Sistema de informações gerencial (SIG) - Prova 2

Aula (11/12)

Introdução

- Pilares da segurança: Proteger dados sensíveis e garantir a :
    - Integridade
        - A informação deve ser precisa e completa
    - Disponibilidade
        - A informação deve estar disponível quando for necessário
    - Confidencialidade
        - O acesso a informação não deve ser concedido a quem não é autorizado
- Ameaça: Ataca esses pilares;
- Não existe sistema 100% seguro, mas com as medidas certa... é possível reduzir e mitigar as chances de invasão.
- Principal ameaça em ambientes digitais:
    - O usuário - Falha humana
- Como evitar falhas humanas?
    - Tratativas nos códigos
    - Mudar ou adequar a cultura da empresa
    - Treinamentos
    - Orientações
    - Dicas e boas práticas

Malwares

- Malware é um termo para qualquer software malicioso, projetado para prejudicar ou explorar dispositivos, serviços ou rede.
- Softwares maliciosos que incluem vírus, worms, trojans, ransomwares e spywares.
- Eles incluem:
    - Anexos de e-mail mal-intencionados
    - Anúncios maliciosos em sites populares (malvertising)
    - Instalações falsas de software
    - Unidades USB infectadas
    - Aplicativos infectados
    - E-mails de phishing
    - Mensagens de texto
- As consequências são graves, e envolvem:
    - Danos a sistemas
    - Roubo de dados
    - Interrupção de operações
    - Extorsão financeira

Phishing

- Tentativas de enganar usuários para que divulguem informações confidenciais, como senhas de aplicativos e acessos a bancos, geralmente por meio de emails falsificados.
- Consequências:
    - Roubo de identidade, acesso não autorizado a sistemas, perdas financeiras imensuráveis.

Ataque DDoS

- Ataques que sobrecarregam sistemas com tráfego excessivo, tornando-os indisponíveis para os usuários legítimos.
- O hacker dispara para um mesmo servidor diversas requisições ao mesmo tempo, podendo ser de diferentes IPs ou VMs.
- O servidor, sobrecarregado, pode apresentar lentidão, instabilidade e até parar de funcionar.
- Consequências:
    - Interrupção de serviços, perda de receita, danos à reputação.

Vulnerabilidades

- A vulnerabilidade na segurança da informação se refere a situações que colocam a empresa em uma posição mais suscetível a ataques e ações mal-intencionadas.
- Vulnerabilidades de rede
    - Falhas da rede que podem expor a empresa à ação de terceiros, como falta de senha ou senha fraca para a rede wi-fi e ausência de um firewall.
- Softwares desatualizados
    - Quando os sistemas e aplicações que rodam nos computadores de um negócio estão desatualizados, eles ficam mais vulneráveis às ameaças.
- Ausência de uma política de segurança da informação bem estruturada
    - Em empresas que não contam com uma sólida política de segurança da informação, os usuários não sabem quais regras e melhores práticas adotar no dia a dia de seus processos para se proteger das ameaças.

Ameaça x Vulnerabilidade

- Ameaças são ações que buscam explorar vulnerabilidades para roubar dados ou prejudicar sistemas e usuários.

Normas de Segurança da Informação

- ISO/IEC 27001 e 27002
    - Fornece diretrizes de melhores práticas para os controles de segurança da informação
    - Foi criada para ajudar as organizações a implementar os controles e processos necessários para proteger as informações
- NIST - Cybersecurity Framework
    - Conjunto de diretrizes para gerenciar e reduzir riscos de cibersegurança
    - Se diferencia por não ser uma norma, mas sim um framework que combina diretrizes em um conjunto
- LGPD
    - Legislação brasileira que regula o tratamento de dados pessoais
    - Estabelece diretrizes para a coleta, processamento, armazenamento e compartilhamento de dados pessoais

Revisão

- Ameaças e Vulnerabilidades;
    - Principais Ameaças:
        - Falhas Humanas,
        - Malwares,
        - Phishing,
        - DDoS;
    - Principais Vulnerabilidades:
        - Softwares desatualizados,
        - Falta de políticas,
        - Vulnerabilidades de rede/infra;

Aula (12/13)

Segurança Física

- Envolve a proteção dos ativos físicos da organização contra ameaças como roubo, vandalismo, desastres naturais ou falhas de hardware
- São exemplos: Cartões de Identificação, Biometria e câmeras de Vigilância e Alarmes.
- A segurança física também envolve medidas específicas de manutenção dos ativos, como o controle de temperatura (ambientes resfriados, com temperatura monitorada), alarmismo contra incêndios, estabilizadores e backups de energia (como geradores e nobreaks) e sistemas de bloqueio para impedir acessos físicos não autorizados.

Segurança Lógica

- Se refere às tecnologias e processos que protegem a integridade e a confidencialidade dos dados em sistemas computacionais.
- Isso inclui o controle de acesso aos dados, as redes e os sistemas de computação. Exemplos:
- Autenticação: senhas, tokens e biometria para confirmação de identidade.
- Autorização: Controle de acesso discricionário (DAC), Baseado em Função (RBAC) e Baseado em Atributos (ABAC).
    - Active Directory (AD)

Ferramentas de Segurança

- Firewall: Ferramenta essencial para proteger redes contra tráfego indesejado ou malicioso (pode ser hardware ou software)
- IDS/IPS: IDS e IPS são ferramentas fundamentais para a detecção e resposta a incidentes de segurança.
    - IDS: Sistema de Detecção de Intrusão - Monitora o tráfego de rede e envia alertas quando atividades suspeitas são detectadas.
    - IPS: Sistema de Prevenção de Intrusão - Bloqueia ativamente as ameaças detectadas, tomando ações para impedir que o ataque cause danos.
- Antivírus e Antimalwares: Softwares que detectam e removem vírus, trojans, malwares...
- Autenticação Multifatorial (MFA): Exige que os usuários forneçam duas ou mais formas de verificação de identidade para acessar sistemas críticos
- Backups: Planos de Recuperação de Desastres - São medidas cruciais para garantir a continuidade dos negócios e a proteção dos dados em situações adversas.
    - Backup Completo: Copia todos os dados, sendo a forma mais simples, mas também a mais demorada.
    - Backup Incremental: Copia apenas as alterações feitas desde o último backup (completo ou incremental), economizando tempo e espaço.
    - Backup Diferencial: Copia todas as mudanças feitas desde o último backup completo.
- Recuperação de Desastres:
    - RPO (Recovery Point Objective):
        - Define quanto tempo de dados a organização está disposta a perder após um incidente.
    - RTO (Recovery Time Objective):
        - Estabelece quanto tempo a organização tem para restaurar seus sistemas e operações.

Aula (14/15)

Infraestrutura de TI

- Servidores, redes, armazenamento de dados, equipamentos de segurança e aplicações que trabalham juntas para garantir o funcionamento da corporação
- Infraestrutura física:
    - refere-se aos recursos tangíveis, como servidores, data centers, dispositivos de rede e sistemas de energia
    - refere-se aos aos componentes digitais, como sistemas operacionais, virtualização, redes e aplicativos

Servidores

- Centralização, Automação e Alta Disponibilidade
- Servidor de Arquivos
- Servidor Web
- Servidor Banco de Dados
- Servidor de E-mail
- O que difere um servidor de uma máquina-estação?
    - Capacidade de processamento

Armazenamento

- Soluções para guardar fisicamente grandes volumes de dados
    - NAS (Network Attached Storage): Synology NAS
        - Para armazenamento compartilhado em rede.
    - SAN (Storage Area Network): EMC Unity
        - Soluções de armazenamento de alto desempenho para grandes volumes de dados
    - SSDs e HDs

Infraestrutura Lógica

- Sistemas Operacionais: Controlam e gerenciam o hardware
    - Linux: (Ubuntu, CentOS)
    - Windows Server: Usado em muitos ambientes corporativos
- Redes: Tratam da organização e configuração de componentes e serviços que permitem a comunicação, o gerenciamento de dados e o funcionamento de uma rede
    - Endereçamento IP e Sub-redes
    - Roteamento e Protocolos de Roteamento
    - DNS (Domain Name System)
- Virtualização: Permite criar versões simuladas (ou virtuais) de recursos computacionais em um único host.
    - VMware, VirtualBox, KVM
- Nuvem: Infraestrutura escalável e sob demanda
    - Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

Existem dois tipos de Infraestrutura de TI

- On-Premise : Infraestrutura local, onde todos os servidores, sistemas e redes estão fisicamente dentro da empresa.
    - Este modelo oferece controle total sobre os recursos, mas exige altos custos iniciais e manutenção contínua.
- Vantagens:
    - Controle total sobre hardware e dados.
    - Maior segurança física e personalização.
    - Custo fixo a longo prazo, sem depender de mensalidades.
- Desvantagens:
    - Alto custo inicial (hardware e manutenção).
    - Escalabilidade limitada e demorada.
    - Manutenção constante e complexidade de atualização.
- Nuvem (Nuvem) : Infraestrutura fornecida como um serviço por terceiros, acessível pela internet.
    - Ele oferece liberdade e escalabilidade, permitindo que as empresas paguem apenas pelo que usam.
- Vantagens:
    - Escalabilidade rápida e flexível conforme demanda.
    - Custos variáveis, pagos conforme uso.
    - Acesso de qualquer lugar, fácil colaboração.
- Desvantagens:
    - Dependência de internet para acesso.
    - Segurança e privacidade dependem do provedor.
    - Custos contínuos podem aumentar com o uso prolongado.

Modelo OSI

- Define uma arquitetura de rede composta por 7 camadas. Cada camada é responsável por um conjunto específico de funções na comunicação de dados.
- Camada Física: Trata da transmissão física dos dados através de meios como cabos, sinais elétricos e ópticos.
- Camada de Enlace de Dados: Garante a entrega correta dos pacotes entre dispositivos na mesma rede local.
- Camada de Rede: Aqui, a principal função é o roteamento dos pacotes entre diferentes redes. O IP (Internet Protocol) opera nesta camada, determinando como os pacotes de dados são endereçados e roteados ao longo das redes.

- Camada de Transporte: Responsável por garantir que os dados cheguem ao destino sem erros e de forma ordenada.
- Camada de Sessão: Estabelece, gerencia e finaliza as sessões de comunicação entre os dispositivos.
- Camada de Apresentação: Cuida da representação dos dados para que sejam compreensíveis pelos sistemas envolvidos.
- Camada de Aplicação (Layer 7): Esta camada é a que mais interage com os usuários finais, fornecendo serviços de rede diretamente para aplicações como navegadores de internet, e-mail, e FTP. Utiliza de protocolos como HTTP/HTTPS, SMTP (para e-mail), FTP e DNS.

Modelo TCP/IP

- Camada de Acesso à Rede: Equivalente à combinação das camadas física e de enlace do OSI. Trata da transmissão dos dados pelo meio físico - cabeamento e entrega correta dos pacotes.
- Camada de Internet: Equivalente à camada de rede no OSI. Cuida do endereçamento e roteamento dos pacotes e utiliza os protocolos de IP e ICMP (para diagnóstico e controle de tráfego).
- Camada de Transporte: Semelhante à camada de transporte do OSI, ela utiliza os protocolos TCP e UDP.
    - O TCP é orientado a conexão e garante entrega confiável e ordenada de pacotes
    - UDP é não orientado à conexão e oferece uma entrega mais rápida, mas sem garantias de confiabilidade.
- Camada de Aplicação: Tem o mesmo princípio da camada de aplicação do OSI.

IP

- O IP é o protocolo fundamental para o roteamento de pacotes de dados na internet. Ele é responsável por garantir que os pacotes sejam entregues aos dispositivos corretos, utilizando endereços IP únicos para identificar dispositivos em uma rede.
    - IPV4 - 32 bits
    - IPV6 - 128 bits

TCP

- O TCP é um protocolo de transporte orientado à conexão, o que significa que ele estabelece uma conexão entre os dispositivos antes de começar a transferir dados.
- Ele garante a entrega correta dos pacotes, detectando erros e pedindo retransmissões quando necessário.
- Handshake:
    - O dispositivo A envia um sinal de SYN para iniciar a comunicação.
    - O dispositivo B responde com um SYN-ACK para confirmar a solicitação.
    - O dispositivo A envia um ACK final para confirmar o recebimento da resposta.

UDP

- Ao contrário do TCP, o UDP é um protocolo de transporte não orientado à conexão. Ele não realiza a negociação entre os dispositivos antes de começar a enviar dados e não garante a entrega dos pacotes ou a ordem de chegada.
- Isso o torna mais rápido, mas menos confiável.
- O UDP é comumente utilizado em aplicações que exigem rapidez e podem tolerar perdas de pacotes.
- São exemplos: streaming de vídeo e áudio, jogos online e VoIP.

HTTP

- O HTTP é um protocolo de aplicação usado na comunicação entre clientes (navegadores) e servidores web. Ele define como os navegadores e servidores trocam informações.
    - HTTP: É usado sem criptografia, o que torna os dados suscetíveis a interceptação e manipulação.
    - HTTPS: A versão segura do HTTP, que utiliza criptografia SSL/TLS para proteger os dados durante a transmissão.

Classificação de Redes

- PAN
    - Rede de pequena escala, usada para conectar dispositivos pessoais como celulares, tables, laptops e dispositivos
        - Distância limitada
        - Bluetooth, infravermelho
- LAN
    - Rede de computadores que cobre uma área geograficamente pequena, como uma casa, escritório ou campus universitário. Geralmente, as LANs são privadas e operam com alta velocidade de transmissão, geralmente usando cabos Ethernet ou Wi-Fi.
        - Distância limitada
        - Casa, escritório, universidade
- MAN
    - Cobre uma área maior que uma LAN, geralmente uma cidade ou uma região metropolitana. Ela é projetada para conectar diversas LANs dentro de uma área geograficamente ampla.
        - Distância abrangente
        - Usada por empresas para conectar diferentes filiais em uma cidade ou região
- WAN
    - Rede que cobre uma vasta área geográfica, como países ou continentes. A internet é a maior WAN do mundo.
        - Distância global

Topologias de Redes

- Topologia em Barramento
    - Todos os dispositivos estão conectados a um único cabo coaxial central (barramento) ou meio de comunicação.
        - Vantagem: Baixo custo de instalação.
        - Desvantagem: Se o cabo central falhar, toda a rede é afetada. A performance também diminui com o aumento de dispositivos.
- Topologia em Estrela
    - Na topologia em Estrela, existe um HUB ou Switch ao centro da rede, que conecta-se por meio de um cabo a cada nó individualmente.
        - Vantagem: Facilidade de gerenciamento e manutenção. Se um dispositivo falhar, os outros continuam funcionando.
        - Desvantagem: Se o ponto central falhar, toda a rede fica inoperante.
- Topologia em Anel
    - Esse tipo de topologia de rede consiste em ligações ponto a ponto, ou seja, são pares de dispositivos que, em seu conjunto, formam um ciclo fechado — como um formato de anel.
    - Assim, a informação é transmitida sob a forma de um pacote de dados que é enviada de maneira rotativa segundo uma direção específica.
        - Vantagem: A comunicação é eficiente, pois os dados circulam apenas em uma direção.
        - Desvantagem: Uma falha em qualquer dispositivo ou conexão pode afetar toda a rede.
- Topologia em Malha (mesh)
    - É feito por meio de uma ligação ponto a ponto entre cada par de computadores da rede.
    - Cada dispositivo está conectado a vários outros dispositivos, criando múltiplos caminhos para a transmissão de dados.
        - Vantagem: Alta redundância e confiabilidade; se um caminho falhar, há outros disponíveis.
        - Desvantagem: Alto custo e complexidade de instalação e manutenção.