Aula 5

Segurança em Sistemas de Informação

Prof. Douglas Eduardo Basso

Conversa Inicial

- Nessa aula vamos apresentar conceitos de BYOD e as *sandboxes*, as tecnologias emergentes, as multifuncionalidades do celular
- Na sequência vamos trazer a segmentação de rede, os conceitos de rede desmilitarizada (DMZ), as redes falsas e armadilhas criadas pelas *honeypots*, as VLANs, como o isolamento e a segmentação de rede podem ser úteis na gestão, gerência e segurança de rede

- No tópico posterior temos a segurança na computação em nuvem, os modelos e as classificações da computação em nuvem, abordaremos os principais mecanismos de autenticação e autorização para IoT, além dos riscos e ameaças dessas redes e quais são os ataques mais encontrados nesse cenário

BYOD e *Sandbox*

BYOD

- O termo BYOD (*Bring Your Own Device*), ou "traga o seu próprio dispositivo", se refere a propriedade de ativos, onde as organizações deixam em aberto a seus colaboradores a utilizar seus próprios dispositivos para trabalhar na organização

Sandbox

- A *sandbox* é uma plataforma de testes onde é possível inserir aplicações para prototipagem e testes sem impactar o ambiente de produção

- Vantagens das *Sandboxes*
  - Aumento da criatividade
  - Criação de cenários para treinamento
  - Ambiente livre para desenvolvedores
  - Conformidade com regras de utilização
  - Otimização e ganho de tempo
  - Execução de testes sem impacto no ambiente produtivo

Mobilidade

- As tecnologias que estão sento utilizadas nas telecomunicações estão melhorando muito a abrangência de acesso à Internet, com a chegada de novas tecnologias como a 5G a qualidade e velocidade de acesso será ainda maior
- O uso de dispositivos móveis está cada vez maior, contribuindo para o uso desses recursos para a vida profissional e pessoal em sociedade

Tecnologias emergentes

- Tecnologia vestível
- Tecnologia flexível
- Baterias duráveis

Ksyu Deniska /Shutterstock

Mudanças no ambiente corporativo

- A mobilidade corporativa tem ganhado muito espaço a cada dia, está sendo empregada em diversos ramos de negócio, com as novas tecnologias de comunicação, a computação em nuvem e a virtualização é possível que os colaboradores possam acessar qualquer aplicação empresarial de qualquer lugar e momento

Segmentação de Rede

- Gerenciar de maneira adequada as redes de corporativas não é uma tarefa muito simples, a segurança de um ambiente computacional deve ser bem estruturada e organizada, uma boa prática é realizar uma separação dessas redes em segmentos, isso pode ser importante sobre vários aspectos como
  - Gestão, organização, segurança, propriedade, finalidade, localidade e desempenho

DMZ

- Uma DMZ também conhecida como rede de perímetro, é uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a Internet
- Quaisquer dispositivos situação nessa área – isto é, entre a rede confiável (geralmente a rede privada local) e a rede não confiável (geralmente à Internet) – está na zona desmilitarizada

Honeypot

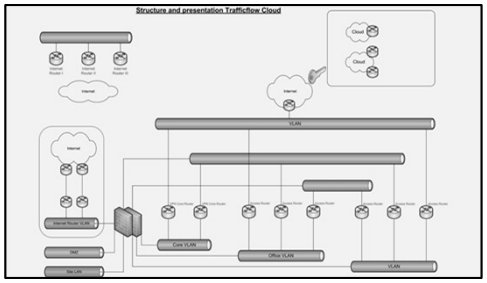
- A *honeypot* é uma ferramenta de coleta de informações que pode ajudar a compreender e entender as várias ameaças existentes ao seu negócio e identificar o surgimento de novas ameaças
- Com o conhecimento obtido de uma *honeypot*, os estudos e esforços de segurança podem ser priorizados e focados

Tipos de *Honeypot*

- Armadilhas de Mensagens
- Armadilha de Banco de Dados
- Armadilhas para Vírus
- Armadilhas para Web

VLAN

- Podemos considerar uma VLAN com sendo basicamente uma rede lógica onde é possível agrupar vários dispositivos seguindo algum tipo de critério como
  - Localização, grupos de trabalhos, por departamentos, pelo tipo de tráfego, pela finalidade, pela propriedade, entre outros
- Um cenário é apresentado para exemplificar o emprego das VLANs



Bildagentur Zoonar Gmbh/Shutterstock

Segurança de Nuvem Privada, Pública e Mista

Computação em nuvem

- A computação em nuvem é o conjunto de recursos virtuais facilmente utilizáveis e acessíveis, tais como *hardware*, *software*, plataformas de desenvolvimento e serviços
- Esses recursos podem ser dinamicamente reconfigurados para se ajustarem a uma carga de trabalho variável, permitindo a otimização do seu uso

- Características da computação em nuvem
  - Autoatendimento sob demanda
  - Amplo acesso a serviços de rede
  - Variedade de recursos
  - Elasticidade rápida
  - Serviços mensuráveis

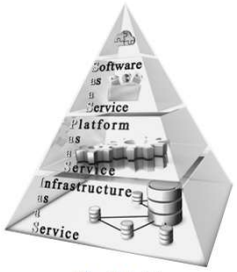
Virtualização

- A virtualização ajudou as empresas a usar os recursos de hardware com mais eficiência
- Ela possibilitou desvincular o ambiente de software e do hardware
- Agora os servidores existem como se fossem um único arquivo, uma máquina virtual
- É possível movê-los de um hardware para o outro, duplicá-los quando desejar e criar uma infraestrutura mais escalonável e flexível

Modelos de computação em nuvem

- Software como Serviço (Software as a Service – SaaS)
- Infraestrutura como Serviço (Infrastructure as a Service – IaaS)
- Plataforma como Serviço (Platform as a Service – PaaS)

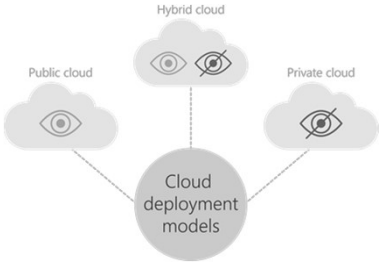
- **Software como Serviço (*Software as a Service* – SaaS)**
- **Infraestrutura como Serviço (*Infrastructure as a Service* – IaaS)**
- **Plataforma como Serviço (*Platform as a Service* – PaaS)**



Yabresse/Shutterstock

Tipos de computação em nuvem

- **Computação em Nuvem Privada (*Private Cloud*)**
- **Computação em Nuvem Pública (*Public Cloud*)**
- **Computação em Nuvem Comunitária (*Community Cloud*)**
- **Computação em Nuvem Híbrida (*Hybrid Cloud*)**



Luna2631/Shutterstock

Segurança na computação em nuvem

- **Será que a nuvem é segura?**
- **Será que as minhas informações estarão seguras?**
- **Quem vai garantir que os provedores de serviços de nuvem estão tratando os meus dados de maneira segura?**

- **Essas são perguntas que recebemos diariamente**
- **Quando se decide usar um provedor de serviços na nuvem ou terceirizar os recursos de TI, questões desse tipo sempre geram preocupação**

- **Segurança Física de Centros de Informática**
  - **Com monitoramento 24 horas por dia, durante toda a semana, com câmeras de segurança internas e externas e um controle de acesso restrito, garantindo a segurança física dos centros de processamento**
- **Restrições Baseadas em Geolocalização**
  - **Faz o filtro em relação aos acessos conforme a escolha do cliente em relação à sua localização geográfica, criando regras de utilização, armazenamento e controle de maneira geral**

- **Criptografia de Dados em Repouso e Transporte**
  - **São recursos utilizados para garantir a confidencialidade dos dados armazenados para que não sejam legíveis por qualquer usuário ou aplicativo não autorizado**

Segurança em Fog Cloud (IoT)

Internet das Coisas

- **A Internet das Coisas (IOT) pode ser considerada "um ecossistema computacional de sensores e recursos interconectados, que permitem a tomada de decisões inteligentes"**

Premissas de Segurança de Dispositivos IoT

- **Recomendações e requisitos de segurança dos fabricantes e fornecedores de IoT**
- **Testar, avaliar e homologar as soluções de IoT em um ambiente segmentado do ambiente de produção**
- **Fazer a desativação de todos os serviços que não são utilizados ou que apresentem vulnerabilidades, alterações de senhas**

- Fazer a inclusão de todos os dispositivos IoT nas atividades de gerenciamento de rede, rotinas de atualizações de software e segurança
- Fazer a separação da rede de dispositivos IoT, criar um ambiente segregado, usar autenticação e emprego de criptografia

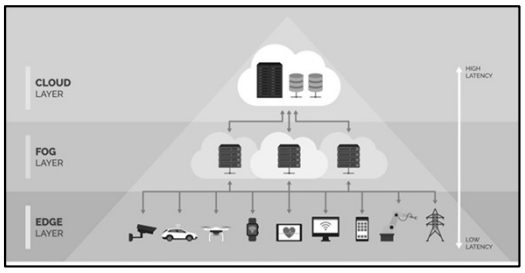
Computação em Neblina (*Fog Computing*)

- É um novo paradigma da computação que consegue trazer as características e todas as funcionalidades da computação em nuvem para mais perto dos seus usuários e aplicações, com a melhoria das redes de comunicações com melhor latência, mais largura de banda, qualidade de serviços, maior disponibilidade, alta confiabilidade e promovendo ampla mobilidade

- Características da computação em neblina
  - Distribuição geográfica e suporte à mobilidade
  - Suporte à aplicação de baixa latência
  - Portabilidade, escalabilidade e interoperabilidade
  - Uso eficiente de largura de banda
  - Suporte à localização e suporte à contexto
  - Disponibilidade e eficiência energética
  - Privacidade e segurança

Computação de Borda (*Edge Computing*)

- A computação de borda (*edge computing*) é a camada de rede que faz a conexão dos dispositivos finais e aos seus usuários, oferecem todos os recursos computacionais, é nessa camada onde acontecem os processamentos locais do usuário e suas fontes de dados
- No próximo slide temos a ilustração de toda a arquitetura apresentada



Elenabsl/Shutterstock

Segurança na computação em neblina

- Técnicas de detecção de intrusão
- Autenticação e autorização
- Segurança de rede e infraestrutura
- Segurança de dados
- Privacidade
- Protocolos seguros e eficientes
- Verificação de localização

Segmentação de Rede para IoT, Autenticação, Registro e Autorização

Segmentação de Rede IOT

- Com o crescimento do tráfego dessas redes, conectividade cada vez maior de dispositivos a aplicações com diferentes funcionalidades em várias localidades, com o progresso da IoT é preciso estabelecer um plano desse segurança digital com conectividade de rede segmentada, com bloqueios a comunicação não seguras ou maliciosas e limitando a disseminação e proliferação de malwares por toda a rede

Autenticação em Redes IoT

- A autenticação deve prover acesso apenas a dispositivos autorizados, elementos não autorizados não podem participar da comunicação e atividades da rede

- As atividades de autenticação devem atender duas propriedades
  - Garantia de autenticação da origem, isso valida ao receptor que a mensagem recebida foi enviada por um dispositivo confiável
  - Garantia de autenticação de dados, que faz a prevenção a violação da integridade e confidencialidade no transporte dos dados

Recursos de segurança de dados

- A segurança de informações armazenadas em banco de dados utiliza alguns recursos que podem ser utilizados para diminuir as probabilidades de ocorrência de incidentes de segurança
  - Acesso de administração
  - Segurança local e física

- Blindagem de servidores
- Criptografia
- Auditoria e gerencia de eventos
- Cópias de segurança

- **Requisitos de Dispositivos IoT**
  - **Finalidade – apresentar proteção a dados pessoais e ativos**
  - **Prioridade – atender a tríade de segurança: integridade, confidencialidade e disponibilidade**
  - **Tolerância a falhas de dispositivos – não comprometer o sistema, sem consequências críticas**

- **Reação a Ameaças – regras de desligamento ou recuperação à ameaça**
- **Suporte Técnico – atualizações periódicas de software, gerenciamento de correções, sem impactar na disponibilidade**
- **Tempo de Vida do Dispositivo – renovação e atualização constante de dispositivos**
- **Locais de utilização – ambientes regulares e severos**

- **Boas Práticas para fabricantes de dispositivos IoT**
  - **Identificação de dispositivo – criar ID físico e lógica de maneira única**
  - **Configurações de dispositivo – gerenciamento e alterações de configurações previstas apenas para administradores e equipe autorizada**
  - **Proteção de dados – blindar os dados transmitidos e armazenados de ataques e acessos indevidos**

- **Acesso lógico a interfaces – filtrar e restringir acessos a recursos, serviços e protocolos das conexões de rede apenas para administradores e equipe autorizada**
- **Atualizações de software – criar e elaborar políticas periódicas de atualizações de software e de segurança**
- **Reportar status de segurança – ter disponível informações de estado de segurança, colaborando também na auditoria de segurança e eventos**

Riscos e ameaças IoT

- **Dentro desse cenário, as principais ameaças e riscos as redes IoT que podem ser destacadas são**
  - **Ataques Físicos**
  - **Ataque de Rede**
  - **Ataques aos Softwares e Aplicativos**
  - **Ataques aos Canais de Comunicação**
  - **Ataque de Análise de Criptografia**

Ataques a Redes IoT

- **São alguns dos ataques mais comuns no mundo IoT, são eles**
  - ***Jamming* e *Tampering***
  - **Desativação e Colisão**
  - **Exaustão, Dessincronização e Repetição**

- ***Hello flood*, *Sinkhole* e *Sybil***
- **Encaminhamento seletivo**
- ***Eavesdropping* e *Flooding***
- ***Malware* e Interseção**
- ***Spoofing and message forging***