Introdução à segurança

Objetivos da Segurança (1/3)

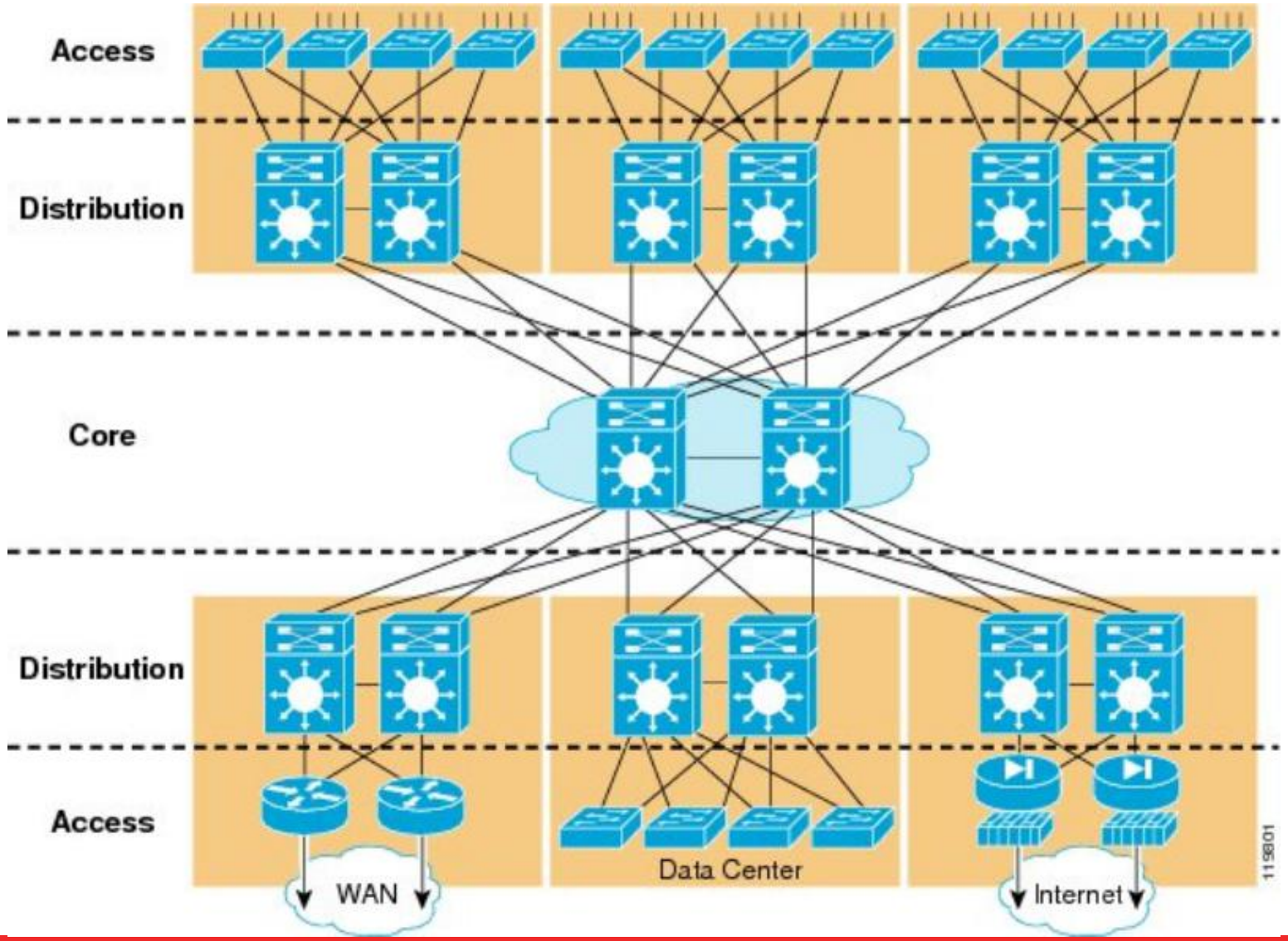
- **Defesa contra catástrofes**
  - Fenómenos naturais
  - Temperatura anormal, relâmpagos, picos de energia, inundações, radiação…
- **Degradação dos sistemas informáticos físicos**
  - Setores degradados, falha da fonte de alimentação, erros em células da RAM ou SSD…
- **Solução**
  - Prevenção realista: focar nos eventos mais prováveis
  - Cópias da informação (Backups)
  - Replicação
  - Informação
  - Recursos computacionais

Objetivos da Segurança (2/3)

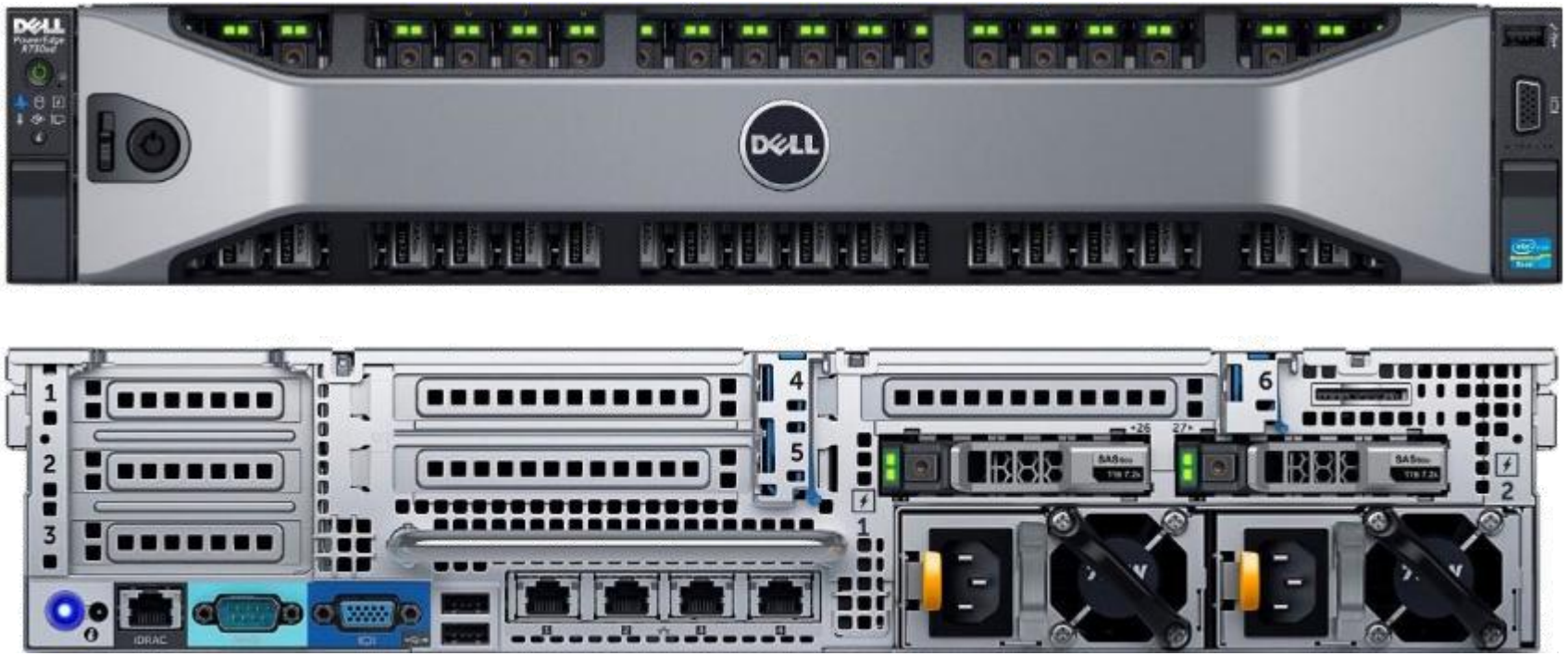
- **Defesa contra falhas e erros comuns**
  - Falhas de energia
  - Falhas internas aos sistemas operativos
    - Linux Kernel Panic, Windows Blue Screen, OSX panic
    - Bloqueios
    - Consumo anormal de recursos
  - Erros no Software / Erros nas Comunicações

- **Soluções**
  - Redundancia de componentes (fontes, discos, ventoinhas, ligações)
  - Sistemas Transacionais
  - Encaminhamento dinâmico, retransmissões

Redundância de Sistemas



Redundância de Subsistemas

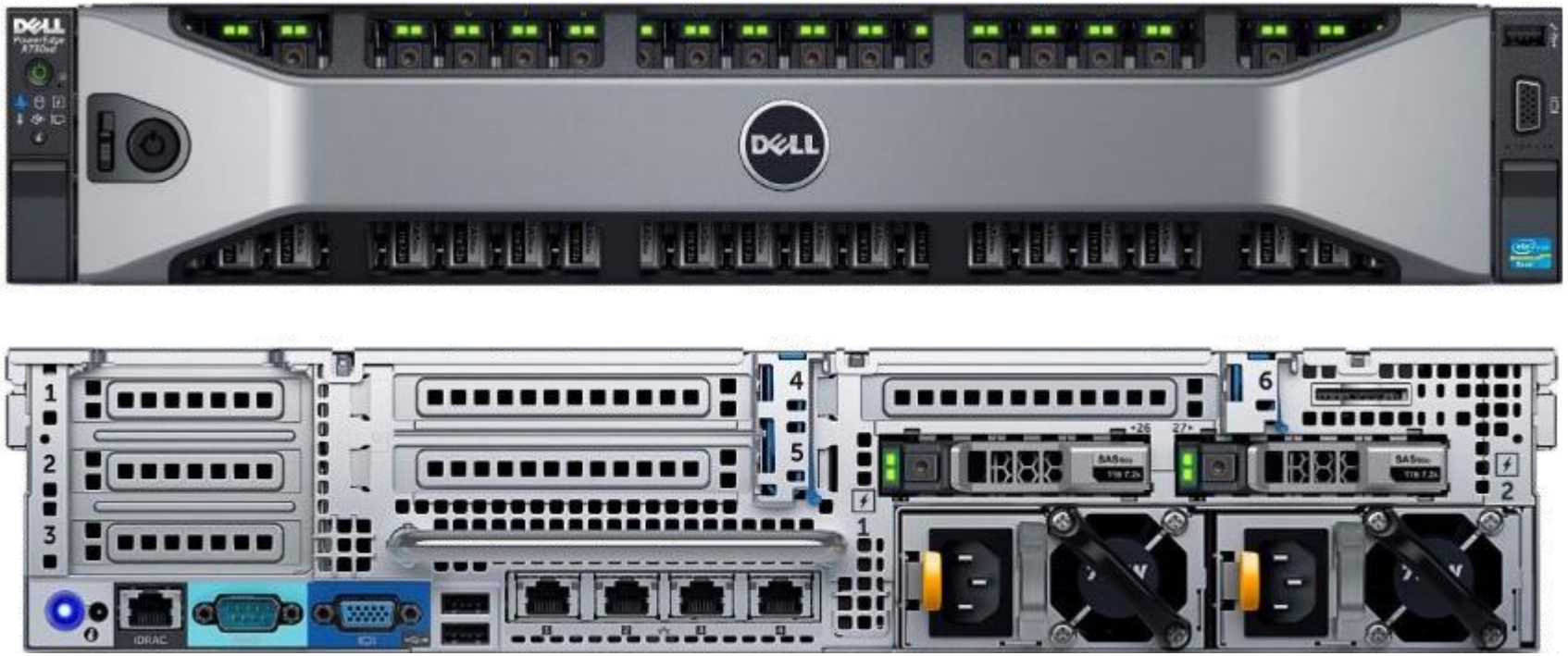


Fonte: DELL

Objetivos da Segurança (3/3)

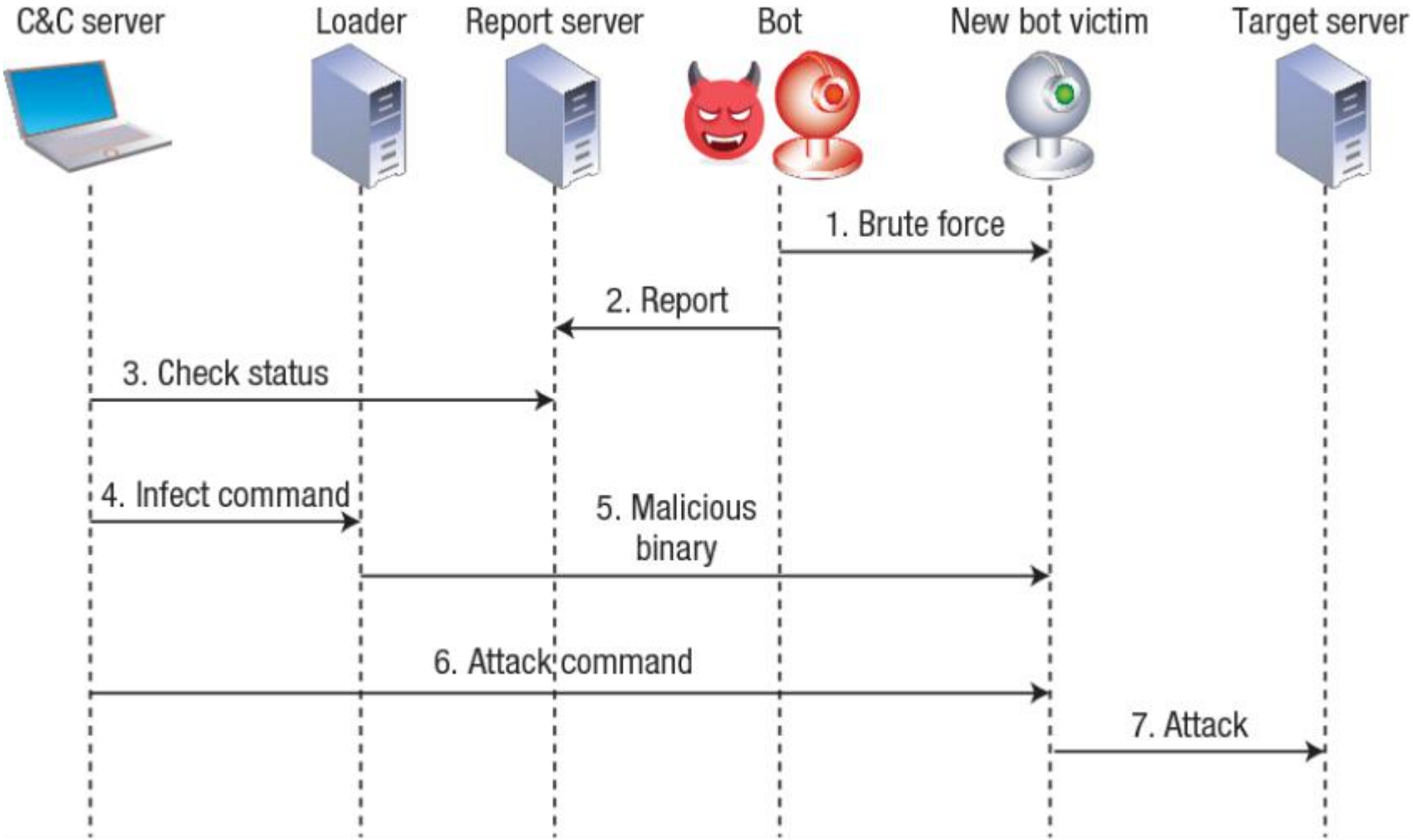
- **Defesa contra atividades não autorizadas (adversários)**
  - Iniciados por alguém “de dentro”, ou “de for a)
- **Tipos de atividades não autorizadas:**
  - Acesso a informação
  - Alteração de informação
  - Utilização de recursos
  - CPU, memória, impressão, rede…
  - Negação de serviço (DoS)
  - Vandalismo
  - Interferência do funcionamento normal, sem benefício direto para o atacante

Redundância de Subsistemas



Fonte: DELL

Encadeamento de atividades



Operação e comunicação da botnet Mirai botnet.
Mirai causa uma negação de serviço distribuída (DDoS) a servidores, propagando-se constantemente para dispositivos IoT mal configurados

Fonte: Kolias, Constantinos et al. “DDoS in the IoT: Mirai and Other Botnets.” Computer 50, 2017: 80-84

Segurança nos Sistemas Computacionais: Problema Complexo

- **Computadores podem fazer muitos estragos num curto espaço de tempo**
  - Podem processar grandes quantidades de informação
  - Processam informação a grande velocidade
- **O número de vulnerabilidades aumenta sempre**
  - Complexidade incremental dos sistemas
  - Pressões de mercado (time to market, ou custo)
- **Redes permitem novos mecanismos de ataque**
  - Ataques anónimos de qualquer ponto do planeta
  - Ataques distribuídos sobre várias geografias
  - Exploração de aplicações e sistemas inseguros

Segurança nos Sistemas Computacionais: Problema Complexo

- **Usuários não possuem noção do risco**
  - Não conhecem o problema
    - ... o impacto
    - ... as boas práticas
    - ... ou as soluções
- **Usuários são desleixados**
  - Tomam riscos
  - Não querem saber (não possuem/identificam responsabilidade)
  - Não estimam o risco de forma adequada

Aproximação Pragmática

- **A proteção perfeita de um sistema é impossível**
  - Solução: considerar equilíbrio entre custo e eficiência
  - Problema: determinar o custo e a eficiência
- **Segurança tem custos elevados**
  - Tecnologia dedicada, recursos adicionais, profissionais treinados, processos
  - Solução: Instalar o mínimo necessário
- **Proteção, valor e punição**
  - Adotar uma proteção “suficientemente boa” para os ataques mais comuns
  - Provocar menos interferência nas tarefas do que o dano causado pelos atacantes
  - Utilizar polícia e tribunais para seguir e processar atacantes
  - É importante não permitir a existência de uma noção de impunidade

Glossário

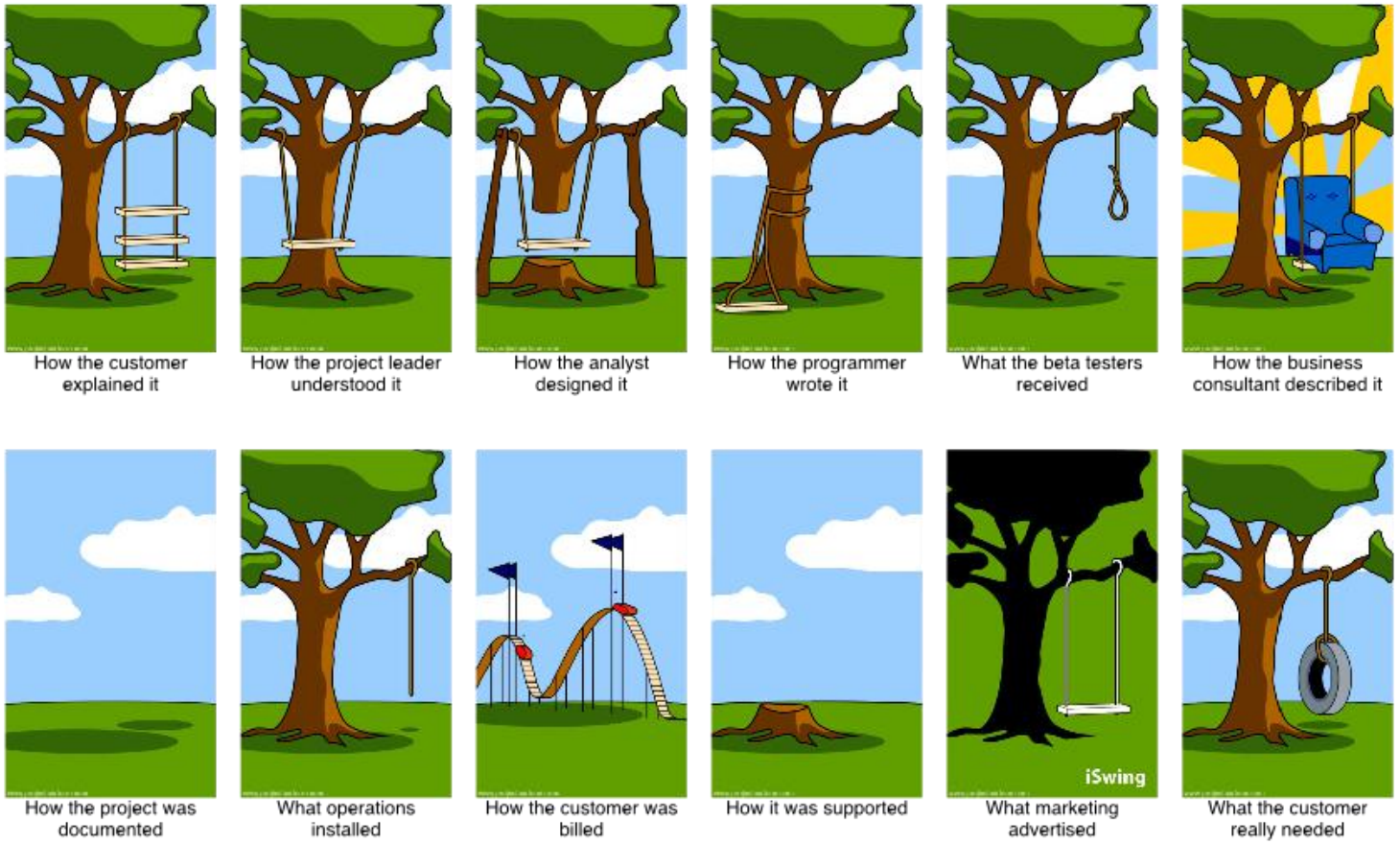
- **Vulnerabilidade**
  - Uma fraqueza do sistema que o torna sensível a ataques
  - Pode estar presente em qualquer ponto do ciclo de vida

- **Ataque**
  - Uma série de ações que levam à execução de atividades ilegais
  - Frequentemente exploram vulnerabilidades

- **Risco / Ameaça**
  - O dano resultante de um ataque

- **Defesa**
  - Conjunto de políticas, mecanismos e tecnologias com vista a:
    - Reduzir o número de vulnerabilidades
    - Detetar ataques passados, atuais ou futuros
    - Reduzir o risco para os sistemas

Aplicado ao desenvolvimento de produtos



O desenvolvimento de projetos é uma tarefa complexa, cruzando vários domínios de conhecimento, várias equipas, incentivos e experiência nem sempre alinhados.
As vulnerabilidades podem ser introduzidas em qualquer ponto.

Riscos da Segurança

- **Informação, tempo e recursos (dinheiro)**
  - Destruição ou alteração de informação
- **Confidencialidade**
  - Acesso não autorizado a informação
- **Privacidade**
  - Recolha não autorizada de informação pessoal
  - Armazenamento (ou distribuição) desta informação
- **Disponibilidade de recursos**
  - Disrupção de sistemas, comunicações ou processos
- **Impersonificação**
  - Exploração não autorizada de perfis de identidade
    - Relacionado com pessoas, serviços, entidades

Principais fontes de Vulnerabilidades

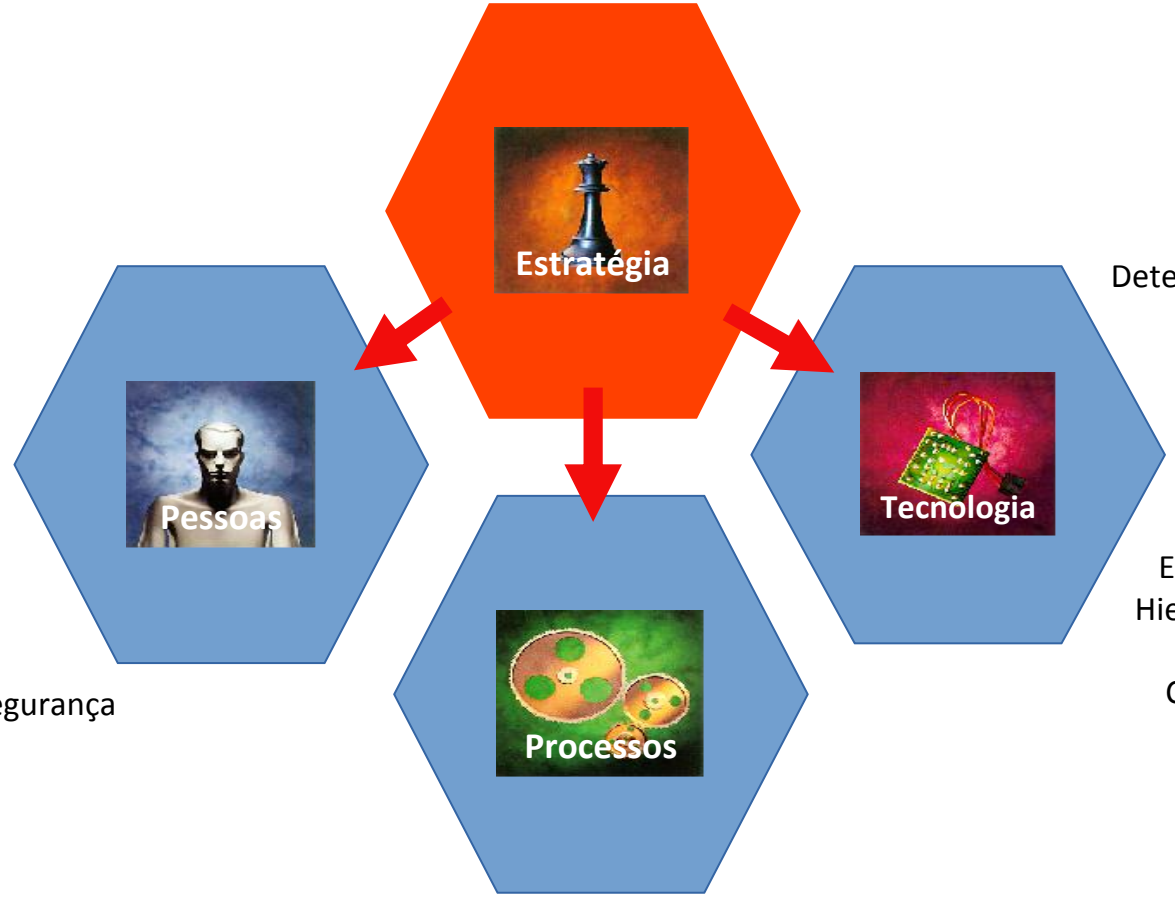
- **Aplicações hostis ou erros em aplicações**
  - Root kits: Inserem elementos no Sistema Operativo
  - Worms: Programas controlados por um atacante
  - Vírus: Código executável p/ infetar ficheiros (ex, Macros)

- **Usuários**
  - Ignorantes e descuidados
  - ... telnet vs ssh, FTP vs FTPS, IMAP vs IMAPS, HTTP vs HTTPS
  - Falsa noção de segurança (ex: tenho um anti-vírus, estou protegido)
  - Hostis

- **Administração deficiente**
  - A configuração por omissão raramente é a mais segura
  - Restrições de Segurança vs Operações Flexíveis
  - Exceções a indivíduos

- **Comunicações sobre ligações não controladas/conhecidas**

Dimensões a considerar



Seleção
Treino
Sensibilização
Organização da segurança

Deteção de Vulnerabilidades
Firewalls
Autenticação
Controlo de Acesso
Registos Auditáveis
Criptografia
Assinaturas Digitais
Entidades de Certificação
Hierarquias de Certificação
Deteção de ataques
Controlos de integridade

Políticas de segurança
Procedimentos administrativos de segurança
Procedimentos de auditoria e resposta a incidentes

Políticas de Segurança

Conjunto de orientações relativas à segurança que regem um domínio

- **Organização possui uma hierarquia de políticas**
  - Aplicáveis a cada domínio particular
  - Podem existir sobreposições (ex, hierarquias)
  - Podem possuir âmbitos e níveis de abstração distintos
- **Devem ser coerentes entre si**

Políticas de Segurança

- **Definem o poder de cada sujeito**
  - princípio do privilégio mínimo; Hardening
- **Definem os procedimentos de segurança**
  - quem faz o quê e quando
- **Definem requisitos mínimos de seg. dos sistemas**
  - Níveis de segurança, Grupos de segurança
  - Autorizações e autenticação correspondentes (fraca/forte, simples/multifatorial, remota/presencial)
- **Definem a estratégias de defesa e de resposta**
  - Arquitetura defensiva
  - Monitoria de atividades críticas/deteção de sinais de ataques
  - Reação a ataques ou outras disrupções
- **Definem o que é correto e incorreto (legal/ilegal)**
  - Modelo de lista negra: Tudo o que não é proibido é permitido
  - Modelo de lista branca: Tudo o que não é permitido é proibido

Mecanismos de Segurança

- **Mecanismos implementam políticas**
  - Enquanto políticas defines as orientações
  - Mecanismos tornam as políticas efetivas
- **Mecanismos de segurança genéricos:**
  - Confinamento
  - Autenticação
  - Controlo de acesso
  - Execução Privilegiada
  - Filtragem
  - Registo
  - Algoritmos e protocolos criptográficos
  - Auditorias

Níveis de Segurança

- **Definido por:**
  - Políticas de segurança existentes
  - Correção e efetividade da sua especificação/ implementação
- **Critério de Avaliação (NCSC TCSEC, Orange Book)**
  - Classes: D, C (1, 2), B (1, 2, 3) e A (1)
  - D: Inseguro
  - A1: mais seguro
    - Políticas de proteção existentes e dispendiosas
    - Procedimentos formais de validação da especificação
    - Controlo rigoroso da implementação
- **Critério de Avaliação ITSEC**
  - Níveis E1 até E6
  - Nível de especificação formal e correção da implementação

NCSC TCSEC Nível C

- **C1 – Discretionary Security Protection**
  - Identificação e Autenticação
  - Separação de utilizadores e dados
  - Controlo de acesso discricionário (DAC), capaz de aplicar limites de acesso por utilizador
  - Necessário existir documentação do sistema e manuais

- **C2 – Controlled Access Protection**
  - DAC com mais detalhe
  - Rastreio individual das ações através de mecanismos de login
  - Registos para auditorias
  - Limpeza de objetos ao serem re-usados (Object Reuse)
  - Isolamento de recursos

NCSC TCSEC Nível C

- **Política de Object Reuse**
  - All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects.
  - No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system."

- **Storage object:** An object that supports both read and write accesses.

Políticas de Segurança em Sistemas Distribuídos (SD)

Tem de englobar múltiplos sistemas e redes

- **Domínios de segurança:**
  - Definição de um conjunto de sistemas e rede
  - Definição de um conjunto de usuários aceites/autorizados
  - Definição de um conjunto de atividades aceites/não aceites
- **Gateways de segurança**
  - Definição das interações de entrada e saída de um domínio

Políticas de Segurança em SD

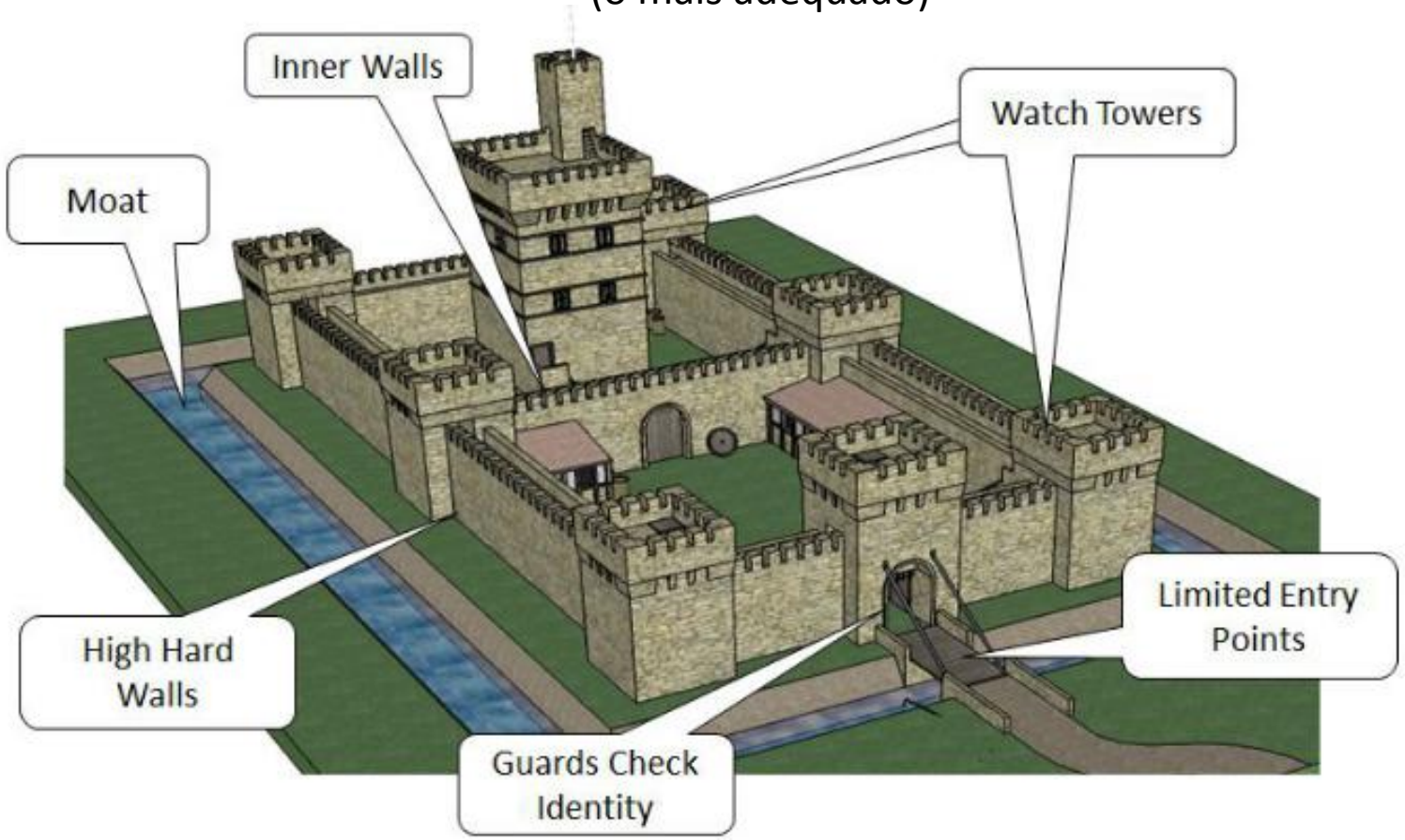
Defesa em perímetro

(mínimo aconselhado mas insuficiente)

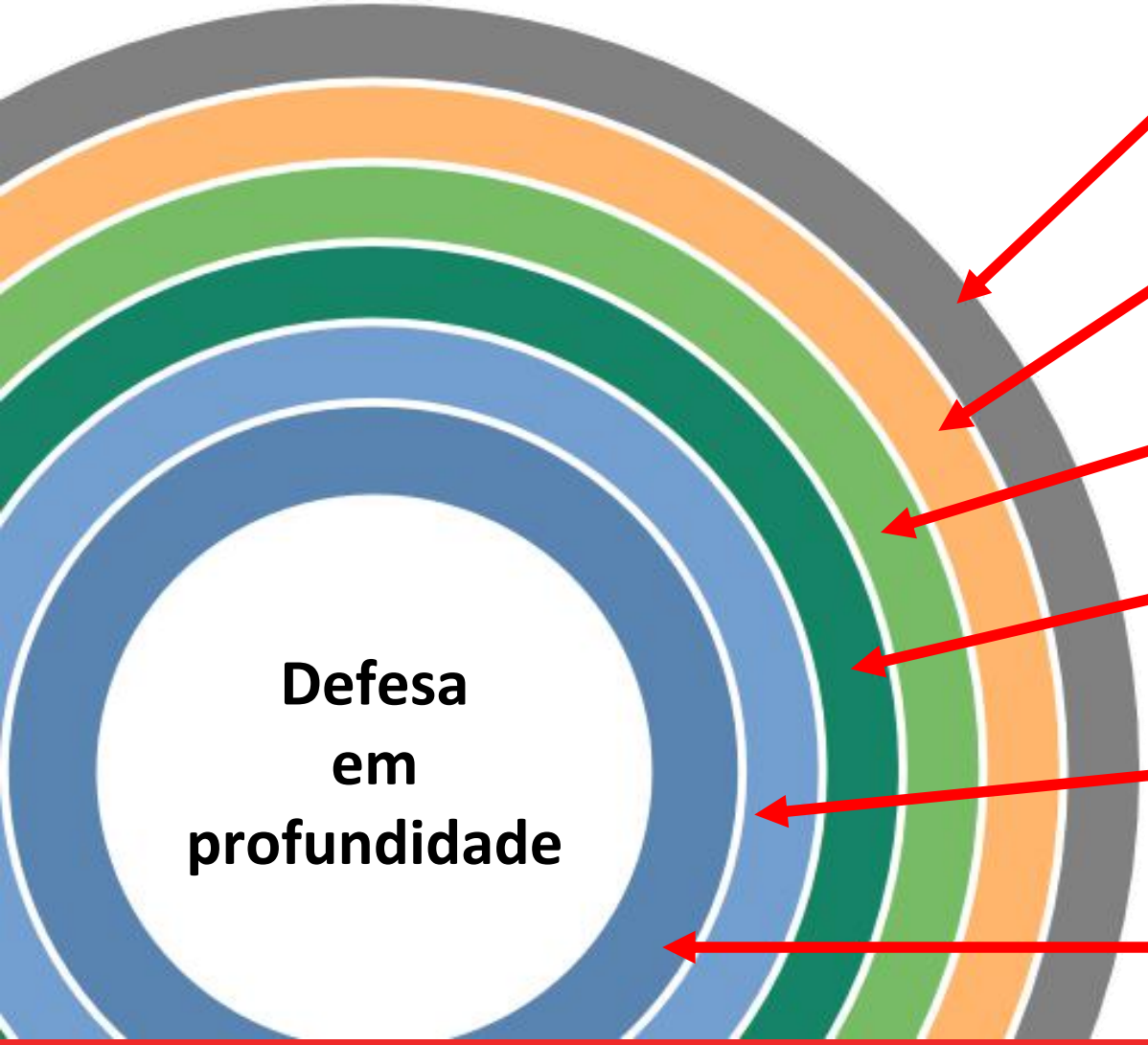
Políticas de Segurança em SD

Defesa em profundidade

(o mais adequado)



Políticas de Segurança em SD



Políticas, procedimentos, sensibilização

Infraestrutura Física

Infraestrutura de Rede

Servidores físicos

Aplicações e Serviços

Gestão de informação

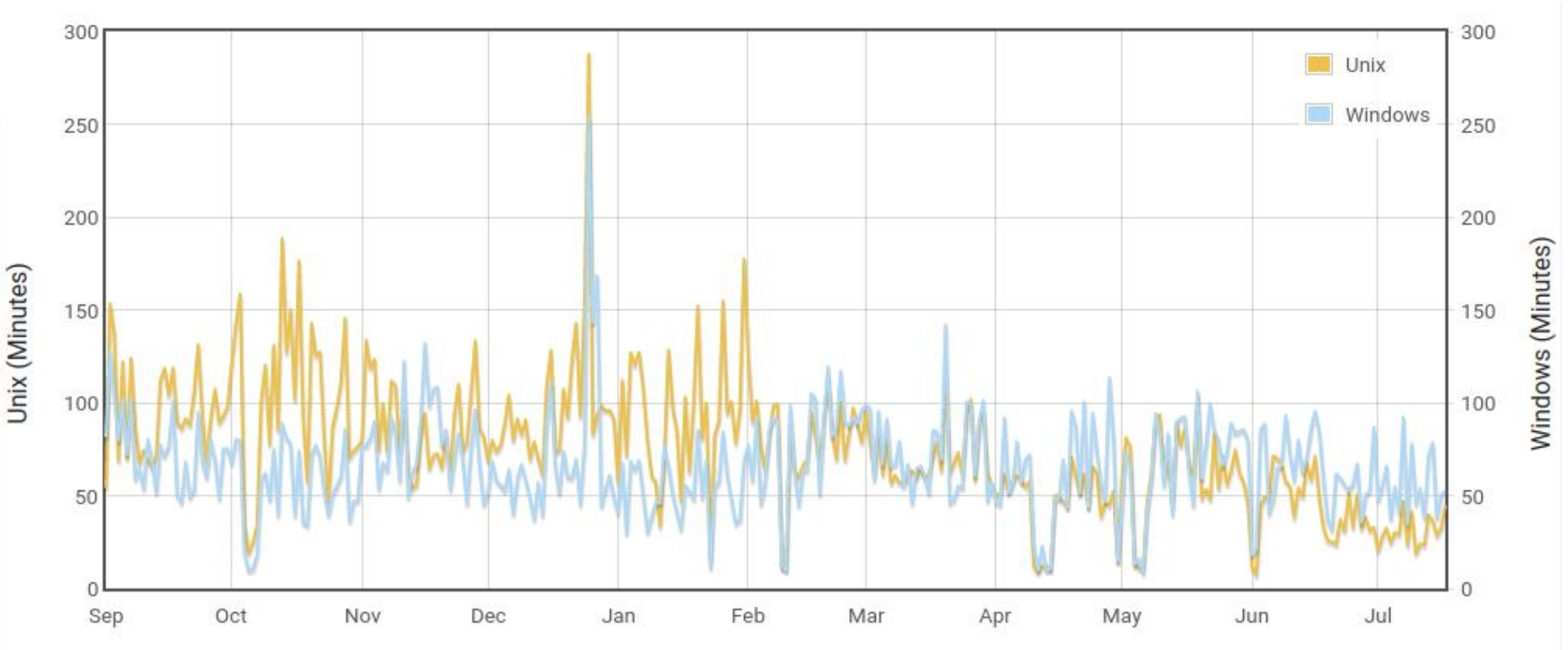
Políticas de Segurança em SD

- **Ataques específicos**
  - Concebidos para um sistema/rede particulares
  - Idealizados e concebidos em tempo real
  - Por especialistas (red-teams, OFFSEC)

- **Ataques genéricos/autónomos**
  - Explorando vulnerabilidades conhecidas/comuns
  - Implementadas para muitos sistemas
  - Afetam o tempo médio de sobrevivência:
    - Duração entre dois ataques automáticos consecutivos
    - Existe uma rede de sensores de rede a calcular isto
  - Executados por profissionais, curiosos, estudantes, ...

Mean Survival Time

(http://isc.sans.org/survivaltime.html)



Mecanismos de Segurança para SD

- **Sistemas Operativos Confiáveis**
  - Níveis de segurança, certificação
  - Ambientes de execução segura
  - Sandboxes / Máquinas Virtuais
- **Firewalls e Sistemas de segurança**
  - Controlo de tráfego entre redes
  - Monitorização (carga de tráfego, comportamento…)
- **Comunicações Seguras / VPNs**
  - Canais seguros sobre redes públicas / inseguras
  - Extensão segura das redes da organização

Mecanismos de Segurança para SD

- **Autenticação**
  - Local
  - Remota (sobre a rede)
  - Single Sign-On
  - Segredos, Tokens, biometria, dispositivos, localização
- **Entidades de Certificação /PKI**
  - Gestão de chaves públicas e certificados
- **Cifra de ficheiros e dados em sessões**
  - Privacidade/confidencialidade de dados transmitidos
  - Privacidade/confidencialidade de dados armazenados

Mecanismos de Segurança para SD

- **Deteção de intrusões**
  - Deteção de atividades proibidas ou anómalas
  - Baseado na rede / baseado nos sistemas
- **Inventariação de vulnerabilidades**
  - Pesquisa para resolução de problemas ou exploração
  - Baseado na rede / baseado no sistemas
- **Testes de Penetração**
  - Avaliação das vulnerabilidades
  - Demonstração de tentativas de penetração
  - Teste de mecanismos de segurança instalados
  - Determinação da existência de políticas de segurança mal aplicadas

Mecanismos de Segurança para SD

- **Monitorização de conteúdos**
  - Deteção de vírus, Worms e outras ciber-pragas
- **Administração da segurança**
  - Desenvolvimento de políticas de segurança
  - Aplicação das políticas de forma distribuída
  - Co-administração / contratação de equipas externas
- **Resposta a Incidentes / Seguimento em Tempo Real**
  - Capacidade para detetar e reagir a incidentes em tempo real
  - Meios para resposta rápida e efetiva a incidentes