* **Os firewalls impedem o tráfego de rede indesejado.**
* **Os roteadores conectam pelo menos duas redes.**
* **Os sistemas de detecção de invasão monitoram as atividades suspeitas de uma rede.**
* **Os níveis de corte são determinados pelos limites permitidos para erros antes de acionar uma bandeira vermelha.**

**3.1.5 Controles de Acesso Administrativos em Detalhes**

**O conceito de controles de acesso administrativo envolve três serviços de segurança: autenticação, autorização e contabilidade (AAA).**

**Autenticação**

**O primeiro A no AAA representa a autenticação. A autenticação verifica a identidade de um usuário para evitar o acesso não autorizado.**

**Além disso, os usuários precisam verificar sua identidade fornecendo um dos seguintes:**

* **Algo que saibam (como uma senha)**
* **Algo que tenham (como um token ou cartão)**
* **Algo que eles são (como uma impressão digital)**

**No caso da autenticação de dois fatores, que está se tornando cada vez mais a regra, o sistema requer uma combinação de duas das alternativas acima, em vez de apenas uma, para verificar a identidade de alguém.**

**Autorização**

**Alguns sistemas fazem isso usando uma lista de controle de acesso, ou uma ACL. Uma ACL determina se um usuário tem certos privilégios de acesso depois de se autenticar. Só porque você pode fazer logon na rede corporativa não significa que você tenha permissão para usar a impressora colorida de alta velocidade, por exemplo.**

**Contabilidade**

**Não relacionada à contabilidade financeira, a contabilidade em AAA acompanha o que os usuários fazem – incluindo o que eles acessam, a quantidade de tempo que acessam os recursos e quaisquer alterações que fazem.** **O Accounting controla e monitora em tempo real.**

**3.1.6 O que é identificação?**

**A identificação aplica as regras estabelecidas pela política de autorização. Sempre que o acesso a um recurso é solicitado, os controles de acesso determinam se o acesso deve ser concedido ou negado.**

**3.1.8 Gerenciamento de Identidade Federada**

**O gerenciamento de identidades federadas refere-se a várias empresas que permitem que seus usuários usem as mesmas credenciais de identificação para obter acesso às redes de todas as empresas do grupo. Infelizmente, isso amplia o escopo e aumenta a probabilidade de um efeito em cascata caso ocorra um ataque.**

**3.1.9 Métodos de Autenticação**

**O que você sabe**

**Senhas, frases secretas ou PINs são exemplos de algo que o usuário *conhece*. As senhas são o método mais popular usado para autenticação.**

**Os termos frase secreta, código de acesso, chave de acesso ou PIN são chamados genericamente de senha. Uma senha é uma string de caracteres protegidos usada para comprovar a identidade de um usuário.**

**O que você tem**

**Cartões inteligentes e chaveiros de segurança são exemplos de algo que os usuários possuem e que podem ser usados para fins de autenticação.**

**Um cartão inteligente é um pequeno cartão de plástico, do tamanho de um cartão de crédito, com um pequeno chip embutido nele. O chip é um portador de dados inteligente, capaz de processar, armazenar e proteger dados.** **Na maioria dos casos, as chaves de segurança são usadas para autenticação de dois fatores (2FA)**

**Quem você é**

**Características físicas únicas, como impressão digital, retina ou voz, que identificam uma pessoa específica são chamadas de biometria. A segurança biométrica compara as características físicas aos perfis armazenados para autenticar os usuários.**

**Existem dois tipos de identificadores biométricos:**

* **Características fisiológicas – Incluem impressões digitais, DNA, rosto, mãos, retina ou ouvido**
* **Características comportamentais - padrões de comportamento como gestos, voz, andar ou ritmo de digitação.**

**A implementação da biometria envolve um leitor ou dispositivo de digitalização, um software que converte as informações digitalizadas em formato digital e um banco de dados que possui dados biométricos armazenados para comparação.**

**3.1.12 Autorização**

**A autorização controla o que um usuário pode e não pode fazer na rede após a autenticação com sucesso.**

**Quando implementar a autorização**

**A autorização usa um conjunto de atributos que descreve o acesso do usuário à rede para responder à pergunta: "Quais privilégios de leitura, cópia, edição, criação e exclusão esse usuário tem?"** **Os administradores do sistema configuraram a rede para implementar a autorização imediatamente após a autenticação do usuário.**

**Usando autorização**

**Definir as regras de autorização é a primeira etapa no controle de acesso. Uma política de autorização estabelece essas regras.**

**Uma política de associação baseada em grupo define a autorização com base nos membros de um grupo específico. Uma política de nível de autoridade define as permissões de acesso com base na posição de um funcionário na organização.**

**3.1.15 Implementação de Auditabilidade**

**O que é accountability (auditabilidade)?**

**A auditabilidade rastreia uma ação de volta a uma pessoa ou processo que faz essa mudança em um sistema. A auditabilidade então coleta essas informações e relata os dados de uso.**

**Implementação de Auditabilidade**

**A implementação da auditabilidade consiste em tecnologias, políticas, procedimentos e educação. Os arquivos de log fornecem as informações de detalhes com base nos parâmetros escolhidos.** **As políticas e procedimentos da empresa determinam quais ações devem ser registadas e como os arquivos de log são gerados, revisados e armazenados.**

**Oferecer responsabilidade**

**A retenção de dados, eliminação de mídia e requisitos de conformidade geram auditabilidade. Muitas leis exigem a implementação de medidas para proteger diferentes tipos de dados. Essas leis orientam uma empresa sobre o caminho certo para manusear, armazenar e eliminar dados.**

**3.2.1 Segurança Zero Trust**

**Zero Trust é uma abordagem abrangente para proteger todo o acesso em redes, aplicações e ambientes. Essa abordagem ajuda a proteger o acesso de usuários, dispositivos de usuário final, APIs, IoT, microsserviços, contêineres e muito mais. Ele protege a força de trabalho, as cargas de trabalho e o local de trabalho de uma organização. O princípio de uma abordagem de confiança zero é: “Nunca confie, sempre verifique”. Assumir confiança zero sempre que alguém ou algo solicitar acesso a ativos.** **Os três pilares da confiança zero são força de trabalho, cargas de trabalho e local de trabalho.**

**Confiança zero para a força de trabalho**

**Este pilar consiste em pessoas (por exemplo, funcionários, prestadores de serviços, parceiros e fornecedores) que acessam aplicativos de trabalho usando seus dispositivos pessoais ou gerenciados por empresas. Esse pilar garante que apenas os usuários certos e dispositivos seguros possam acessar aplicativos, independentemente da localização.**

**Confiança zero para cargas de trabalho**

**Esse pilar está preocupado com aplicativos que estão sendo executados na nuvem, em data centers e outros ambientes virtualizados que interagem uns com os outros. Ele se concentra no acesso seguro quando uma API, um microsserviço ou um contêiner está acessando um banco de dados dentro de um aplicativo.**

**Confiança zero para o local de trabalho**

**Este pilar se concentra no acesso seguro para qualquer e todos os dispositivos, inclusive na Internet das Coisas (IoT), que se conectam a redes empresariais, como terminais de usuário, servidores físicos e virtuais, impressoras, câmeras, sistemas de AVAC, quiosques, bombas de infusão, sistemas de controle industrial e muito mais.**

**3.2.2 Modelos de controle de acesso**

**Discretionary access control (DAC)**

* **Este é o modelo menos restritivo e permite que os usuários controlem o acesso aos seus dados como proprietários desses dados.**
* **O DAC pode usar ACLs ou outros métodos para especificar quais usuários ou grupos de usuários têm acesso às informações.**

**Controle de acesso obrigatório (MAC)**

* **Isso aplica o controle de acesso mais rigoroso e é normalmente usado em aplicações militares ou de missão crítica.**
* **Ele atribui rótulos de nível de segurança às informações e permite que os usuários tenham acesso com base em sua autorização de nível de segurança.**

**Controle de acesso baseado em funções (RBAC)**

* **As decisões de acesso são baseadas nas funções e responsabilidades de um indivíduo dentro da organização.**
* **Diferentes funções recebem privilégios de segurança e indivíduos são atribuídos ao perfil RBAC para a função.**
* **As funções podem incluir diferentes posições, classificações de cargo ou grupos de classificações de emprego.**
* **Também conhecido como um tipo de controle de acesso não discricionário.**
* **Controle de acesso baseado em atributos (ABAC)**
* O ABAC permite o acesso com base em atributos do objeto (recurso) a ser acessado, o sujeito (usuário) acessando o recurso e fatores ambientais sobre como o objeto deve ser acessado, como a hora do dia.

**Controle de acesso baseado em regras (RBAC)**

* **A equipe de segurança de rede especifica conjuntos de regras ou condições associadas ao acesso a dados ou sistemas.**
* **Essas regras podem especificar endereços IP permitidos ou negados, ou determinados protocolos e outras condições.**
* **Também conhecido como RBAC Baseado em Regras.**
* **Controle de acesso baseado em tempo (TAC)**
* TAC Permite o acesso a recursos de rede com base na hora e no dia.
* Outro modelo de controle de acesso é o princípio do privilégio mínimo, que especifica uma abordagem limitada, conforme necessário, para conceder direitos de acesso ao usuário e ao processo a informações e ferramentas específicas. O princípio do privilégio mínimo afirma que os usuários devem receber a quantidade mínima de acesso necessária para desempenhar sua função de trabalho.
* Uma exploração comum é conhecida como escalação de privilégios. Nesta exploração, vulnerabilidades em servidores ou sistemas de controle de acesso são exploradas para conceder a um usuário não autorizado, ou processo de software, níveis de privilégio mais altos do que deveriam ter. Depois que o privilégio é concedido, o agente de ameaça pode acessar informações confidenciais ou assumir o controle de um sistema.

**3.2.3 Sistemas de controle de acesso à rede (NAC)**

**Network Access Control (NAC) são compatíveis com o gerenciamento de acesso ao aplicar políticas organizacionais relacionadas às pessoas e aos dispositivos que estão tentando acessar a rede. Os sistemas NAC permitem que profissionais de cyberscurity monitorem os usuários e dispositivos conectados à rede e controlem manualmente o acesso conforme necessário.**

**Os sistemas de controle de acesso à rede oferecem os seguintes recursos:**

* **Aplicação rápida de políticas de acesso que foram criadas para diferentes condições operacionais.**
* **Reconhecer e criar perfis de usuários e dispositivos conectados para evitar que softwares mal-intencionados em sistemas não compatíveis causem danos.**
* **Fornecer acesso seguro aos convidados da rede, geralmente através de portais de registro.**
* **Avaliar a conformidade do dispositivo com as políticas de segurança por tipo de usuário, tipo de dispositivo e sistema operacional antes de permitir o acesso à rede.**
* **Atenuar os incidentes de segurança ao bloquear, isolar ou reparar dispositivos não compatíveis.**

**Como as redes BYOD e IoT expandem muito a superfície de ataque da rede, os recursos de automação do sistema NAC tornam prático o controle focado do acesso à rede por esses dispositivos. O sistema NAC está configurado para impor políticas organizacionais. As políticas relevantes são decretadas para permitir ou negar o acesso à rede de acordo com uma ampla gama de fatores que o sistema NAC detecta nos dispositivos que estão tentando acessar. Sem os sistemas NAC, seria impossível para o pessoal de segurança cibernética avaliar os milhares de dispositivos que poderiam tentar acessar a rede.**