

Segurança Informática e nas Organizações

José Mendes 107188

2023/2024



universidade
de aveiro

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 anómalos, introduzido por aspetos ambientais
(como velocidade de armazenamento, quantidade de RAM, comunicação confiáveis)



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 Auditoria

Qual é o verdadeiro comportamento da solução?

Identificar desvios dos atributos esperados

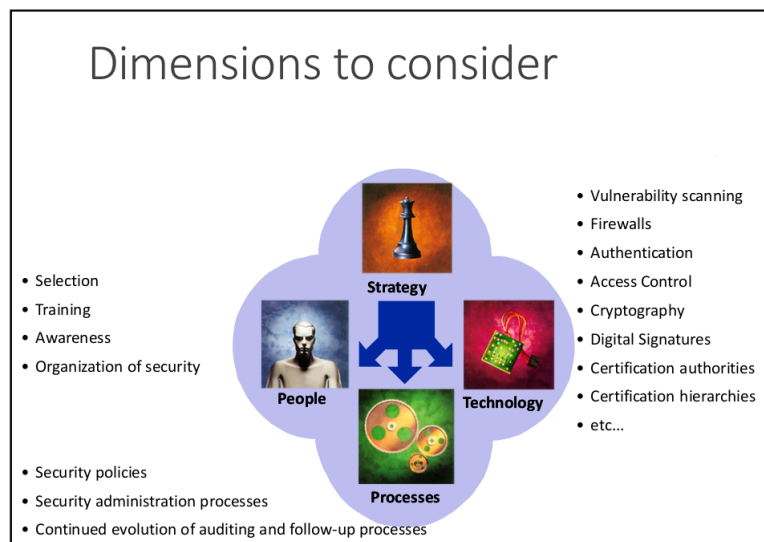
- Faults, erros, comportamentos

Identificar o risco para a solução ser modificada

- Exposição a possíveis atacantes;
- Incentivos 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 Seguranga tem muitas perspetivas interligadas.

Defensive: Focado em manter previsão,

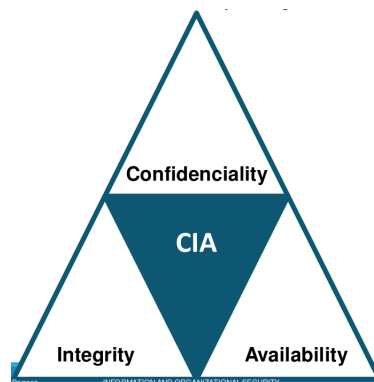
Offensive: Focado em explorar a previsibilidade.

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

Outras:

- Engenharia Inversa: Recuperar o design de projetos contruídos;
- 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);

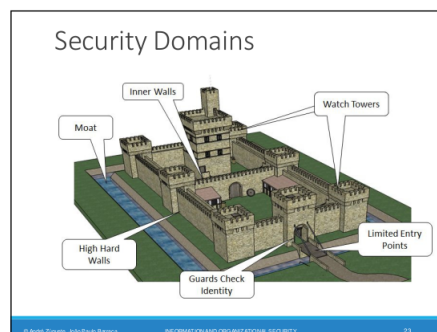
1.5 Conceitos Base

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 guidelines relacionados com a segurança, que mandam sobre o domínio.

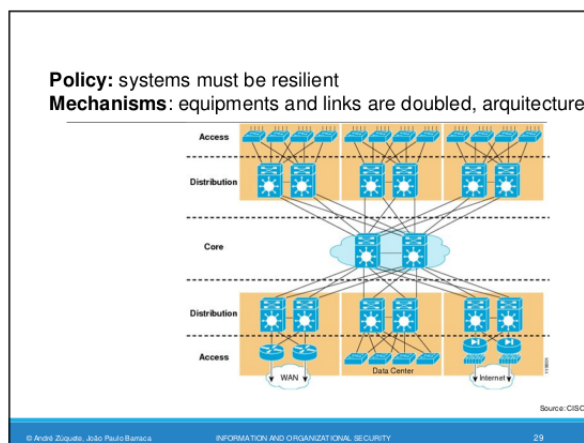
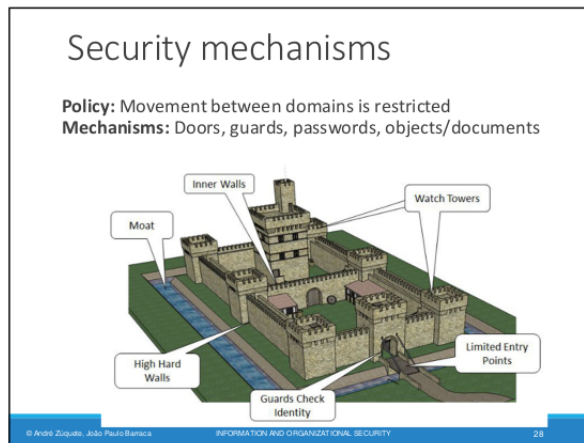
- Organizações têm múltiplas políticas;
 - Aplicáveis a cada domínio específico;
 - Podem dar overlap e terem scopes diferentes/níveis abstratos;
- As múltiplas políticas têm de ser coerentes;
- Exemplos:
 - Users apenas podem acessar serviços web;
 - Os assuntos devem ser autenticados para entrar no domínio;
 - Walls devem ser construídas de betão;
 - Comunicações devem ser encriptadas;
- Define o poder para cada assunto;
 - Least privilege principle: cada assunto apenas deve ter os privilégios 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;
 - * Monitorização de atividades críticas 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;

- Mecanismos de segurança genéricos:

- Confinamento (sandboxing);
- Autenticação;
- Controlo de acesso;
- Execução privilegiada;
- Filtragem;
- Logging;
- Auditoria;
- Algoritmos criptográficos;
- Protocolos criptográficos;



1.5.4 Controlos

Controlos são qualquer 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 | <ul style="list-style-type: none">- Fences- Gates- Locks | <ul style="list-style-type: none">- CCTV | <ul style="list-style-type: none">- Repair Locks- Repair Windows- Redeploy access cards |
| Technical | <ul style="list-style-type: none">- Firewall- Authentication- Antivirus | <ul style="list-style-type: none">- Intrusion Detection Systems- Alarms- Honeypots | <ul style="list-style-type: none">- Vulnerability patching- Reboot Systems- Redeploy VMs- Remove Virus |
| Administrative | <ul style="list-style-type: none">- Contractual clauses- Separation of Duties- Information Classification | <ul style="list-style-type: none">- Review Access Matrixes- Audits | <ul style="list-style-type: none">- Implement a business continuity plan- Implement an incident response plan |

Horizontal: Relação ao evento
Vertical: Relação à sua natureza

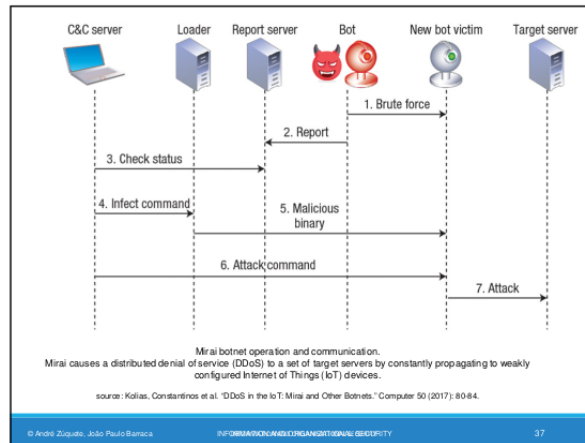
1.6 Segurança na Prática

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 atacantes (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 atacantes constroem ataques em cadeia complexos;
 - First exploration
 - Lateral movement
 - Exfiltration



- 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

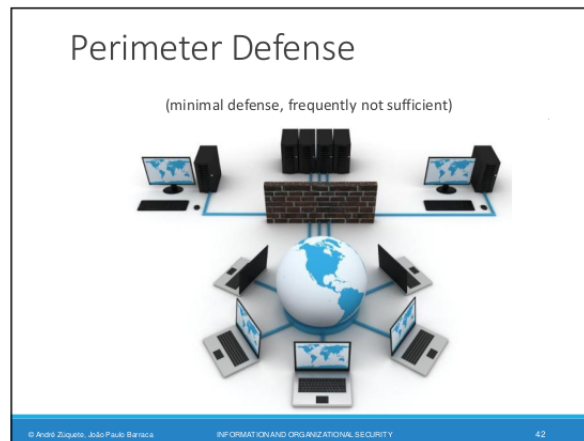
Administração defeituosa

- 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, adaptadores, 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)