**ESTUDO DO CASO 1 - Marcello Santos**

1. **O firewall e o servidor Web usados pela Linen Planet fornecem serviços de criptografia? Em caso afirmativo, que tipo de proteção estava em vigor?** Sim, ambos oferecem criptografia. O uso do protocolo HTTPS é uma indicação clara de que a comunicação é protegida por SSL/TLS. Essa criptografia assegura que os dados enviados entre o cliente e o servidor sejam confidenciais e não possam ser interceptados por terceiros.
2. **Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro?** Embora o HTTPS garanta a segurança da comunicação, uma vulnerabilidade significativa foi a exposição das credenciais da CTO. O compartilhamento inseguro de senhas em público, mesmo que de maneira verbal, coloca em risco a segurança. Para reforçar a proteção, é importante usar autenticação multifator e adotar uma política rigorosa de controle de credenciais.

**ESTUDO DO CASO 2**

1. **A política da ATI sobre o uso da Web parece dura para você? Por que ou por que não?** A política pode parecer restritiva, mas do ponto de vista da segurança corporativa, é uma medida essencial para proteger a rede interna contra acessos indesejados e garantir o bom uso dos recursos da empresa. Embora restrinja a navegação recreativa, ela tem o objetivo de manter a produtividade e proteger a integridade dos sistemas.
2. **Você acha que Ron foi justificado em suas ações?** Embora Ron tenha agido de boa fé, seu comportamento não justifica a violação das regras estabelecidas pela empresa. As políticas de uso da web são claras, e, independentemente das intenções, ele deveria ter respeitado essas diretrizes.
3. **Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?** Andy deve ser compreensivo, considerando o histórico de Ron. Uma conversa construtiva sobre a importância de seguir as políticas da empresa e a sensibilização sobre as consequências de não respeitá-las pode ser mais eficaz do que uma punição severa. O objetivo deve ser educar e reforçar a cultura de segurança.

**EXERCÍCIOS DE REVISÃO**

1. **O que é um pentest? Quais são as etapas de um pentest?** O pentest é uma simulação de ataque para identificar vulnerabilidades em sistemas. Ele envolve planejamento, reconhecimento, varredura de sistemas, exploração das falhas, manutenção do acesso e elaboração de um relatório técnico com recomendações.
2. **Explique o funcionamento de três ataques de segurança cibernética que podem comprometer diretamente a disponibilidade de sistemas.**

* **DDoS (Distributed Denial of Service):** Sobrecarga de servidores com tráfego excessivo, tornando-os inacessíveis.
* **Ransomware:** Criptografa os dados e exige pagamento para liberar o acesso.
* **Botnets:** Redes de dispositivos comprometidos que podem ser usadas para realizar ataques coordenados, interrompendo serviços.

1. **O texto da questão 3 dos exercícios faz referência a qual conceito importante para a segurança da informação?** O conceito de **conformidade** ou **compliance**, que se refere à adesão às normas legais, políticas internas e obrigações contratuais.
2. **Faça um quadro comparativo resumindo as características dos firewalls, IDS e IPS.**

* **Firewall:** Controla o tráfego entre redes com base em regras.
* **IDS (Sistema de Detecção de Intrusão):** Monitora a rede e detecta atividades suspeitas, mas não bloqueia.
* **IPS (Sistema de Prevenção de Intrusão):** Detecta e impede ataques em tempo real.

1. **Cite pelo menos três conselhos sobre como proteger suas senhas.**

* Use senhas longas e complexas.
* Não reutilize senhas em múltiplos serviços.
* Utilize autenticação em dois fatores sempre que possível.

1. **Ana deseja enviar mensagens criptografadas para Bob e Carlos. Como ela deve proceder com o uso de chaves públicas e privadas?** Para Bob, Ana deve usar a chave pública dele para criptografar a mensagem. Bob usará sua chave privada para decifrar. Para Carlos, Ana usará sua chave privada para assinar a mensagem, e Carlos pode verificar a autenticidade com a chave pública de Ana.
2. **Como são utilizadas as chaves criptográficas do Banco do Brasil, conforme o certificado digital apresentado?** O Banco do Brasil usa sua chave privada para estabelecer conexões seguras, enquanto os usuários utilizam a chave pública para verificar a identidade do site e garantir a segurança da comunicação.
3. **Quais são dois benefícios de segurança proporcionados pelo uso de certificados digitais em transações eletrônicas?**

* **Confidencialidade:** A criptografia assegura que os dados são privados.
* **Autenticidade:** O certificado digital permite validar a identidade do site, evitando fraudes.

1. **Cite três registros importantes da atividade dos usuários que devem ser mantidos para auditoria de segurança.**

* Tentativas de login e logout.
* Acessos a informações sensíveis.
* Alterações em configurações críticas do sistema.