**Vulnerabilidades, Credenciais, Engenharia Social, Proteção e Prevenção**

**Vulnerabilidades**

**Fator Humano**

Erros, negligência, falta de conhecimento, conscientização, etc. Isso tudo leva a uma grande vulnerabilidade, que pode ser prejudicial tanto para a pessoa (Ataques Phishing) quanto para um sistema.

**Exemplo:** Um funcionário anotar sua senha em um post-it e colar no monitor, ou clicar em um link de phishing

**Políticas de Segurança**

A falta de políticas claras ou até a falta de políticas podem levar a erros em sua aplicação, causando grandes problemas.

**Exemplo:** Uma empresa que não possui uma política clara sobre o uso de dispositivos pessoas para trabalho, levando os dados corporativos a serem armazenados em dispositivos não seguros.

**Credenciais**

**O que é?**

São informações usadas para verificar a identidade de um usuário ou processo, permite o acesso a sistemas, aplicativos e dados.

Geralmente, consiste em **nome de usuário e senha**. As credenciais são de própria responsabilidade.

**Senhas fortes**

Senhas fortes são senhas que são longas (Mínimo de 12-15 caracteres), complexas (combinação de letras minúsculas e maiúsculas, números e símbolos) e senhas únicas para cada conta

Senhas fortes são menos vulneráveis a ataques de força bruta (tentativa de todas as combinações possíveis) e ataques de dicionários (tentativa de palavras comuns)

Exemplo de senha fraca: “senha123”.

Exemplo de senha forte: “Tr@v£lh@rS3gur0l2024”.

**Senhas complexas vs Força Bruta**

Quanto mais longa e complexa é a senha, mais forte e segura ela é contra ataques de força bruta.

Exemplo:

Senha numérica de 4 caracteres – 10.000 combinações – 1 segundo para ser descoberta

Senha fraca de 6 letras – 308 milhões de combinações - ± 2 minutos para descobrir

Senha complexa de 8 caracteres – 6,6 quatrilhões de combinações - ± 5 anos para descobrir

Senha complexa com + de 12 caracteres – Milhões de anos para descobrir

**Gerenciadores de Senhas**

Aplicativos que criam senhas fortes e únicas para cada conta, ele também guarda suas senhas e armazenam elas de forma criptografada (segura). O usuário precisa de uma senha mestre para acessar todas as outras senhas (acessar o aplicativo).

**MFA e 2FA**

MFA: Autenticação de Múltiplos Fatores

2FA: Autenticação de Dois Fatores

Adicionar uma camada de segurança além da senha.

Essas proteções são extremamente seguras e fortalecem sua conta.

**Noções Básicas**

* **Não compartilhar senhas:** Senhas são pessoais.
* **Alterar senhas regularmente e imediatamente se houver suspeita de comprometimento**
* **Evitar reuso de senhas:** Se você utilizar a mesma senha em todas as contas, caso uma seja descoberta, todas serão comprometidas.

**Para criação de senhas e teste:**

<https://bitwarden.com/password-strength/>

Recomendação de gerenciador de senhas:

**BitWarden**

**Engenharia Social**

**Definição**

Arte de manipular psicologicamente as pessoas para que realizem ações específicas ou divulguem informações confidenciais

É uma tática de ataque que explora a confiança e outros aspectos psicológicos humanos

**O fator humano é o principal alvo.**

**Características**

* **Manipulação emocional:** Medo, curiosidade, ganância, senso de urgência. Geralmente, se aproveitam de pessoas mais vulneráveis (Menos espertas, “boazinhas demais”, pessoas em dias ruins, etc.)
* **Uso de autoridade ou familiaridade**: Fingem ser chefes, colegas, técnicos.
* **Aparência legítima**: e-mails, sites e telefonemas que parecem reais.
* **Persistência e persuasão**: Tentativas contínuas e bem elaboradas.

**Técnicas**

**Baiting (Isca):** O invasor oferece algo atraente para a vítima em troca de informações para que ela execute ações maliciosas.

**Exemplo:** Alguém deixa um Pen Drive infectado com um rótulo escrito “Salários da Empresa”.

**Pretexting (Pretexto):** O invasor cria um cenário falso (pretexto) e se passa por alguém que não é para obter informações privadas da vítima.

**Exemplo**: Um invasor liga para um cliente e se passa por um funcionário da empresa e solicita as credenciais do cliente para realizar uma “atualização urgente”.

**Troca Equivalente:** O invasor oferece um suposto serviço ou benefício em troca de informações ou acesso.

**Exemplo:** Um invasor liga aleatoriamente para números de uma empresa, oferecendo “suporte técnico”. Eventualmente, encontra alguém com um problema real e se oferece para ajudar em troca da desativação temporária do antivírus ou do fornecimento do acesso remoto.

**Tailgating:** Também conhecido como “Piggybacking”. Um invasor não autorizado segue de perto uma pessoa autorizada para entrar em uma ária fisicamente restrita.

**Exemplo:** Um invasor espera perto de uma porta com controle de acesso e, quando um funcionário autorizado abre a porta, o invasor entra rapidamente atrás dele, muitas vezes fingindo estar com as mãos ocupadas ou em uma ligação.

**Phishing/Spear-Phishing:** Como mencionado, o phishing utiliza e-mails ou mensagens em massa.

O **Spear Phishing** é uma versão altamente direcionada e personalizada de phishing, focada em um indivíduo específico.

**Proteção**

**Proteção e Intervenção**

São medidas que são implementadas para defender ativamente os sistemas e dados contra ataques em andamento ou para minimizar o impacto caso um incidente de segurança ocorra.

Intervenções são o conjunto de medidas adotadas para proteger sistemas, redes e dados contra ameaças cibernéticas e minimizar o risco de incidentes de segurança.

**São como o sistema imunológico e os mecanismos de defesa do corpo.**

**Firewall**

Atuam como uma barreira de segurança entre uma rede interna confiável e redes externas não confiáveis (como a internet).

Eles monitoram e controlam o tráfego da rede de entrada e saída com base em um conjunto de regras de segurança predefinidas, bloqueando o tráfego malicioso ou não autorizado.

**Exemplo**: Um firewall pode ser configurado para bloquear todas as conexões exceto aquelas para o servidor Web.

**IPS e IDS**

**IDS (Sistemas de Detecção de Intrusão)**

Monitora o tráfego da rede, quando identifica uma ameaça, ele emite um alerta

**IPS (Sistemas de Prevenção de Intrusão)**

Detecta e toma ações para bloquear ou prevenir a ameaça automaticamente.

**Antivírus e Antimalware**

Programas projetados para detectar, prevenir e remover software malicioso de computadores e redes

Eles usam assinaturas de malware conhecido e análise heurística (comportamental) para identificar novas ameaças.

**Exemplo:** Seu software antivírus escaneia um arquivo baixado da internet e o identifica como um trojan, movendo-o para quarentena antes que possa ser executado

**Criptografia**

Processo de codificar dados (transformá-los de texto plano em texto cifrado) de forma que apenas usuários autorizados com a chave de descriptografia podem acessar os dados. Isso protege os dados contra invasões e ataques.

**Controle de Acesso**

Garantir que usuários, programas e processos tenham apenas o nível mínimo de permissões de acesso necessário para realizar suas tarefas legítimas, isso limita o dano potencial caso uma conta seja comprometida.

**Backups Regulares**

Criar cópias de segurança de dados importantes e sistemas em intervalos regulares e armazená-los em local seguro (Idealmente off-site ou em nuvem).

É crucial testar periodicamente o processo de restauração para garantir que os backups sejam utilizáveis.

**Exemplo:** Após um ataque de ransomware que criptografa todos os arquivos de um servidor, a empresa consegue restaurar todos os arquivos através do backup.

**Caça aos Vazamentos**

Verifique se o seu e-mail já foi vazado: haveibeenpwned.com

**Prevenção**

**Atualizações de Software**

Aplicar correções de segurança (patches) fornecidos pelos fabricantes para sistemas operacionais, navegadores, aplicativos e firmware assim que disponíveis.

Essas atualizações frequentemente corrigem vulnerabilidades conhecidas

**Exemplo:** Configurar o Windows Update para baixar e instalar atualizações de segurança automaticamente.

**Políticas de Segurança**

Definir, documentar e comunicar políticas de segurança da informação abrangentes que cobrem áreas como o uso aceitável de recursos, segurança de senhas, uso de e-mail, acesso remoto, resposta a incidentes, etc.

**Treinamento e Conscientização**

Educar regularmente os funcionários e usuários sobre as ameaças cibernéticas atuais (especialmente engenharia social, phishing), boas práticas de segurança e suas responsabilidades na proteção dos ativos da informação.

**Análise de Vulnerabilidade**

Escaneamento automatizado ou manual de sistemas e redes para identificar vulnerabilidades conhecidas.

Simulação controlada de um ataque cibernético contra um sistema para identificar vulnerabilidades exploráveis antes que hackers reais o façam.

**Configuração Segura de Sistemas**

Implementar configurações de segurança robustas em sistemas operacionais, servidores, dispositivos de rede e aplicativos desde o início.

Isso inclui desabilitar serviços e portas desnecessárias, remover software padrão não utilizado, aplicar restrições de acesso, etc.

**Monitoramento Contínuo**

Utilizar ferramentas e processos pra monitorar constantemente os logs de sistemas, tráfegos de rede e atividades dos usuários em busca de comportamentos anormais, atividades suspeitas, etc.

**Planejamento de Respostas (PRI)**

Planejamento de Respostas a Incidentes

Ter um plano definido e testado sobre como identificar, conter, erradicar, recuperar e aprender com um incidente de segurança.

O plano deve detalhar papéis, responsabilidades, procedimentos de comunicação e etapas técnicas.

**Exemplo:** Um PRI que descreve os passos a serem seguidos se um vazamento de dados for detectado, incluindo quem contatar, como isolar os sistemas afetados e quando notificar as autoridades ou clientes.

**Plano de Ação Pessoal**

**Com todo conteúdo e informações passadas sobre segurança, vamos idealizar um Plano de Ação**

Em um arquivo **Word** liste **10 ações concretas** que vocês podem tomar hoje ou esta semana para melhorar a sua segurança digital pessoal baseadas no que aprenderam.

Exemplos: Trocar a senha do e-mail ou de alguma aplicação, ativar medidas de segurança, verificar permissões de apps etc.