Segurança em SI

Objectivos de aprendizagem

- Porque são os sistemas de informação vulneráveis à destruição, erro e abuso?
- Qual é o valor comercial da segurança e do controlo?
- Quais são os componentes de uma *framework* organizacional para a segurança e o controlo?
- Quais são as ferramentas e tecnologias mais importantes para salvaguardar os recursos de informação?

Segurança em SI

- Proteger sistemas através de meios técnicos – firewalls, sistemas de detecção de intrusões, etc. – é necessário, mas não suficiente

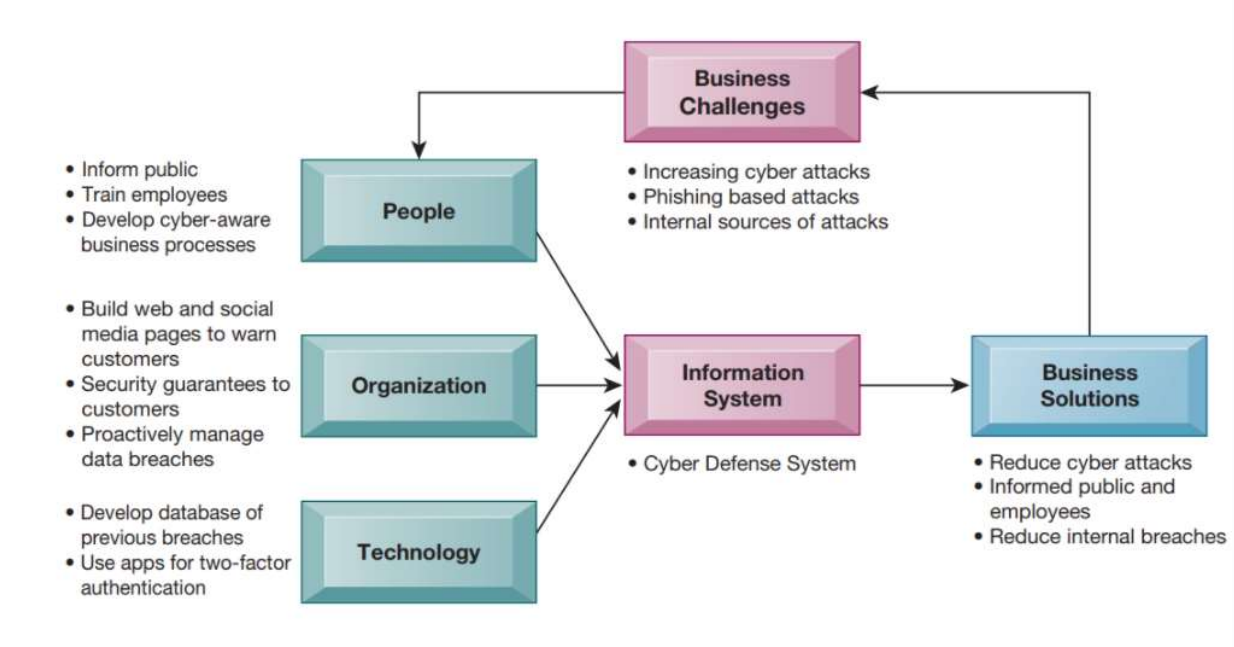


Figura 5.1 A segurança nos sistemas de informação

Vulnerabilidade dos SI à destruição e abuso

- Caso uma organização seja alvo de um ataque informático existe a possibilidade desta nunca mais recuperar
- As organizações devem atribuir um prioridade elevada a:
  - Segurança
    - *Políticas, procedimentos e medidas técnicas utilizadas para impedir o acesso não autorizado, alteração, roubo ou danos físicos aos sistemas de informação*
  - Controlo
    - *Métodos, políticas e procedimentos organizacionais que garantem a segurança dos bens da organização, exactidão e fiabilidade dos seus registos*

Vulnerabilidade dos SI à destruição e abuso

- Porque é que os sistemas são vulneráveis
  - Acessibilidade das redes
  - Problemas de hardware (avarias, erros de configuração, danos causados por uso indevido ou crime)
  - Problemas de software (erros de programação, erros de instalação, alterações não autorizadas)
  - Catástrofes
  - Utilização de redes/computadores fora do controlo da empresa
  - Perda e roubo de dispositivos portáteis

Vulnerabilidade dos SI à destruição e abuso

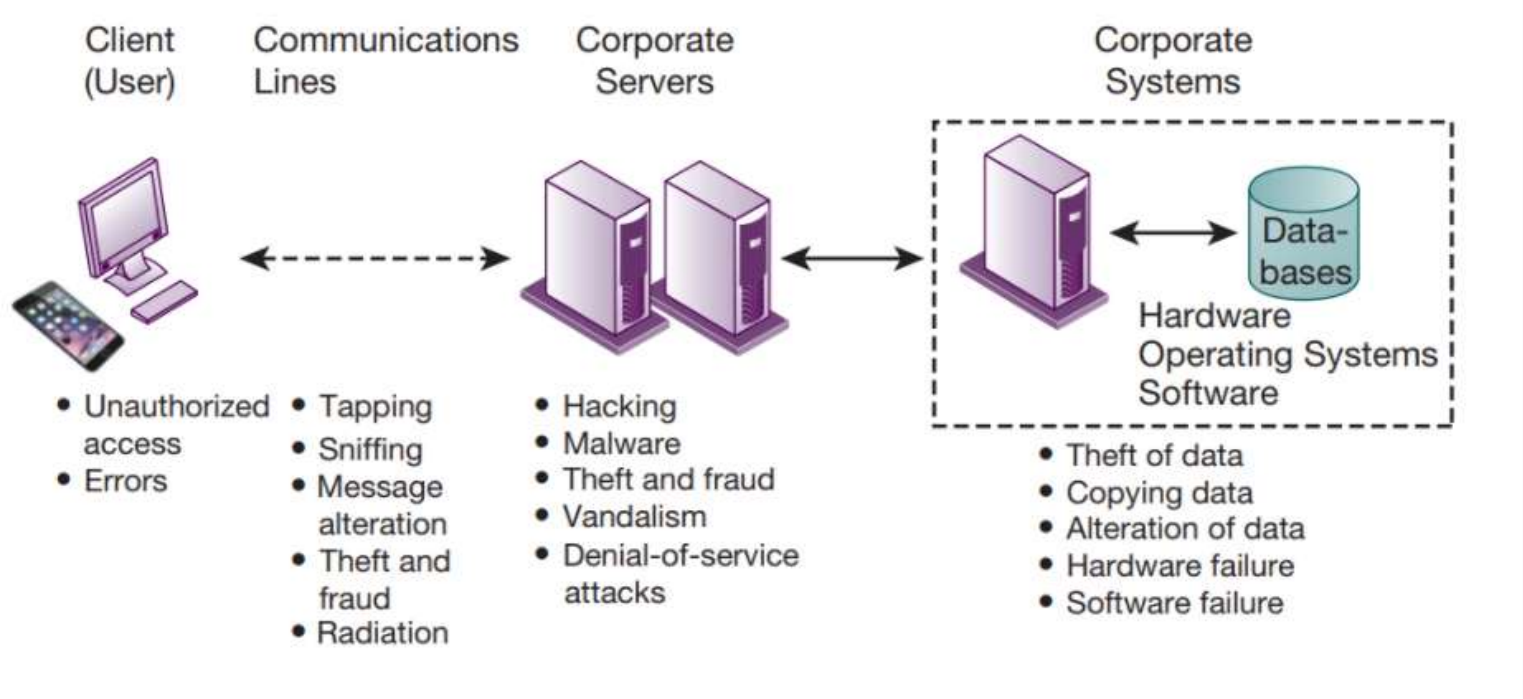


Figura 5.2 A arquitectura de uma aplicação baseada na Web inclui tipicamente um cliente Web, um servidor e sistemas de informação empresariais ligados a bases de dados. Cada um destes componentes apresenta desafios e vulnerabilidades de segurança. Inundações, incêndios, falhas de energia, e outros problemas eléctricos podem causar perturbações em qualquer ponto da rede.

Vulnerabilidade dos SI à destruição e abuso

- Vulnerabilidades da Internet
  - Rede aberta a qualquer pessoa
  - O tamanho da Internet significa que os abusos podem ter um amplo impacto
  - Utilização de endereços fixos da Internet cria alvos fixos
  - VOIP não encriptado
  - E-mail, P2P, IM (Instant Messaging)
    - *Intercepção*
    - *Anexos com software malicioso*
    - *Transmissão de segredos comerciais*

Vulnerabilidade dos SI à destruição e abuso

- Desafios de segurança dos sistemas Wireless
  - Bandas de radiofrequência pouco protegidas
  - Os SSIDs (Service Set Identifiers) que identificam os pontos de acesso de uma rede Wi-Fi são transmitidos múltiplas vezes e podem facilmente ser obtidos por programas intrusivos, como os snifers
  - Em muitas localizações não possuem protecções básicas quanto a ataques

Muitas redes Wi-Fi podem ser facilmente ser acedidas por intrusos utilizando programas sniffer, de modo a obter um endereço de acesso aos recursos de uma rede sem autorização

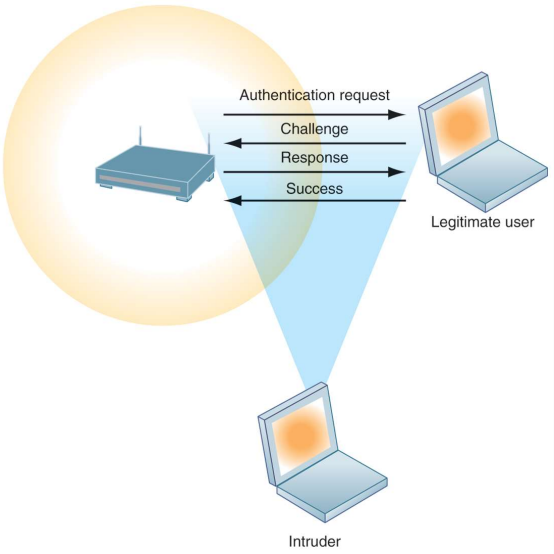


Figura 5.3

Vulnerabilidade dos SI à destruição e abuso

- Malicious software (malware)
  - Vírus
    - *Programa de software que se associa a outros programas de software ou ficheiros de dados com o objectivo de ser executado (poderá ter consequências bastante nefastas)*
  - Worms
    - *Programas de computador independentes que se copiam a si próprios de um computador para outros computadores através de uma rede*

Peritos em segurança informática afirmam que os dispositivos móveis representam agora um maiores riscos de segurança

Blogs, wikis e sites de redes sociais surgiram como novos canais para a utilização malware

IoT introduz desafios de segurança adicionais dos próprios dispositivos ligados à Internet

A Panda Security relatou que em 2017 tinha identificado e neutralizado um total de 75 milhões de ficheiros malware, cerca de 285.000 novas amostras por dia (Panda Security, 2017).

Vulnerabilidade dos SI à destruição e abuso

- Malicious software (malware)
  - Cavalos de Tróia (Trojan horses)
    - *Programa de software que parece ser benigno mas que depois faz algo diferente do esperado*
  - SQL injection attacks
    - *Hackers submetem dados a formulários Web que exploram código desprotegido do site com o objectivo de efectuar consultas ilícitas à base de dados*
  - Spyware
    - *Pequenos programas instalam-se sub-repticiamente em computadores para monitorizar a actividade de navegação na Web dos utilizadores e servir de publicidade*
  - Key loggers
    - *Registar cada toque de tecla no computador para roubar números de série, palavras-passe, lançar ataques pela Internet*
  - Ransomware
    - Impede os utilizadores de aceder ao seu sistema e exige-lhes o pagamento de um resgate para devolver o acesso. As primeiras versões de ransomware foram criadas no final dos anos 80 e o pagamento tinha de ser enviado através de correio postal. Hoje, os autores do ransomware exigem que o pagamento seja enviado através de criptomoeda ou cartão de crédito.

Vulnerabilidade dos SI à destruição e abuso

Figura 5.4 Exemplos de ataques possíveis

Vulnerabilidade dos SI à destruição e abuso

- Hackers e crime informático
  - Hackers (indivíduo que pretende obter acesso não autorizado a um sistema) vs. crackers (tipicamente utilizado para designar um hacker com intenção criminosa)
  - As suas actividades incluem
    - *Intrusão de sistemas*
    - *Roubo de produtos e dados*
    - *Cibervandalismo: perturbação ou ruptura intencional, desfavorecimento, ou mesmo destruição de um website ou do sistema de informação empresarial*

Vulnerabilidade dos SI à destruição e abuso

- Crimes informáticos
  - Spoofing
    - *Por exemplo, falsificar identidades através de endereços de e-mail falsos*
    - *Redireccionar a ligação Web para um endereço diferente do pretendido, com o site destino mascarado*
  - Sniffer
    - *Programa de escuta que monitoriza a informação que viaja através da rede*
    - *Permite aos hackers roubar informação pessoal, tal como e-mail, ficheiros de empresas, relatórios confidenciais, etc.*
    - *Pode ser utilizado de forma legal para detectar problemas na rede*

Vulnerabilidade dos SI à destruição e abuso

- Crimes informáticos (cont.)
  - Denial-of-service attacks (DoS)
    - *Inunda os servidores com milhares de pedidos falsos de modo a gerar o colapso da rede*
    - *Para sites de e-commerce estes ataques podem ser bastante dispendiosos*
  - Distributed Denial-of-service attacks (DDoS)
    - *Utiliza imensos computadores para lançar um DoS*
    - *Botnets*

      Redes de PCs "zombies" infiltrados por bot malware

      90% do spam mundial e 80% do malware é realizado através de botnets

      O botnet Mirai infectou inúmeros dispositivos IoT em Outubro de 2016 e depois usou-os para efectuar um ataque DDoS contra a empresa Dyn, cujos servidores monitorizam e reencaminhou tráfego da Internet

      A rede de bots Mirai sobrecarregou os servidores Dyn, derrubando websites como GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter

      Uma variante da botnet Mirai atacou empresas financeiras em Janeiro de 2018

Vulnerabilidade dos SI à destruição e abuso

- Crime informático
  - Definido como "qualquer violação do direito penal que envolve um conhecimento da tecnologia informática para a sua perpetração, investigação ou acusação“
  - O computador pode ser alvo de crime, por exemplo
    - *Violação da confidencialidade de dados protegidos*
    - *Aceder a um sistema informático sem permissão*
  - O computador pode ser um instrumento de crime, por exemplo
    - *Roubo de segredos comerciais*
    - *Utilização do correio electrónico para ameaças ou assédio*

De acordo com o Estudo Anual do Instituto Ponemon (2017) acerca dos custos associados ao Cibercrime, o custo médio anual da segurança de cibercrime para empresas de referência em sete países diferentes foi de 11,7 milhões de dólares

Vulnerabilidade dos SI à destruição e abuso

- Exemplos de crime informático

COMPUTERS AS TARGETS OF CRIME
Breaching the confidentiality of protected computerized data
Accessing a computer system without authority
Knowingly accessing a protected computer to commit fraud
Intentionally accessing a protected computer and causing damage negligently or deliberately
Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer
Threatening to cause damage to a protected computer
COMPUTERS AS INSTRUMENTS OF CRIME
Theft of trade secrets
Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
Schemes to defraud
Using email or messaging for threats or harassment
Intentionally attempting to intercept electronic communication
Illegally accessing stored electronic communications, including email and voice mail
Transmitting or possessing child pornography by using a computer

Vulnerabilidade dos SI à destruição e abuso

- Roubo de identidade
  - Apropriação de informações pessoais (número de segurança social, dados da carta de condução ou números de cartões de crédito) para se fazer passar por outra pessoa
  - De acordo com o Estudo de Fraude de Identidade da Javelin Strategy & Research (2018), este tipo de fraude afectou 16,7 milhões de consumidores americanos em 2017 que perderam quase 17 mil milhões de dólares por fraude de identidade nesse ano (Javelin, 2018)
- Phishing
  - Criação de sítios Web falsos ou envio de mensagens de correio electrónico que pareçam empresas legítimas para pedir aos utilizadores dados pessoais confidenciais
  - Gémeos malvados
    - *Redes sem fios que fingem oferecer ligações Wi-Fi de confiança à Internet*
  - Pharming
    - *Redirecciona os utilizadores para uma página web falsa, mesmo quando o indivíduo digita o endereço correcto*
    - *De acordo com um estudo do* Ponemon Institute *(2017) o custo médio de uma violação de dados em 419 empresas inquiridas foi, em média, de 3.62 milhões de dólares (Ponemon, 2017).*

Vulnerabilidade dos SI à destruição e abuso

- Click fraud
  - Ocorre quando um indivíduo ou programa de computador imita um utilizador legítimo com intenção de saber mais sobre o anunciante ou fazer uma compra
  - A fraude do clique tornou-se um grave problema no Google e noutros sites que apresentam publicidade *online pay-per-click*
- Ameaças globais
  - Cyberterrorism – unifica dois medos modernos: tecnologia e terromismo

    "The electronic age has now made cyberterrorism possible. A onetime mainstay of science fiction, the doomsday machine, looms as a real danger. The conjunction of technology and terrorism make for an uncertain and frightening future." Walter Laqueur
  - Cyberwarfare - actividade concebida e operacionalizada por estados governamentais com o intuito de prejudicar outro estado, recorrendo a sistemas informáticos para causar danos e perturbações

Vulnerabilidade dos SI à destruição e abuso

- Ameaças internas: colaboradores
  - As ameaças à segurança têm frequentemente origem dentro de uma organização
  - Estudos evidenciam que a falta de conhecimento dos utilizadores é a maior causa de violações da segurança das redes
  - Muitos colaboradores esquecem as suas *passwords* de acesso aos sistemas informáticos ou partilham-nas com os seus colegas de trabalho, o que compromete o sistema
  - Engenharia social
    - *Processo levado a cabo por intrusos que enganam os colaboradores de uma organização para que estes revelem as suas passwords. Estes intrusos fingem ser membros legítimos da empresa que precisa da informação*

Vulnerabilidade dos SI à destruição e abuso

- Vulnerabilidade do software
  - O software comercial contém falhas que criam vulnerabilidades de segurança
    - *Bugs ocultos – a inexistência de bugs é algo impossível de garantir a 100 % (especialmente dada a complexidade dos sistemas actuais)*

      Por exemplo, em Fevereiro de 2017, a Cloudflare, um fornecedor de serviços que ajuda a optimizar o desempenho e a segurança de websites, relatou que tinha corrigido um defeito de software que tinha exposto dados sensíveis durante meses. Os dados incluíam palavras-passe de utilizador, cookies, e outros dados de autenticação.
    - Especialmente problemáticos são as zero-day vulnerabilities, problemas no *software que o seu criador desconhece*
    - *Patches*

      Os vendedores libertam *upgrades* para reparar falhas. No entanto, estes problemas são muitas vezes explorados mais rapidamente do que os patches são libertados e implementados

Valor Empresarial da Segurança e Controlo

- Falhas nos sistemas informáticos podem levar a uma perda parcial, ou total, da função comercial
- As empresas actualmente estão mais vulneráveis do que nunca, possuem dados como:
  - Dados pessoais e financeiros confidenciais (médicos, avaliações de desempenho)
  - Dados organizacionais: segredos comerciais, novos produtos, estratégias
- Alguns peritos acreditam que 40% de todas as empresas não recuperarão de perdas de dados que não sejam reparadas no prazo de três dias
- As empresas devem proteger não só os seus próprios bens de informação mas também os dos clientes, empregados e parceiros comerciais
- A segurança e os controlos inadequados também suscitam questões de responsabilidade

Valor Empresarial da Segurança e Controlo

- Requisitos legais e regulamentares
  - De forma global os regulamentos governamentais estão a forçar as empresas a levar a segurança e o controlo mais a sério
  - As empresas enfrentam novas obrigações legais para a retenção e armazenamento de registos electrónicos, bem como para a protecção da privacidade

Valor Empresarial da Segurança e Controlo

- Provas electrónicas
  - Provas de crimes de colarinho branco assumem muitas vezes o formato digital
    - *Dados sobre computadores, e-mail, mensagens instantâneas, transacções de comércio electrónico*
  - O controlo adequado dos dados pode poupar tempo e dinheiro ao responder a um pedido de descoberta legal
- Investigação forense informática:
  - Recolha científica, exame, autenticação, preservação e análise de dados de suportes informáticos para utilização como prova em tribunal
  - Inclui a recuperação de dados ambientais e ocultos
- O CIO, especialistas em segurança, pessoal de sistemas de informação e assessoria jurídica corporativa devem todos trabalhar em conjunto para ter um plano que possa ser executado se surgir uma necessidade legal

Framework de segurança para SI

- As organizações necessitam de conhecer os seus riscos e os mecanismos que devem ser activivados para proteger os SI (plano de risco)
- Controlos dos sistemas de informação podem ser manuais ou automáticos, com carácter geral e aplicacional
  - Controlos gerais
    - *Criam directivas relativas a design, segurança, utilização de programas informáticos e segurança de ficheiros de dados em toda a infra-estrutura tecnológica da organização*
    - *Devem ser aplicados a todas as aplicações computacionais*
    - *Consistem em combinar hardware, software e procedimentos manuais que permitem criar um ambiente de controlo global*

Framework de segurança para SI

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access and use of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files maintained internally or by an external hosting service are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

Framework de segurança para SI

- Controlos aplicacionais
  - Controlos específicos para uma dada aplicação informática, por exemplo recursos humanos ou processamento de encomendas
  - Incluem procedimentos automatizados e manuais
  - Devem assegurar que apenas os dados autorizados são processados de forma correcta por essa aplicação
  - Podem ser classificados em:
    - *Controlos de entrada*
    - *Controlos de processamento*
    - *Controlos de saída*

Os controlos dos SI não devem ser um pensamento pós implementação. Devem ser incluídos na concepção dos sistemas, considerando as condições de execução e o **comportamento** dos seus utilizadores

Framework de segurança para SI

- Antes de serem gastos recursos em segurança é necessário identificar os activos que precisam de protecção e a extensão da sua vulnerabilidade
- Avaliação dos riscos: Determina o nível de risco para a empresa se um processo específico não for devidamente controlado
- Nem todos os riscos podem ser antecipados e medidos...
- Os gestores de empresas que trabalham com SI devem tentar determinar:
  - O valor dos activos de informação
  - O tipo de ameaça
  - Os pontos de vulnerabilidade
  - A frequência provável de um problema
  - O potencial de danos

Framework de segurança para SI

- Após a identificação dos principais riscos as organizações devem desenvolver uma política de segurança
- Política de segurança
  - Consiste em *guidelines* que identificam riscos de informação, identificando objectivos de segurança aceitáveis e mecanismos para atingir esses objectivos
    - *Quais são os bens de informação mais importantes da empresa?*
    - *Quem gera e controla esta informação na empresa?*
    - *Quais são as políticas de segurança existentes para proteger a informação?*
    - *Que nível de risco está a gestão disposta a aceitar para cada um destes bens?*
    - *Está disposta, por exemplo, a perder dados de crédito de clientes uma vez a cada 10 anos?*
    - *Ou irá construir um sistema de segurança para os dados dos cartões de crédito que possa resistir ao desastre de uma vez em cada cem anos?*

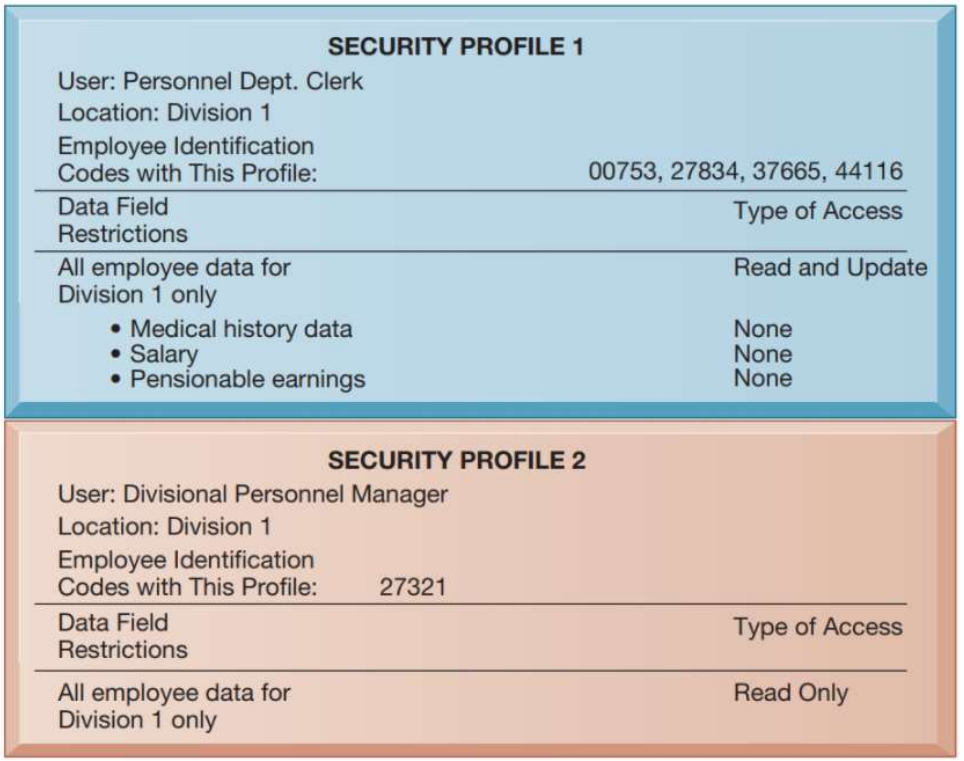
Framework de segurança para SI

- Política de segurança (cont.)
  - Leva a cabo outras políticas
    - *Políticas de utilização e autorização*

      Define as utilizações aceitáveis e níveis de acesso dos utilizadores aos recursos de informação
- Gestão de identidades
  - Processos empresariais e ferramentas que identificam utilizadores válidos do sistema e controlam o seu acesso
    - *Identificam e autorizam diferentes categorias de utilizadores*
    - *Especificam que utilizadores do sistema podem aceder*
    - *Autenticam os utilizadores e protegem as identidades*

Framework de segurança para SI

Estes dois exemplos representam dois perfis de segurança ou padrões de segurança de dados que podem ser encontrados num sistema de pessoal. Dependendo do perfil de segurança, um utilizador teria certas restrições no acesso a vários sistemas, locais ou dados de uma organização.



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

Figura 5.5

Framework de segurança para SI

- Planeamento da recuperação em caso de catástrofe: concebe planos para a restauração de serviços interrompidos
- Planeamento contínuo do negócio: concentra-se no restabelecimento das operações comerciais após a catástrofe
- Para ambos os planos:
  - É necessário identificar os sistemas/processos mais críticos da empresa
  - É imprescindível analisar o impacto do negócio para determinar o impacto de uma interrupção
  - A direcção deve determinar quais os sistemas que devem ser restaurados em primeiro lugar

Framework de segurança para SI

- Auditoria a SI
  - Examina o segurança global da empresa (recorrendo se necessário a *software* automático), abordando todos os SI existentes
  - Revê tecnologias, procedimentos, documentação e formação
  - Pode mesmo simular uma catástrofe para testar a resposta da tecnologia, colaboradores do departamento de SI e outros funcionários
  - Lista e classifica todos os pontos fracos do controlo e estima a probabilidade da sua ocorrência
  - Avalia o impacto financeiro e organizacional de cada ameaça

Framework de segurança para SI

Este gráfico é uma página de amostra de uma lista de pontos fracos de controlo que um auditor pode encontrar num sistema de empréstimo num banco comercial local. Este formulário ajuda os auditores a registar e avaliar os pontos fracos de controlo e mostra os resultados da discussão desses pontos fracos com a direcção, bem como quaisquer medidas correctivas tomadas pela direcção.

Figura 5.6

Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2018**		**Received by: T. Benson** **Review date: June 28, 2018**	
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	5/10/18	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	5/10/18	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		

Protecção dos recursos de informação

- Software de gestão de identidade
  - Automatiza o controlo de todos os utilizadores e privilégios
  - Autentica os utilizadores, protege as identidades, controla o acesso
- Autenticação
  - Sistemas de *passwords*
  - Tokens
  - Smart cards
  - Autenticação biométrica

Protecção dos recursos de informação

- Firewall
  - Combina *hardware* e *software para* impedir o acesso de utilizadores não autorizados a redes privadas
  - Identifica nomes, endereços IP, aplicações e outras características dos tráfego de entrada
  - Contrapõe esta informação com as regras de acesso que o administrador do sistema programou
  - Reside normalmente num computador específico, separado da rede
  - As tecnologias incluem:
    - *Filtragem estática de pacotes*
    - *Tradução de endereços de rede (NAT)*
    - *Filtragem das aplicações que podem aceder à rede interna*

Protecção dos recursos de informação

A firewall é colocada entre a rede privada da empresa e a Internet pública ou outra rede desconfiada para proteger contra o tráfego não autorizado

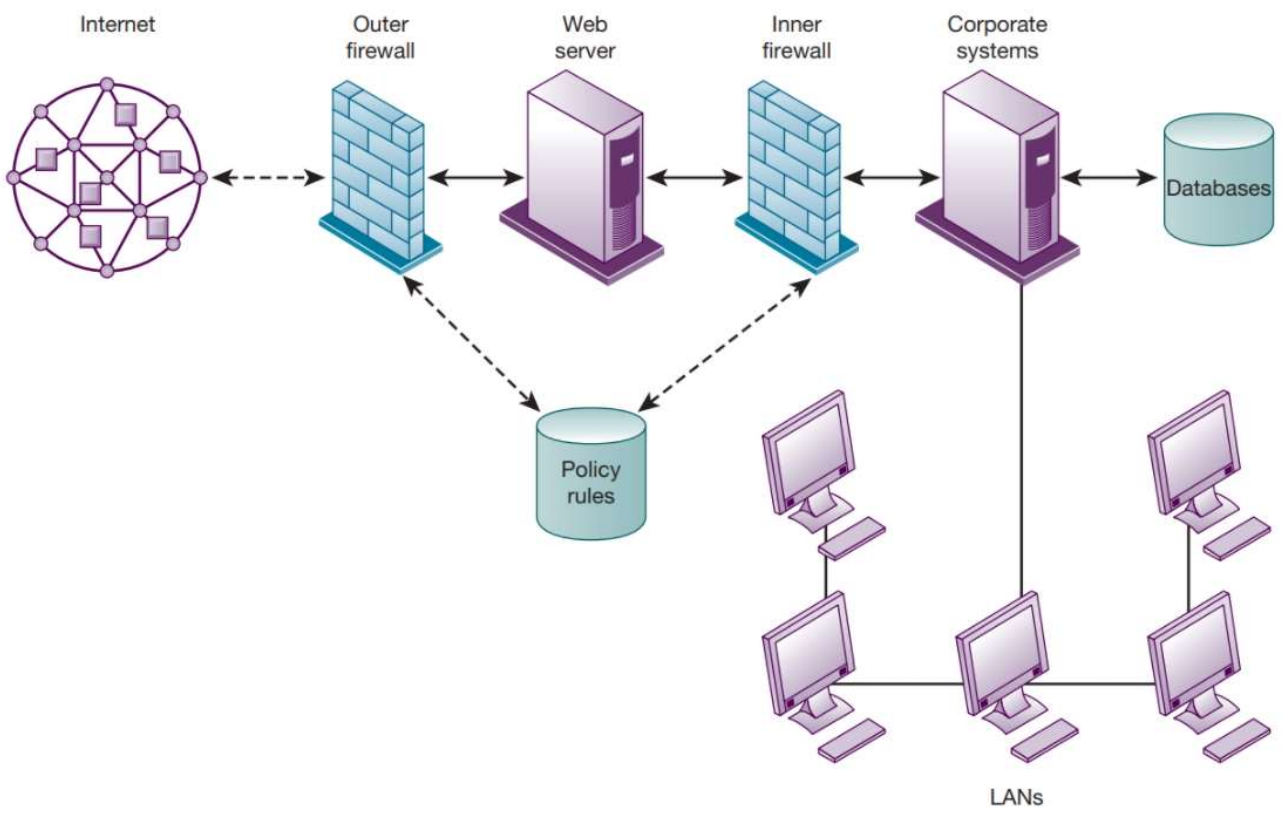


Figura 5.7

Protecção dos recursos de informação

- Sistemas de detecção de intrusões
  - Monitorizam pontos críticos em redes empresariais para detectar e dissuadir intrusos
  - Examina os acontecimentos à medida que acontecem para descobrir os ataques em curso
- Antivírus e software anti-spyware
  - Verifica computadores quanto à presença de *malware* e pode muitas vezes eliminá-lo também
  - Requer actualização contínua
- Unified threat management (UTM) systems – combinam numa única aplicação várias ferramentas de segurança, incluindo firewalls, redes privadas virtuais, sistemas de detecção de instrusões, software anti-spam,…

Protecção dos recursos de informação

- Segurança em redes wireless
  - Standard inicial para Wi-Fi: Wired Equivalent Privacy (WEP) – pouco seguro porque as suas chaves de encriptação são relativamente fáceis de quebrar
    - *A sua segurança pode ser melhorada se usado em conjunto com Virtual Private Network (VPN) para acesso a dados internos*
  - O Wi-Fi Alliance Industry Trade Group finalizou a especificação do 802.111 (também conhecido por Wi-Fi Protected Access 2 ou WPA2) que, ao contrário das chaves de encriptação estáticas utilizadas pelo WEP, utiliza chaves muito mais longas que são alteradas continuamente
  - Em 2018 foi introduzido o WAP3

Protecção dos recursos de informação

- Segurança em redes wireless
  - Encriptação - Transformação de texto ou dados em texto encriptado que não pode ser lido por destinatários não intencionais (recorrendo a uma chave de encriptação)
  - Dois métodos de encriptação:
    - *Secure Sockets Layer (SSL)* e o *seu sucessor Transport Layer Security (TLS)*
    - *Secure Hypertext Transfer Protocol (S-HTTP)*

Protecção dos recursos de informação

- Dois métodos de encriptação
  - Encriptação de chave simétrica
    - *Emissor e receptor utilizam uma chave única, partilhada*
  - Encriptação de chave pública
    - *Utiliza duas chaves matematicamente relacionadas: Chave pública e chave privada*
    - *O remetente encripta a mensagem com a chave pública do destinatário*
    - *Destinatários descodificam a mensagem com a sua chave privada*

Protecção dos recursos de informação

- Encriptação através de chaves públicas

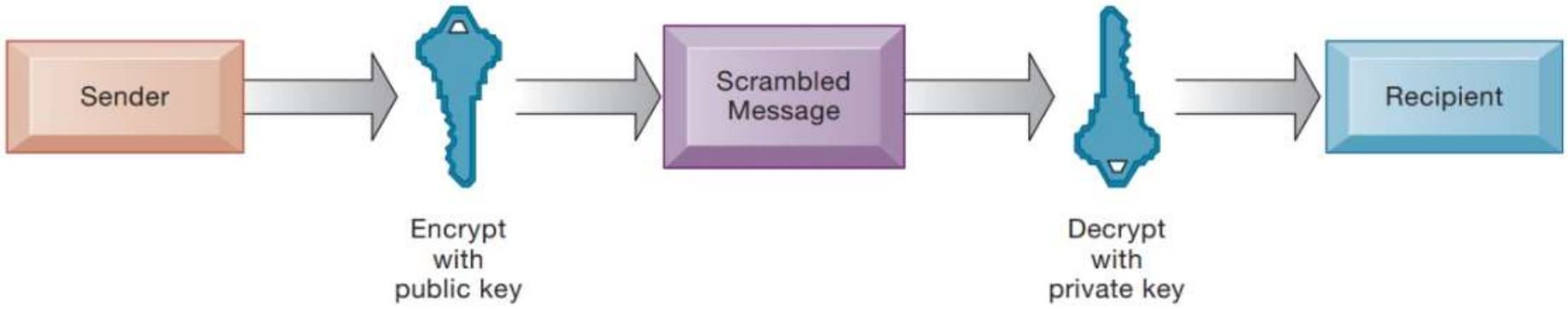


Figura 5.8 Um sistema de encriptação de chave pública pode ser visto como uma série de chaves públicas e privadas que bloqueiam dados quando estes são transmitidos e desbloqueiam dados quando são recebidos. O remetente localiza a chave pública do destinatário num directório e utiliza-a para encriptar uma mensagem. A mensagem é enviada de forma encriptada através da Internet ou de uma rede privada. Quando a mensagem encriptada chega, o destinatário utiliza a sua chave privada para decifrar os dados e ler a mensagem.

Protecção dos recursos de informação

- Certificado digital
  - Ficheiro de dados utilizado para estabelecer a identidade dos utilizadores e dos bens electrónicos para protecção das transacções *online*
  - Utiliza um terceiro de confiança, autoridade de certificação (AC) para validar a identidade de um utilizador
  - AC verifica a identidade do utilizador, armazena informação no servidor da AC, que gera um certificado digital encriptado contendo informação de identificação do proprietário e cópia da chave pública do proprietário
- Infra-estrutura de chave pública (PKI)
  - Utilização de criptografia de chave pública trabalhando com autoridade certificadora
  - Amplamente utilizado no comércio electrónico

Protecção dos recursos de informação

Os certificados digitais ajudam a estabelecer a identidade das pessoas ou dos bens electrónicos. Protegem as transacções online, fornecendo comunicações seguras e encriptadas

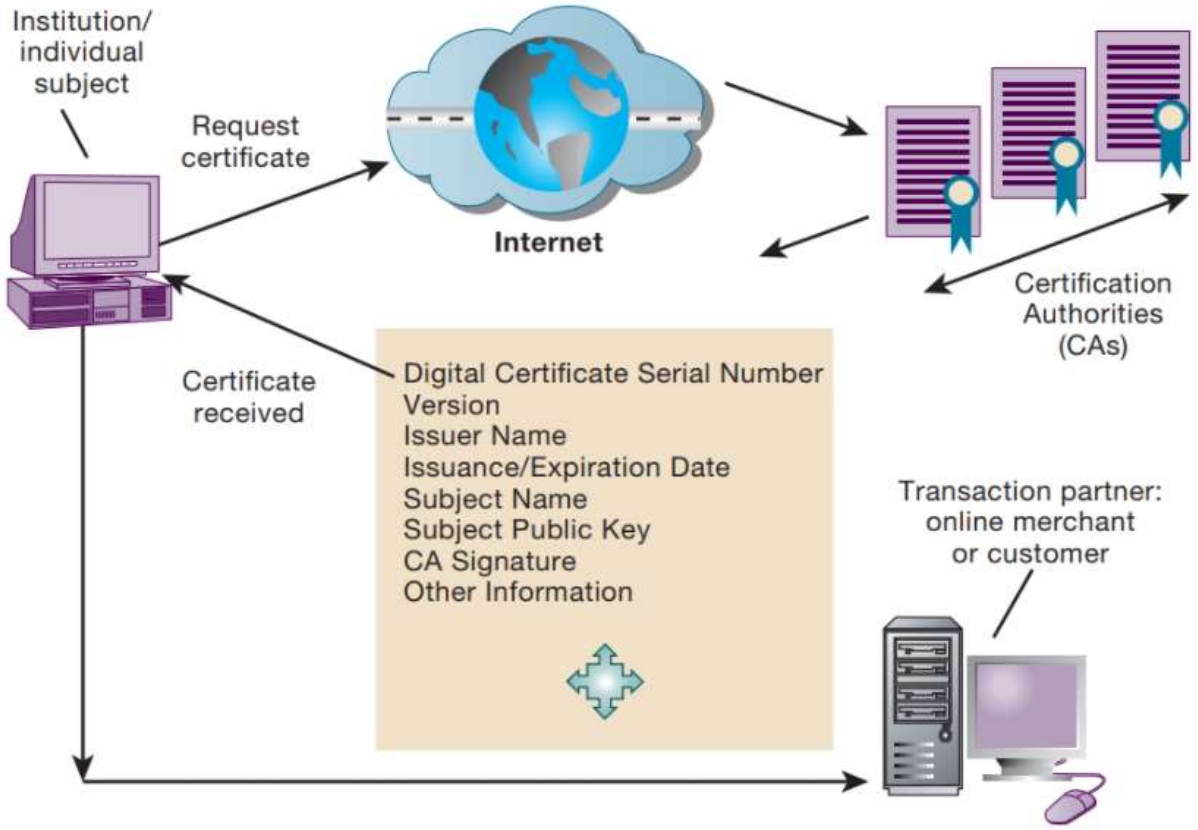


Figura 5.9

Protecção dos recursos de informação

- Transacções seguras com *blockchain*
  - *Blockchain* está a ser utilizado como uma abordagem alternativa a transacções seguras que fomenta a segurança entre diversos actores
  - *Blockchain* é uma sequência de "blocos" digitais que contêm registos de transacções. Cada bloco está ligado aos outros blocos e as cadeias de blocos são continuamente actualizadas e sincronizadas
  - Esta dependência dificulta a adulteração de um único registo porque seria necessário alterar o bloco que contém esse registo bem como os que estão ligados a ele para evitar a sua detecção
  - A segurança num *blockchain* é assegurada através criptografia, uma vez que todas as transacções são encriptadas

Protecção dos recursos de informação

- Transacções seguras com *blockchain*
  - Os participantes da rede blockchain têm as suas próprias chaves privadas que são atribuídas às transacções que criam e actuam como assinatura digital pessoal
  - Se um registo for alterado, a assinatura torna-se inválida, e a rede da cadeia de bloqueios saberá imediatamente que algo está errado
  - Como as cadeias de *blockchain* não são mantidas num local central, não têm um único ponto de falha e não podem ser alteradas a partir de um único computador.
  - A tecnologia de *blockchain* é especialmente adequada para ambientes com elevados requisitos de segurança e actores mutuamente desconhecidos

Protecção dos recursos de informação

- Assegurar a disponibilidade do sistema
  - O processamento de transacções *online* requer 100% de disponibilidade, sem tempo de paragem
- Sistemas informáticos tolerantes a falhas
  - Para disponibilidade contínua, por exemplo, mercados bolsistas
  - Contêm componentes redundantes de *hardware*, *software* e fornecimento de energia que criam um ambiente que fornece um serviço contínuo e ininterrupto
- Computação de alta disponibilidade
  - Ajuda a recuperar rapidamente da queda
  - Minimiza, não elimina o tempo de paragem

Protecção dos recursos de informação

- Controlo do tráfego na rede: inspecção do tipo de pacotes em utilização
- *Outsourcing* para questões de segurança
- Segurança na *cloud*
- Segurança em plataformas móveis: as empresas devem garantir que as suas políticas de segurança englobam aspectos relacionados com a utilização de dispositivos móveis

Protecção dos recursos de informação

- Assegurar a qualidade do software
  - Métricas de *software*: Avaliações objectivas do sistema sob a forma de medições quantificadas
    - *Número de transacções*
    - *Tempo de resposta online*
    - *Impressos de pagamento impressos por hora*
    - *Bugs conhecidos por cem linhas de código*
  - Testes iniciais e regulares
  - Walkthrough: é uma forma de revisão software "em que um designer ou programador lidera membros da equipa de desenvolvimento através de um produto de software, e os participantes fazem perguntas e comentários sobre possíveis erros, violação das normas de desenvolvimento".
  - Debugging: Processo através do qual os erros são eliminados

Referências

- Ken Laudon, Jane P. Laudon, Management Information Systems: Managing the Digital Firm, Prentice Hall, 2020