RESOLUÇÃO DOS ESTUDOS DE CASO:

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS

1. Introdução

A segurança da informação em ambientes corporativos vai além da implementação de ferramentas tecnológicas. Ela depende de políticas organizacionais claras, infraestrutura de proteção (como firewalls e servidores proxy), bem como da conscientização dos colaboradores. Este trabalho apresenta a análise e resolução de dois estudos de caso abordando falhas e controles relacionados à criptografia, firewalls e proxies, conforme discutido por Whitman e Mattord (2022).

2. Estudo de Caso 1: Criptografia e Firewalls

2.1 Utilização de Criptografia no Servidor Web

O servidor Web da empresa Linen Planet utiliza criptografia do tipo SSL/TLS, conforme indicado pelo ícone de segurança (cadeado) no navegador da intrusa. Essa tecnologia garante:

Confidencialidade: impede que terceiros leiam os dados transmitidos.

Integridade: assegura que os dados não foram alterados durante a transmissão.

Autenticidade: confirma que o cliente está se comunicando com o servidor legítimo.

Apesar disso, a violação da segurança ocorreu por meio de engenharia social e escuta física em ambiente público, evidenciando uma falha de segurança comportamental.

2.2 Medidas de Segurança Recomendadas

Para prevenir esse tipo de incidente, são recomendadas as seguintes medidas:

Autenticação multifator (MFA);

Proibição de compartilhamento de senhas;

Treinamento contínuo em segurança da informação;

Acesso remoto seguro por VPN;

Utilização de senhas temporárias ou tokens;

Monitoramento de acessos e alertas de segurança.

Esse caso ilustra que, mesmo com criptografia e firewalls, falhas humanas continuam sendo grandes ameaças.

3. Estudo de Caso 2: Servidores Proxy e Firewalls em Nível de Aplicação

3.1 Análise da Política de Uso da Web

A política de uso da internet da ATl, embora rígida, é justificada do ponto de vista organizacional. Ela protege os sistemas, controla o uso da largura de banda, previne riscos legais e mantém a produtividade. O uso de proxies permite filtrar conteúdos, controlar acessos e monitorar atividades online de forma eficaz.

3.2 Avaliação da Conduta de Ron

Ron Hall, embora com boas intenções, agiu de maneira imprudente ao violar conscientemente uma política de segurança da empresa. Mesmo sendo um funcionário confiável, ele tentou acessar sites bloqueados repetidamente, o que configura desrespeito às normas internas.

3.3 Ação Recomendada ao Gestor

Andy, supervisor de Ron, deve adotar uma abordagem equilibrada:

Conversar com Ron sobre a importância de seguir políticas de segurança;

Reforçar a confiança depositada no funcionário, sem ignorar a violação;

Apoiar a participação de Ron no curso exigido;

Comunicar ao setor de segurança, caso julgue o ato como não intencional.

Essa abordagem respeita tanto a política da organização quanto o histórico do funcionário.

4. Conclusão

Os estudos de caso demonstram que a segurança da informação é resultado de uma combinação entre tecnologia, políticas organizacionais e comportamento humano.

Ferramentas como firewalls, criptografia e servidores proxy são eficazes, mas a educação e a

cultura de segurança são fundamentais para mitigar riscos.

UC Sistemas Computacionais e Segurança

Exercícios de Revisão

Prof. Calvetti

1) O que é um pentest? Quais são as etapas de um pentest?

R: Pentest é um processo controlado que simula um ataque real a um sistema, rede ou aplicação, com o objetivo de identificar vulnerabilidades que poderiam ser exploradas por cibercriminosos.

Etapas de um Pentest:

Planejamento e Reconhecimento (Recon): definição de escopo, autorização, coleta de informações públicas (passiva e ativa).

Varredura e Enumeração: identificação de portas abertas, serviços em execução, sistemas operacionais.

Ganho de Acesso: exploração das vulnerabilidades encontradas para invadir o sistema.

Manutenção do Acesso: testes para ver se o invasor conseguiria manter o acesso no sistema comprometido.

Limpeza de Rastros: simulação de técnicas usadas por atacantes para apagar evidências.

Relatório: documentação detalhada com vulnerabilidades, impactos e sugestões de correção.

2) Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.

R: 1) Ataque DDoS (Distributed Denial of Service): Consiste em sobrecarregar um servidor ou rede com um grande volume de tráfego gerado por vários dispositivos, tornando o serviço indisponível para usuários legítimos.

2) Ransomware: É um malware que criptografa os dados do sistema da vítima e exige pagamento de resgate. Enquanto os dados estão inacessíveis, o sistema pode se tornar inutilizável, afetando a

disponibilidade.

3) Ataque de Exploração de Recursos: Ataques que abusam de falhas em aplicações ou sistemas para consumir recursos como CPU, memória ou disco, resultando em lentidão extrema ou queda completa do serviço.

3) Leia o fragmento de texto a seguir. Todas as empresas devem observar a legislação local, os seus regulamentos internos e as obrigações contratuais, além dos acordos internacionais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso. (HINTZBERGEN, 2018)

O texto acima se refere a um conceito que pode ser considerado importante quando se trata de segurança da informação. De qual conceito estamos falando (em uma palavra)?

R: Compliance

4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

Função Principal:

Firewall - Controla o tráfego de entrada e saída com base em regras

IDS - Detecta atividades suspeitas ou anômalas

IPS - Detecta e impede ataques em tempo real

Tipo de Ação:

Firewall - Preventiva (bloqueia ou permite)

IDS - Somente monitora (alerta)

IPS - Preventiva (bloqueia)

Local de Atuação:

Firewall - Entre redes (perímetro)

IDS - Após o firewall, na rede

IPS - Junto ao tráfego, inline

5) Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.

R:

1. Use senhas fortes e únicas: Utilize combinações de letras maiúsculas, minúsculas, números e símbolos. Evite palavras comuns ou dados pessoais.

2. Ative a autenticação em dois fatores (2FA): Isso adiciona uma camada extra de proteção mesmo que a senha seja descoberta.

3. Não reutilize senhas: Utilize um gerenciador de senhas para criar e armazenar senhas diferentes para cada serviço.

6) Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique: a) A vulnerabilidade b) A ameaça c) Uma ação defensiva para mitigar a ameaça

R:

a) Vulnerabilidade: A estação de trabalho está com a tela desbloqueada e sem supervisão. Isso representa uma falha de controle de acesso físico e lógico.

b) Ameaça: Alguém não autorizado pode acessar o computador e obter informações confidenciais, instalar malware ou realizar alterações indevidas no sistema.

c) Ação defensiva: Implementar políticas de bloqueio automático de tela após inatividade e conscientização dos usuários sobre a importância de bloquear o terminal ao se ausentar.

7) Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique: a) A vulnerabilidade b) A ameaça c) Uma ação defensiva para mitigar a ameaça

R:

a) Vulnerabilidade: Anotações com senhas coladas no monitor. Isso expõe dados sensíveis a qualquer pessoa que esteja fisicamente próxima.

b) Ameaça: Acesso indevido a contas ou sistemas por pessoas não autorizadas, comprometendo a confidencialidade e integridade das informações.

c) Ação defensiva: Educação e treinamento de usuários sobre boas práticas com senhas, uso de gerenciadores de senhas e proibição de anotações visíveis com informações sensíveis.

8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber a mensagem de maneira que apenas ele possa decifrá-la. Carlos não está preocupado com o sigilo da mensagem, mas deseja ter certeza de que foi mesmo Ana que a enviou. Assuma que todos têm seu par de chaves pública e privada, que todas as chaves públicas são acessíveis. Visando a atender os requisitos de Bob e Carlos, descreva, em termos de uso das chaves:

a) como Ana deverá cifrar a mensagem antes de enviar para Bob;

b) como Bob deverá decifrar a mensagem de Ana corretamente;

c) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

d) como Carlos deverá decifrar a mensagem de Ana corretamente.

R:

a) Para Bob (sigilo): Ana deve cifrar a mensagem com a chave pública de Bob.

b) Bob para decifrar: Bob usa sua chave privada para decifrar a mensagem enviada por Ana.

c) Para Carlos (autenticidade): Ana deve cifrar a mensagem com sua própria chave privada, provando que foi ela quem enviou.

d) Carlos para verificar: Carlos usa a chave pública de Ana para verificar que a mensagem foi realmente enviada por ela.

9) Observe as imagens a seguir: As imagens apresentam informações do certificado digital do site www.bb.com.br. Com base nelas, responda:

9.a) Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.

9.b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.

R:

a) Utilização do certificado:

O site (Banco do Brasil) envia seu certificado digital ao navegador do usuário, que o utiliza para verificar a autenticidade do site.

O navegador usa a chave pública do Banco para estabelecer uma conexão segura (SSL/TLS).

O conteúdo transmitido é criptografado com a chave pública do banco e decifrado com a chave privada do banco.

b) Dois benefícios de segurança:

Autenticidade: Garante que o usuário está se comunicando com o site verdadeiro do Banco do Brasil.

Confidencialidade: Os dados trocados são criptografados, protegendo contra interceptações.

10) Observe a imagem a seguir: De acordo com a norma ISO 27002:2013, "convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares". (ABNT, 2013)

Cite 3 registros importantes da atividade dos usuários que podem registrados para posterior auditoria de segurança.

R:

1. Tentativas de login (bem-sucedidas e fracassadas) - ajuda a identificar acessos não autorizados.

2. Acessos a arquivos sensíveis ou áreas restritas do sistema - controle de quem acessa informações críticas.

3. Alterações em configurações de segurança ou permissões - monitoramento de mudanças que afetam o controle de acesso.

Jhonatan de Lima Alves dos Santos - 824215769