Segurança e Auditoria de Sistemas

Vamos compreender os principais conceitos de segurança da informação.

Principais Conceitos:

- A segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.
- É preciso garantir os princípios da segurança da informação: Confidencialidade, integridade, disponibilidade.
- É preciso trabalhar com os elementos do risco: Ativos, vulnerabilidades, agentes de ameaças, ameaças, probabilidade, impacto.
- A aplicação de mecanismos de defesa, controles de segurança e técnicas de segurança de redes é definida a partir de uma visão de riscos.

Segurança da informação é identificar, proteger, detectar, responder e recuperar.

Em segurança da informação, proteger significa implementar controles de segurança a partir da identificação e da avaliação dos riscos. Essa é a prevenção, e uma vez feita, um ataque em andamento é identificado, uma resposta, então, é dada e a recuperação do ambiente original é realizada.

- Identificar os riscos.
- Proteger e prevenir com os controles de segurança.
- Detectar ataques cibernéticos.
- Responder aos ataques cibernéticos.
- Recuperar o ambiente original.

Princípios da segurança da informação (CID):

- Confidencialidade.
- Integridade.
- Disponibilidade.

Riscos de Segurança

Riscos de segurança podem virar incidentes de segurança quando um agente de ameaça explora vulnerabilidades de um ativo. Quando isso ocorre, uma ameaça se torna um incidente de segurança e o nível de risco é calculado pela probabilidade e pelo impacto existente.

Risco (R) é o produto da Probabilidade (P) com o Impacto (I): $R = P * I$

Exemplo: Um cracker (agente de ameaça) utiliza um exploit para fazer um ataque, ou seja, para explorar uma vulnerabilidade de um ativo, um ativo pode ser a informação, as pessoas, os sistemas, os bancos de dados e os dispositivos físicos, como um notebook.

Diferentes tipos de riscos existem e devem ser considerados. Danos à reputação ou à marca, crime cibernético, risco político e terrorismo são alguns dos riscos que as organizações privadas e públicas de todos os tipos e tamanhos do mundo devem enfrentar cada vez mais. Há uma norma de gestão de riscos, a ABNT NBR ISSO 31000:2018, que abrange riscos de forma mais ampla, e, em segurança da informação, há uma norma específica, a ABNT NBR ISO/IEC 27005:2019. Isso reforça a

importância da visão de riscos para que possamos trabalhar com segurança da informação, pois é a partir da identificação dos riscos que a proteção pode ser realizada.

Controles de Segurança

Controles de segurança devem ser aplicados nos ativos, para eliminarem vulnerabilidades. Os controles podem ser:

- **Físicos:** Controle de acesso.
- **Tecnológicos:** Gerenciamento de contas e senhas.
- **Processos:** Norma de atualização de senhas.

Foram apresentados os principais conceitos que o acompanharão durante toda sua jornada em segurança da informação. Lembre-se sempre de que a segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.

Vamos explorar o mundo dos ataques cibernéticos que tanto afetam as empresas. Nosso objetivo é que você compreenda melhor o mercado de trabalho de segurança da informação, que sofre transformações constantes com os novos negócios, novas tecnologias e com a evolução dos ataques cibernéticos.

Fxmsp, o “Deus Invisível”

Em 2020, um hacker ganhou notoriedade. É o caso de Fxmsp, o “Deus Invisível”, um cidadão de Cazaquistão de 37 anos de idade na data. O nome real dele é Andrey Turchin, ele ainda não foi preso, sendo acusado de conspiração, fraude eletrônica, fraude por acesso ilícito a dispositivos e abuso do uso do computador (hacking).

O mapa das vítimas de Fxmsp mostra a abrangência global de seus ataques. São 300 empresas de 44 países. As revelações são do Group-IB, após pargar US$ 1,5 milhões por todas as informações roubadas e os segredos para as invasões.

Com relação a ataques cibernéticos, considere as afirmativas a seguir:

- Ataques cibernéticos podem ser feitos a partir de qualquer localidade pela internet.
- Ataques cibernéticos podem ser realizados a partir da exploração de uma única vulnerabilidade.
- É um desafio a proteção contra ataques cibernéticos, porque todas as vulnerabilidades devem ser tratadas, para o criminoso, basta encontrar um ponto fraco.
- Em um ataque cibernético, o agente de ameaça explora vulnerabilidades utilizando técnicas de ataques, incluindo ferramentas.

Todas as afirmações representam características de ataques cibernéticos: Qualquer localidade onde haja acesso à internet, exploração de uma única vulnerabilidade, necessidade de proteger contra todas as vulnerabilidades e uso de ferramentas e técnicas de ataques que levam ao incidente de segurança.

As atividades criminosas de Fxmsp eram conhecidas desde 2016. Suas vítimas eram de todos os setores.

Chama a atenção a lista de vítimas de Fxmsp, que inclui empresas de cibersegurança, como Mc Affe, Symantec e Trend Micro.

Além das atividades criminosas, Turchin foi inovador: Vendia as informações obtidas oferecendo uma experimentação, com acesso prévio limitado para potenciais compradores, a fim de que pudessem verificar a qualidade e a confiabilidade de seus produtos.

Além disso, Turchin sabia como monetizar suas façanhas, tendo contratado um gerente comercial, um "laranja", que negociava as informações com potenciais compradores. Ele vendia não somente as informações, mas também o acesso à empresa e ainda códigos-fonte.

E como era o modus operandi de Fxmsp?

Ele realizava os ataques focando um serviço em especial, o Remote Desktop Protocol, na porta TCP 3389.

Qual dos ataques possibilitou a descoberta de serviços específicos, como o RDP?

- Scan

O scan de portas possibilita o mapeamento dos serviços existentes na empresa ou em determinada faixa de endereços IP.

RDP é o serviço disponibilizado pelo Windows para acesso remoto, o Microsoft Terminal Services. O acesso remoto possibilita que acesso externos sejam feitos a equipamentos, que, muitas vezes, estão na rede interna da empresa. Isso facilita atividades como administração remota ou suporte remoto, porém abre uma brecha significativa que pode ser explorada em ataques. O firewall tem que liberar a porta TCP 3389 para que o RDP funcione, e, já que o firewall possibilita essas conexões, os ataques passam diretamente pelo firewall.

O firewall bloqueia tráfegos baseados em suas regras, que são basicamente as origens, os destinos e os serviços/portas liberadas pela empresa. No caso do RDP (porta TCP 3389), a regra deve definir quem pode fazer o acesso remoto a quais equipamentos da empresa. Uma vez liberado o tráfego desse protocolo, o suporte técnicos, por exemplo, pode acessar os equipamentos via Microsoft Terminal Services, em que uma senha de acesso é solicitada. O hacker também pode explorar esse acesso ao serviço para realizar os ataques.

No caso do RDP, uma vez que Fxmsp conseguiu o acesso ao serviço, qual é o passo posterior do ataque, considerando que há a necessidade de senha para acessar o equipamento?

- Força bruta para descobrir a senha.

Uma vez obtida a conexão no equipamento via RDP, o hacker precisa acessar o serviço com a senha. Um ataque para descobrir a senha é o ataque de força bruta, em que diferentes combinações são testadas até o sucesso.

Uma vez descoberta a senha de acesso ao equipamento via RDP, Fxmsp passa para o passo posterior, que visa ao domínio do equipamento ou servidor. Ele desabilita o antivírus e o firewall, além de criar contas adicionais e descobrir outras credenciais da rede. Outra medida dele é a instalação de backdoor, que abre uma porta no servidor para que acessos posteriores possam ser feitos diretamente pelo atacante.

Metasploit é uma ferramenta para criação de exploits, que são utilizados por profissionais de segurança da informação para explorar vulnerabilidades e testar a segurança de diferentes serviços e aplicações.

O Meterpreter utiliza o Metasploit para criar um backdoor que funciona na memória da vítima, sem persistência e uso de criptografia na comunicação com o servidor de comando e controle. Informações podem vazar via esse backdoor.

Fxmsp utilizava esse backdoor a cada 15 dias para evitar a sua detecção. Qual controle de segurança é capaz de detectar uma comunicação de backdoor, da rede interna, para o servidor de comando e controle na internet?

- IDS/IPS

IDS/IPS monitora o tráfego em busca de padrões que indicam ataques em andamento. O ataque de Fxmsp, que acionava o backdoor a cada 15 dias, mostra que IDS/IPS podem ser evadidos. Firewall bloqueia, antivírus detecta vírus em equipamentos, autenticação faz parte do controle de acesso e a criptografia protege a mensagem.

As informações das empresas eram roubadas com a movimentação lateral a partir do acesso obtido via RDP, explorando-se, ainda, as relações de confiança existentes na rede. Para finalizar, Fxmsp fazia com que mudanças de senhas ou restauração de back-ups, que poderiam ser feitas pelas empresas em caso de desconfiança de um ataque, não resolvessem o comprometimento do equipamento e servidor, já que os back-ups também continham o backdoor.

Qual seria a sua recomendação para que sua empresa não tenha o serviço RDP explorado, como ocorreu com cerca de 300 empresas de 44 países que foram vítimas de Fxmsp?

- Uso de portas alternativas TCP para o RDP e controles de autenticação.

Caso a empresa precise utilizar o RDP, é recomendável que a porta padrão seja alterada. Porém, isso apenas minimiza a possibilidade de ataque. Outra medida importante é habilitar controles de autenticação, como o travamento em caso de tentativa de ataque de força bruta.

A Criptografia faz Parte do Dia a Dia de Todos

Os dados de seu dispositivo móvel são armazenados com criptografia, o acesso online ao seu banco é feito usando um canal seguro com criptografia, a sua comunicação com amigos e familiares com Whatsapp, por exemplo, é protegida por criptografia, e ninguém consegue escutar as mensagens ou ter acesso a elas no meio do caminho.

A Criptografia é Utilizada pelas Empresas

Como profissional de segurança, você pode utilizar a criptografia para melhorar a segurança da sua empresa.

- Criptografia dos dados armazenados no notebook.
- Conexão remota do home office utilizando VPN para proteger a comunicação pela internet.
- Criptografia do banco de dados para proteger as informações de vendas armazenadas.
- Criptografia das conexões ao website de vendas online utilizando HTTPS/TLS/SSL.

O que é Criptografia

Criptografia é ocultar o significado das mensagens, e não ocultar a mensagem em si. Esta é a esteganografia.

- No caso da criptografia, em caso de a mensagem ser interceptada, o conteúdo está protegido.
- Já no caso da esteganografia, a mensagem está oculta.

A ferramenta Online Cryptograph Tools contém exemplos desde a cifras simples, como a Cifra de César, como criptografia de chave simétrica e hash.

A seguir temos um exemplo de aplicação da Cifra de César.

Vamos utilizar como senha a palavra “CRIPTO” e substituir cada letra da palavra avançando três letras no alfabeto. Por exemplo, a letra “C” vamos substituir por “F”, a letra “R” será alterada pela letra “U” e assim por diante. O resultado será “FULSWR”.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Outro exemplo de algoritmo de criptografia é a que utiliza funções hash. Funções de hash são utilizadas para verificação da integridade. Estes algoritmos realizam um cálculo matemático nas mensagens ou nos documentos. O receptor recebe a mensagem juntamente com o hash e utiliza o mesmo algoritmo para calcular o hash da mensagem recebida. O hash recebido e o hash calculado devem ser comparados, e devem ser iguais, o que garante a integridade da mensagem ou do documento. Alguns exemplos de funções de hash são o MD5 e a família SHA (SHA-1, SHA-256 e SHA-512). É importante ressaltar que o MD5 e o SHA-1 não devem mais ser utilizados na prática, pois são susceptíveis a ataques de colisão. Neste ataque, mensagens diferentes podem gerar o mesmo hash, impossibilitando a validação da integridade.

Um exemplo é a frase “Teste_Senha”, que gerará o hash em SHA-256 *86a974f91abd5da4ed443a69f8c4c0bb361b39a396c70d0819c4f85c05e2eab4*.

Qualquer alteração das letras, como para maiúsculas ou minúsculas, a hash será alterada, porém o tamanho é fixo. Cada palavra frase sempre vai conter uma hash única.

Protocolos que usam Criptografia

- TLS é o protocolo padrão da internet atualmente, em substituição ao SSL, que possui muitas falhas de segurança.
- HTTPS é o uso do HTTP protegido por TLS/SSL.
- VPN é um túnel virtual nos moldes do TLS, para comunicação remota ou entre empresas que se comunicam por uma rede pública e não confiável.
- IPSec é um dos protocolos mais utilizados por VPNs.

A criptografia tem um papel importante para a proteção de dados armazenados, ainda mais em um mundo em que as informações estão distribuídas em datacenters de empresas, dispositivos e usuários e nuvem.

Ataques Cibernéticos

Os ataques cibernéticos acontecem com exploração de vulnerabilidades. E vulnerabilidades podem existir em protocolos, algoritmos e softwares em geral.

O objetivo é desenvolver softwares robustos e seguros, que não sejam explorados em ataques.

O momento em que as vulnerabilidades são encontradas e corrigidas é importante. Caso a reparação seja feita durante a codificação, o custo médio é de US$ 25 por falha. Já quando a reparação é feita no último estágio, quando o software está em produção, o custo médio é de US$ 16.000 por falha, ou seja, 640 vezes maior se comparado com um trabalho de reparação rápida. Estes valores não consideram ainda impactos de reputação ou outros operacionais, como os de suporte para atualizações de software em produção após a descoberta de vulnerabilidade sendo explorada em massa por todo mundo.

Ciclo de Vida de Desenvolvimento Seguro

Há um conjunto de práticas de ciclo de vida de desenvolvimento seguro. O ciclo de desenvolvimento possui estas etapas básicas: Treinamento, requisitos, concepção, implementação, verificação, lançamento e resposta. A codificação é apenas uma destas etapas.

- Treinamento » Requisitos » Concepção (Design) » Implementação » Verificação » Lançamento » Resposta.

Neste ciclo de vida, o desenvolvimento seguro possui práticas importantes. Veja a seguir alguns exemplos:

- Prover treinamento.
- Definir requisitos de segurança.
- Definir métricas e relatórios de conformidade
- Executar modelagem de ameaças.
- Estabelecer requisitos de design.
- Definir e usar padrões de criptografia.
- Gerenciar e usar padrões de segurança no uso de componentes de terceiros.
- Utilizar ferramentas aprovadas.
- Executar análise estática ou static analysis security testing (SAST).
- Executar análise dinâmica ou dynamic analysis security testing (DAST).
- Executar testes de penetração ou pentests.
- Estabelecer um processo padrão de resposta a incidentes.

Principais Vulnerabilidades do OWASP

Veja a seguir as principais vulnerabilidades de acordo com o Top 10 do OWASP (2020) que devem ser conhecidas e evitadas no desenvolvimento de sistemas:

- **Falhas de Injeção:** Como no SQL, NoSQL, sistema operacional e LDAP, dados não confiáveis são enviados como parte de um comando ou consulta.
- **Autenticação Quebrada:** Incluindo o gerenciamento das sessões, que possibilita o acesso a senhas, credenciais de acesso ou sessões.
- **Exposição de Dados Sensíveis:** Que podem vazar durante a transmissão e armazenamento.
- **XML External Entities (XXE):** Em que há o acesso a entidades externas por documentos XML mal configurados, o que abre um leque de possibilidades de ataques.

- **Controle de Acesso Quebrado:** Com falha nas restrições de privilégios e possibilitam acessos desnecessários.
- **Má Configuração de Segurança:** Que fornece informações que podem ser utilizadas em ataques, e abrem acessos a informações e funções que não deveriam.
- **Cross-Site Scripting XSS:** Que possibilita a execução de códigos diretamente no navegador da vítima, devido à falta de validações dos dados processados.
- **Desserialização Insegura:** Que pode resultar em ataques que incluem ataques replay, ataques de injeção, escalada de privilégios e execução de código remoto.
- **Uso de Componentes com Vulnerabilidades Conhecidas:** Incluindo bibliotecas, frameworks e outros módulos de software que têm os mesmos privilégios da aplicação.
- **Registro e Monitoramento Insuficiente:** Que dificulta a detecção e resposta a incidentes de segurança.

Um conceito importante no desenvolvimento de sistemas é o DevSecOps. No modelo shift-left da esteira de desenvolvimento, considerando os custos de correção de softwares, o objetivo é fazer os testes e as validações de segurança desde o início do desenvolvimento. No DevSecOps, há o empoderamento dos desenvolvedores, que passam a fazer, junto com a equipe de segurança e utilizando ferramentas de segurança, os testes e validações de segurança em todas as etapas de desenvolvimento. O DevSecOps é importante no modelo de desenvolvimento atual, que adota metodologia ágeis e necessita seguir as práticas de segurança que vai do treinamento ao processo de resposta a incidentes.

Apesar do constante surgimento de novas tecnologias de segurança, ainda há muitas ameaças que precisam ser tratadas. Portanto, o fortalecimento da cultura de segurança e privacidade depende de um conjunto de elementos, a política de segurança e privacidade, o treinamento, a conscientização e a participação ativa da alta administração.

Segurança de Dados

Dados são registros que servem como matéria-prima para a construção da informação e do conhecimento, por meio da análise, manipulação e processamento de dados. Exemplos: Dados pessoais, tais como nome, CPF, endereço.

Informação são os dados processados sobre algo ou alguém, e o conhecimento é um conjunto de informações úteis que foram adquiridas por meio de aprendizados e experiência.

A segurança de dados anda de mãos dadas com a segurança da informação. Eles existem em meio físico, em meio digital e com as pessoas. E fluem constantemente, sob a forma de transmissão, sendo processados ou estando armazenados.

Exemplo: Documento confidencial sendo enviado pelos Correios, executivos conversando sobre um projeto estratégico em um voo comercial, dados/informação migrando da empresa para um provedor de nuvem, e depois de um provedor de nuvem para outro.

Estado dos Dados

Dados existem em diferentes estados:

- Em processamento ou Data-In-Use (DIU).
- Em transmissão ou Data-In-Motion (DIM).
- Em armazenamento ou Data-At-Rest (DAR).

Cada um destes estados apresenta riscos e precisa de segurança da informação e privacidade.

Fluxo da Classificação da Informação

A informação precisa ser classificada, de acordo com o fluxo que se inicia na criação:

- Criação da Informação » Classificação da Informação » Rotulagem da informação » Manuseio da Informação.

Exemplo de classificação de informação:

- Pública » Interna » Confidencial » Secreta.

Quem classifica a informação? O seu proprietário, que cria a informação.

Ciclo de Vida e Tratamento dos Dados/Informação

Os dados/informação possuem um ciclo de vida desde a sua criação à destruição. Cada etapa deste ciclo de vida é importante para a segurança e privacidade.

- **Ciclo de Vida:** Criação » Armazenamento » Uso » Compartilhamento » Arquivamento » Destruição.

Controles de Segurança

Os principais controles de segurança no contexto do armazenamento de dados: Criptografia, gestão de identidades e controle de acesso (físico e lógico), logs/registros de acesso.

A criptografia de dados é um dos principais controles de segurança que podem ser utilizados pelas empresas. A criptografia funciona com as chaves criptográficas. Você pode proteger os dados utilizando a criptografia, mas tem que pensar como será o gerenciamento das chaves, e precisa saber dos aspectos envolvidos, que estão em forma de perguntas:

- Cada usuário terá sua própria chave criptográfica para proteger seus dados? E se ele esquecer ou perder a chave, como sua empresa atuará?
- Você usará chave criptográfica na sua aplicação, que fará a criptografia dos dados antes de serem armazenados no banco de dados? E onde estará esta chave, na própria aplicação? E no caso de um comprometimento desta chave, como você fará a atualização?
- Ou você utilizará a criptografia do banco de dados? Quem terá acesso a esta chave? E o provedor de nuvem? O que você fará em caso de comprometimento desta chave?

Vimos que a proteção dos dados é cada vez mais importante para você, como cidadão, porque precisa ter a sua privacidade preservada e a LGPD cumprida pelas empresas com as quais você se relaciona. E como profissional, porque as empresas precisam adequar seus sistemas e processo para proteger os dados e as informações, incluindo as confidenciais e sigilosas, sem deixar de lado as pessoas, já que a segurança e privacidade é de responsabilidade de todos.

Ataques em Dispositivos Móveis

Em um dispositivo móvel há camadas e componentes que podem ser explorados em ataques: Hardware, firmware, sistema operacional e aplicação.

O foco aqui é na camada de aplicação, no desenvolvimento seguro dos aplicativos. Mas, pensando em um ambiente corporativo, o ataque pode acontecer em mais pontos. No ambiente do usuário, há aquele usuário que pode sofrer ataques de phishing, além de ataques aos dispositivos (que podem ser roubados) e aos aplicativos, sistemas ou plataformas. Além desse ambiente do usuário, podem ser atacados os dados que trafegam pelo provedor de internet e a própria internet, além do ambiente da empresa, que se comunica com o usuário.

As 10 Maiores Vulnerabilidades em Aplicativos Móveis

Segundo a OWASP, as 10 maiores vulnerabilidades em aplicativos móveis são as que são demonstradas a seguir e devem ser conhecidas pelos desenvolvedores para que não sejam incluídas em seus próprios aplicativos:

- **Uso impróprio de plataforma:** Uso incorreto de característica da plataforma ou falha no uso de controles de segurança da plataforma, como as permissões ou biometria. Exemplo: Devido a uma implementação equivocada de como um segredo era armazenado após o uso do Touch ID do IOS, era possível passar pela autenticação do aplicativo Citrix Worx. Com a implementação, bastava seguir os passos: Reboot do dispositivo móvel, abrir o aplicativo, iniciar a autenticação mas cancelar o Touch ID, fechar o aplicativo e abri-lo novamente, a autenticação estava feita. O aplicativo assumia que o usuário estava autenticado quando o processo era cancelado e o aplicativo reiniciado.
- **Armazenamento de dados inseguro:** A proteção deve considerar um agente de ameaça que tem a posse física do dispositivo móvel, ou um malware ou outro aplicativo que é executado no dispositivo: A proteção de arquivos pode ser insuficiente e o acesso a recursos de privacidade quando os dados são usados podem estar implementados incorretamente. É o que aconteceu com o Tinder no passado, que na primeira implementação, ao mostrar as pessoas próximas ao usuário, possibilitava a descoberta da exata localização. Na segunda implementação, o desenvolvedor mudou para o envio de distância ao invés da localização, mas ainda era possível descobrir a localização com a triangulação e uso de localização falsa.
- **Comunicação insegura:** Dados que trafegam em um modelo cliente-servidor podem ser interceptados em diferentes pontos, tais como uma rede de acesso comprometido, dispositivos do provedor de internet atacados ou por um malware no dispositivo móvel. Exemplo: Um relógio inteligente para crianças implementou incorretamente a comunicação e era possível o acesso ao dispositivo, com os resultados: Descoberta da localização, chamada para a criança, criação de um canal de escuta sem o conhecimento da criança, envio da mensagem de áudio sem consentimento, acesso a dados da criança (foto, data de nascimento, nome, peso, altura).
- **Autenticação insegura:** Ataques que exploram vulnerabilidades de forma automatizada em busca de acessos. Exemplo: Um aplicativo implementou incorretamente a autenticação de dois fatores, permitindo o ataque de força bruta.
- **Criptografia insuficiente:** A proteção deve considerar um agente de ameaça que tem a posse física do dispositivo móvel, ou um malware ou outro aplicativo que é executado no dispositivo. Exemplo: “PRODKEYPRODKEY12” era a chave criptográfica utilizada em um aplicativo, que estava no próprio código-fonte, em formato decimal. Descoberta a chave, que era utilizada também para cifrar as senhas dos usuários, era possível acessar contas de qualquer usuário. Havia problemas também na forma como a segurança da camada de transporte era implementada, bem como a verificação de certificados digitais SSL.
- **Autorização insegura:** Ataques que exploram vulnerabilidades de forma automatizada em busca de acessos. Exemplo: Um carro inteligente teve o seu acesso remoto implementado com autorização insegura, que permitia que, após o acesso ao servidor, a identificação do usuário pudesse ser modificada e outro carro pudesse ser acessado.

- **Má qualidade de código:** A proteção deve considerar agentes de ameaça que podem utilizar entrada não confiáveis para as chamadas do código, que podem levar à execução de códigos arbitrários. As vulnerabilidades 0-day surgem muitas vezes da má qualidade de código. O buffer overflow é um exemplo em que o uso da memória não é gerenciado e permite a execução de códigos arbitrários. É o que aconteceu com o Whatsapp, onde códigos arbitrários podiam ser executados a partir do envio de um conjunto de pacotes junto com uma ligação.
- **Modificação de código:** A exploração pode ser pelo uso de fontes de aplicativos de terceiros que hospedam os códigos modificados, ou pela instalação pelo usuário vítima de phishing. Envolvem também a modificação do binário, modificação dinâmica de memória ou hooking de métodos.
- **Engenharia reversa:** O atacante analisa o aplicativo com a ajuda de diversas ferramentas para entender e explorar as funções. É a técnica utilizada para analisar o código-fonte, bibliotecas e algoritmos, podendo levar a descoberta de propriedade intelectual, uso de criptografia e suas chaves, e informações sobre servidores e back-end.
- **Funcionalidade exposta:** A exposição em aplicativos pode revelar funcionalidades de sistemas de back-end, que pode então ser explorada diretamente. Mesmo backdoors podem ser inseridas sem intenção, como ocorreu com um aplicativo de troca de arquivos, que permitia conexões remotas sem nenhuma autenticação.

Vulnerabilidades

- O objetivo da segurança é de preservar a confidencialidade, integridade e disponibilidade da informação.

Esse objetivo só é possível com o entendimento dos riscos de segurança da informação, que avalia o ambiente e busca a implementação de controles de segurança para tratar as vulnerabilidades dos ativos.

As vulnerabilidades existem nos ativos e são exploradas por agentes de ameaças com o uso de técnicas de ataques. Quando isso acontece, uma ameaça se torna um incidente de segurança, o que resulta em impactos para a empresa. E o cálculo da probabilidade de isso ocorrer com o impacto é o risco, que é algo que pode ou não acontecer.

Ativos possuem vulnerabilidades, que podem ser exploradas.

Tratar as vulnerabilidades é a principal forma de diminuir os riscos. As vulnerabilidades precisam ser identificadas nos diferentes ativos de um ambiente para serem tratadas.

Testes de Segurança

Há testes de segurança diferentes que visam a identificação das vulnerabilidades.

O que diferencia um tipo de teste de outro é a visão de onde ele é realizado (interno ou externo) e o tipo de informação que o profissional de segurança tem para a realização dos testes. A seguir vamos conhecer um pouco mais os testes de segurança interno e externo.

- **Interno:** O teste de segurança a partir do ambiente interno normalmente é feito em empresas que desenvolvem software e é conhecido como análise de vulnerabilidades. A análise de vulnerabilidades estática ou SAST é uma análise de código-fonte. Já a análise de

vulnerabilidades dinâmica ou DAST é uma análise com o software em execução, em tempo real.

- **Externo:** Os testes de segurança a partir do ambiente externo são conhecidos como testes de penetração ou pentest. Outros nomes utilizados são testes de intrusão e ethical hacking. Há três principais tipos de pentest, que variam de acordo com o acesso prévio a informações do ambiente testado: O teste de caixa preta (black box) é feito sem nenhum conhecimento prévio do ambiente. O teste de caixa branca (white box) é feito com o máximo de conhecimento prévio do ambiente, incluindo código-fonte, documentação e diagramas. O teste de caixa cinza (gray box) é feito com algum conhecimento prévio do ambiente, como uma credencial de usuário comum.

As análises de código-fonte, realizadas no SAST, podem ser feitas com o uso de ferramentas ou manualmente. As ferramentas conseguem identificar erros no código, mas dificilmente conseguem identificar falhas na especificação e na lógica.

O teste de caixa preta pode também ter algumas limitações na identificação de vulnerabilidades.

Exemplo: Uso de mecanismo criptográfico para autenticar um usuário de diferentes sites. Neste exemplo, um usuário autenticado no site A pode visitar o site B automaticamente. Neste implementação, a validação é feita com o uso de um hash do nome do usuário e data, que é enviado ao site B pelo site A e pelo usuário. O site B pode então comparar o hash para validar o usuário. O problema de segurança é que, uma vez descoberto o funcionamento, qualquer agente de ameaça que captura o hash pode chegar ao site B. O teste de caixa preta enxerga o hash, sem saber a sua função, de uma forma direta, que só pode ser identificada com uma análise de código.

Menos vulnerabilidades significam menos chances de exploração dos ativos da empresa, ou seja, menos incidentes de segurança.

Controles de Auditoria

Os controles de auditoria podem ser de diferentes natureza. Veja a seguir os tipos de controles e alguns exemplos:

Tecnológico, Técnico ou Lógico

- Firewall.
- VPN.
- …

Processual, Administrativo, Operacional

- Atualização periódica de sistema operacional.
- Comunicação de incidentes de segurança.
- …

Físico

- Sistema de supressão de incêndio.
- Circuito fechado de TV.
- …

A definição de controles é feita a partir de uma avaliação de riscos, que levam em consideração os requisitos de segurança e privacidade derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas e transmitidas.

Uma vez implantado o controle, é preciso verificar a eficiência e eficácia do controle, que deve estar cumprindo o seu papel.

A auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação.

O auditor precisa ter conhecimentos e competência técnica para verificar os controles. É preciso conhecer as principais normas e frameworks utilizados para a definição de controles.

Um deles é o NIST Cybersecurity Framework, que define os controles para a identificação, proteção, detecção, resposta e recuperação.

COBIT

O Control Objectives for Information and Related Techonology (COBIT) é um framework de governança de TI que trata de uma visão organizacional, que tem relação com a segurança e privacidade.

Avaliar, direcionar e monitora ou evaluate, direct and monitor (EDM). Ex: Garantir a definição e manutenção do framework de governança e garantir a otimização do risco.

Alinhar, planejar e organizar, ou align, plan and organize (APO). Ex: Gerenciar a arquitetura corporativa, gerenciar riscos e gerenciar segurança.

Construir, adquirir e implementar ou build, acquire and implement (BAI). Ex: Gerenciar disponibilidade e capacidade, gerenciar mudanças de TI, gerenciar ativos e gerenciar configuração.

Entregar serviço e suporte ou deliver, service and support (DSS). Ex: Gerenciar operações, gerenciar requisição de serviços e incidentes, gerenciar continuidade e gerenciar serviços de segurança.

Monitorar, verificar e avaliar ou monitor evaluate and asses (MEA). Ex: Gerenciar monitoramento de desempenho e conformidade, gerenciar sistema de controle interno e gerenciar garantia.

ITIL

O Information Technology Infrastructure Library (ITIL) provê um conjunto de melhores práticas que visa auxiliar as empresas a entregar e suportar serviços de TI, composto por 34 práticas de gerenciamento. Veja as a seguir:

Práticas de Gerenciamento Geral

- Gerenciamento de estratégia.
- Gerenciamento financeiro de serviços.
- Mensuração e reporte.

- Gerenciamento de conhecimento.
- Gerenciamento de relacionamentos.
- Gerenciamento de portfólio.
- Gerenciamento de força de trabalho e talento.
- Gerenciamento de riscos.
- Gerenciamento de mudança organizacional.
- Gerenciamento de fornecedores.
- Gerenciamento de arquitetura.
- Melhoria contínua.
- Gerenciamento de segurança da informação.
- Gerenciamento de projetos.

Práticas de Gerenciamento de Serviço

- Análise de negócio.
- Gerenciamento de nível de serviços.
- Gerenciamento de continuidade de serviços.
- Gerenciamento de incidentes.
- Gerenciamento de lançamento.
- Gerenciamento de configuração de serviços.
- Gerenciamento de catálogos de serviços.
- Gerenciamento de disponibilidade.
- Gerenciamento de monitoramento e eventos.
- Gerenciamento de requisição de serviços.
- Habilitação de mudanças.
- Gerenciamento de ativos de TI.
- Design de serviço.
- Gerenciamento de capacidade e desempenho.
- Service desk.
- Gerenciamento de problemas.
- Validação e teste de serviços.

Práticas de Gerenciamento Técnico

- Gerenciamento de implantação.
- Gerenciamento de infraestrutura e plataforma.
- Gerenciamento e desenvolvimento de software.

NBR ISO/IEC 27002

A norma ABNT NBR ISO/IEC 27002 provê um conjunto de objetivos de controles:

- Políticas de segurança da informação.
- Organização da segurança da informação.
- Segurança em recursos humanos.
- Gestão de ativos.
- Controle de acesso.
- Criptografia.
- Segurança física e do ambiente.

- Segurança nas operações.
- Segurança nas comunidades.
- Aquisição, desenvolvimento e manutenção de sistemas.
- Relacionamento na cadeia de suprimentos.
- Gestão de incidentes de segurança da informação.
- Aspectos de segurança da informação na gestão de continuidade do negócio.
- Conformidade.

Os controles podem ter naturezas diferentes, como técnicos ou lógicos, administrativos, processuais ou operacional, ou físicos. Os objetivos são muitos e dependem dos riscos identificados e avaliados. A verificação da eficiência e eficácia dos controles é feita pela auditoria, que tem papel importante para a segurança das empresas e para a conformidade regulatória e geral.

Auditoria

A auditoria é uma inspeção e verificação formal para validar eficiência e eficácia, verificar conformidade com padrões ou normas, e se os registros estão corretos.

Em uma auditoria de segurança da informação, é preciso verificar se os riscos forma identificados, se os controles necessários forma definidos e se os controles foram implantados adequadamente.

Técnicas e Ferramentas para Auditoria

Quais técnicas e ferramentas utilizar?

As técnicas e ferramentas envolvem:

- Interação com as pessoas.
- Análises manuais.
- Análises técnicas com ferramentas.

Exemplo de técnicas e ferramentas para auditoria de segurança:

- Análise das políticas, processos e procedimentos de segurança e privacidade.
- Entrevistas com todas as áreas da empresa para percepção sobre se a política de segurança é de conhecimento organizacional e se está sendo seguida.
- Visita ao data center para analisar a segurança física.
- Análise de configuração do firewall.
- Análise do fluxo para gestão de identidades.
- Pentest para identificar vulnerabilidades do ambiente.
- Análise de logs do banco de dados.
- Análise dos relatórios do IDS/IPS.
- Análise do antivírus.
- Análise de código do sistema corporativo.
- Teste de phishing.

ISO 27001

ABNT NBR ISO/IEC 27001 é uma norma para sistema de gestão de segurança da informação (SGSI). Uma empresa pode ser certificada na ISO 27001 e o auditor deve avaliar o SGSI.

Para a auditoria ISO 27001, uma técnica importante é a declaração de aplicabilidade. Ela declara quais controles de segurança são aplicáveis para a empresa, com base nos riscos específicos do ambiente e do escopo que está sendo auditado.

Uma auditoria de segurança engloba um conjunto de elementos, como as configurações dos sistemas operacionais, compartilhamento de redes, aplicações e acessos, a validação de processo e do nível de maturidade em segurança dos usuários. Alguns assuntos que são normalmente alvos de auditoria são:

- Proteção de e-mail, principalmente contra phishing e filtro de spam.
- Senhas de usuários, para verificar se estão de acordo com a política de senha da empresa.
- Gerenciamento de usuários, para verificar se há contas ativas que não deveriam, como de ex-funcionários.
- Backups, para verificar se é feito e se está íntegro.
- Acesso físico, para evitar acessos indevidos de pessoas não autorizadas.
- Atualização de software, para verificar se os sistemas estão em versões livres de vulnerabilidades.
- Vulnerabilidades, para identificar pontos fracos que podem ser explorados em ataques.

Os procedimentos, técnicas e ferramentas para auditoria são utilizados para obter dados e informações e para analisar e validar as evidências e os controles existentes. Além disso, são utilizados para organizar os resultados. O conhecimento e a competência técnica do auditor são essenciais para definir procedimentos, técnicas e ferramentas na fase de planejamento da auditoria, e para utilizá-los no trabalho em campo.