Ameaças e Vulnerabilidades

Ameaças e Vulnerabilidades

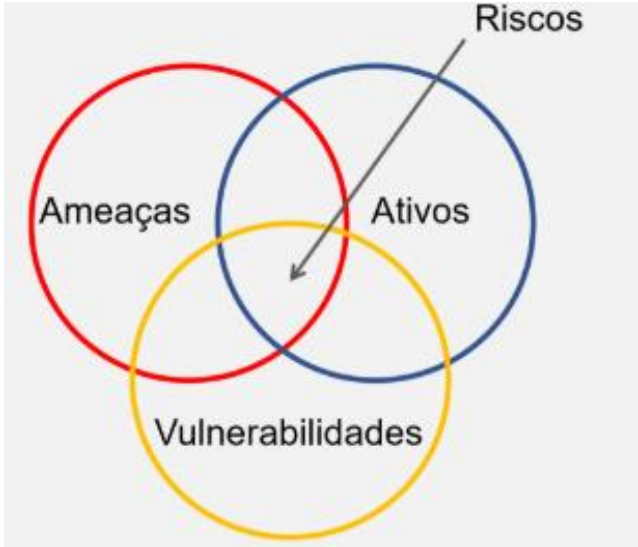
Unidade 3-Ameaças e Vulnerabilidades

- 3.1-Definição de ameaça e vulnerabilidade
- 3.2-Tipos de ameaças
- 3.3-Como tratar as ameaças e vulnerabilidades
- 3.4-Golpes na Internet
- 3.5-Exploração das vulnerabilidades
- 3.6-Mitigação das vulnerabilidades
- 3.7-Formas de propagação das ameaças
- 3.8-Formas de proteção contra as ameaças

3.1 Definições de Ameaças e Vulnerabilidades

AMEAÇA: É a possibilidade de um agente, interno ou externo, explorar acidentalmente ou propositalmente uma vulnerabilidade específica.

VULNERABILIDADE: Também pode ser chamada de falha ou fraqueza, por exemplo, uma parede rachada, dentro de uma rede podemos encontrar esta “rachadura”, ou falha, em um design mal panejado, implementação mal realizada, ou até em controles internos de um sistema mal realizado, levando a rede a abrir pequenas falhas na política de segurança.



3.1 Definições de Ameaças e Vulnerabilidades

"Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas" General Sun Tzu (ano 400 AC).

3.1 Definições de Ameaças e Vulnerabilidades

- O tratamento de ameaças é mais efetivo quando realizado por uma equipe qualificada pois demanda várias ações:
  - A detecção de vulnerabilidades que está presente nos sistemas da organização é o mínimo a ser feito;
  - O histórico das ações tomadas e tratadas, assim como informações sobre o funcionamento da ameaça;
  - Qual o envolvimento com outras áreas da empresa que lidaram com a ameaça além do pessoal de tecnologia ou da informação.

3.1 Definições de Ameaças e Vulnerabilidades

- Uma empresa só é capaz de responder rapidamente e adequadamente as ameaças quando possui total conhecimento sobre as seguintes ações: Que vulnerabilidades possuo? A que ameaças estou suscetível? Quais agentes estão envolvidos? Qual são os impactos históricos e possíveis da exploração destas ameaças?

- Um dos desafios da área de segurança da informação para uma abordagem realista e eficiente dos negócios da empresa exige uma abordagem ampla com foco nas ameaças, as principais áreas envolvidas, para a análise e tratamento de riscos são: Segurança da Informação, Risco, Auditoria, Compliance (estar em conformidade com leis e regulamentos externos e internos), Governança, Anti-Fraude, Segurança Empresarial, Jurídico e Recursos Humanos.

3.2-Tipos de Ameaças

Scan

- É um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operacional, atividade e serviços) e identificar possíveis alvos para outros ataques.
- A principal forma de prevenção é a manutenção de um firewall na empresa e uma configuração adequada da rede.

3.2-Tipos de Ameaças

Fraude

- A fraude, ou o scam (com "m"), abrange uma quantidade ampla de tipos de ataque.
- Um dos mais comuns deles é o phishing, que, para obter informações do usuário, usa de estratégias como a cópia da interface de sites famosos e envio de e-mails ou mensagens falsas com links suspeitos.
- O principal meio de evitar fraudes é a conscientização dos usuários por meio de treinamentos sobre cuidados na rede.

3.2-Tipos de Ameaças

Worm

- Worms são alguns dos malwares mais comuns e antigos.
- Malware são softwares com o intuito de prejudicar o computador “hospedeiro”.
- Essa categoria engloba tanto os vírus quanto os worms, entre diversos outros tipos de programas maliciosos.
- Os worms são perigosos devido à sua capacidade se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa.
- O principal meio de prevenção é a manutenção de antivírus e treinamentos de conscientização.

3.2-Tipos de Ameaças

Adware

- É qualquer programa que executa automaticamente e exibe uma grande quantidade de anúncios (ad = anúncio, software = programa) sem a permissão do usuário.

3.2-Tipos de Ameaças

Backdoor (Porta dos Fundos)

- É um recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas críticas não documentadas existentes em programas instalados, softwares desatualizados e do firewall para abrir portas do roteador.

3.2-Tipos de Ameaças

Browser Hijacker (sequestro do navegador)

- É um tipo de vírus que tem por objetivo a alteração das principais configurações do navegador.
- Quando instalado, altera a homepage e os mecanismos de busca.
- Exibem anúncios em sites legítimos e redirecionam a vítima para sites maliciosos que podem conter exploits (sequência de comandos) ou outras pragas digitais.

3.2-Tipos de Ameaças

Cavalo de Troia (Trojan Horse)

- Conhecidos por normalmente responder pelo primeiro estágio de infecção de dispositivos digitais, os Cavalos de Troia têm como objetivo manter-se ocultos enquanto baixam e instalam ameaças mais robustas em computadores e laptops.
- Podendo vir em arquivos de música, mensagens de e-mail, escondidos em downloads e sites maliciosos, se aproveitam de vulnerabilidades do navegador utilizado para instalar a praga no computador.
- Cavalo-de-troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada.

3.2-Tipos de Ameaças

Spyware

- Os spywares são programas espiões utilizados para captar informações sobre os costumes dos usuários na internet, com o propósito de distribuir propaganda “customizada”.

3.2-Tipos de Ameaças

Ransonware

- São códigos maliciosos que sequestram arquivos ou todo o sistema da vítima por meio de técnicas de criptografia.
- Após o “sequestro”, o malware exibe mensagens exigindo o depósito de uma quantia em dinheiro, ou a compra de um determinado produto, prometendo o envio de senha que irá liberar os arquivos. Porém, mesmo após o pagamento, a vítima não recebe senha alguma.

3.2-Tipos de Ameaças

Trojan Banking

- É o trojan caracterizado pelo roubo de dados bancários, de sites de compras, redes sociais e servidores de e-mail.
- As técnicas são as mesmas de um trojan comum, sendo distribuído como um programa ou arquivo legítimo, em sites infectados ou mensagens de e-mail.

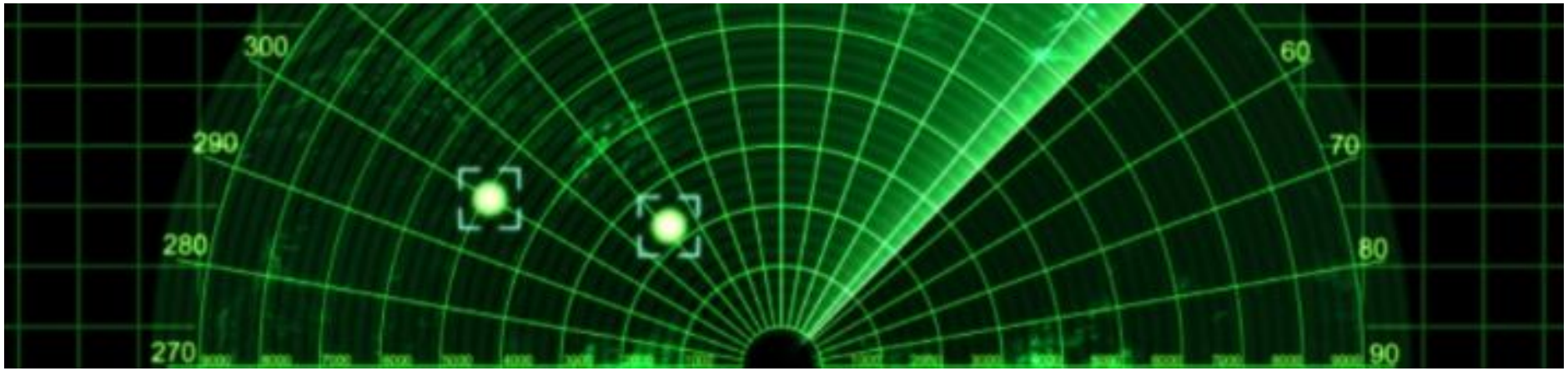
3.2-Tipos de Ameaças

Keyloggers

- Os keyloggers são aplicativos destinados a capturar o que é digitado no teclado.

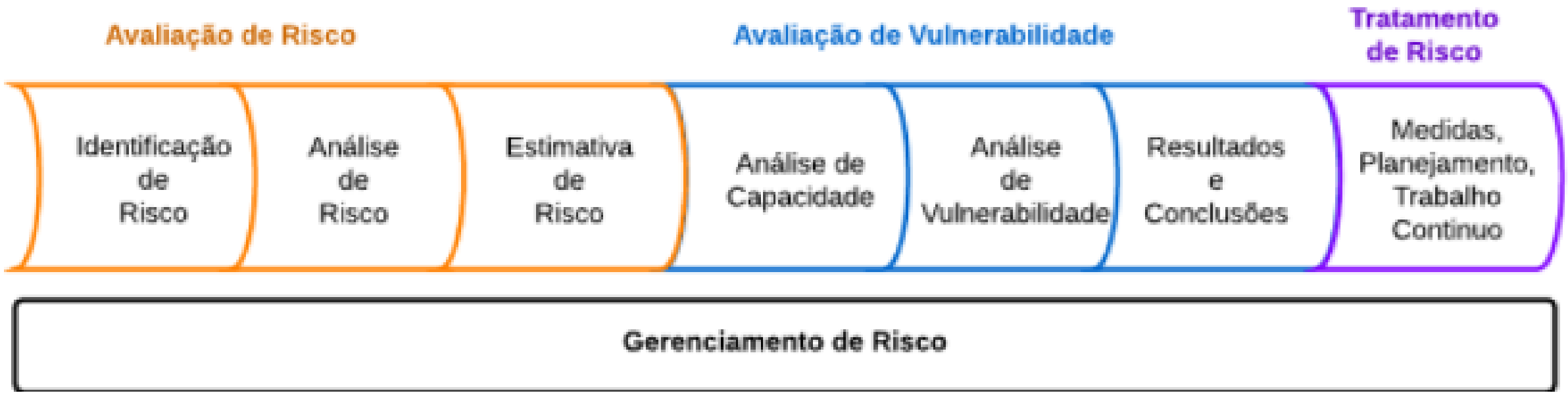
3.3-Como Tratar as Ameaças e Vulnerabilidades

- Atualmente, com o despertar do mercado para os conceitos de Segurança da Informação, muito se fala sobre alguns termos como Análise de Vulnerabilidade, Análise de Risco e Testes de Penetração, também chamados de *PenTest*.
- O problema é que essas nomenclaturas acabam gerando confusão na cabeça de muita gente.



3.3-Como Tratar as Ameaças e Vulnerabilidades

Relembrando risco...



3.3-Como Tratar as Ameaças e Vulnerabilidades

- Como parte do *Gerenciamento de Risco*, a *Avaliação de Vulnerabilidade* é definida como o processo de encontrar e verificar vulnerabilidades em um ambiente.
- Após identificarmos e avaliarmos os riscos, é ela quem vai produzir uma imagem do estado atual de exposição do ambiente a estes riscos, para que estes possam ser tratados.
- Trata-se de um processo contínuo de identificação, remediação e reporte dos resultados para que medidas possam ser tomadas, reiniciando o processo como um todo.

3.3-Como Tratar as Ameaças e Vulnerabilidades

Análise de Capacidade

- Inicialmente, temos a Análise de Capacidade, que é o processo responsável por revisar a capacidade de um grupo contra os objetivos almejados, identificando as lacunas que devem ser preenchidas.
- O termo “capacidade” é definido como a habilidade de indivíduos, organizações e sistemas em executar funções de maneira efetiva e sustentável. Aqui precisamos definir o que pode ser feito, como pode ser feito e o que precisamos para fazê-lo.
- Por exemplo, se desejamos realizar uma análise de vulnerabilidade em nossos servidores internos, precisamos antes verificar se temos a mão de obra especializada e as ferramentas necessárias para tal, como um analisador de protocolo.

3.3-Como Tratar as Ameaças e Vulnerabilidades

- Um dos maiores desafios dos gestores é o fato das organizações conviverem com uma quantidade quase infinita de vulnerabilidades e ameaças que comprometem a segurança da informação, mas disporem de recursos limitados para gerenciá-los.

3.3- Como Tratar as Ameaças e Vulnerabilidades

Alcançar o equilíbrio entre investimento, priorização de recursos e segurança é um dos nossos grandes objetivos e nos ajuda a vencer desafios como:

- Tratar a segurança da informação conforme os objetivos de negócio;
- Alcançar excelência na **Gestão de Riscos** (Risk Management) e Vunerabilidades;
- Atender os normativos, proteger as informações e monitorar controles;
- Adotar as melhores práticas de mercado para governança de segurança da informação e TI;
- Conhecer os impactos das vulnerabilidades e ameaças sobre a infraestrutura de TI;
- Tomar decisões com base em métricas e indicadores;
- Monitorar continuamente os riscos, e agir proativamente para tratar as vulnerabilidades nos ativos de TI;
- Conhecer as fontes de riscos;
- Implementar workflow e acompanhar o tratamento das vulnerabilidades e riscos.

3.4 - Golpes na Internet

- Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por este motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários.

3.4 - Golpes na Internet

- Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.
- De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar *sites*, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

3.4 - Golpes na Internet

- Engenharia Social

Práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas.

3.4 - Golpes na Internet

- Técnicas de Engenharia Social

Passos de um ataque:	**Engenharia Reversa:**
• Estudo da Vítima	• Sabotagem
• Entrar em Contato	• Propaganda
• Finalizar o Golpe	• Suporte
Aproximação Direta:	**Softwares Maliciosos:**
• Equipe de Manutenção	• Back Doors
• Suporte em TI	• Keyloggers
• Colega de Trabalho	• Softwares que Alteram Configurações
• Diretor	**Falhas de Segurança na Natureza Humana:**
• Delegação de Confiança	• Autoridade
Vasculhar Lixo	• Afabilidade
Espiar e Escutar	• Reciprocidade
Sites Falsos	• Consistência
E-mail Falso	• Validação Social
	• Escassez

3.4 - Golpes na Internet

- Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato. Dessa forma, o golpista pode ser considerado um estelionatário.
- Seguem os principais golpes aplicados na internet....

3.4 - Golpes na Internet

Furto de identidade (*Identity theft*)

- O furto de identidade, ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.
- No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de *e-mail* e envie mensagens se passando por você ou falsifique os campos de *e-mail*, fazendo parecer que ele foi enviado por você.
- Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponíveis e mais convincente ele pode ser.
- Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito. Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

3.4 - Golpes na Internet

Furto de identidade (*Identity theft*)

- É necessário também que você fique atento a alguns indícios que podem demonstrar que sua identidade está sendo indevidamente usada por golpistas, tais como:
  - você começa a ter problemas com órgãos de proteção de crédito;
  - você recebe o retorno de *e-mails* que não foram enviados por você;
  - você verifica nas notificações de acesso que a sua conta de *e-mail* ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando;
  - ao analisar o extrato da sua conta bancária ou do seu cartão de crédito você percebe transações que não foram realizadas por você;
  - você recebe ligações telefônicas, correspondências e *e-mails* se referindo a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.

3.4 - Golpes na Internet

Fraude de antecipação de recursos (*Advance fee fraud*)

- A fraude de antecipação de recursos, ou *advance fee fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.
- A melhor forma de se prevenir é identificar as mensagens contendo tentativas de golpes. Uma mensagem deste tipo, geralmente, possui características como:
  - oferece quantias astronômicas de dinheiro;
  - solicita sigilo nas transações;
  - solicita que você a responda rapidamente;
  - apresenta palavras como "urgente" e "confidencial" no campo de assunto;
  - apresenta erros gramaticais e de ortografia (muitas mensagens são escritas por meio do uso de programas tradutores e podem apresentar erros de tradução e de concordância).

3.4 - Golpes na Internet

Phishing

- Phishing ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.
- O phishing ocorre por meio do envio de mensagens eletrônicas que:
  - tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
  - procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
  - informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
  - tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

3.4 - Golpes na Internet

Phishing

- Exemplos de situações envolvendo *phishing* são:
  - Páginas falsas de comércio eletrônico ou *Internet Banking*
  - Páginas falsas de redes sociais ou de companhias aéreas
  - Mensagens contendo formulários
  - Mensagens contendo *links* para códigos maliciosos
  - Solicitação de recadastramento

3.4 - Golpes na Internet

Pharming

- *Pharming* é um tipo específico de *phishing* que envolve a redireção da navegação do usuário para *sites* falsos, por meio de alterações no serviço de DNS (***D****omain* ***N****ame* ***S****ystem*). Neste caso, quando você tenta acessar um *site* legítimo, o seu navegador *Web* é redirecionado, de forma transparente, para uma página falsa. Esta redireção pode ocorrer:
  - por meio do comprometimento do servidor de DNS do provedor que você utiliza;
  - pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;
  - pela ação direta de um invasor, que venha a ter acesso às configurações do serviço de DNS do seu computador ou *modem* de banda larga.

3.4 - Golpes na Internet

Golpes de comércio eletrônico

- Golpes de comércio eletrônico são aqueles nos quais golpistas, com o objetivo de obter vantagens financeiras, exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial.

3.4 - Golpes na Internet

Golpe do *site* de comércio eletrônico fraudulento

- Neste golpe, o golpista cria um *site* fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.
- Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como: enviar *spam*, fazer propaganda via *links* patrocinados, anunciar descontos em *sites* de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.

3.4 - Golpes na Internet

Golpe envolvendo *sites* de compras coletivas

- *Sites* de compras coletivas têm sido muito usados em golpes de *sites* de comércio eletrônico fraudulentos.
- Além dos riscos inerentes às relações comerciais cotidianas, os *sites* de compras coletivas também apresentam riscos próprios, gerados principalmente pela pressão imposta ao consumidor em tomar decisões rápidas pois, caso contrário, podem perder a oportunidade de compra.
- Golpistas criam *sites* fraudulentos e os utilizam para anunciar produtos nos *sites* de compras coletivas e, assim, conseguir grande quantidade de vítimas em um curto intervalo de tempo.

3.4 - Golpes na Internet

Golpe do *site* de leilão e venda de produtos

- O golpe do *site* de leilão e venda de produtos é aquele, por meio do qual, um comprador ou vendedor age de má-fé e não cumpre com as obrigações acordadas ou utiliza os dados pessoais e financeiros envolvidos na transação comercial para outros fins. Por exemplo:
  - o comprador tenta receber a mercadoria sem realizar o pagamento ou o realiza por meio de transferência efetuada de uma conta bancária ilegítima ou furtada;
  - o vendedor tenta receber o pagamento sem efetuar a entrega da mercadoria ou a entrega danificada, falsificada, com características diferentes do anunciado ou adquirida de forma ilícita e criminosa (por exemplo, proveniente de contrabando ou de roubo de carga);
  - o comprador ou o vendedor envia *e-mails* falsos, em nome do sistema de gerenciamento de pagamentos, como forma de comprovar a realização do pagamento ou o envio da mercadoria que, na realidade, não foi feito.

3.4 - Golpes na Internet

Boato (*Hoax*)

- Um boato, ou *hoax*, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.
- Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

3.5 - Exploração das Vulnerabilidades

- Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.
- Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

3.6 - Mitigação das Vulnerabilidades

Maneiras de mitigação de vulnerabilidades

- Kerberos Delegation – aplicações agentes serão capazes de se autenticar em nome dos usuários: Para mitigar, deve-se prevenir que contas sensíveis de usuários sejam delegadas. Aplicações que usam Kerberos Delegation deveriam ser configuradas com Constrained Delegation. Dessa forma, a conta de serviço só pode delegar contas de usuários limitadas a um conjunto de funcionalidades dentro das aplicações agentes.
- Porta de firewall abertas para permitir conexões de controladores de domínio: Para mitigar, devem-se fazer verificações periódicas na rede para garantir boas práticas para operações de rede e monitoramento pró-ativo do tráfego na rede.

3.6 - Mitigação das Vulnerabilidades

Maneiras de mitigação de vulnerabilidades

- Administradores do Active Directory podem falsificar o SID para obter acesso aos recursos: Para mitigar, deve-se ativar filtro SID para permitir que os controladores de domínio no domínio de confiança removam todos os SIDs que não estão relacionados ao domínio de confiança em qualquer dado recebido.
- Usuários com credenciais de Active Directory podem acessar outros recursos: Para mitigar, deve-se ativar a Autenticação Seletiva para explicitamente garantir acesso aos recursos.
- Diferentes políticas que podem introduzir diferentes níveis de garantia de operações: Para mitigar, devem-se fazer verificações em ambas as florestas para garantir as boas práticas para operações de Active Directory e para garantir que processos de segurança e controles como o gerenciamento de atualizações e antivírus são executados de acordo com a política de segurança.

3.7 - Formas de Propagação das Ameaças

Independente do tipo de tecnologia usada, ao conectar o seu computador à rede ele pode estar sujeito a ameaças, como:

- **Furto de dados:** informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador.
- **Uso indevido de recursos:** um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar *spam*, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante.
- **Varredura:** um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades.
- **Interceptação de tráfego:** um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia.

3.7 - Formas de Propagação das Ameaças

- **Exploração de vulnerabilidades:** por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disto, equipamentos de rede (como *modems* e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para *sites* fraudulentos.
- **Ataque de negação de serviço:** um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar.
- **Ataque de força bruta:** computadores conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.
- **Ataque de personificação:** um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

3.8 - Formas de Proteção Contra as Ameaças

- Alguns cuidados que se deve tomar ao usar redes, independentemente da tecnologia, são:
  - Mantenha seu computador atualizado, com as versões mais recentes e com todas as atualizações aplicadas;
  - Utilize e mantenha atualizados mecanismos de segurança, como programa *antimalware* e *firewall* pessoal;
  - Seja cuidadoso ao elaborar e ao usar suas senhas;
  - Utilize conexão segura sempre que a comunicação envolver dados confidenciais;
  - Caso seu dispositivo permita o compartilhamento de recursos, desative esta função e somente a ative quando necessário e usando senhas difíceis de serem descobertas.

3.8 - Formas de Proteção Contra as Ameaças

Wi-Fi

- Habilite a interface de rede Wi-Fi do seu computador ou dispositivo móvel somente quando usá-la e desabilite-a após o uso;
- Desabilite o modo *ad-hoc* (use-o apenas quando necessário e desligue-o quando não precisar - As redes ad hoc são redes sem fio que dispensam o uso de um ponto de acesso comum aos computadores conectados a ela, de modo que todos os dispositivos da rede funcionam como se fossem um roteador, encaminhando comunitariamente informações que vêm de dispositivos vizinhos). Alguns equipamentos permitem inibir conexão com redes *ad-hoc*, utilize essa função caso o dispositivo permita;
- Use, quando possível, redes que oferecem autenticação e criptografia entre o cliente e o AP (evite conectar-se a redes abertas ou públicas, sem criptografia, especialmente as que você não conhece a origem);
- Evite o acesso a serviços que não utilizem conexão segura ("https");

3.8 - Formas de Proteção Contra as Ameaças

Bluetooth

- Mantenha as interfaces *bluetooth* inativas e somente as habilite quando fizer o uso;
- Configure as interfaces *bluetooth* para que a opção de visibilidade seja "Oculto" ou "Invisível", evitando que o nome do dispositivo seja anunciado publicamente. O dispositivo só deve ficar rastreável quando for necessário autenticar-se a um novo dispositivo ("pareamento");
- Altere o nome padrão do dispositivo e evite usar na composição do novo nome dados que identifiquem o proprietário ou características técnicas do dispositivo;
- Sempre que possível, altere a senha (PIN) padrão do dispositivo e seja cuidadoso ao elaborar a nova;
- Evite realizar o pareamento em locais públicos, reduzindo as chances de ser rastreado ou interceptado por um atacante;
- Fique atento ao receber mensagens em seu dispositivo solicitando autorização ou PIN (não responda à solicitação se não tiver certeza que está se comunicando com o dispositivo correto);
- No caso de perda ou furto de um dispositivo *bluetooth*, remova todas as relações de confiança já estabelecidas com os demais dispositivos que possui, evitando que alguém, de posse do dispositivo roubado/perdido, possa conectar-se aos demais.

3.8 - Formas de Proteção Contra as Ameaças

Banda larga fixa

- Altere, se possível, a senha padrão do equipamento de rede (verifique no contrato se isto é permitido e, caso seja, guarde a senha original e lembre-se de restaurá-la quando necessário);
- Desabilite o gerenciamento do equipamento de rede via Internet (WAN), de tal forma que, para acessar funções de administração (interfaces de configuração), seja necessário conectar-se diretamente a ele usando a rede local (desta maneira, um possível atacante externo não será capaz de acessá-lo para promover mudanças na configuração).