Aula 4

Segurança em Sistemas de Informação

Prof. Douglas Eduardo Basso

Conversa Inicial

- O objetivo desta aula é elencar os principais ataques à segurança. Vamos detalhar a engenharia social, aprendendo quais são os tipos de criminosos virtuais, as principais motivações para ataques virtuais, a classificação dos ataques. Será apresentado um guia sobre riscos, ameaças e vulnerabilidades. Na sequência, destacaremos as técnicas de mitigação e contramedidas de segurança

Ataques à Segurança

- Os sistemas de informação são instrumentos fundamentais na gestão administrativa e estratégica de qualquer organização. São sistemas que precisam garantir a tríade de segurança da informação (confidencialidade, integridade e disponibilidade) e gerir quem são os proprietários e utilizadores dos sistemas

- A área de segurança da informação deve proteger as informações, com o objetivo de preservar o seu valor, fazendo-se necessária para
  - Garantir a continuidade dos negócios
  - Reduzir ao mínimo possível os riscos que podem surgir
  - Potencializar ao máximo os retornos dos investimentos feitos ao negócio
  - Gerar cada vez mais boas oportunidades à organização

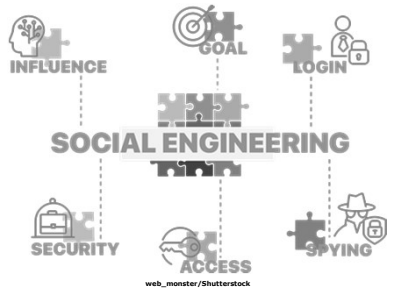
Categorias de *hackers*

- Existem algumas categorias que descrevem cada tipo de hacker
  - Algumas delas
    - ***Blue hat***
    - ***Grey hat***
    - ***Black hat***

- ***White hat***
- ***Hackers* governamentais**
- **Hacktivistas**
- ***Insiders***

Engenharia social

- **É um conjunto de métodos e técnicas de manipulação psicológica de pessoas com o intuito de promover a execução de ações e a divulgação de informações confidenciais de determinada organização**



Motivos de ataques à segurança

- **Adquirir e escalar privilégios de acesso a sistemas**
- **Capturar dados e informações pessoais de usuários**
- **Fazer o roubo de dados e informações corporativas, segredos industriais ou propriedades intelectuais**
- **Buscar informações bancárias**
- **Coletar informações de organizações**

- **Tornar um sistema inoperante, dificultar o bom funcionamento de sistemas de informação**
- **Estabelecer acesso a redes, computadores e sistemas, de maneira não autorizada, e criar um ataque a partir desse acesso**
- **Utilizar os recursos da estrutura de tecnologia invadida para outros fins**
- **Expor vulnerabilidades e colocar sistemas em risco**

Riscos e ameaças

- **Uma ameaça é todo e qualquer fato capaz de, de forma eventual, causar um dano ou prejuízo a uma organização. Já o risco pode ser conceituado como uma possibilidade de determinada ameaça se consolidar em algum fato que afete e comprometa um serviço ou sistema**

Vulnerabilidades

- **Naturais**
- **Organizacionais**
- **Físicas**
- ***Hardware***
- ***Software***
- **Meios de armazenamento**
- **Humanas**
- **Comunicação**

Técnicas de mitigação e contramedidas

- **As técnicas de mitigação são mecanismos essenciais na área de segurança da informação. Visam minimizar os impactos de ataques cibernéticos em organizações. Uma contramedida é posta em prática para mitigar o risco em potencial**

Incidentes

- **Vazamento de informações**
- **Má utilização de recursos de tecnologia da informação**
- **Exclusão de informações**
- **Codificação maliciosa**

- **Problemas e falhas em equipamentos de tecnologia da informação**
- **Iniciativas e tentativas de invasão**
- **Ataques de engenharia social**
- **Acesso feito de forma indevida e não autorizada (acessos físicos e lógicos)**

Impactos

- Aumento de gastos com seguros
- Fuga de clientes, contratos, fornecedores e colaboradores
- Danos à reputação e à imagem das pessoas ou da organização

- Diminuição de produtividade e desempenho
- Multas e penalidades jurídicas
- Prejuízos financeiros diversos
- Gastos maiores com recuperação, retrabalho, reparação e recuperação de problemas

- Entre os controles físicos, podemos elencar os principais que devem ser levados em consideração
  - Proteção e gerência dos equipamentos
  - Controles de acesso
  - Localização geográfica
  - Infraestrutura de *datacenter*

Códigos maliciosos

- ***Malware***
- ***Phising***
- ***Spam***
- **Vírus**
- **Worm**
- **Cavalo de Troia**

- ***Hoax***
- **Bomba lógica**
- ***Spyware***
- ***Botnets***
- ***Ransomware***
- ***Rootkit***

Recuperação de desastres

- O propósito de um plano de recuperação de desastres é minimizar as consequências de um desastre e tomar medidas necessárias para garantir que funcionários, ativos e processos de negócio estejam disponíveis novamente em um tempo aceitável

Controle de Acesso, Autorização e Contabilização

Controle de acesso

- O controle de acesso compreende um conjunto de processos para gerenciar todo o ciclo de vida dos acessos dos usuários, internos ou externos, dentro de uma organização. Os controles de acesso são uma combinação de acessos lógicos, relacionados a sistemas de informação e acessos físicos

Tipos de controle de acesso

- Entre alguns tipos de acessos, podemos destacar uma lista com alguns deles
  - Acesso às informações
  - Acesso às aplicações de negócio
  - Acesso a equipamentos de tecnologia da informação
  - Acesso a redes e serviços

Atividades de controle de acesso

- Cadastro, registros, desligamentos e cancelamentos de acesso de usuários
- Registros e controles de perfil de acesso dos usuários
- Gestão de direitos para acesso de usuários avançados, administradores e privilegiados
- Provisionamento de acesso, informações secretas, métodos de autenticação
- Revisão periódica de direitos de acesso a usuários

Autenticação

- A partir da década de 1960, com a criação dos primeiros computadores multiusuários, surgiu a importância e a necessidade de fazer a identificação dos usuários que acessavam os sistemas e as informações. Dessa maneira, também foi necessário separar e filtrar o conteúdo de acesso de cada usuário. Com isso, começavam a surgir os primeiros sistemas de autenticação, que vêm evoluindo até os dias de hoje

Tipos de autenticação

- Autenticação por conhecimento
- Autenticação por propriedade
- Autenticação por característica

Autenticação multifator

- Umas das melhores formas de ajudar a proteger os acessos é habilitar multifatores de autenticação. Em autenticação de sistemas, podemos utilizar: senhas (algo que o usuário conhece), biometria (algo que o usuário é) e *tokens* (algo que o usuário tem)

Autorização

- É de grande valia que o controle de acesso a sistemas e informações esteja alinhado com a norma e o modelo de segurança adotados pela organização, seguindo uma política de segurança da informação. Mesmo que os utilizadores dos sistemas estejam devidamente identificados e autenticados, é necessário ainda verificar as questões de autorização e permissões de acesso

Tipos de autorização

- Autorização de acesso mandatória
- Autorização de acesso discricionária
- Autorização de acesso funcional
- Autorização de acesso reivindicada

Contabilização

- A contabilização é uma forma de monitorar o comportamento dos usuários relacionados aos sistemas, uma maneira de controlar o consumo de recursos computacionais (rede, impressão, armazenamento, entre outros). É muito útil no contexto de gerência de recursos, na cobrança pelos serviços, no planejamento de recursos e na verificação de qual departamento precisa ser ajustado e melhorado

Implementação do *Authentication, Authorization and Accounting* (AAA)

AAA

- O *framework* AAA apresenta algumas maneiras de autenticação a dispositivos e sistemas e faz o controle em relação aos níveis de acesso dos usuários, aos recursos que estão disponíveis, às atribuições, ao que pode ser acessado e executado, além do controle de todas as ações feitas pelo usuário para contabilização e atividades de auditoria

Remote Authentication Dial in User Service (Radius)

- O protocolo de autenticação, autorização e auditoria Radius realiza todos os processos de identificação digital do usuário, autoriza os acessos que esse usuário pode ter e realiza os registros desses acessos. Um servidor com o protocolo Radius consegue dar suporte a uma série de métodos e técnicas de autenticação

Padrão IEEE 802.1X

- O padrão IEEE 802.1X é um protocolo criado para controle de acesso a redes, que provê mecanismos de segurança para uma série de dispositivos (principalmente para redes locais e redes sem fio). Ele fornece meios de autenticação a equipamentos que desejam se conectar a uma determinada rede

Elementos do padrão 802.1X

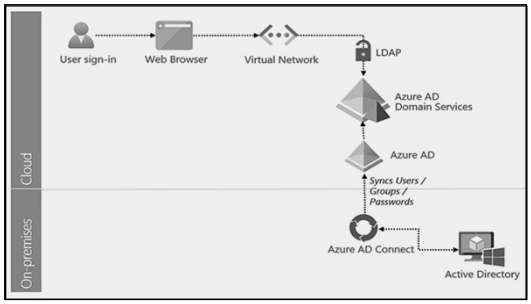
- O usuário ou cliente que precisar ser autenticado no sistema é chamado de "suplicante"
- O servidor atual que efetua o processo de autenticação geralmente usa o protocolo Radius para prover a consulta em uma base de usuários e validar efetivamente a autenticação
- O dispositivo entre os dois primeiros elementos pode ser um ponto de acesso sem fio ou um comutador (*switch*). Este equipamento é chamado de autenticador

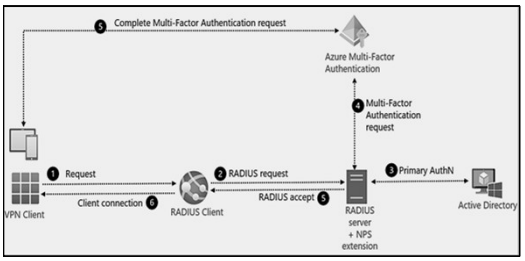
Lightweight Directory Access Protocol (LDAP)

- O LDAP é um protocolo para aplicativos utilizado para atuar com diversos serviços de diretório. Esses serviços fazem armazenamento de conta, usuários, senhas, objetos e vários outros elementos. Esse tipo de protocolo tem funções para compartilhamentos de informações para vários dispositivos de rede

Cenários de uso AAA

- Existem alguns cenários em que os processos de autenticação utilizam os todos os componentes apresentados anteriormente. Um ambiente bem comum encontrado atualmente são as aplicações hospedadas na nuvem. Um exemplo disso é a plataforma Microsoft Azure, que é destinada à execução de aplicativos e serviços, baseada nos conceitos da computação em nuvem





Introdução à Procedimentos de Auditoria

Auditoria

- A auditoria pode ser entendida como um conjunto de procedimentos e técnicas utilizadas para controlar e avaliar um sistema de informação com o intuito de analisar se as atividades executadas pelos sistemas de informação estão em conformidade com os regulamentos de sua organização

Elementos de auditoria de tecnologia da informação (TI)

- Revisão de administração de sistemas
- Avaliação de infraestrutura
- Avaliação de aplicativos e sistemas de informação
- Avaliação de redes
- Avaliação de continuidade de negócios

Auditoria de sistemas

- Fazer uma avaliação dos meios físicos, das tecnologias utilizadas e de como são feitos os processamentos dos dados realizados durante a operação dos processos de negócio
- Analisar os controles empregados e checar sua eficiência e eficácia

- Promover a qualidade e utilidade das informações obtidas
- Avaliar a adequação de todos os sistemas, procedimentos e sistemas de controle que garantam a segurança da tecnologia da informação e seu relacionamento direto com os componentes de TI (*software*, *hardware*, rede, entre outros)

Etapas de auditoria

- Planejamento e preparação
- Execução da auditoria
- Resultados e relatórios de auditoria
- Planos de ação e correção

Gerenciamento de *log*

- Coletar e armazenar volumes massivos de dados
- Processar e normalizar *logs* de diversas fontes
- Armazenar e reter *logs* para longo prazo
- Proteger os dados do registro de eventos contra adulteração ou destruição
- Criar relatórios de *logs*
- Analisar *logs*

Soluções *Security Information and Event Management* (Siem)

- Apresenta um painel de informações com visualização de dados em tempo real
- Possui mecanismos de alertas, de detecção e análise de ameaças
- Tem uma gama completa de relatórios
- Faz correlação entre eventos de diferentes fontes de dados
- Possui inteligência para encontrar e classificar ameaças

Estratégias de auditoria

- Questionários
- Entrevistas
- *Checklists*

Auditoria de segurança física

- Avaliação de sistemas elétricos e energia
- Avaliação de condições ambientais
- Avaliação de controles de acesso físico
- Checagem de equipamentos e planos de emergência
- Monitoramento físicos de instalações
- Avaliação de cabeamento e montagem de equipamentos físicos

Auditoria de segurança lógica

- Avaliação de equipamentos de rede, como servidores, *switches*, roteadores, pontos de acesso, câmeras de segurança, centrais telefônicas, entre outros
- Verificação das camadas de segurança, soluções de antivírus, antispams, *firewalls*, filtros de aplicações e conteúdo, alinhando essa checagem às regras e normas organizacionais e verificando se estão em conformidade

- **Localização de equipamentos ativos não mapeados na infraestrutura, como um modem ou algum tipo de equipamento que não esteja autorizado, dispositivos que não estão devidamente identificados e registrados na rede**