Segurança Informática e nas Organizações

José Mendes 107188

2023/2024

1 Introdução

1.1 Segurança

Segurança - É o assunto focado na previsão de sistemas, processos, ambientes, ...
Ao longo de todos os aspetos do ciclo de vida de um sistema:

- Planeamento
- Desenvolvimento
- Execução
- Processos
- Pessoas
- Clientes e Supply Chain
- Mecanismos
- Standards e Regulamentos
- Propriedade Intelectual

1.1.1 Planeamento

Design de uma solução está de acordo com alguns requisitos dentro de um contexto normativo.

Sem flaws

- Todos os estados da operação são os previstos;
- Não há estados adicionais que fogem da lógica esperada (mesmo se transições forçadas são usadas);

Dentro do scope de um contexto normativo

- Especifico para cada atividade e setor (Ex: ISO 27001, ISO 27007, ISO 37001);

1.1.2 Desenvolvimento

Implementação de uma solução de acordo com o design, sem outros modos de operação.

Sem bugs a comprometer uma execução correta

- Sem crashes;
- Sem resultados invalidos ou inesperados;
- Com tempos de execução corretos;
- Com consumo de recursos adequado;
- Sem leaks de informação;

Software

- Requer uma implementação cuidadosa;
- Requer testes para obter uma implementação com os comportamentos esperados;

1.1.3 Execução

Código executa tal como foi escrito, com todos os processos previstos.

O ambiente é controlado, não pode ser manipulado ou observado.
Sem a existência de comportamentos anomalos, introduzido por aspetos ambientais (como velocidade de armazenamento, quantidade de RAM, comunicação confiaveis)

1.1.4 Pessoas e Parceiros

O comportamento do Staff não pode ter um impacto negativo na solução.

- As normas existem para regular que ações são expectáveis;
- O Staff é treinado para distinguir comportamento correto de comportamento incorreto;
- O Staff tem os incentivos corretos para se comportar adequadamente;
- Quando o Staff é comprometido, ou se desvia, as ações têm impacto limitado;

1.1.5 Análise e Audiroia

Qual é o verdadeiro comportamento da solução?

Identificar desvios dos atributos esperados

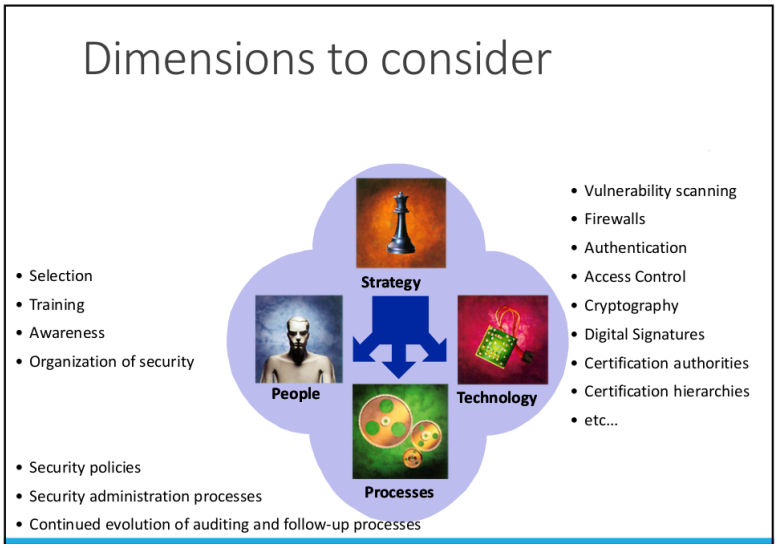
- Faults, erros, comportamentos

Identificar o risco para a solução ser modificada

- Exposição a possíveis ataquantes;
- Incentivos que que alguém possa ter para modificar a solução;
- Identificar potenciais actors (threats);

Identificar o impacto dos desvios

- Perda total de dados? Denial of Service? Increase Operation Cost?



1.2 Perspetivas

A Segutrança tem muitas perspetivas interligadas.

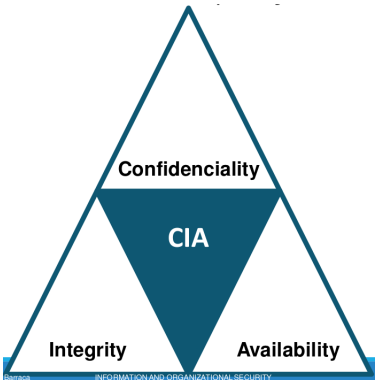
Defensive: Focado em manter previsão,
Offensive: Focado em explorar a previsibilidade.

- Pode ter uma intenção maliciosa/criminosa;
- Pode ter como objetivo, a validação da solução (Red Teams);

Outras:

- Engenharia Inversa: Recuperar o design de porjetos contruidos;
- Forensics: Extrair informação e reconstruir eventos anteriores;
- Recuperação de Desastres: Minimizar o impacto de ataques;
- Auditoria: Avaliar se a solução está de acordo com um conjunto de requisitos;

1.3 Objetivos de Segurança de Informação



Confidencialidade: A informação pode apenas ser acessada por um grupo restrito de entidades;

Medidas:

- Encryptar informação;
- Usar passwords de acesso (fortes);
- Usar sistemas de gestão de identidade e autenticação;
- Doors, Strong Walls;
- Security personnel;
- Treinar (o Staff);

Integridade: A informação permanece inalterada (Pode ser aplicada ao comportamento de dispositivos e serviços);

Medidas:

- Controlo de identidade (hashes);
- Backups;
- Controlo de acesso;
- Dispositivos de armazenamento robustos;
- Processos de verificação de dados;

Disponibilidade: A informação está disponível a target entities (Pode ser aplicada aos serviços e dispositivos);

Medidas:

- Backups;
- Planos de recuperação de desastres;
- Redundância;
- Virtualização;
- Monitorização;

Privacidade: Como a informação pessoal é tratada (isto envolve: Obtida, Processada, Armazenada, Partilhada, Eliminada);

Medidas:

- Controlo de acesso;
- Processos transparentes;
- Ciphers;
- Integridade e controlo de autenticação;
- Logs;

1.4 Objetivos da Segurança

Defesa contra eventos catastróficos:

- Fenómenos naturais;
- Temperaturas extremas, inundações, trevoada, trovões, radiação, ...

Degradação do Hardware do computador:

- Falha no fornecimento de energia;
- Bad sectors em discos;
- Bit errors em células RAM ou SSD;

Defesa contra falhas normais:

- Queda de energia;
- Falhas internas do sistema;
  - Linux Kernel panic, Windows blue screen, OS X panic;
  - Deadlocks;
  - Uso anormal de recursos;
- Falhas de software / Falhas de comunicação;

Defesa contra atividades não autorizadas (adversários):

- Iniciado por alguém "de fora" ou "de dentro";

Tipos de atividades não autorizadas:

- Acesso a informação;
- Alteração de informação;
- Utilização de recursos (CPU, memory, print, network, ...);
- Denial of Service;
- Vandalismo (interferir com o funcionamento normal do sistema, sem obter benefícios);

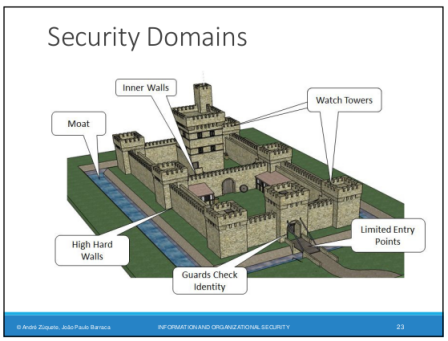
1.5 Conceitos Base

1. Domínios;
2. Políticas;
3. Mecanismos;
4. Controlos;

1.5.1 Domínios

Um conjunto de entidades que partilham atributos de segurança semelhantes.

- Permite gerir segurança de uma forma agregada;
  - A gestão define os atributos do domínio;
  - As entidades adicionadas ao domínio herdam os atributos do "grupo";
- Comportamento e interações são homogéneas dentro do domínio;
- Domínios podem ser organizados em hierarquias;
- As interações entre domínios são, normalmente, controladas;



1.5.2 Políticas

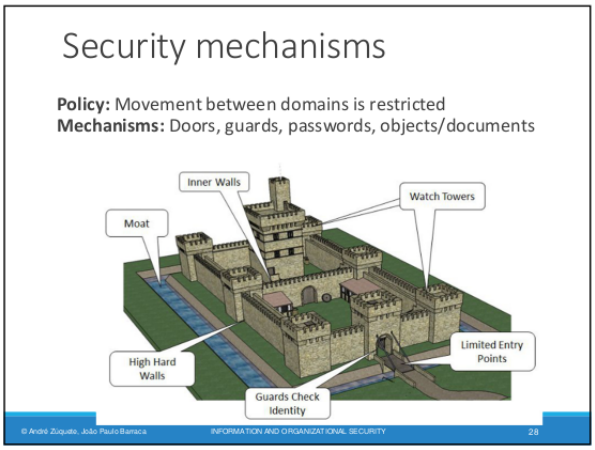
Conjunto de guidelnes relacionados com a segurança, que mandam sobre o domínio.

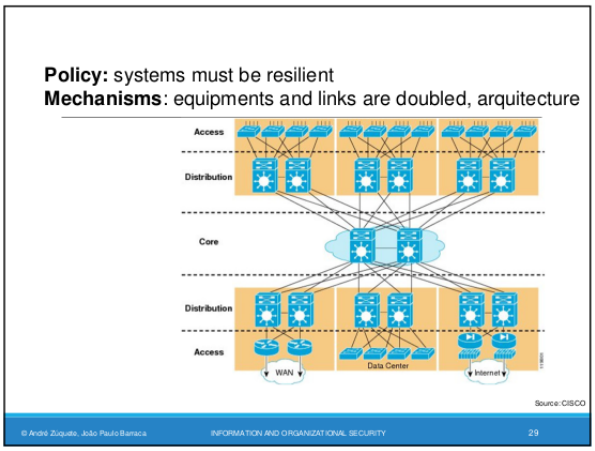
- Organizações têm múltiplas políticas;
  - Aplicavéis a cada domínio específico;
  - Podem dar overlap e terem scopes diferentes/níveis abstratos;
- As múltiplas políticas têm de ser coerentes;
- Exemplos:
  - Users apenas podem acessar serviços web;
  - Os assuntos devem ser autenticados para entrar no domínio;
  - Walls devem ser construidas de betão;
  - Comunicações devem ser encriptadas;
- Define o poder para cada assunto;
  - Least privilege principle: cada assunto apenas deve ter os previlégios necessários para executar as suas tarefas;
- Define procedimentos de segurança (quem faz o quê em que situação);
- Define os requisitos de segurança mínimos para um domínio;
  - Security levels, Security Groups
  - Autorização é necessária (and the related minimum authentication requirements (Strong/weak, single/multifactor, remote/face-to-face))
  - Define estratégias de defesa e táticas de contra-ataque;
    - Arquitetura defensiva;
    - Monotorização de atividades criticas ou sinais de ataque;
    - Reação contra ataques ou outros cenários anormais;
  - Define que atividades são legais e ilegais;
    - Forbid list model: Some activities are denied, the rest are allowed;
    - Permit list model: Some activities are allowed, the rest is forbidden;

1.5.3 Mecanismos

- Implementam as políticas;
  - Definem, num nível mais elevado, o que precisa de ser feito ou evitado;
  - São usados para implementar políticas;

- Mecânismos de segurnaça genéricos:
  - Confinamento (sandboxing);
  - Autenticação;
  - Controlo de acesso;
  - Execução priveligiada;
  - Filtragem;
  - Logging;
  - Auditoria;
  - Algoritmos criptográficos;
  - Protocolos criptográficos;





1.5.4 Controlos

Controlos são quqlquer aspeto que permita minimizar o risco (proteger as propriedades **CIA**)

- Controlos incluem políticas e mecanismos, mas também:
  - Standards e regulamentos;
  - Processos;
  - Técnicas;
- Controlos são explicitamente definidos e podem ser auditáveis;
  - E.g.: ISO 27001 defines 114 controls in 14 groups (... asset management, physical security, incidente management...)

	Prevention	Detection	Correction
Physical	- Fences - Gates - Locks	- CCTV	- Repair Locks - Repair Windows - Redeploy access cards
Technical	- Firewall - Authentication - Antivirus	- Intrusion Detection Systems - Alarms - Honeypots	- Vulnerability patching - Reboot Systems - Redeploy VMs - Remove Virus
Administrative	- Contractual clauses - Separation of Duties - Information Classification	- Review Access Matrixes - Audits	- Implement a business continuity plan - Implement an incident response plan

Horizontal: Relação ao evento
Vertical: Relação à sua natureza

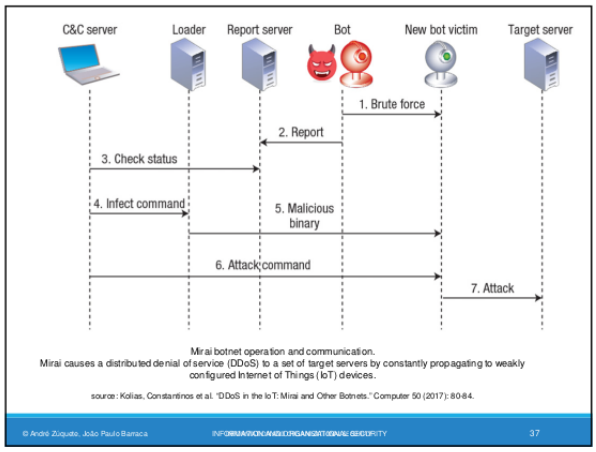
1.6 Segurança na Prática

Prevenção realista.

- Segurança perfeita é impossível;
- Focar nos eventos mais prováveis (pode depender de localização, legal framework, . . .)
- Considerar o custo e o profit;
  - Um grande número de controlos tem um low cost;
  - No entanto, não limite superior para o custo de uma estratégia de segurança;
- Considerar todos os domínios e entidades;
  - Um simples breach pode escalar para um problema maior;
- Considerar impacto (Under the light of CIA and other potential impact areas (e.g., brand))
- Considerar o custo e o tempo de recuperação;
- Caracterizar ataquantes (definir controlos específicos para esses, vão sempre existir atacantes com mais recursos);
- Considerar que o sistema será comprometido (Ter planos de recuperação);

1.7 Segurança em Sistemas Computacionais

- Computadores podem fazer grandes danos em pouco tempo;
  - Gerem grandes quantidades de informação;
  - Processam e comunicam com grande velocidade;
- O número de **weaknesses está sempre a aumentar**;
  - Devido a complexidade acrescida;
- As redes permitem mecanismos de ataque mais sofisticados;
  - Ataques anónimos de qualquer parte do mundo;
  - Espalha-se rapidamente através de barreira geográficas;
  - Exploitation of insecure hosts and applications
- Os ataquantes constroem ataques em cadeia complexos;
  - First exploration
  - Lateral movement
  - Exfilration



- A maior parte das vezes os users não sabem dos riscos
  - Não sabem os problemas, impacto, boas práticas nem as soluções;
- A maior parte das vezes os users são descuidados
  - Porque tomam riscos;
  - Não querem saber (não têm/identificam alguma responsabilidade);
  - Não estimam o risco corretamente;

1.8 Maiores fontes de vulnerabilidades

Aplicações hostis ou com bugs

- Rootkits: Insert elements in the operating system
- Worms: Software programs controlled by an attacker
- Virus: Pieces of code that infect other files (e.g., macros)

Users

- Ignorantes, descuidados, não querem saber
- Usam alternativas não seguras
- Confiam que as aplicações de segurança resolvem os problemas
- Download de software de fontes não confiáveis
- hostis

Administração defeituosa

- A configuração default é a mais segura
- Security restriction vs flexible operation
- Excessões a indivíduos

Comunicação através de redes desconhecidas/não controladas

- Public hotspots, campus networks, hostile governments

1.9 Perimeter Defense

Proteção contra atacantes externos

- Internet, Foreign users, outras organizações

Assume que os users internos são confiáveis e partilham as mesmas políticas

- Amigos, família, colaboradores

Usados em cenários domésticos ou em pequenas empresas

Limitações:

- Muito simples;
- Não protege contra ataques internos (users previamente confiáveis, atacantes que adquiriram acesso interno);

1.10 Defesa em Profundidade

Proteção contra atacantes externos e internos

- Da internet, de outras organizações, de users internos;

Assume domínios bem definidos pela organização

- Walls, doors, authentication, security personell, ciphers, secure networks

Limitações

- Precisa de coordenação entre os diferentes controlos (podemos acabar com controlos overlapping, mas também com "buracos" nos perímetros de segurança);

1.11 Zero Trust

Modelos de defesa sem perímetros específicos

- Não há confiança por herança nas entidades só por serem internas (na verdade, pode não haver noção de "interno" e "externo");

Modelo recomendado para novos sistemas

- Sistemas tradicionais deviam migrar para este modelo;
- Implies the design of systems/services specific for this model
- Legacy systems vão precisar de camadas de proteção adicionais (Firewalls, filtros, adapatadores, plugins)

1.11.1 Princípios (NCSC)

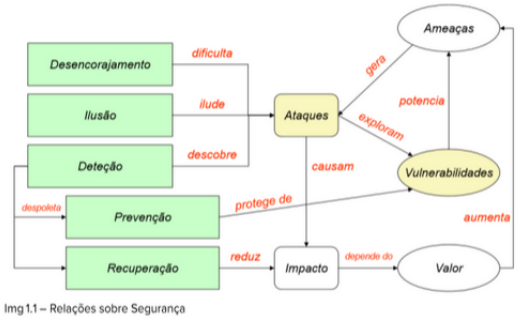
1. Saber a arquitetura (users, devices, services e data)
2. Saber as identidades (users, devices, services e data)
3. Avaliar o comportamento do user, service e saúde do device
4. Usar políticas para autorizar requests
5. Autenticar e autorizar em todo o lado (No open APIs, or IP address-based access)
6. Focar a Monitorização nos users, devices e services
7. Não confiar em nenhuma rede, incluindo a nossa (Os atacantes internos não devem ter mais privilégios que os externos)
8. Escolher services feitos para **zero trust** (evitar legacy services, mas podem ser integrados)

2 Vulnerabilidades

Uma empresa é tão mais suscetível de ataques quanto maior a sua dimensão, uma vez que ataques bem sucedidos serão mais rentáveis

De forma a prevenir **ataques**, que exploram **vulnerabilidades**, as organizações devem investir na **defesa** dos seus sistemas, de forma a garantir a segurança da informação que armazenam.

2.1 Segurança de Informação



Img 1.1 – Relações sobre Segurança

2.1.1 Medidas (e algumas ferramentas)

No entanto, **defesa** é um conceito abstrato, que na realidade ganha forma em cinco medidas.

Desencorajamento: através da punição dos infratores (restrições legais e forensic evidences) e utilização de barreiras de segurança (firewalls, Autenticação, Sandboxing, . . .)

Deteção: sistema de deteção de intrusões (e.g Seek, Bro, Suricata), ou através de auditorias e análises forenses;

Ilusão: dos atacantes com honeypots ou honeynets (como que pishing para atacantes) e follow-up com análise forense;

Prevenção: através de políticas de segurança (e.g least priviledge principle), deteção (e.g OpensVas, metasploit) e correção de vulnerabilidades (e.g updates regulares);

Recuperação: com backups, sistemas redundantes, recuperação forense;

2.2 Vulnerabilidade

É um erro no software que pode ser diretamente usado por um atacante para ganhar acesso a um sistema ou rede.

Um erro é uma vulnerabilidade se permitir a um atacante usá-lo para violar uma política de segurança para esse sistema.
Isto exclui políticas de segurança completamente "abertas" em que todos os users são confiáveis, ou onde não há consideração do risco do sistema.

Uma vulnerabilidade **CVE** é um estado num sistema computacionas (ou conjunto de sistemas) que podem:

- Permitir ao atacante executar comandos como outro user;
- Permitir ao atacante aceder a dados que é contrário às restrições de acesso específicadas para esses dados;
- Permitir a um atacante fingir ser outra entidade;
- Permitir ao atacante realizar denial of service;

2.3 Exposição

Problema de configuração que permite ao atacante aceder a informação ou capacidades que o podem auxiliar, sem conseguir no entanto comprometer diretamente o sistema.

Um problema de configuração ou um erro é uma exposição se não permitir diretamente comprometer a segurança do sistema, mas pode ser um componente importante para a realização de um ataque bem sucedido, e é uma violação de uma política de segurança.

Uma exposição descreve um estado no sistema computacional (ou conjunto de sistemas) que não é uma vulnerabilidade mas pode:

- Permitir a um atacante conduzir atividades para obter informação;
- Permitir a um atacante esconder atividades;
- Inclui uma capacidade que se comporta como esperado, mas pode ser facilmente abusada;
- É o ponto primário de entrada em que um atacante pode tentar usar para ganhar acesso ao sistema ou aos dados;
- É considerado um poblema por algumas políticas de segurança;

2.4 CVE - Common Vulnerabilities and Exposures

É um repositório público de vulnerabilidades, que lista e descreve vulnerabilidades e exposições de segurança.

Dicionário de vulnerabilidades e exposições sobre segurança de informação

- Para gestão de vulnerabilidades;
- Para gestão de resolução de problemas;
- Para alertar sobre novas vulnerabilidades;
- Para deteção de intrusões;

Usa identificadores comuns para os mesmos CVEs

- Permite a partilha de dados entre produtos de segurança;
- Oferece um baseline index point para avaliar coverage of tools and services;

Detalhes sobre uma vulnerabilidade podem ser mantidos privados

- Parte da divulgação responsável: até que o proprietário forneça uma solução;

(Ver imagem no slide 4)

2.4.1 Identificadoes CVE

Aka CVE names, CVE numbers, CVE-IDs, CVEs

Identificador único e comum para vulnerabilidades de segurança de informação publicamente conhecidas

- Têm status "candidate" ou "entry";
- Candiddato: Em review para inclusão na lista;
- Entry: Aceite na lista CVE;

Formato

- Numero identificador CVE (CVE-Year-Order);
- Status (candidate, entry);
- Descrição curta da vulnerabilidade ou exposição;
- Referências a fontes de informação;

2.4.2 Benefícios do CVE

Fornece uma linguagem comum para os problemas referenciados

- Facilita a partilha de dados entre ferramentas e serviços;
- Sistemas de deteção de intrusões;
- Ferramentas de acesso;
- Bases de dados de vulnerabilidades;
- Researchers;
- Equipes de resposta a incidentes;

Vai liderar para melhorar as ferramentas de segurança (mais compreensívo, melhores comparações, interoperabilidade)

Vai originar mais inovação (Ponto focal para discutir questões críticas de conteúdo de banco de dados)

2.4.3 CVE e ataques

Ataques são tornados possíveis através de múltiplas vulnerabilidades (um CVE para cada vulnerabilidade)

2.5 Deteção de Vulnerabilidades

Ferramentas específicas podem ser usadas para detetar vulnerabilidades
Estas exploram vulnerabilidades conhecidas, testando padrões (e.g buffer overflow, SQL injection, XSS, ...)

Ferramentas específicas podem replicar ataques conhecidos
Usar exploits conhecidos para vulnerabilidades conhecidas. Podem ser usadas para implementar medidas de defesa.

Vital para certificar a robustez de um sistema de produção e aplicações
Serviço muitas vezes oferecido por empresas externas.

Pode ser aplicado a:

- Source code;
- Aplicações em execução (análise dinâmica);
- Externamente como um cliente remoto;

Não dever ser aplicado cegamente a sistemas de produção
Potencial perda de dados/corrupção, DoS, atividade ilegal, ...

2.6 CWE - Common Weakness Enumeration

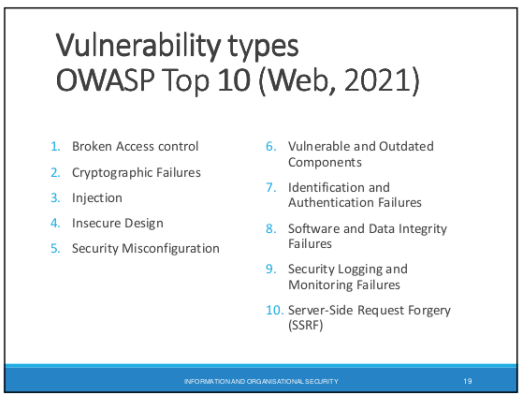
De forma complementar temos outro repositório, mas focado na exploração das causas das vulnerabilidades, ou seja, identifica as vulnerabilidades provocadas pelos developers devido a uma utilização incorreta do software.

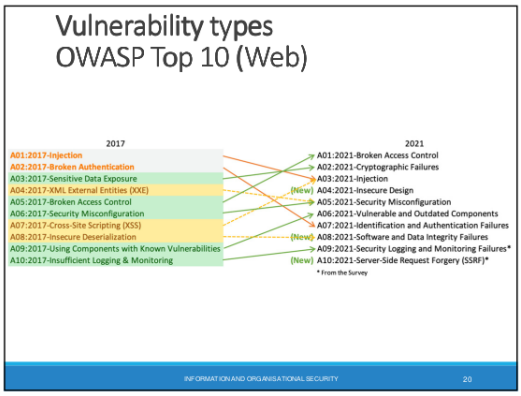
São encontradas no código, design, arquitetura do sistema. Cada CWE representa um único tipo de vulnerabilidade. É mantido pelo MITRE e esta lista fornece detalhes para cada CWE.

Um CWE podem organizar-se de forma hierárquica, havendo um pai que fornece uma descrição genérica e vários filhos, cada um focado numa parte concreta do problema.

Níveis mais profundos de CWEs, oferecem mais granularidade, normalmente com menos filhos, ou sem filhos.

CWE $\neq$ CVE





2.7 Rastreamento de Vulnerabilidades por parte dos vendedores

Durante o ciclo de desenvolvimento, as vulnerabilidades são tratadas como bugs, pode existir uma equipa de segurança ou não. Qunado o software está disponivel, as vulnerabilidades também sõa rastreadas globalmente, para cada sistema e software disponivel ao público.

O rastreamento público ajuda a:

- Focar a discussão à volta do problema;
- Aos defensores a facilmente testar o sistema, aumentando a segurança;
- Aos atacantes a facilmente saberem quais as vulnerabilidades a explorar;

As vulnerabilidades são rastreadas de forma privada (consitui um arsenal para ataques futuros contra alvos)

O conhecimento sobre vulnerabilidades é publicamente disponível e pode ser trocado por dinheiro. Mas também pode ser trocado de forma privada por ainda mais dinheiro.

2.8 Rastreamento de Vulnerabilidades

Não é algo fácil de fazer, uma ver que os exploits não são sempre conhecidos, o impacto e o custo podem ser difíceis de estimar (underestimated).

Feeds anteriores podem criar um falso sentido de segurança.

Possuir uma **comunicação dinâmica** é bom:

- Para os defensores, pois eles podem testar e implementar defesas;
- Para atacantes, pois estes podeqm incorporar os exploits;

2.9 Ataques de dia zero

Aka Zero Day (or Zero Hour) Attacks/Threat.

Este tipo de ataque caracteriza-se por explorar uma vulnerabilidade desconhecida. Este ocorre no dia zero do conhecimento da vulnerabilidade, para a qual não existe um security fix.

Se for explorada de forma discreta, pode durar meses ou até anos, conhecido por atacantes e não pelos outros, frequentemente parte do arsenal de ataque, sendo inclusive comercializadas em certos mercados (negro).

2.10 Sobrevivência

Como sobreviver a um ataque Dia Zero? Como podemos reagir a um destes ataques?

Apesar de ser o oposto do que geralmente é esperado dos sistemas (estandardização, protocolos bem definidos e regulares), a **diversidade** é a chave para a sobrevivência.

Isto porque dada a sua exclusividade, operações e protocolos distintos são mais difíceis de contornar, uma vez que requerem um estudo dedicado do sistema em particular e não podem ser aplicados de forma generalizada a outros.

Dada a sua diversidade, o SO Android terá menos probabilidade de ser atacado que o iOS.

2.11 CERT - Computer Emergency Readiness Team

Esta é uma equipa responsável por resistir a ataques em sistemas distribuídos (em rede), limitando o dano e garantindo a continuidade dos serviços críticos.

CERT/CC (Coordination Center) @ CMU

Um componente de um maior programa CERT, é um centro importante para problemas de segurança na internet.

2.12 CSIRT - Computer Security Incident Response Team

Dentro das equipas CERT, há uma componente de sigla CSIRT, cuja responsabilidade é receber, analisar e responder a relatórios de incidente e atividade.

2.13 Alertas de Segurança e activity trends

Vital para a disseminação rápida de conhecimento sobre novas vulnerabilidades (e.g US-CERT Cyber Security Alerts, SANS Internet Storm Center, Cisco Security Center, ...)