Quais são os três pilares da segurança da informação? Qual a importância de cada um? Seja detalhista.

1. Confidencialidade, integridade e disponibilidade

Hoje, o maior ativo de pessoas, empresas e até países são seus dados. Se você pensar que todo o seu patrimônio, número do seu CPF, seus investimentos, contagem do tempo de contribuição para aposentadoria, imagens dos seus filhos do nascimento até hoje, são dados armazenados na internet, você começa a entender o tamanho do risco e da responsabilidade que é manter a informação devidamente protegida de indivíduos mal intencionados.

O primeiro pilar da segurança da informação visa proteger essa representação digital das suas informações e dados que estão armazenados em vários servidores espalhados pelo mundo. A confidencialidade garante que o acesso a informações sensíveis seja feito somente por pessoas autorizadas, ou seja, ninguém a não ser você deve ter acesso a sua vida digital. Ela se materializa quando, por exemplo, uma rede social protege o controle dos seus posts através de um usuário e senha.

A garantia de acesso à informação e aos sistemas é garantida pela disponibilidade, nesse conceito a segurança da informação atua para que servidores que rodam aplicações, bancos de dados que armazenam informações ou links que dão acesso a esses ativos, estejam sempre online e disponíveis para seus usuários.

2. Prevenção, Detecção e Resposta

Nesse pilar encontramos ações desempenhadas pela segurança da informação para garantir a sustentação do primeiro pilar que já foi mencionado nesse artigo. Essas ações evitam que um incidente de segurança ocorra, agindo para percebe-lo no menor tempo possível e evitar ao máximo seus danos.

Para a prevenção dos incidentes se adota medidas de proteção do ambiente, para entender esse conceito precisamos falar sobre superfície de ataque. Qualquer sistema, servidor, aplicação ou ambiente que tenha um acesso remoto, através da web ou outro tipo de conectividade está sujeito a invasões e a superfície de ataque que podem ser comprometidos por um cibercriminoso.

A prevenção atua na proteção desses ativos, evitando que, por exemplo, portas de comunicação estejam abertas, aplicações ou sistemas operacionais estejam desatualizados e assim por diante. Outra parte importante do processo de resposta a incidentes é a investigação para determinar o que aconteceu, porque aconteceu e como evitar que aconteça novamente. A inteligência criada a partir dessa investigação será aplicada às fases de prevenção e detecção para melhorar a resiliência do ambiente.

3. Tecnologia, Processos e Pessoas

O último pilar da Segurança da Informação é o que sustenta suas melhores práticas e seus objetivos iniciais. Classificamos como tecnologia todos as ferramentas, sejam elas hardware ou software, que permitem a prevenção, detecção e resposta aos incidentes de segurança, incluímos aqui antivírus, firewalls, IDS, IPS, aplicações de análise forense, SIEMs, etc.

A proteção de ambientes complexos contra ameaças cada vez mais sofisticadas e direcionadas só é possível por meio de processos muito bem definidos que permitem máxima eficiência no uso da tecnologia para sustentar o pilar 2. A documentação extensiva e em profundidade é crucial para permitir que a prevenção, detecção e resposta aos incidentes ocorram de maneira continuada, cada uma delas ocorre através de ações logicamente coordenadas e só surtirão efeito se seguirem estes processos lógicos.

Pessoas são o componente mais importante deste pilar, quem opera a tecnologia, cria processos e torna a Segurança da Informação possível. Estes profissionais travam uma guerra diária justamente com quem está “do outro lado”. Através da capacidade analítica e criativa são capazes de produzir tecnologias e processos, para prevenir, detectar e responder a ataques digitais, garantindo assim a confidencialidade, integridade e disponibilidade de dados, sistemas e aplicações.

O que é não repúdio? Qual sua importância para segurança da informação?

O que significa não repúdio?

O fato de as informações eletrônicas poderem ser facilmente alteradas faz com que seja necessária a existência de um sistema no qual as partes confiem nos dados que são compartilhados e utilizados nas transações diárias. Essa exigência para a confiança é conhecida como não repúdio.

O não repúdio é importante no comércio eletrônico para prevenir que as partes integrantes de uma transação venham a contestar ou negar uma transação após sua realização. O primeiro objetivo de um sistema de não repúdio é provar quem foi o autor de determinada ação e manter as necessárias evidências de tal informação para resolver eventuais disputas ou auditorias.

O não repúdio deve ser visto sob a ótica legal e técnica. Sob uma perspectiva legal, o não repúdio é definido como suficiente evidência para persuadir a autoridade legal (juiz, jurado ou árbitro) a respeito de sua origem, submissão, entrega e integridade, apesar da tentativa de negação pelo suposto responsável pelo envio.

Em termos gerais, repudiar algo é negar sua existência e, para tanto, os serviços de não repúdio usam os métodos de criptografia, que impedem que um indivíduo ou uma entidade neguem a execução de uma ação particular relacionada aos dados (tais como mecanismos para a não rejeição de autoridade, fornecendo prova da origem; para a prova da obrigação, da intenção, ou do compromisso; ou para a prova da posse).

Sob uma perspectiva técnica, o termo não repúdio é utilizado dentro da tecnologia de autenticação para descrever um serviço que fornece prova da integridade e da origem dos dados, ambos por meio de um relacionamento que não seja capaz de ser forjado e que possa ser verificado por quaisquer terceiros interessados, a qualquer tempo, ou fornece a garantia elevada de que esses dados são genuínos, e que não podem ser subsequentemente refutados.

Em que situações o não repúdio é aplicado?

Na maioria dos casos, é por meio da assinatura digital que temos contato com o não repúdio. A assinatura digital é uma forma de assinar um documento de forma eletrônica e é feita por meio de uma tecnologia de criptografia que vincula um Certificado Digital do assinante ao documento a ser assinado. Esse processo possui total validade jurídica, equivalente a uma assinatura de próprio punho.

Sua adoção é feita por empresas para eliminar o processo manual de recolhimento de assinaturas, reconhecimento de firma, despacho físico de documentos e para otimizar a gestão de documentos. Como resultado, há redução de custos, simplificação de processos, aumento da segurança e agilização na formalização e documentos.

Seu uso pode ser feito em diversos tipos de documentos eletrônicos. Entre eles estão: contratos, laudos, certificados, e-mails, procurações, imagens, petições, balanços, resultados de exames, formulários web, prontuários médicos, mandatos, declarações, arquivos eletrônicos transferidos entre empresas (EDI), relatórios e propostas com diferentes fins. Assim, o custo com emissão, armazenamento e descarte de todos esses itens é eliminado ou reduzido.

A assinatura digital apresenta admissibilidade e validade legal, ambas garantidas pelo artigo 10 da MP nº 2.200-2, que institui a Infraestrutura de Chaves Públicas Brasileiras — ICP-Brasil. Dessa forma, a presunção de veracidade jurídica é conferida aos signatários nas declarações de documentos em formato eletrônico.

Ainda de acordo com a ICP-Brasil, a assinatura digital garante autenticidade, integridade, confiabilidade e o não repúdio. Essa assinatura digital fica vinculada ao documento eletrônico de tal forma que, caso qualquer alteração seja feita no documento, a assinatura se torna automaticamente inválida.

Desse modo, a técnica permite não apenas verificar a autoria do documento, como também estabelecer uma forma de “imutabilidade lógica” de seu conteúdo, pois qualquer alteração do documento, por menor que seja, como a inserção de mais um espaço entre duas palavras, por exemplo, invalida a assinatura.

Qual sua função?

O princípio da irretratabilidade, mais conhecido como princípio do não repúdio, garante a autenticidade de algum documento quando utilizado por determinadas ferramentas, como no caso do Certificado Digital, anteriormente citado. Ou seja, uma pessoa ou entidade não pode negar a

autoria da informação fornecida. Quando assinamos digitalmente algum documento, nós garantimos dois dos princípios básicos da segurança da informação: a autenticidade e a integridade.

Autenticidade

O princípio da autenticidade na segurança da informação indica que aquela pessoa que está enviando a mensagem, produzindo o documento ou realizando uma transação é realmente quem alega ser. Ou seja, sua função é garantir que a informação é proveniente do executor indicado.

Integridade

O princípio da integridade na segurança da informação visa a garantir que a mensagem, documento ou transação permaneça na forma original ou que apresente somente as alterações permitidas pelo autor ou pessoa responsável. De forma resumida, o princípio da integridade tem como objetivo proteger a informação contra alterações não autorizadas.

Então, se um Certificado Digital está de acordo com o processo de certificação da ICP-Brasil, além de garantir o não repúdio, assegura também a autenticidade e integridade do documento ou transação.

Como você percebeu ao longo da leitura, o não repúdio é uma forma de garantir autenticidade para as transações eletrônicas realizadas por meio de Certificados Digitais a fim de otimizar os processos do dia a dia, proporcionando segurança e comodidade, tanto para as empresas, quanto para os clientes.

O que é MFA? Qual sua utilidade para segurança da informação?

Mais do que nunca, a segurança das informações que estão associadas às pessoas, às empresas, aos governos, a tudo na vida, tem sido crucial. O volume de dados que o mundo produz e o valor que boa parte dessa informação tem, requer preocupações crescentes quanto à integridade, ao sigilo, à privacidade e inviolabilidade de tais dados.

E apesar disso tudo, quase diariamente temos conhecimentos de problemas relacionados à segurança dos dados, em empresas de todos os portes, dos mais diversos segmentos e em todos os lugares do mundo, como por exemplo, a recente exposição dos mais de 270000 arquivos da Data Deposit Box, que usava o serviço Amazon S3.

Assim, tecnologias, protocolos, métodos, sistemas e tudo que pode ser feito para tornar a segurança da informação maior, tem sido adotado. Entre tudo que se vê, o MFA ou Multi-Factor Authentication, já é um padrão em muitas áreas.

Entendendo o MFA

Definido da forma mais simples possível, Multi-Factor Authentication ou Autenticação Multi Fator, em sua tradução para o português, é o uso de dois ou mais fatores ou agentes para verificação quanto a autenticidade de algo.

Em termos mais práticos, é a utilização de dois ou mais métodos para atestar a identidade de alguém para concessão de acesso a um sistema, documento ou informação.

Quando você acessa alguma das suas redes sociais ou sua conta de e-mail, se o dispositivo que usa para o acesso não tem seus dados de login gravados, você tem que informar um usuário e uma senha. Isso corresponde a um método de autenticação de um fator.

No entanto, a maior parte das redes sociais, os principais serviços de e-mail, entre outros serviços diferentes na Internet e mesmo no mundo físico, como no caixa eletrônico do seu banco, já utilizam mais do que um meio para certificar-se que o usuário que está utilizando o serviço, de fato é autorizado a fazê-lo.

Assim, nas configurações de segurança do Facebook, é possível selecionar um método de segurança adicional, além dos tradicionais usuário e senha e que no caso pode ser um aplicativo de autenticação (Google Authenticator ou o Duo Mobile) ou o envio de um SMS que contém um código de verificação, para um número telefônico previamente cadastrado.

No caso do Facebook e outros serviços que adotam uma segunda camada de proteção, por meio de outra forma de autenticação, costuma-se chamar como TFA, ou Two-Factor Authentication, ou em sua tradução, Autenticação de Dois Fatores, mas que também pode ser considerada como uma MFA, visto que além do método convencional, há pelo menos mais duas alternativas que podem ser escolhidas.

No caso de um site, adotar MFA ou TFA, significa fortalecer os protocolos de segurança quanto ao acesso ao seu painel de controle ou à área de administração do site.

Por que usar o MFA?

Parece desnecessário responder a essa pergunta, uma vez que é evidente até aqui que a segurança é o cerne da questão.

Todavia, os menos atentos, podem acreditar que usuários e senhas suficientemente fortes, bastam em termos de segurança e por isso, supor que é desnecessário ir além.

Nomes de usuário e senhas tradicionais podem ser roubados e assim independentemente do quão complexos sejam e mesmo que você os altere com frequência, toda a privacidade e inviolabilidade que você imaginaria ter, foi por água abaixo, como foi o caso da Data Deposit Box, ou da Origin, plataforma online da Eletronic Arts, em 2019.

Mesmo nos casos de usuários precavidos, empresas muito seguras, sistemas sólidos, os tradicionais usuário e senha, estão sujeitos a ataques de força bruta ou de dicionário, ou ainda variações de phishing.

Ao implementar um MFA em seus sistemas ou no seu site, você tem a possibilidade de contar com várias camadas de segurança, cada qual com um nível de dificuldade de acordo com os requisitos de segurança que seus dados necessitam.

Mais do que simplesmente incluir um ou mais métodos de autenticação, a variedade de métodos e consequentemente suas características, podem tornar praticamente inacessível os dados guardados sob o MFA, por parte de um cibercriminoso.

Como funciona o MFA?

A implantação de um método de dois ou mais fatores de autenticação, pode variar de acordo com as necessidades e as tecnologias disponíveis. Um exemplo, é a autenticação adaptativa, por meio da qual são incluídos fatores diferentes dependendo da situação – incrementando a segurança e as exigências conforme o risco de violação varia.

Ou seja, o sistema que requer credenciais para conceder acesso, tem condições de verificar se um acesso é potencialmente arriscado, escolhendo os métodos de acordo com o local em que um usuário ou grupo deles realiza o acesso, por exemplo.

Ao ser implantado um modelo de autenticação adaptativa, são definidos perfis para os usuários, contendo particularidades de cada um, como que dispositivos têm acesso (dispositivos registrados), de que locais ele realiza os acesso, dias e horários de acesso, frequência, entre outros aspectos.

Quando um usuário efetua o acesso, é verificado seu endereço IP, o dispositivo utilizado, horário e demais dados, os quais são confrontados com o perfil, determinando assim uma pontuação associada ao risco do acesso e a partir daí o usuário pode ser submetido a fatores de autenticação adicionais e/ou variáveis.

O modelo adaptativo, é o ideal, mas nem sempre pode ser aplicado, porque os recursos e custos de implementação são maiores, já que nos sistemas mais complexos, há inteligência artificial e até mesmo Machine Learning, que neste caso alimenta o perfil de acordo com o comportamento do usuário ao longo do tempo, fortalecendo ainda mais a segurança do ambiente e dos dados nele contidos.

O mais comum, é adotar um modelo preestabelecido ou fixo, em que por padrão sempre haverá pelo menos dois fatores de autenticação já previamente conhecidos para todo e qualquer acesso.

Há ainda modelos intermediários, como o utilizado pela Microsoft em alguns dos seus serviços, como por exemplo, o Outlook. Nele, há a autenticação padrão e o serviço é capaz de identificar os dispositivos cadastrados previamente no seu perfil.

Se um acesso é feito por um dispositivo não cadastrado, um segundo método de autenticação é requerido do usuário, como por exemplo, o envio de um código numérico de verificação ou um SMS para um número já cadastrado.

O acesso ao perfil / conta na Microsoft, é um outro exemplo de autenticação de dois fatores e sempre que o usuário acessa seu perfil para alterar dados relevantes, outro fator é submetido ao usuário para que a atualização seja efetivada.

Eis algumas alternativas que podem ser adotadas em um segundo, terceiro ou enésimo fator de autenticação:

O que é um ataque DDoS? Cite um exemplo real.

Os ataques de rede distribuídos muitas vezes são chamados de ataques de negação de serviço distribuído (DDoS). Esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto.

Entre os alvos comuns de ataques DDoS estão:

Sites de compras virtuais

Cassinos on-line

Qualquer empresa ou organização que dependa do fornecimento de serviços on-line

Como funciona um ataque DDoS

Os recursos de rede, como servidores Web, conseguem atender a um limite finito de solicitações simultaneamente. Além do limite de capacidade do servidor, o canal que conecta o servidor à Internet também tem largura de banda/capacidade finita. Sempre que o número de solicitações excede os limites de capacidade de qualquer componente da infraestrutura, o nível do serviço tende a sofrer de uma das seguintes maneiras:

A resposta às solicitações é muito mais lenta do que o normal.

Algumas ou todas as solicitações dos usuários podem ser totalmente ignoradas.

Em geral, o objetivo final do invasor é impedir totalmente o funcionamento do recurso da Web, ou seja, uma "negação de serviço" total. O invasor também pode solicitar um pagamento para interromper o ataque. Em certos casos, um ataque DDoS pode até ser uma tentativa de desacreditar ou prejudicar os negócios de um concorrente.

Utilização de "redes zumbi" de botnets para realizar ataques DDoS

Para enviar uma grande quantidade de solicitações ao recurso da vítima, o criminoso virtual em geral estabelece uma "rede zumbi" de computadores infectados. Como o criminoso controla as ações de cada computador infectado da rede zumbi, a simples escala do ataque pode sobrecarregar os recursos da Web da vítima.

A natureza dos ataques DDoS atuais

Do início à metade dos anos 2000, esse tipo de atividade criminosa era bem comum. Entretanto, o número de ataques DDoS bem-sucedidos tem caído. Essa queda nos ataques DDoS pode ser atribuída ao seguinte:

Investigações policiais que acarretaram a prisão de criminosos no mundo todo

Contramedidas técnicas que deram certo contra os ataques DDoS

O que é uma vulnerabilidade zero-day? Qual seu impacto na segurança da informação?

O que são vulnerabilidades zero day?

As chamadas vulnerabilidades zero day são falhas de segurança que atingem programas de computador. Esse nome vem do fato de que essa brecha é desconhecida para a empresa desenvolvedora até o momento em que hackers ou bug bounty hunters descobrem.

Ou seja, utilizamos a nomenclatura de zero day quando um sistema é comprometido por um malware antes que o fabricante tenha consciência disso, descobrindo a vulnerabilidade apenas no momento do ataque.

A classificação desse tipo de problema se dá de duas formas:

falhas de segurança graves, mas que ainda não foram descobertas e utilizadas por hackers;

vulnerabilidades de segurança graves que são desconhecidas dos desenvolvedores, mas já são utilizadas para ataques.

A ideia que se passa por meio do nome vulnerabilidade zero day é a gravidade e a urgência necessária na correção dessas brechas, uma vez que muitos usuários podem ser atingidos.

Geralmente, existem duas formas básicas em que tais brechas são descobertas. A primeira é quando whitehackers, hackers do bem, se reúnem para identificar e reportar falhas de segurança em softwares. A segunda é quando os blackhackers, os cibercriminosos, buscam encontrar brechas de segurança que possam ser utilizadas em seus ataques.

Na maioria dos casos, buscam esse tipo de falha em softwares populares e amplamente utilizados ao redor do mundo. Isso porque ao encontrar uma brecha como essa, o número de usuários que se pode atingir é muito maior.

Como funciona a exploração de vulnerabilidades zero day?

Os cibercriminosos estão sempre em busca de novas formas de atuação e as vulnerabilidades zero day nem sempre são iguais ou possibilitam determinadas atuações, sendo que sua exploração depende muito da própria falha e as possibilidades que ela abre para o atacante.

Por exemplo, hackers podem descobrir uma determinada falha que permita a disseminação de um vírus na rede e ele pode circular por anos até que, enfim, sua presença seja detectada e a brecha corrigida.

Contudo, mesmo que a correção ocorra, por meio de um patch lançado pelos desenvolvedores, o cibercriminoso ainda pode continuar tirando proveito disso, uma vez que nem todos os usuários atualizam seus sistemas.

Uma situação muito parecida ocorre também quando especialistas em segurança, os whitehackers, descobrem falhas e avisam os desenvolvedores. Quando isso acontece, a brecha se torna pública e os cibercriminosos também tentam utilizá-la, partindo do princípio de que nem todos os usuários atualizarão seus programas. No entanto, ela deixa de ser chamada de zero day.

Um dos grandes exemplos que tivemos nos últimos anos foi o ransomware WannaCry, um dos maiores ataques da história da computação. Por meio de uma falha no sistema operacional Windows, mais de 200 mil máquinas foram contaminadas em 150 países. O Brasil foi o quinto país mais afetado e os cibercriminosos cobravam cerca de U$300 para a liberação dos arquivos dos usuários.

Quais as consequências das invasões?

Existe uma série de complicações que um ataque hacker pode trazer para a sua empresa, mas separamos as principais entre elas.

Perda de dados

Com a transformação digital, boa parte das informações fundamentais para o funcionamento dos negócios estão dentro dos sistemas utilizados pela empresa, por exemplo, cadastros de clientes, dados logísticos, financeiro, entre outros. Ao sofrer um ataque, boa parte dessas informações pode ser perdida, o que pode levar ao colapso do negócio em casos que não há nenhum tipo de plano de recuperação.

Sistemas danificados

Algumas falhas são exploradas por cibercriminosos que não estão interessados em retorno financeiro, apenas em destruir os arquivos e prejudicar os usuários. Em casos como esses, vírus que deletam partes importantes de sistemas são distribuídos por meio das vulnerabilidades zero day, fazendo com que os programas deixem de funcionar corretamente, exigindo manutenção em massa de todas as máquinas de uma empresa.

Roubo de informações

Por fim, temos o roubo de dados, uma das atividades mais lucrativas realizadas pelos hackers, uma vez que eles podem exigir um resgate para a devolução dessas informações, vendê-las no mercado negro ou, até mesmo, divulgá-las apenas para prejudicar a empresa.

Com o advento de legislações, como a LGPD, invasões e vazamentos de dados não prejudicam mais apenas a imagem das organizações, elas podem ser punidas com sanções em formas de multa e, até mesmo, impedimento da coleta de novos dados.

Como é possível se proteger?

Claro que existem formas de buscar se proteger de ataques que explorem vulnerabilidades zero day. Reunimos algumas dicas para auxiliar você.

Prevenção

Você conhece todos os programas utilizados dentro da empresa? Manter uma lista acerca dos sistemas em uso e verificar de forma constante possíveis notícias sobre falhas e brechas faz parte de uma rotina de prevenção de ataques.

Atualização constante

Busque manter todos os seus programas sempre atualizados, evitando ser vítima de brechas já corrigidas pelos desenvolvedores, mas que ainda são utilizadas pelos cibercriminosos em seus ataques.

Manutenções periódicas

Outro ponto muito importante para se proteger é manter uma manutenção constante de todas as máquinas em sua empresa, evitando programas desconhecidos de sua equipe e garantindo que tudo esteja atualizado.

Sistema de segurança

Ferramentas de segurança, que reúnem todas as informações acerca de atualização, programas em uso, controle de acesso e outros dados são fundamentais para uma política de proteção eficaz.

A consultoria em segurança da informação por uma empresa especializada também é interessante para auxiliar a descobrir quais são as brechas existentes em sua organização além das vulnerabilidades zero day.

A Strong Security é especializada em segurança da informação e pode ajudar você a proteger-se contra brechas e ataques de cibercriminosos. Entre em contato conosco e saiba como!

6. Aponte a principal característica ou a diferença de:

- Malware

Os Malware, palavra proveniente de “Malicious Software”, são ameaças virtuais desenvolvidas com o intuito de executar atividades maliciosas em computadores e smartphones.

- Ransomware

Essa ameaça virtual é capaz de sequestrar os documentos, arquivos e informações de um usuário, tornando-os inacessíveis, geralmente mediante criptografia, e apenas os liberando através de pagamento (ransom) da vítima. Além disso, ele também é capaz de impedir o acesso do proprietário ao seu equipamento infectado. Uma maneira de amenizar os prejuízos causados por esse malware é realizar um backup regular dos seus arquivos, de modo que, caso um invasor os sequestre, haverá uma cópia desses documentos.

- Vírus

O vírus é um software, geralmente malicioso, que atua se replicando e infectando arquivos e programas de computadores. Desse modo, quando esses arquivos são executados, ele é ativado e espalhado, podendo comprometer de maneira muito grave os sistemas computacionais, causando lentidão através do consumo de recursos, corrompendo arquivos, roubando informações, danificando softwares, entre outras consequências.

- Worm

O Worm, diferentemente do vírus, é um programa independente e que possui a característica de se autorreplicar em sistemas informatizados, sem a necessidade de utilizar um programa hospedeiro. Ele possui a capacidade de causar danos sem a necessidade de ser ativado pela execução do usuário. A sua atuação engloba a exploração de falhas e vulnerabilidades de sistemas de informação, podendo ocasionar graves danos à sua funcionalidade, além da possibilidade de realizar o roubo de informações, entre outros danos.

- Spyware

Spyware, ou Software Espião, é um tipo de malware cuja função é se infiltrar em sistemas computacionais, com o intuito de coletar informações pessoais ou confidenciais do usuário, sem o seu conhecimento, e as enviar ao invasor remotamente pela internet.

- Key logger

Esse tipo de spyware é capaz de coletar, armazenar e enviar a criminosos todas as informações que são digitadas no teclado pelo usuário, como sites visitados, senhas, entre outras informações.

O que é engenharia social? Cite 03 técnicas de engenharia social.

Engenharia Social é o nome utilizado para definir o método mais habitual de se obter informações confidenciais de acesso a sistemas restritos a usuários autorizados. É o caso em que uma pessoa, dotada de má-fé, abusa da ingenuidade ou da confiança de um usuário para persuadi-lo, ainda que de forma velada, a fornecer informações como números de cartões de crédito, senhas, documentos pessoais, entre outros.

Esse tipo de ato é baseado na interação humana e é conduzido por pessoas que usam o engano para violar os procedimentos de segurança que geralmente deveriam ter seguido. Diante disso, os criminosos utilizam a manipulação psicológica para convencer os usuários a cometerem erros de segurança ou divulgarem informações confidenciais.

Sendo assim, a Engenharia Social explora emocionalmente as potenciais vítimas, testando diversas iscas até ativar o gatilho que deixa o alvo vulnerável. Geralmente, ela pode se aproveitar de temas atuais, promoções atrativas ou falsos anúncios de premiações.

Como atua o engenheiro social?

O engenheiro social não é exatamente um profissional da engenharia exata. Trata-se de uma pessoa capacitada que apresenta habilidades e conhecimentos que o qualificam para praticar a engenharia social. Normalmente, é alguém com boa comunicação, simpático, com poucas resistências e, sobretudo, que apresenta um bom domínio de técnicas de persuasão e inteligência analítica necessárias para estudar o alvo com precisão.

De certa forma, o engenheiro social faz com que pessoas quebrem procedimentos e normas de segurança, seja por meio de ligações, e-mails, sites ou por contato pessoalmente. Eles enviam inúmeras mensagens diárias e spams na esperança de encontrar usuários inexperientes que possam ser vítimas do ataque, bem como para alcançar um número maior de vítimas.

Todos os indivíduos apresentam características e padrões de comportamento específicos. É observando esses aspectos que um engenheiro social obtém o que precisa para atuar. Nesse sentido, os colaboradores, tanto da área técnica quanto dos setores mais humanizados ficam sujeitos a falhar na proteção contra um ataque desse tipo, porque têm vulnerabilidades humanas e cometem erros em algum momento.

Quais os tipos de ataques de Engenharia Social?

Apesar de o nome Engenharia Social sugerir técnicas sofisticadas ou mirabolantes, a maioria dos ataques é feita de forma simples, sem que seja preciso achar e explorar falhas em sistemas de segurança, e não necessariamente acontece apenas em ambientes digitais.

De modo geral, esses ataques acontecem de diversas formas diferentes e podem ser realizados em qualquer lugar em que a interação humana esteja envolvida. A seguir, confira os principais tipos de ataques!

Conheça o ThreatX: Solução contra ameaças digitais

Baiting

Nessa técnica, que acontece mais em ambientes de trabalho, o criminoso infecta um dispositivo — geralmente um pen drive — com um malware e o deixa em algum lugar aleatório. A pessoa que encontra o dispositivo o conecta, por curiosidade, em um algum PC ou notebook para tomar conhecimento do conteúdo que está ali. Não raras as vezes, essa pessoa instala os arquivos que ali estão para saber do que se tratam. Feito isso, o criminoso passa a ter acesso a praticamente todos os sistemas do dispositivo infectado.

Phishing

Apesar de ser uma técnica antiga da Engenharia Social, o e-mail de phishing ainda é muito eficiente. Ele ocorre quando um cibercriminoso forja comunicações com a vítima, que acredita estar diante de um e-mail legítimo. Em geral, o normal é que os fraudadores se passem por bancos ou empresas de cartão de crédito solicitando informações sensíveis, como senhas e dados de cadastro, ou mesmo solicitando a instalação de falsos softwares de segurança etc.

Vale dizer que um ataque de phishing nem sempre vem por e-mail. Alguns fraudadores tentam esse tipo de contato também via telefone e redes sociais. Muitas vezes, apesar de fraudulentos, esses contatos podem parecer muito realistas e convincentes.

Pretexting

Essa técnica é aquela na qual fraudadores se passam por pessoas ou empresas de confiança da vítima. De posse de informações básicas, dessas que ficam disponíveis em uma breve pesquisa na internet, o criminoso solicita confirmação de dados e atualizações de cadastro, inclusive de senhas. A vítima, achando que está em contato com alguém de confiança, fornece os dados tranquilamente, sem saber que se trata de um golpe.

Quid pro quo

O ataque de quid pro quo acontece quando um hacker solicita informações confidenciais de alguém em troca de algo. O próprio termo é traduzido como “isso por aquilo”, no qual o cibercriminoso oferece à vítima algo em troca desses dados sensíveis.

A estratégia mais usual consiste em se passar por alguém do setor de tecnologia e abordar vítimas que tenham problemas relacionados à esfera. Conforme as instruções do criminoso, a vítima fornece acesso aos códigos, desabilita programas importantes e instala malwares, presumindo que conseguirá solucionar seu problema.

Spear phishing

O spear-phishing é uma versão mais direcionada do phishing, focada em indivíduos e empresas específicas. Nesse tipo de ataque, o criminoso se passa por algum executivo ou membro da organização, e se aproxima dos colaboradores com o objetivo de obter informações sensíveis, por meio de uma demanda urgente exigindo uma transação financeira imediata para uma conta específica, por exemplo.

Em geral, o spear phishing exige muito mais esforço em nome do agressor e pode levar semanas e meses para acontecer. Isso porque eles costumam ser mais difíceis de detectar e têm melhores taxas de sucesso quando são realizados com habilidade.

Presencial

Como dito, os ataques de Engenharia Social não acontecem somente em ambientes digitais. Aliás, eles são muito comuns no mundo físico. Criminosos que se passam por autoridades, por exemplo, entram na casa ou no trabalho das pessoas e coletam um vasto leque de dados importantes para a efetivação de fraudes.

São muitos os exemplos de fraudadores que se passam por bombeiros, técnicos, e até mesmo pessoal de limpeza, para entrar em prédios, principalmente os corporativos, para roubar segredos e objetos de valor financeiro considerável. Além disso, os próprios furtos de smartphones são armas valiosas de criminosos que estão interessados, entre outras coisas, em cometer fraudes.

Como funciona e como se dá o ciclo da engenharia social?

De modo geral, os ataques de engenharia social acontecem em uma ou mais etapas. Primeiramente, o criminoso investiga a vítima em potencial para obter as informações necessárias para o ataque, como pontos de entrada e protocolos de segurança fracos, essenciais para prosseguir com a prática.

Em seguida, ele busca conquistar a confiança da vítima e fornecer estímulos para atividades subsequentes que violam as práticas de segurança, como revelar dados confidenciais ou conceder acesso a recursos críticos, por exemplo. Nesse sentido, o ataque de engenharia social é baseado no erro humano e não na vulnerabilidade de softwares ou sistemas operacionais.

Por isso, como não envolve nenhuma questão técnica que possa ser reconhecida pelos dispositivos de segurança tradicionais, esses ataques estão entre os maiores riscos cibernéticos às empresas atualmente e requer diversos cuidados básicos para prevenção contra os golpes.

Como os usuários podem se proteger?

Como dito, esse tipo de ataque explora a confiança e as emoções das vítimas. Dessa forma, é essencial treinar os colaboradores e os clientes nas melhores práticas de segurança da informação, que envolvem cuidados indispensáveis no dia a dia.

O primeiro ponto é adotar uma certa desconfiança e manter-se vigilante. Saber que esse tipo de ataque pode acontecer é o jeito mais eficaz de garantir segurança, principalmente quando informações sensíveis fazem parte de um determinado assunto.

Quanto menos divulgar informações, ainda que elas não pareçam tão confidenciais assim, melhor. Se não for possível verificar a identidade do interlocutor e a procedência das credenciais, todo cuidado ainda é pouco. Além disso, é importante ter em mente que grandes instituições não solicitam senhas ou outras informações sensíveis por telefone e e-mail.

Nunca se deixar levar pela pressão que criminosos tentam impor quando querem informações também é uma boa dica. Portanto, não se deve acreditar que coisas do tipo “sua conta será encerrada” e “seu nome será negativado” são verdadeiras. Manter a calma e procurar informações em fontes confiáveis é sempre o mais indicado.

De forma resumida, separamos as principais dicas de como se proteger dos engenheiros sociais, são elas:

não tenha engajamento com e-mails e ligações desconhecidas;

não clique em links ou navegue em sites cuja procedência desperte suspeita;

não baixe ou abra anexos de fontes suspeitas ou desconhecidas;

sempre desconfie de interações que solicitem a divulgação de dados pessoais ou confidenciais, de cunho sigiloso ou de acesso à rede corporativa;

não confie em pedidos urgentes que incluam dinheiro ou informações confidenciais;

não divulgue informações confidenciais sobre você ou sua empresa, seja por telefone, online ou pessoalmente;

proteja todos os dispositivos móveis e as máquinas, tanto pessoais quanto da empresa, e mantenha as atualizações em dia;

verifique a procedência e a veracidade de endereços de e-mail, números de telefone e outras ofertas ou contatos na web.

Como investir na segurança das empresas?

Os ataques de Engenharia Social podem ser poderosos e conseguem causar problemas grandiosos às empresas. Portanto, precisam ser tratados com seriedade e devem estar dentro da estratégia geral de gestão de risco de uma organização.

Existem diversas ferramentas e ações que podem garantir que as informações e os dados de uma empresa estejam seguros, como Firewall, Antivírus, Webfilter, VPN, Antiphishing, como o Threat X, da ClearSale, entre outros. No entanto, as pequenas ações por parte das pessoas que atuam nas empresas são imprescindíveis nesse caso.

Portanto, estabelecer uma cultura de segurança como compromisso dentro da organização ainda é a maneira mais eficiente de garantir boas práticas entre colaboradores e prestadores de serviços. Para fazer isso, todo tipo de ação de educação, de treinamento, de aprimoramento e de conscientização é válida, a fim de que os colaboradores conheçam os riscos e saibam quais ações tomar para evitar e reportar golpes e ciberataques.

Além disso, uma política clara e bem-acabada de segurança da informação, processos de segurança física, controles de acessos online e off-line, cuidados com descarte de lixo, controle e acompanhamento de visitantes e parcerias com empresas especializadas em gestão de risco são práticas fundamentais para evitar que a Engenharia Social faça mais uma vítima.

Esperamos que, com este artigo, você tenha entendido o que é a Engenharia Social e qual a melhor forma de se proteger dela. Então, se você gostou do nosso post e deseja compartilhar suas dúvidas e suas experiências com a gente, deixe aqui o seu comentário!

Aproveite e entre em contato com a ClearSale por meio do formulário abaixo. Temos um time de especialistas focado em caçar e identificar phishing, perfis falsos em redes sociais e outras vulnerabilidades.

Qual a diferença entre um spam, um phishing e um spear phishing?

Diferenças entre phishing e spear phishing

1. Phishing

Golpes de phishing, geralmente, são campanhas massivas, enviadas para milhares ou milhões de usuários ao mesmo tempo. Mesmo que apenas uma pequena porcentagem dos usuários caia no golpe, ainda assim será rentável.

Como normalmente incluem uma oferta lucrativa ou uma solicitação de ação urgente, como, por exemplo, um formulário que a Receita Federal está solicitando que você preencha o mais rápido possível, as campanhas de phishing se espalham rapidamente.

Os fraudadores tentarão imitar empresas e marcas conhecidas ou agências governamentais com o objetivo de alcançar mais pessoas.

Segundo relatório do FBI, golpes de phishing causaram prejuízos de mais de USD 57 milhões em 2019. O phishing está no topo da lista como a ameaça cibernética que tem o maior número de vítimas.

2. Spear phishing

Spear phishing, por outro lado, é altamente segmentado. Os cibercriminosos estudam e aprendem sobre as suas vítimas e usam muito táticas de engenharia social para dar mais credibilidade à mensagem.

Em vez de tentar se passar por empresas e marcas conhecidas, eles vão para um nível mais pessoal, tentando se passar por alguém que a vítima conhece.

Eles geralmente se apresentam como o CEO, um colega de trabalho ou um parceiro de negócios. Você já ouviu falar da Fraude do CEO?

A Fraude do CEO é um golpe de BEC (Business Email Compromise). Em 2019, de acordo com o FBI, golpes do BEC causaram perdas de USD 1,7 bilhão. É o tipo de golpe que mais causa prejuízos para empresas.

Características de phishing

Há tantas campanhas massivas de phishing sendo enviadas todos os dias que os usuários estão a cada dia mais ligados.

Os principais sinais de um ataque phishing são:

Links e anexos suspeitos.

Ofertas que são boas demais para serem verdadeiras.

Solicitações para o usuário fornecer informações pessoais ou confidenciais.

Endereço de remetente de e-mail falso.

Erros de ortografia e gramática.

Características de spear phishing

Spear phishing, no entanto, é mais difícil de se reconhecer, já que os criminosos estudam as suas vítimas e redigem a mensagem com cuidado.

O e-mail de spear phishing geralmente inclui:

Um endereço de e-mail bem elaborado ou até mesmo um endereço real de alguém que o usuário conhece e teve a conta hackeada.

Informações pessoais sobre o usuário ou o remetente.

Um link, anexo ou pedido para enviar dados confidenciais.

Um pedido urgente de transferência bancária ou pagamento de fatura.

Os sinais de spear phishing podem ser mais difíceis de se ver do que em campanhas massivas de phishing, mas eles também estarão lá.

Se a solicitação parecer estranha ou se a pessoa que enviou o e-mail não costuma escrever assim ou não envia e-mails, tenha cuidado e confirme a mensagem por outros meios, como por telefone, por exemplo.

Lembre-se: qualquer pessoa ou empresa pode ser um alvo para os dois tipos de phishing, por isso, invista em treinamento e segurança, e fique alerta.

9. Descreva como um atacante poderia levantar informações para lançar um spear phishing em uma grande empresa listada na bolsa de valores.