Lista de Revisão - Capítulo 8

Resumo

1 Por que os sistemas de informação são vulneráveis a destruição, erros e uso indevido?
Dados digitais estão vulneráveis a destruição, uso indevido, erro, fraude e falhas de software e hardware. A Internet foi projetada para ser um sistema aberto, por isso deixa os sistemas corporativos internos mais vulneráveis a ações de invasores. Hackers podem desencadear ataques de recusa de serviço (DoS) ou invadir redes corporativas, causando sérios prejuízos aos sistemas. As redes Wi-Fi podem facilmente ser penetradas por invasores com programas sniffer, que obtêm um endereço e, assim, acessam os recursos da rede. Os vírus de computador e worms podem desabilitar sistemas e sites. A natureza dispersa da computação em nuvem dificulta o rastreamento de atividades não autorizadas ou a aplicação de controles a distância. Os softwares também apresentam problemas, pois pode ser impossível eliminar todos os bugs de software e porque as vulnerabilidades dele podem ser exploradas por hackers e softwares mal-intencionados. Por fim, os usuários finais também acabam introduzindo erros.

2 Qual o valor empresarial da segurança e do controle?
Falta de segurança e controles sólidos podem fazer as empresas que dependem de sistemas computacionais para as suas funções empresariais vitais perderem vendas e produtividade. Ativos de informação, tais como registros confidenciais sobre funcionários, segredos comerciais ou planos de negócios, por exemplo, perdem muito de seu valor se forem revelados para pessoas de fora da organização. Além disso, sua revelação expõe a empresa a riscos legais. Novas leis, como a Lei HIPAA, a Lei Sarbanes-Oxley e a Lei Gramm-Leach-Bliley, exigem que as empresas pratiquem uma minuciosa gestão de registros eletrônicos e que adotem rígidos padrões de segurança, privacidade e controle. A possibilidade de ações legais que exijam perícia forense computacional e provas eletrônicas também obrigam as empresas a prestar mais atenção à segurança e à gestão dos registros eletrônicos.

3 Quais são os componentes de uma estrutura organizacional para segurança e controle?
As empresas devem estabelecer um conjunto adequado tanto de controles gerais como de controles de aplicação para seus sistemas de informação. Uma avaliação de risco analisa os ativos de informação, identifica pontos de controle e vulnerabilidades de controle e determina o conjunto de controles com a melhor relação custo-benefício. As empresas também precisam desenvolver uma política de segurança corporativa coerente e planos para dar continuidade às suas operações na hipótese de desastres ou panes. A política de segurança abrange políticas para gestão de identidade e uso aceitável. Uma auditoria de sistemas metódica e abrangente ajuda as organizações a determinar a eficiência da segurança e dos controles adotados em seus sistemas de informação.

4 Quais as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação?
Quando conectados à Internet, firewalls evitam que usuários não autorizados acessem a rede privada. Sistemas de detecção de intrusão monitoram as redes privadas em busca de tráfego de rede suspeito ou tentativas de acessar os sistemas corporativos. Senhas, tokens, smart cards e autenticação biométrica são usados para autenticar usuários de sistemas. Softwares antivírus verificam se há infecções causadas por vírus e worms no sistema de computador e, muitas vezes, eliminam o software mal-intencionado; softwares antispyware, por sua vez, combatem programas spyware danosos e invasivos. A criptografia, isto é, a codificação e o embaralhamento de mensagens são uma tecnologia amplamente utilizada para salvaguardar as transmissões eletrônicas realizadas por redes desprotegidas. Os certificados digitais, combinados com a criptografia de chave pública, oferecem proteção adicional às transações eletrônicas, pois autenticam a identidade do usuário. As empresas podem utilizar sistemas computacionais tolerantes a falhas ou criar ambientes computacionais de alta disponibilidade para garantir que seus sistemas de informação estejam

sempre disponíveis. O uso de métricas de software e testes rigorosos ajuda a melhorar a qualidade e a confiabilidade do software.

Exercícios

- Liste e descreva as ameaças mais comuns aos sistemas de informação contemporâneos.
- Defina malware e descreva as diferenças entre vírus, worm e cavalo de Troia.
- Defina roubo de identidade e phishing e explique por que o roubo de identidade é um problema contemporâneo tão grande.
- Descreva os problemas de segurança e confiabilidade de sistemas criados por empregados.
- Explique como os defeitos de software afetam a confiabilidade e a segurança.
- Explique como a segurança e o controle agregam valor ao negócio.
- Defina controles gerais e descreva cada tipo de controle dessa categoria.
- Defina controles de aplicação e descreva cada tipo de controle dessa categoria.
- Descreva a função da avaliação de risco e explique como ela é conduzida no caso dos sistemas de informação.
- Defina e descreva: política de segurança, política de uso aceitável e gestão de identidade.
- Explique como a auditoria de sistemas de informação promove a segurança e o controle.
- Nomeie e descreva três métodos de autenticação.
- Descreva a função de firewalls, sistemas de detecção de intrusão e software antivírus na promoção da segurança.
- Explique como a criptografia protege as informações.
- Descreva a função dos certificados digitais em uma infraestrutura de chave pública.
- Diferencie plano de recuperação de desastres e plano de continuidade de negócios.