# Segurança Informática e nas Organizações

Resumos
2016/2017

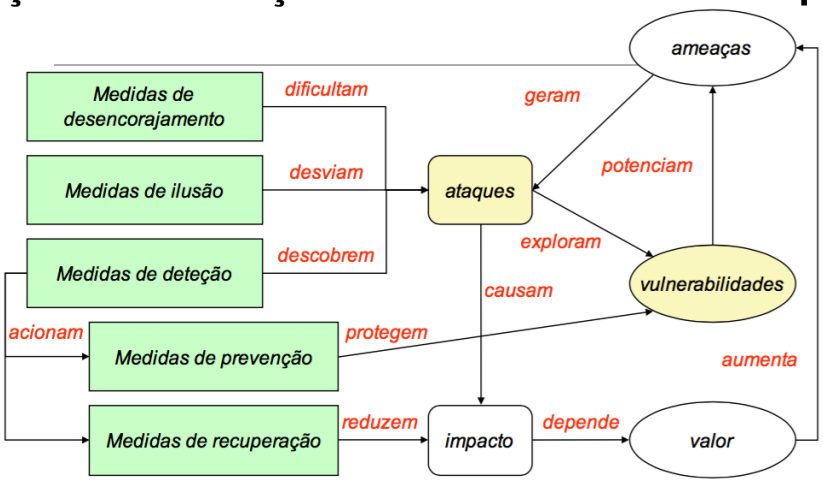
João Alegria | 68661

# Capítulo 2

## Vulnerabilidades

---

### Segurança da Informação: Vulnerabilidades e Ataques




### Medidas e Ferramentas

| **Desencorajamento**<br>Dificultam os ataques | **Ilusão**<br>Desviam os ataques |
|---|---|
| • Punição<br>- Restrições legais<br>- Evidências forenses<br>• Barreiras de Segurança<br>- Firewalls, autenticação, comunicação segura, sandboxing | • Honeypots / Honeynets<br>• Acompanhamento forense |
| **Deteção**<br>Descobrem os Ataques | |
| • Sistemas de detenção de intrusões (ex: Snort)<br>• Auditorias<br>• Análise forense de penetrações | |
| **Prevenção**<br>Protegem Vulnerabilidades | **Recuperação**<br>Reduzem o impacto |
| • Políticas restritivas<br>(ex: princípio do privilégio mínimo)<br>• Pesquisa de vulnerabilidades<br>(ex: OpenVAS)<br>• Eliminação de vulnerabilidades<br>(ex: atualização regular) | • Backups<br>• Sistemas redundantes<br>• Recuperação forense |

acionam

## Prontidão

• O desencorajamento, a ilusão e a deteção servem sobretudo para lidar com problemas conhecidos
  - Tentativas de reconhecimento (ex: port scanning)
  - Ataques genéricos (ex: escura de rede)
  - Ataques específicos (ex: buffer overflows)

• As medidas de prevenção protegem de vulnerabilidades conhecidas ou desconhecidas
  - Vulnerabilidades genéricas
    - ex: Reação a mensagens mal formadas (protocol scrubbers)
    - ex: Ataques furtivos (normalmente para formatos canónicos)
  - Vulnerabilidades específicas
    - ex: Um erro de software em particular

• A aplicação das medidas requer conhecimento sobre:
  - Vulnerabilidades conhecidas (problema, forma de exploração, impacto, etc…)
  - Padrões dos ataques que exploram essas vulnerabilidades (modus operandi, assinaturas de ataques)
  - Padrões anormais de atividade (Mas será fácil estabelecer um padrão de normalidade? ; Os ambientes heterogéneos são um problema)

• As ameaças em rede de computadores são diferentes de outros tipos de ameaças
  - Os ataques podem ser lançadas em qualquer hora, de qualquer local e por intermédios inocentes
  - Podem ser facilmente coordenados (ex: Distributed Denial of Service Attacks (DDoS)
  - São baratos e rápidos
  - Podem ser automatizados

• Requerem uma capacidade permanente (24x7) de reação de ataques
  - Equipas de especialistas em segurança
  - Alertas de ataque na hora
  - Teste e avaliação dos níveis de segurança existentes
  - Procedimentos de reação ágeis

## Deteção de Vulnerabilidades

• Ferramentas específicas podem detectar vulnerabilidades em sistemas
  - Implementam ataques usando vulnerabilidades conhecidas
  - Implementam ataques usando padrões de vulnerabilidades
    - Buffer Overflow, SQL Injection, XSS, etc…

• Vitais para a robustez das aplicações e sistemas implementados
  - Serviço frequentemente contratado

• Podem ser aplicados a:
  - Código desenvolvido (Análise Estática): OWASP LAPSE+, RIPS
  - Aplicação a executar (Análise Dinâmica): Valgrind, Rational AppScan
  - Externamente como um sistema remoto: Metasploit, …

• Não devem ser aplicados de foram cega a sistemas em produção!
  - Potencial perda / corrupção de dados
  - Potencial negação de serviço

### Ataques ou ameaças do dia zero

Este tipo de ataques são chamados de *zero day attacks* uma vez que o autor da aplicação tem zero dias para planear qualquer forma de evitar esse ataque (como por exemplo: aconselhamento forense). Ou seja, o ataque explora vulnerabilidades desconhecidas e, uma vez que não existe quaisquer soluções conhecidas para por fim, possibilita o acesso dos dados e a informações confidenciais.
Uma medida de resistir a este ataque é apostar na diversidade de sistemas operativos para qual o software pode ser lançado ou bloquear com defesas em profundidade com auxílio de firewalls ou utilizar mecanismos de proteção em análise comportamental (*honeypots*)

- Ataque que ocorre no dia zero do conhecimento de vulnerabilidades que o permitem
  - Para as quais não existem soluções conhecidas
  - Pode explorar mesmo um padrão desconhecido

- Ataque que explora vulnerabilidades que:
  - São desconhecidas das vitimas
  - São desconhecidas dos fabricantes implicados
  - São desconhecidas dos organismos e empresas que apoiam a defesa contra ataques

- Podem existir como "dia zero" durante muito tempo
  - Dias… Meses… Anos…

## CVE - Common Vulnerabilities and Exposures

Um CVE consiste num dicionário público de vulnerabilidades e exposições de segurança para gestão de vulnerabilidades e deteção de intrusões. É um método que fornece uma linguagem comum para referir os problemas e facilita a partilha de dados entre investigadores e base de dados vulneráveis.
Uma vez que as vulnerabilidades se encontram acessíveis publicamente, um dado indivíduo é capaz de realizar um ataque a partir do estudo da vulnerabilidade. Este está sempre associado a um software ou a um sistema operativo e o atacante só precisará de um sistema "compatível" com as especificações declaradas no CVE.
Um mecanismo para a redução da utilização por atacantes é limitar o acesso a este tipo de dicionários, deixando apenas acesso a entidades competentes e validadas para tal.

- **Dicionário público de vulnerabilidades e exposições de segurança**

- Para gestão de vulnerabilidades
- Para gestão de correções (*patches*)
- Para alarmística de vulnerabilidades
- Para deteção de intrusões

- **Identificadores comuns do CVE**

- Permite a troca de informações entre produtos de segurança
- Fornece uma base de indexação para avaliar a abrangência de ferramentas e serviços

- **Detalhes de uma vulnerabilidade podem ser restritos**

## CVE: Vulnerabilidades

**• Erro no software**

- Que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede

**• Um erro só é vulnerabilidade se permitir que o atacante viole uma política de segurança**

- Exclui políticas de segurança "abertas" onde todos os utentes são de confiança ou onde não se considera existência de riscos para o sistema

**• Uma vulnerabilidade é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:**

- Permite que um atacante execute comandos em nome de terceiros
- Permite que um atacante aceda a dados ao arrepio do especificado nas restrições de acesso para esses dados
- Permite que o atacante se apresente como outrem
- Permite que o atacante negue a prestação de serviços

## CVE: Exposição

**• Problema de configuração de um sistema ou um erro no software**

- Que permitem aceder a informação ou capacidades que podem auxiliar um atacante

**• O CVE considera um problema de configuração ou um erro como uma exposição se não permitir comprometer diretamente um sistema ou rede**

- Mas for uma componente importante para o sucesso de um ataque e uma violação de uma política de segurança expectável.

**• Uma exposição é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:**

- Permite que um atacante realize recolhas de informação
- Permite a um atacante esconder as suas atividades
- Inclui uma funcionalidade que se comporta como esperado mas que pode ser facilmente comprometida
- É um ponto de entrada frequente para atacantes que tentam obter acesso ao sistema ou a dados
- É considerado problemático por uma política de segurança razoável

## CVE: Benefícios

**• Fornece uma linguagem comum para referir problemas**

**• Facilita a partilha de dados entre**

- Sistemas de deteção de intrusões
- Ferramentas de aferição
- Bases de dados de vulnerabilidades
- Investigadores
- Equipas de resposta a incidentes

**• Permite melhorar as ferramentas de segurança**

- Maior abrangência, facilidade de comparação, interoperabilidade
- Sistemas de alarme e reporte

• **Fomenta a inovação**
- Local primordial para discutir conteúdos críticos das BDs

**LIMITAÇÕES**

Não ajuda à defesa contra ataques do dia zero!

## CVE: Identificadores

• **aka CVE *names*, CVE *numbers*, CVE-IDS, ou CVEs**
•**Identificadores únicos para vulnerabilidades conhecidas e públicas da CVE List**
- Estados possíveis: “candidate” ou “entry”
- Candidate: sob revisão para inclusão na CVE List
- Entry: Aceite na CVE List

• **Formato**
- Identificador numérico CVE (CVE-Ano-Indice)
- Estado (candidate ou entry)
- Descrição sumária da vulnerabilidade ou exposição
- Referência para informação adicional

## CVE e ataques

• **Ataques podem ser compostos / possibilitados por várias vulnerabilidades**
- Um CVE para cada vulnerabilidade
- Pode necessitar de uma sequência de vulnerabilidades
- Pode necessitar de uma das vulnerabilidades

# CWE - Common Weakness and Enumeration

• **Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança**
- De programas, do seu desenho ou da arquitetura de sistemas
- Cada CWE representa um tipo de vulnerabilidade
- Gerida pela MITRE Corporation
  - Uma CWE List é disponibilizada pela MITRE website
  - Esta lista fornece uma definição pormenorizada de cada CWE

• **Os CWEs são catalogados segundo uma estrutura hierárquica**
- CWEs localizados nos níveis superiores fornecem uma descrição genérica sobre o tipo de vulnerabilidades
  - Podem ter vários CWEs filhos associados
- CWEs nos níveis inferiores descrevem problemas de uma forma mais focada
  - Com menos ou sem CWEs filhos

• **Bases de dados de vulnerabilidades**
- NIST NVD (National Vulnerability Database)
- CERT Vulnerability Card Catalog
- US-CERT Vulnerability Notes Database

## CERT - Computer Emergency Readiness Team

- **Organização orientada para assegurar que a tecnologia e as práticas de gestão de sistemas adequados são usados para:**
  - Resistir a ataques em sistemas em rede
  - Limitar estragos e assegurar a continuidade de operação de sistemas críticos apesar da ocorrência de ataques bem sucedidos, acidentes ou falhas

- **CERT / CC (coordination Center) @ CMU**
  - Uma componente do vasto CERT Program
  - Centro primordial para questões de segurança na internet
    - Criado em 1988
    - O verme demonstrou a vulnerabilidade crescente da rede a ataques globalizados

## CSIRT - Computer Security Incident Response Team

- **Uma organização responsável por fornecer serviços de apoio para problemas de segurança em sistemas computacionais**
  - Serviço 24x7 para particulares, empresas, departamentos governamentais e outras organizações
  - Ponto único de contacto para reportar incidentes de segurança computacional
  - Disseminação de informação de incidentes

## Alarmes de segurança

- **Vitais para a disseminação rápida do conhecimento sobre novas vulnerabilidades**
  - US-CERT: Technical Cyber Security Alerts
  - US-CERT (non-technical): Cyber Security Alerts
  - SANS: Internet Storm Center
  - Microsoft: Security Response Center
  - Cisco: Security Center

| **Vulnerabilidades na Prática** | |
|---|---|
| **SQL Injection** | **Cross-Site Scripting** |
| É uma ameaça de segurança que se aproveita de falhas em sistemas com BD via SQL.<br>Os possíveis ataques são:<br>- Exposição da informação<br>- Consulta da informação<br>- Modificação dos dados contidos na BD (através de Insert, Update, Delete)<br>- Falsa autenticação em sistemas de *login*<br><br>Medidas de prevenção:<br>- Utilização de stored procedures<br>- Parametrização de consultas<br>- Limitar privilégios de acesso | É um tipo de vulnerabilidade do sistema de segurança de um computador, encontrado normalmente em aplicações web que ativaram ataques maliciosos ou injectaram client-side script dentro das páginas web vistas por outros utilizadores.<br>Este script pode ser usado pelos atacantes para escaparem aos controlos de acesso que usam a política da mesma origem. |