Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 1

Introdução

Em segurança de sistemas computacionais, podem-se considerar três grandes áreas de atividade, todas relevantes e com as suas especificidades:

- defesa contra catástrofes físicas
- defesa contra faltas / falhas previsíveis
- defesa contra atividades não autorizadas

Defesa contra catástrofes físicas

Conseguir que um sistema computacional, ou o serviço que esse sistema presta, consiga sobreviver a catástrofes onde existam consequências a nível físico.

Catástrofes ambientais	Tremores de terra, incêndios, inundações, quedas de raios, tempestades magnéticas
Catástrofes políticas	Ataques terroristas, motins
Catástrofes materiais	Degradação irreparável ou perda ou roubo de equipamentos computacionais, como: discos magnéticos, computadores portáteis

Todas estas catástrofes são potenciais causas de dano físico irreparável de equipamentos informáticos e potenciais causas de perda irreparável de informação armazenada.
Para que a sobrevivência seja assegurada, pode-se usar hardware com redundância ou equipamentos redundantes com informação replicada. Isto permite que o sistema afetado continue a prestar o serviço esperado com uma perturbação que será determinada apenas pelo tempo que levarem a entrar em funcionamento efetivo os sistemas alternativos não afetados.

Solução: realização periódica de cópias de salvaguarda (backup)
prevenção realista: para catástrofes mais prováveis
replicação da informação e dos recursos computacionais

Defesa contra faltas ou falhas previsíveis

A defesa contra falhas previsíveis visa sobretudo minimizar o impacto de problemas que ocorrem com uma frequência maior, mas cujo impacto global é normalmente menor. Pode-se considerar:

Falha	Solução
Falta de energia • Quebra no fornecimento de energia elétrica	Sistemas de alimentação alternativos (baterias, geradores a combustível)
Falha dos sistemas: • Bloqueio na execução de aplicações ou sistemas operativos (blue-screen)	Sistemas transacionais (garante a transformação da informação guardada se faz de forma coerente através do agrupamento de conjuntos de microalterações em macroalterações atómicas (ex: transferências bancarias))
Falhas de comunicação • Falhas temporárias de conectividade em troços de rede	Encaminhamento alternativo (em caso de falha de um dos caminhos, pode-se usar outros, garantindo que, mais tarde ou mais cedo, a informação consegue chegar ao destino pretendido).

Defesa contra atividades não autorizadas

Defesa de sistemas computacionais face a iniciativas tomadas por indivíduos contra o funcionamento normal dos primeiros. Neste caso o desastre não é simplesmente fruto de circunstâncias que podem ocorrer com um dada probabilidade, mas sim fruto da atividades deliberadas que visam a corrupção ou subversão de sistemas computacionais. As atividades não autorizadas podem ter origem em sujeitos que pertencem à organização detentora do sistema computacional que se quer proteger ou que não pertençam a ela. Os primeiros são sempre os mais difíceis de contrariar, uma vez que possuem habitualmente privilégios acrescidos, em relação aos segundos, que podem usar para iniciar atividades não autorizadas.

- ***Tipos de atividades ilícitas***
  - Acesso a informação
  - Alteração de informação
  - Utilização de recursos (CPU, memória, impressora, rede, etc…)
  - Impedimento de prestação de serviço (Denial of Service - DoS)
  - Vandalismo (interferência com o normal funcionamento do sistema sem qualquer benefício para o sujeito causador)

Complexidade do problema

Os sistemas computacionais unidos por redes (Internet), são cada vez mais explorados para guardar e manipular informação usada no dia-a-dia das pessoas e das organizações. A segurança nos sistemas computacionais são um problema técnico, porque a multiplicidade de arquiteturas de hardware, sistemas operativos e suas versões, protocolos aplicacionais e requisitos aplicacionais fazem com que a definição e implantação de políticas de segurança em sistemas distribuídos ligados à Internet seja difícil, quer de pôr em prática quer de manter.

A Internet permite um acesso rápido a um número elevado de máquinas e redes, o que torna extremamente eficazes todos os ataques que exploram vulnerabilidades de forma automatizada em todo o espaço de endereçamento da Internet.

Os computadores podem fazer muito estrago em pouco tempo	**Existem cada vez mais pontos fracos**	**As redes permitem:**	**Regra geral os utentes são incautos**
- Gerem muita informação - Processam e comunicam rapidamente	- Porque os sistemas são cada vez mais complexos - Porque o time-to-market é cada vez mais reduzido	- Ataques “anónimos” a partir de qualquer lado - Propagação automática de ciberpragas -A existência e uso de programas e máquinas hostis	- Porque não estão cientes dos problemas e soluções - Porque não se preocupam ou arriscam

Atitudes realistas

Costuma-se dizer que não existe segurança a 100%, portanto existirão sempre vulnerabilidades, ataques capazes de as explorar, pessoas dispostas a efetuar tais ataques.

Proteção a 100% é impossível	**A segurança é dispendiosa**	**Proteção, valor e punição**
- Mau equilibrio custo-eficácia no retorno do investimento. Cara porque exige pessoas com muito boa formação em tecnologias de segurança e em equipamentos - Problema: Calcular custos e eficácia	- Em material e pessoas - Dispor apenas do necessário	- Proteção suficiente boa para impedir ataques frequentes - Interferir com o trabalho diário menos do que os danos causados por atacantes - Polícia e tribunais para identificar e punir os atacantes

Segurança: Léxico

Vulnerabilidades, ataques, riscos e defesas

Uma vulnerabilidade é uma característica de um sistema que o torna sensível a certos ataques. Um ataque é um conjunto de passos executados no âmbito da exploração de vulnerabilidades e que permite concretizar uma ação ilícita.

Um risco, ou uma ameaça, é o dano que pode resultar da execução bem-sucedida de um ataque. A defesa consiste no conjunto de políticas e mecanismos desenhados, concretizados e implantados para:

- diminuir as vulnerabilidades de um sistema
- detetar e contrariar/anular ataques passados ou atuais
- minimizar os riscos de ataques bem-sucedidos

⇨ defesa correta

Resumo de Palavras

• **Vulnerabilidade:**
- Característica de um sistema que o torna sensível a ataques
- Na conceção/ no desenvolvimento/ na instalação

• **Ataque**
- Conjunto de passos que levam à execução de uma ou mais atividades ilícitas (normalmente explorando vulnerabilidades)

• **Risco/Ameaça**
- Possibilidade de dano resultante de um ataque
- Dano material ou imaterial

• **Defesa**
-Conjunto de políticas e mecanismos de segurança que visam:
  -Diminuir as vulnerabilidades de um sistema
  -Detetar o mais rápido possível ataques passados ou atuais
  -Diminuir os riscos de um sistema

Resumo dos Riscos

• **Informação, Tempo e Dinheiro**
- Eliminação ou alteraçõess de informaçõess

• **Confidencialidade**
- Acesso não autorizado a informação

• **Privacidade**
- Recolha de dados de índole privada

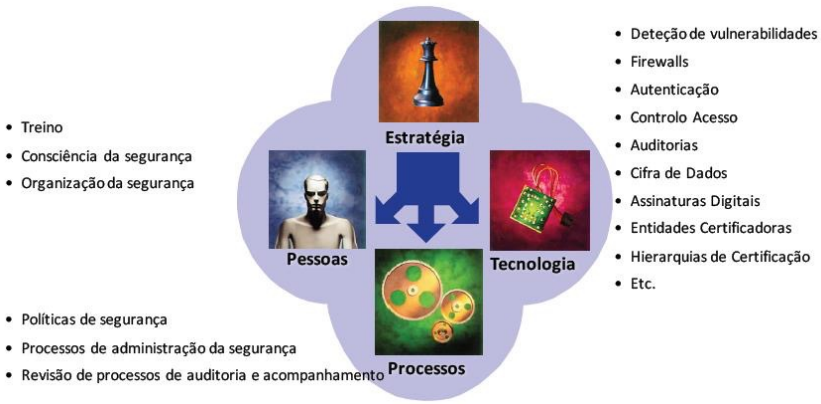
• **Disponibilidade de recursos**
- Rutura de sistemas informáticos

• **Personificação**
- De pessoas ou serviços
- Uso abusivo de sistemas alheios privilegiados

Fontes de vulnerabilidades

• Aplicações com bugs ou hostis
• Utilizadores
• Má Administração
  - Os sistemas são cada vez mais complexos
  - As configurações por omissão nem sempre são as melhores
  - Medidas restritivas de base vs flexibilidade de operação
• Comunicações sobre redes não controladas
  - Geridas por terceiros independentes das fontes de comunicação.

Dimensões a considerar



Políticas de Segurança

As políticas de segurança definem fundamentalmente requisitos de segurança que devem ser respeitados para garantir um determinado resultado.

- Definem o poder/privilégio dos sujeitos
  - Principio do privilégio mínimo
  - Hardening
- Definem procedimentos de segurança
  - Quem deve fazer o quê e em que circunstâncias
- Definem os requisitos de segurança de um domínio
  - Níveis de segurança
  - Autorização necessária (e respetivos requisitos mínimos de autenticação satisfatória)
- Definem estratégias de defesa táticas de contra-ataque
  - Arquitetura defensiva
  - Monitorização de atividades criticas ou de indícios de ataques
  - Reação a ataques ou situações anormais
- Definem o universo de atividades lícitas ou ilícitas
  - Tudo o que não é negado é permitido
  - Tudo o que não é permitido é negado

Mecanismos de segurança

As políticas de segurança são colocadas em prática recorrendo a mecanismos de segurança. Os mecanismos de segurança são a forma prática como as políticas são aplicadas em cenários concretos. Normalmente uma política de segurança pode ser aplicada de diversas formas.

- **Os mecanismos servem para implantação das políticas**
  - As políticas definem o que precisa ser feito
  - Os mecanismos servem para o fazer

- **Mecanismos de segurança genéricos**
  - Confinamento: criam barreiras à difusão de atividades para além de barreiras de segurança.
  - Autenticação
  - Controlo de acesso: permite aferir se um dado sujeito pode ou não realizar uma terminada ação sobre um determinado objeto.
  - Execução privilegiada: estes mecanismos destinam-se a conceber privilégios acrescidos a aplicações especiais que sejam executadas por utentes que normalmente não usufruem desses privilégios.
  - Filtragem: servem para realizar certas formas de confinamento ou controlo de acesso, ou seja, servem para identificar atividades não necessárias ou autorizadas e evitar que as mesmas sejam levadas a efeito.
  - Registo (logging): produzem relatórios mais ou menos exaustivos/pormenorizados de atividades solicitadas ou realizadas.
  - Inspeção: são mecanismos que estão de forma permanente a observar o sistema, de modo a detetar alguma atividade não esperadas, legal ou ilícita.
  - Auditoria: são normalmente mecanismos de inspeção e análise de registos que permitem tirar conclusões após ter acontecido algo de inesperado.
  - Algoritmos criptográficos e afins: mecanismo insubstituível para proteger informação que possa ser fisicamente devassada. Este apenas permite concretizar cifras mais complexas e sofisticadas e agilização da aplicação a conteúdos formados por blocos de bits.
  - Protocolos criptográficos: são trocas ordenadas de dados entre entidades em que parte ou a totalidade dos dados úteis trocados são cifrados.

Segurança em sistemas distribuídos

A defesa dos sistemas computacionais é uma tarefa complexa e árdua, devem ser atribuídas prioridades máximas a técnicas de defesa de perímetro que criem uma primeira barreira aos potenciais atacantes.

Numa primeira fase de concepção de segurança de um sistema distribuído, é preciso subdividir o mesmo em subgrupos de redes e máquinas e enquadrar esses subgrupos de redes e máquinas em domínios de segurança, definindo bem que sujeitos e em que circunstancias os mesmos podem ter acesso a cada perímetro de segurança, tanto para efeitos de administração como para fins de exploração. Deve ainda ser definido o conjunto de atividades autorizadas e proibidas, quer explicita quer implicitamente. Entre cada domínio de segurança, deverá haver um número mínimo de pontos de contacto que deverão ser estabelecidos por pontes de segurança.

Uma ponte de segurança é uma infra-estrutura intrinsecamente segura por definição e que controla, monitoriza e limita as interações entre domínios de segurança, de forma a evitar interações ilegais ou inesperadas entre sujeitos, aplicações ou máquinas operando em domínios de segurança distintos. ⇨ firewall

Políticas em Sistemas Distribuídos

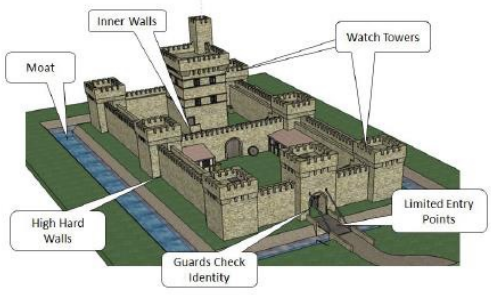
Abrangência de várias máquinas e redes

- Domínios de segurança
  - Definição do conjunto de máquinas e redes do domínio
  - Definição do universo de utentes válidos
  - Definição do universo de atividades lícitas
- Security gateways
  - Definição do conjunto de interações permitidas com o exterior
    - De dentro para fora
    - De fora para dentro

Defesa em Perímetro	Defesa em Profundidade
Consiste em definir um perímetro protegido englobando um conjunto de máquinas e redes e em evitar interações indesejáveis entre os dois lados desse perímetro. O perímetro divide o universo de máquinas e redes em dois: - onde estão os recursos a proteger - onde estão os possíveis abusadores desses recursos	A defesa em profundidade é particularmente útil para detetar problemas mais internos em domínios de segurança que foram originados internamente, ou que, por alguma razão, foram originados externamente ao perímetro de segurança e conseguiram passar através do mesmo. A defesa em profundidade é mais complexa de gerir, mas teoricamente, mais eficaz do que a defesa em perimetro.

Defesa de perímetro

Defesa em Profundidade



Ataques em sistemas distribuídos

Ataques às máquinas	Ataques às redes	Outros
• Roubo • Intrusão • Personificação • Negação de prestação de serviços (DoS)	• Inspeção • Personificação • Interceção • Modificação • Reprodução • Negação de prestação de serviços (DoS)	• Transferência de informação

Modelos de Ataque

Ataques específicos	Ataques automatizados
• Concebidos especificamente para uma máquina ou rede • Conduzidos em tempo real por especialistas	• Concebidos para explorar vulnerabilidades prováveis • Pré-codificadores e lançados contra qualquer máquina ou rede • Tempo médio de sobrevivência - Tempo que medeia entre dois ataques automatizados consecutivos - Existem máquinas sensores que permitem calcular esse tempo • Conduzidos por especialistas, iniciantes, curiosos, etc…

Mecanismos em sistemas distribuídos

Sistemas operativos confiáveis	**Autenticação**	**Firewalls & Security Appliances**
• Níveis de segurança, certificação • Ambientes seguros para servidores • Execução confinada (sandboxing)/máquinas virtuais	• Local • Remota • Single Sing-On	• Controlo de tráfego entre duas redes • Monitorização (carga da rede, etc…)
Autoridades de Certificação/PKI	**Cifra de ficheiros e de sessões**	**Comunicação cifra/VPNs**
• Gestão de certificados de chaves públicas	• Privacidade de dados que circulam na rede • Privacidade de dados guardados em disco	• Canais seguros sobre redes públicas inseguras • Extensão segura de redes organizacionais
Monitorização de conteúdos	**Deteção de intrusos**	**Detetores de vulnerabilidades**
• Deteção de vírus (ciberpragas)	• Deteção de atividades proibidas ou anómalas • Host-based / Network-based	• Procura para efeitos de correção ou exploração • Host-based / Network-based
Testes de penetração	**Administração da Segurança da Empresa**	**Real-Time Security Awareness / Incident Response**
• Análise de vulnerabilidades • Tentativas de penetração para demonstração • Teste dos mecanismos de segurança instalados	• Desenvolvimento de políticas • Aplicação distribuída de políticas • Co-administração de serviços de segurança	• Capacidade de aprender corretamente a existência de problemas em tempo real • Meios para reação rápida e correta ao incidente