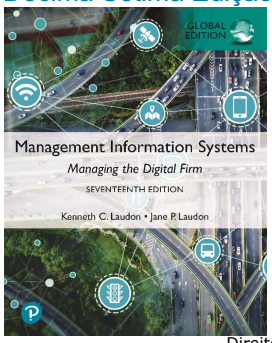
Sistemas de Informação Gerencial: Gerenciando a Empresa Digital

Décima Sétima Edição, Edição Global



Capítulo 8

Protegendo Sistemas de Informação

1

objetivos de aprendizado

8.1 Por que os sistemas de informação são vulneráveis à destruição, ao erro e ao abuso?

8.2 Qual é o valor comercial da segurança e do controle?

8.3 Quais são os componentes de uma estrutura organizacional para segurança e controle?

8.4 Quais são as ferramentas e tecnologias mais importantes para proteger os recursos de informação?

8,5 Como o MIS ajudará minha carreira?

2

Casos de vídeo

- Caso 1: Stuxnet e guerra cibernética
- Caso 2: Ciberespionagem : A Ameaça Chinesa
- Vídeo instrutivo 1: Sony PlayStation hackeado; Dados roubados de 77 milhões de usuários
- Vídeo instrutivo 2: Conheça os hackers: declaração anônima sobre hackers na Sony

3

Ataques cibernéticos na Ásia-Pacífico (1 de 2)

- Problema
  - A tecnologia da informação é difundida
  - Ataques de engenharia social
- Soluções
  - Eduque os clientes sobre práticas de segurança
  - Gerencie violações de dados de forma proativa

4

Ataques cibernéticos na Ásia-Pacífico (1 de 2)

- Processos de negócios robustos precisam ser criados e monitorados
- Demonstra vulnerabilidades em sistemas de tecnologia da informação
- Ilustra algumas das razões pelas quais as organizações precisam prestar atenção especial à segurança do sistema de informação

5

Por que os sistemas são vulneráveis (1 de 2)

- Segurança
  - Políticas, procedimentos e medidas técnicas utilizadas para prevenir acesso não autorizado, alteração, roubo ou danos físicos aos sistemas de informação
- Controles
  - Métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização; exatidão e confiabilidade de seus registros contábeis; e adesão operacional aos padrões de gestão

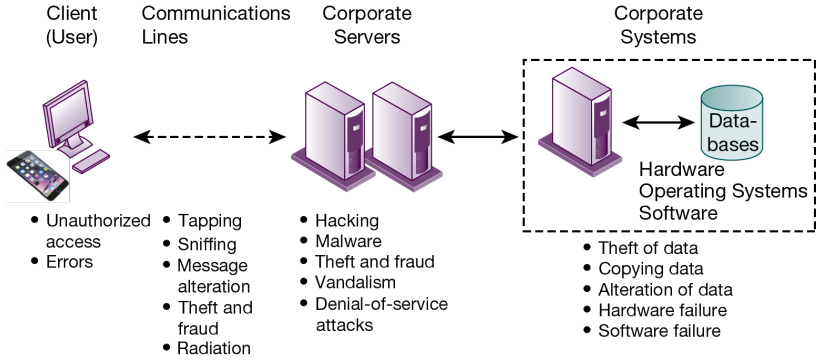
6

Por que os sistemas são vulneráveis (2 de 2)

- Acessibilidade das redes
- Problemas de hardware (avarias, erros de configuração, danos por uso indevido ou crime)
- Problemas de software (erros de programação, erros de instalação, alterações não autorizadas)
- Desastres
- Uso de redes/computadores fora do controle da empresa
- Perda e roubo de dispositivos portáteis

7

Vulnerabilidades Contemporâneas de Segurança



8

Vulnerabilidades da Internet

- Rede aberta a qualquer pessoa; tamanho significa que os abusos podem ter amplo impacto
- Redes corporativas ligadas à Internet mais vulneráveis
- E-mail, mensagens instantâneas e P2P aumentam a vulnerabilidade
  - E-mail: anexos com software malicioso; pode ser usado para transmitir segredos comerciais, dados confidenciais
  - IM: porta dos fundos para uma rede segura
  - P2P: pode transmitir software malicioso, expor dados corporativos

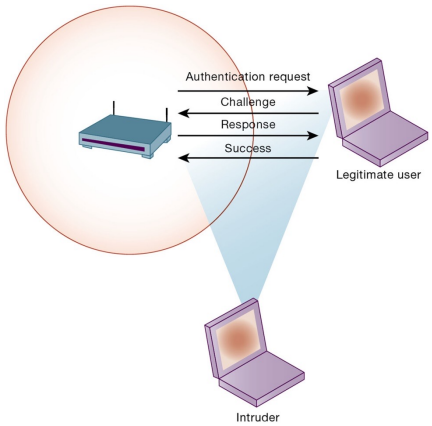
9

Desafios de segurança sem fio

- Redes Bluetooth e Wi-Fi suscetíveis a hackers
  - Bandas de radiofrequência fáceis de digitalizar
  - SSIDs (identificadores de conjunto de serviços)
    - Identifique pontos de acesso, transmita várias vezes, possa ser identificado por programas sniffer
- Condução de guerra
  - Os bisbilhoteiros passam por edifícios e tentam detectar SSID e obter acesso à rede e aos recursos
  - Depois que o ponto de acesso for violado, o invasor poderá obter acesso a unidades e arquivos da rede
- Pontos de acesso não autorizados

10

Fi



11

Software malicioso: vírus, worms, cavalos de Tróia e spyware (1 de 2)

- Malware (software malicioso)
- Vírus
- Vermes
- Worms e vírus transmitidos por
  - Downloads e downloads drive-by
  - E-mail, anexos IM
- Malware em dispositivos móveis
- Malware de redes sociais

12

Software malicioso: vírus, worms, cavalos de Tróia e spyware (2 de 2)

- cavalo de Tróia
- Ataques de injeção SQL
- Ransomware
- Spyware
  - Registradores de chaves
  - Outros tipos
    - Redefinir a página inicial do navegador
    - Redirecionar solicitações de pesquisa
    - Desempenho lento do computador, ocupando memória

13

Hackers e crimes informáticos (1 de 4)

- Hackers vs. biscoitos
- As atividades incluem:
  - Intrusão do sistema
  - Danos no sistema
  - Cibervandalismo
    - Interrupção intencional, desfiguração, destruição de website ou sistema de informação corporativo
- Falsificar e cheirar

14

Hackers e crimes informáticos (2 de 4)

- Ataques de negação de serviço (DoS)
- Ataques distribuídos de negação de serviço (DDoS)
- Redes de bots
- Spam

15

Hackers e crimes informáticos (3 de 4)

- Crime informático definido pelo Departamento de Justiça dos EUA como qualquer violação da lei penal que envolva conhecimento de tecnologia informática para a sua perpetração, investigação ou processo.
- Computador pode ser alvo de crime
- Computador pode ser instrumento de crime

16

Hackers e crimes informáticos (4 de 4)

- Roubo de identidade
  - Phishing
  - Gêmeos malvados
  - Farmacêutica
- Fraude de cliques
- Terrorismo cibernético
- Guerra cibernética

17

Ameaças Internas: Funcionários

- As ameaças à segurança geralmente se originam dentro de uma organização
- Conhecimento interno
- Procedimentos de segurança desleixados
  - Falta de conhecimento do usuário
- Engenharia social
- Tanto os usuários finais quanto os especialistas em sistemas de informação são fontes de risco

18

Sessão interativa: Tecnologia: Capital One: Um Grande Assalto a Banco na Nuvem

- Discussão em aula
  - Quais fatores de gerenciamento, organização e tecnologia foram responsáveis pelo hack do Capitol One?
  - Isso foi um hack interno? Explique sua resposta.
  - Que medidas poderiam ter sido tomadas para evitar o hack do Capital One?
  - As empresas que lidam com dados confidenciais devem usar serviços de computação em nuvem? Explique sua resposta.

19

Vulnerabilidade de software

- Software comercial contém falhas que criam vulnerabilidades de segurança
  - Bugs (defeitos no código do programa)
  - Zero defeitos não podem ser alcançados
  - Falhas podem abrir redes para intrusos
- Vulnerabilidades de dia zero
- Patches e gerenciamento de patches: reparar falhas de software
- Vulnerabilidades no design do microprocessador: Spectre, Meltdown

20

Qual é o valor comercial da segurança e do controle?

- Sistemas informáticos falhados podem levar à perda significativa ou total da função empresarial
- As empresas estão agora mais vulneráveis do que nunca
  - Dados pessoais e financeiros confidenciais
  - Segredos comerciais, novos produtos, estratégias
- Uma violação de segurança pode reduzir o valor de mercado de uma empresa quase imediatamente
- Segurança e controles inadequados também trazem questões de responsabilidade

21

para gerenciamento de registros eletrônicos

- HIPA
  - Regras e procedimentos de segurança médica e privacidade
- Lei Gramm-Leach-Bliley
  - Exige que as instituições financeiras garantam a segurança e a confidencialidade dos dados dos clientes
- Lei Sarbanes-Oxley
  - Impõe responsabilidade às empresas e à sua gestão para salvaguardar a precisão e integridade das informações financeiras que são utilizadas internamente e divulgadas

22

Provas Eletrônicas e Computação Forense

- Evidência eletrônica
  - Evidências de crimes de colarinho branco, muitas vezes em formato digital
  - O controle adequado dos dados pode economizar tempo e dinheiro ao responder a solicitações de descoberta legal
- Perícia computacional
  - Coleta científica, exame, autenticação, preservação e análise de dados de meios de armazenamento de computador para uso como prova em tribunais
  - Recuperação de dados ambientais

23

Controles de Sistemas de Informação

- Pode ser automatizado ou manual
- Controles gerais
  - Governar o design, a segurança e o uso de programas de computador e a segurança de arquivos de dados em geral em toda a organização
  - Controles de software, controles de hardware, controles de operações de computador, controles de segurança de dados, controles de desenvolvimento de sistema, controles administrativos,
- Controles de aplicativos
  - Controles exclusivos para cada aplicativo computadorizado
  - Controles de entrada, controles de processamento

24

Avaliação de risco

- Determina o nível de risco para a empresa se uma atividade ou processo específico não for devidamente controlado
  - Tipos de ameaça
  - Probabilidade de ocorrência durante o ano
  - Perdas potenciais, valor da ameaça
  - Perda anual esperada

25

Tabela 8.5 Avaliação de risco no processamento de pedidos on-line

Exposição	Probabilidade de ocorrência	Faixa de Perda (Média) ($)	Perda Anual Esperada ($)
Falha	30%	US$ 5.000 - US$ 200.000 (US$ 102.500)	US$ 30.750
Desfalque	5%	US$ 1.000 - US$ 50.000 (US$ 25.500)	US$ 1.275
Erro do usuário	98%	US$ 200 - US$ 40.000 (US$ 20.100)	US$ 19.698

26

Política de segurança

- Classifica os riscos da informação, identifica metas de segurança e mecanismos para atingir essas metas
- Impulsiona outras políticas
- Política de uso aceitável (AUP)
  - Define usos aceitáveis dos recursos de informação e equipamentos de computação da empresa
- Gerenciamento de identidade
  - Identificando usuários válidos
  - Controlando o acesso

27

Figura 8.3 Regras de acesso para um sistema pessoal

SECURITY PROFILE 1

User: Personnel Dept. Clerk
Location: Division 1
Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager
Location: Division 1
Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

28

desastres e planejamento de continuidade de negócios

- Planejamento de recuperação de desastres
  - Elabora planos para restauração de serviços interrompidos
- Planejamento de continuidade de negócios
  - Concentra-se na restauração das operações comerciais após um desastre
- Ambos os tipos de planos necessários para identificar os sistemas mais críticos da empresa
  - Análise de impacto nos negócios para determinar o impacto de uma interrupção
  - A gestão deve determinar quais sistemas serão restaurados

29

O papel da auditoria

- Auditoria de sistemas de informação
  - Examina o ambiente geral de segurança da empresa, bem como os controles que regem os sistemas de informação individuais
- Auditorias de segurança
  - Revise tecnologias, procedimentos, documentação, treinamento e pessoal
  - Pode até simular desastre para testar respostas
- Liste e classifique os pontos fracos do controle e a probabilidade de ocorrência
- Avalie o impacto financeiro e organizacional de cada

30

Figura 8.4 Exemplo de lista de deficiências de controle do auditor

Function: Loans Location: Peoria, IL	Prepared by: J. Ericson Date: June 16, 2020		Received by: T. Benson Review date: June 28, 2020	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/20	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/20	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

31

Ferramentas e tecnologias para salvaguardar sistemas de informação (1 de 3)

- Software de gerenciamento de identidade
  - Automatiza o controle de todos os usuários e privilégios
  - Autentica usuários, protegendo identidades, controlando acesso
- Autenticação
  - Sistemas de senha
  - Fichas
  - Cartões inteligentes
  - Autenticação biométrica
  - Autenticação de dois fatores

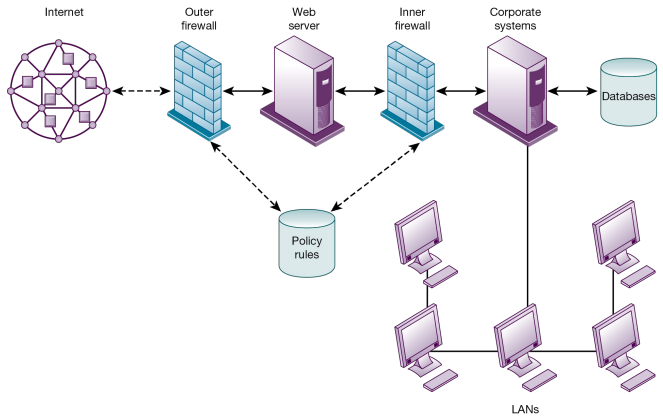
32

Ferramentas e tecnologias para salvaguardar sistemas de informação (2 de 3)

- Firewall
  - Combinação de hardware e software que impede que usuários não autorizados acessem redes privadas
  - Filtragem de pacotes
  - Inspeção estatal
  - Tradução de endereço de rede (NAT)
  - Filtragem de proxy de aplicativo

33

Figura 8.5 Um Firewall Corporativo



34

Ferramentas e tecnologias para salvaguardar sistemas de informação (3 de 3)

- Sistema de detecção de intrusão
  - Monitora pontos de acesso em redes corporativas para detectar e impedir intrusos
- Software antimalware e antispyware
  - Verifica a presença de malware nos computadores e muitas vezes também pode eliminá-lo
  - Requer atualização contínua
- unificados de gerenciamento de ameaças (UTM)

35

Protegendo redes sem fio

- Segurança WEP
  - Chaves de criptografia estáticas são relativamente fáceis de quebrar
  - Melhorado se usado em conjunto com VPN
- Especificação WPA2
  - Substitui WEP por padrões mais rígidos
  - Chaves de criptografia mais longas e em constante mudança
- WPA3é a especificação mais recente, com criptografia ainda mais forte

36

Criptografia e infraestrutura de chave pública (1 de 3)

- Criptografia
  - Transformar texto ou dados em texto cifrado que não pode ser lido por destinatários não intencionais
  - Dois métodos para criptografia em redes
    - Camada de soquetes seguros (SSL) e sucessor Transport Layer Security (TLS)
    - Protocolo Seguro de Transferência de Hipertexto (S- HTTP)

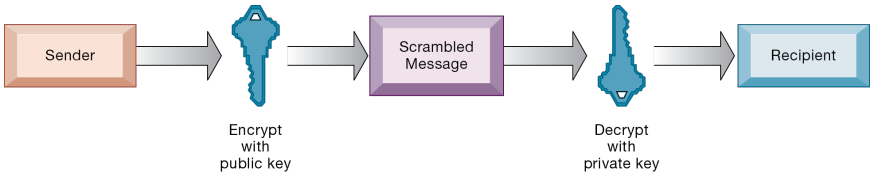
37

Criptografia e infraestrutura de chave pública (2 de 3)

- Dois métodos de criptografia de mensagens
  - Criptografia de chave simétrica
    - Remetente e destinatário usam chave única e compartilhada
  - Criptografia de chave pública
    - Usa duas chaves matematicamente relacionadas: chave pública e chave privada
    - Remetente criptografa mensagem com chave pública do destinatário

38

pública



39

Criptografia e infraestrutura de chave pública (3 de 3)

- Certificado digital
  - Arquivo de dados usado para estabelecer a identidade de usuários e ativos eletrônicos para proteção de transações online
  - Usa um terceiro confiável, autoridade de certificação (CA), para validar a identidade de um usuário
  - CA verifica a identidade do usuário, armazena informações no servidor C A, que gera certificado digital criptografado contendo informações de identificação do proprietário ecópia da chave pública do proprietário
- Infraestrutura de chave pública (PKI)
  - Uso de criptografia de chave pública trabalhando com autoridade de certificação
  - Amplamente utilizado no comércio eletrônico

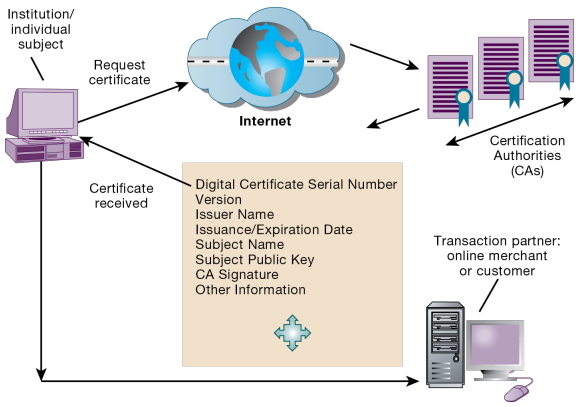
40

Protegendo transações com Blockchain

- Banco de dados de transações seguras
- Criptografia usada para verificar usuários e transações
- Descentralizado
- Os registros não podem ser alterados
- Blockchain tem algumas vulnerabilidades que exigem atenção à segurança e aos controles

41

Figura 8.7 Certificados Digitais



42

sistema

- O processamento de transações online requer 100% de disponibilidade
- Sistemas de computador tolerantes a falhas
  - Contêm componentes redundantes de hardware, software e fonte de alimentação que criam um ambiente que fornece serviço contínuo e ininterrupto
- Terceirização de segurança
  - Provedores de serviços de segurança gerenciados (MSSPs)

43

Alcançando Resiliência Digital

- Trata de como manter e aumentar a resiliência da organização e de seus processos de negócios
- Chama a atenção para questões gerenciais e organizacionais, além da infraestrutura de TI
- Um único elo fraco pode causar uma interrupção se a resiliência não tiver sido explicitamente projetada, medida e testada

44

Sessão interativa: Gestão: PayPal aumenta sua resiliência digital

- Discussão em aula
  - Por que a resiliência digital é tão importante para uma empresa como o PayPal?
  - Como o PayPal se beneficiou ao medir sua resiliência digital? Que questões foram abordadas?
  - Qual é o papel das questões gerenciais e organizacionais para tornar a infraestrutura de TI de uma organização mais resiliente?

45

computação em nuvem e plataforma digital móvel (1 de 2)

- Segurança na nuvem
  - A responsabilidade pela segurança reside na empresa proprietária dos dados
  - As empresas devem garantir que os fornecedores forneçam proteção adequada:
    - Onde os dados são armazenados
    - Atendendo aos requisitos corporativos, leis legais de privacidade
    - Segregação de dados de outros clientes
    - Auditorias e certificações de segurança

46

computação em nuvem e plataforma digital móvel (2 de 2)

- Protegendo plataformas móveis
  - As políticas de segurança devem incluir e cobrir quaisquer requisitos especiais para dispositivos móveis
    - Diretrizes para uso de plataformas e aplicativos
  - Ferramentas de gerenciamento de dispositivos móveis
    - Autorização
    - Registros de inventário
    - Controlar atualizações
    - Bloqueie/apague dispositivos perdidos
    - Criptografia
  - Software para segregar dados corporativos em dispositivos

47

Garantindo a qualidade do software

- Métricas de software: Avaliações objetivas do sistema na forma de medições quantificadas
  - Número de transações
  - Tempo de resposta on-line
  - Cheques de folha de pagamento impressos por hora
  - Bugs conhecidos por cem linhas de código
- Testes precoces e regulares
- Passo a passo: Revisão da especificação ou documento de design por um pequeno grupo de pessoas qualificadas
- Depuração: Processo pelo qual os erros são eliminados

48

carreira?

- A empresa: Supermercados de valor nº 1
- Descrição do cargo: Especialista em suporte de gerenciamento e acesso de identidade, nível básico
- Requisitos de trabalho
- Questões de entrevista
- Dicas do autor

49

direito autoral

Este trabalho é protegido pelas leis de direitos autorais dos Estados Unidos e é fornecido exclusivamente para uso dos instrutores no ensino de seus cursos e na avaliação do aprendizado dos alunos. A divulgação ou venda de qualquer parte desta obra (inclusive na World Wide Web) destruirá a integridade da obra e não é permitida. O trabalho e os materiais dele nunca devem ser disponibilizados aos alunos, exceto pelos instrutores que utilizam o texto que o acompanha em suas aulas. Espera-se que todos os destinatários deste trabalho cumpram estas restrições e honrem os propósitos pedagógicos pretendidos e as necessidades de outros instrutores que dependem destes materiais.

50