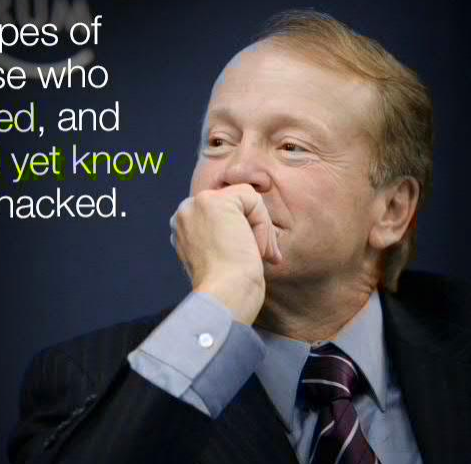


CIBER SEGURANÇA – GESTÃO DE AMEAÇAS

There are two types of
companies: those who
have been hacked, and
those who don't yet know
they have been hacked.

John Chambers
Chief Executive Officer of Cisco



Evolução da Segurança da Informação

- Evolução dos Sistemas Informáticos (≈60 anos)
 - Poucos Centros de Computação isolados
 - Sistema em *time-share*
 - As redes de comunicação de dados (sistemas distribuídos)
 - A computação pessoal
 - A computação ubíqua e a convergência de tecnologias



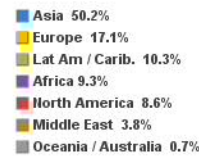
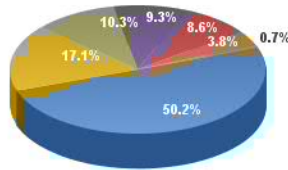
Complexidade: tecnológica



Complexidade: redes sociais

- Estatísticas sobre a Internet

World Regions	Population (2017 Est.)	Population % of World	Internet Users 31 Mar 2017	Penetration Rate (% Pop.)	Growth 2000-2017	Users % Table
Africa	1,246,504,865	16.6 %	345,676,501	27.7 %	7,557.2%	9.3 %
Asia	4,148,177,672	55.2 %	1,873,856,654	45.2 %	1,539.4%	50.2 %
Europe	822,710,362	10.9 %	636,971,824	77.4 %	506.1%	17.1 %
Latin America / Caribbean	647,604,645	8.6 %	385,919,382	59.6 %	2,035.8%	10.3 %
Middle East	250,327,574	3.3 %	141,931,765	56.7 %	4,220.9%	3.8 %
North America	363,224,006	4.8 %	320,068,243	88.1 %	196.1%	8.6 %
Oceania / Australia	40,479,846	0.5 %	27,549,054	68.1 %	261.5%	0.7 %
WORLD TOTAL	7,519,028,970	100.0 %	3,731,973,423	49.6 %	933.8%	100.0 %

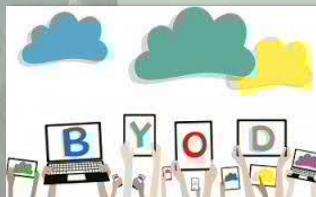


[//www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)

Tecnologias disruptivas



Cloud Computing



Threat Landscape

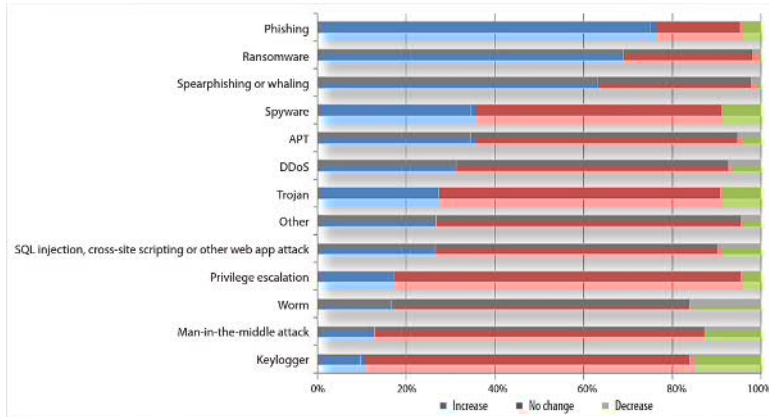


Figure 5. Phishing, Ransomware, Spearphishing Most on the Rise

[Exploits at the Endpoint: SANS 2016 Threat Landscape Survey](#)

Key Findings

How Attackers Get into User Endpoints

75% of identified, impactful threats initially entered via email attachment

46% of attacks were executed by users clicking web links in email

41% also experienced attacks involving web drive-by or downloads

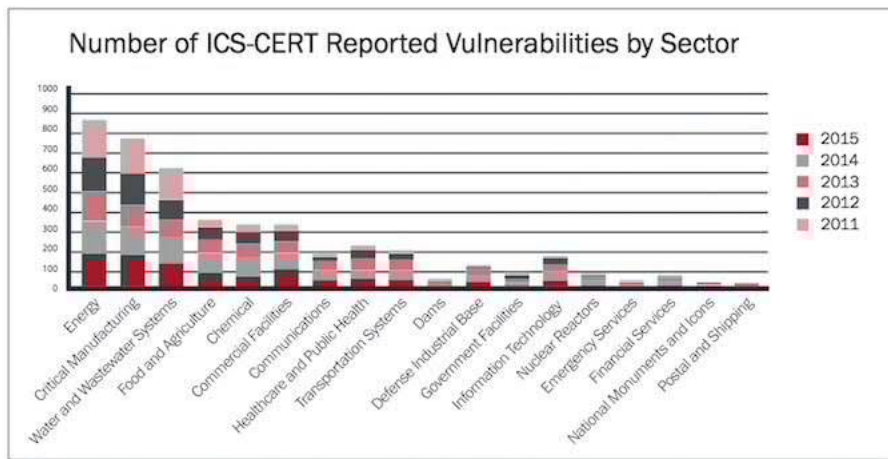
How Attackers Bypass Endpoint Defenses

48% through user error

38% through social engineering

37% through zero-day/unknown

Vulnerabilidades



<http://securityaffairs.co/wordpress/51891/reports/annual-vulnerability-coordination-report.html>

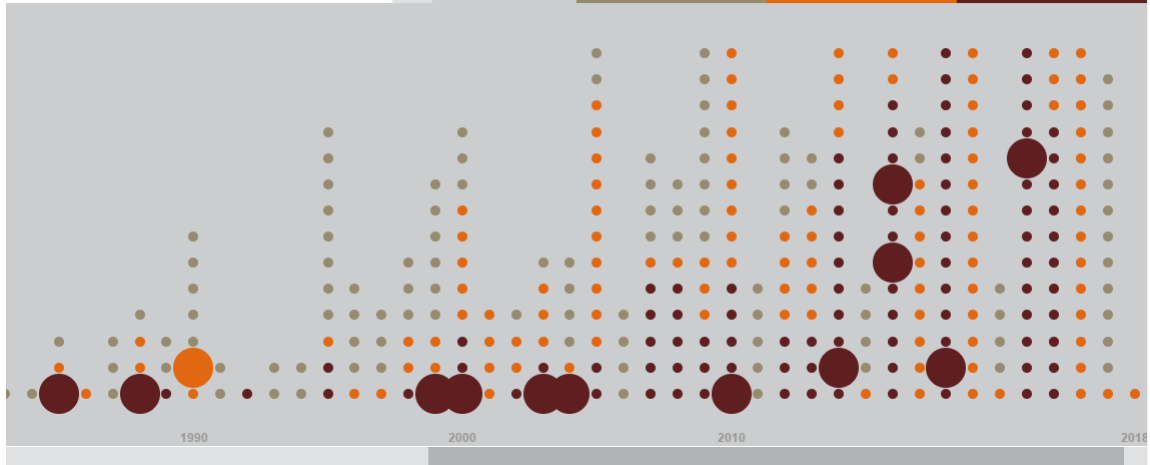
Malware: From benign virus to damaging code



Technology advances

Regulation, legislation
and policy

Incidents and threats


<https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>

Henrique Santos DSI/UMinho – Maio 2017

alphacam

vero

HEXAGON

How governments are advancing cyberthreat in...



Technology advances

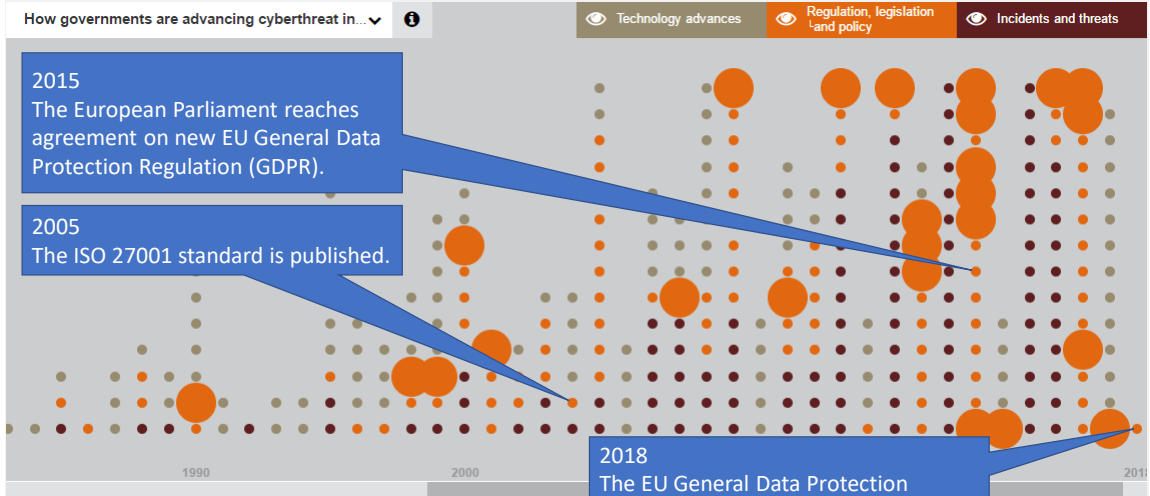
Regulation, legislation
and policy

Incidents and threats

2015
The European Parliament reaches
agreement on new EU General Data
Protection Regulation (GDPR).

2005
The ISO 27001 standard is published.

2018
The EU General Data Protection
Regulation scheduled to go into effect.


<https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>

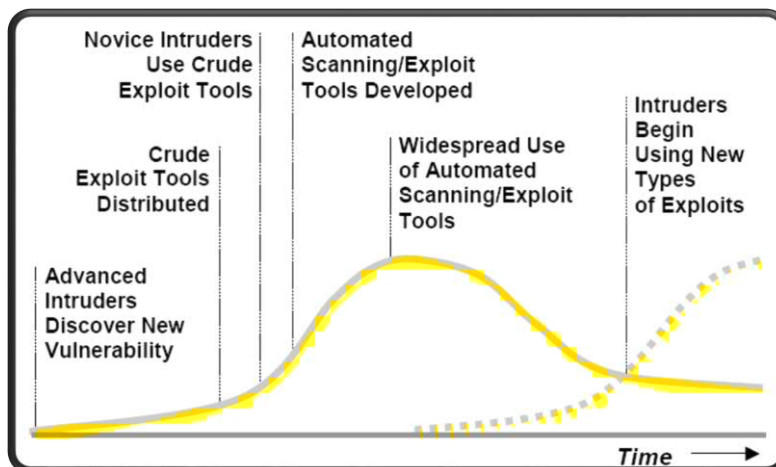
Henrique Santos DSI/UMinho – Maio 2017

alphacam

vero

HEXAGON

Ciclo de exploração de vulnerabilidades



Fonte: H.F. Lipson, CERT Coordination Center, CMU/DEI-2002-SR-009

Reações

- Em 2009 o presidente os EUA, Barak Obama, declara a "infra-estrutura digital" Americana como um **recurso crítico**
- Em Maio de 2010 o Pentágono cria o *Cyber Command* (Cybercom), dirigido pelo General Keith Alexander, director da NSA

*"[...] direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, **conduct full spectrum military cyberspace operations** in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."*
- O Reino Unido criou também uma unidade especial, sediada no *Government Communications Headquarters* (GCHQ)
- Outros países assumem idêntica estratégia (Irão, Coreia do Norte, Rússia e China – segundo relatórios dos EUA)

Fundamentos

- **Segurança** é uma “medida” de confiabilidade (**qualidade de um sistema que nos permite confiar, de uma forma justificada, no seu serviço**) no que respeita a falhas que afetam a integridade, confidencialidade e disponibilidade (...) do sistema
- **Falhas**, (neste contexto) são manifestações para o exterior de erros internos do sistema (desvios do especificado)
- **Recurso**, qualquer bem ou ativo que tem valor para a organização

Fundamentos

- **Evento de SegInfo**, é a ocorrência num sistema, serviço ou rede, de um estado identificado que reflete:
 - Uma possível violação de uma política de SegInfo;
 - Uma falha numa defesa; ou
 - Uma situação desconhecida, relevante para a SegInfo
- **Incidente de SegInfo**, é a ocorrência de um ou mais eventos de SegInfo indesejáveis, com uma probabilidade significativa de comprometer a operação da organização

Fundamentos

- **Controlo de SegInfo**, é a forma de gerir o **risco**, incluindo **políticas, procedimentos, guias, boas práticas**, ou ainda **estruturas organizacionais**, que podem ser de natureza **administrativa, técnica, legal**, ou de **gestão** – por vezes também referido como contramedida, ou salvaguarda.
- **Risco**, é o efeito da incerteza nos objetivos
 - Efeito é o desvio relativamente ao que é esperado (negativo ou positivo)
 - Incerteza é o estado (mesmo que parcial) de falta de informação, compreensão ou conhecimento, relacionado com um evento, as suas consequências, ou a sua probabilidade

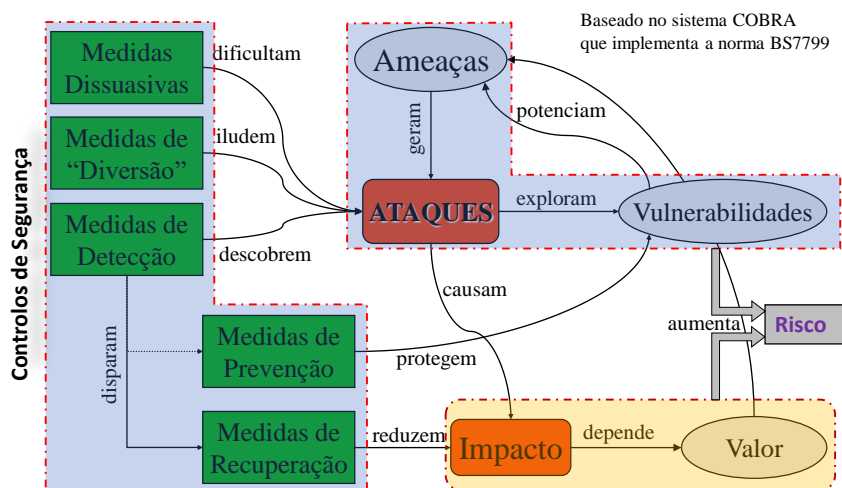
Perceção do Risco

- **Risco**
 - Quantificado...
Probabilidade x Valor
 - Qualificado...
Alto, Médio, Baixo, ...
- Não é o mesmo para todos nós!

Qual o limite
aceitável?
“**Confiança**”



Modelo para SegInfo



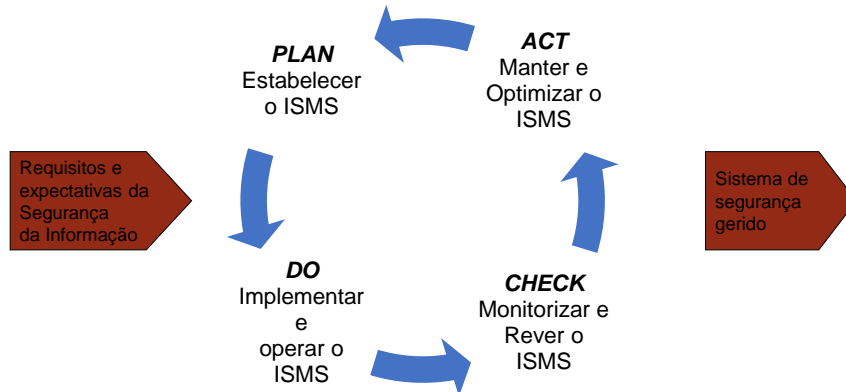
"Management is the process of achieving objectives using a given set of resources"

in Whitman, Management of Information Security, p9

Nesta perspectiva a Segurança da Informação é uma actividade de Gestão 😊

Gestão da SegInfo

- Assente no modelo de processo PDCA (ISO/IEC 27000/1 – estabelecimento e gestão de um ISMS)



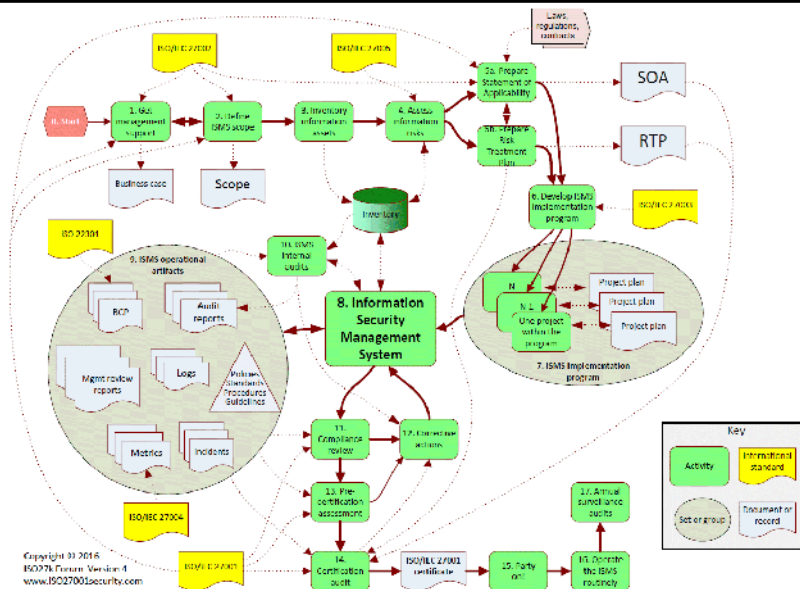
Henrique Santos DSI/UMinho – Maio 2017

alphacam

vero
software

Part of
HEXAGON

ISMS (27k) –
certificação
(vista geral)



Copyright © 2016
ISO27k Forum Version 4
www.iso27001security.com

Henrique Santos DSI/UMinho – Maio 2017

alphacam

vero
Software


 Part of **HEXAGON**

Controlos de SegInfo

- Política de segurança
 - Recursos que são o foco da segurança e o que se deve garantir
- Políticas ou procedimentos em uso:
 - Política de gestão de *passwords* – 74%
 - Política formal para o uso inapropriado – 71%
 - Política de educação e consciencialização – 67%
 - Monitorização de ligações à Internet – 65%
 - Política de Segurança corporativa – 62%
 - Práticas de gestão do risco – ≈ 55%
 - ...
 - Contratação de *ex-hackers* – 14%

Fonte: E-Crime Watch Survey – CSO magazine

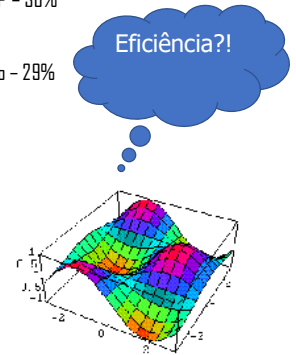
Tecnologias de SegInfo

- Primeira linha de defesa (L1): Gestão e planeamento da infra estrutura (incluindo Controlo de Acesso)
- Segunda linha de defesa (L2): Filtragem (*firewalls*)
- Terceira linha de defesa (L3): monitorização e deteção de intrusões
- Quarta linha de defesa (L4): criptografia...
- Quinta linha de defesa (L5): utilizadores



Tecnologias de SegInfo mais usadas:

- Anti-Vírus – 97%
- *Firewalls* – 94%
- Virtual Private Network (VPN) – 85%
- Anti-Spyware/Adware – 80%
- *Cifra (dados em trânsito) – 71% (↑)*
- Detecção de Intrusões (IDS) – 69%
- Ferramentas para gestão de vulnerabilidades e *patch* – 65%
- Filtragem web/URL – 61%
- *Firewalls ao nível da aplicação – 53% (↑)*
- ...
- PKI – 36%
- Smart cards e outros dispositivos para OTP – 36%
- *Soluções NAC integradas – 34% (↑)*
- Ferramentas específicas para virtualização – 29%
- *Específico wireless – 27% (↓)*
- Biometrias – 23%



Fonte: CSI Computer Crime & Security Survey

Tecnologias de SegInfo mais eficazes

- *Firewalls – 68%*
- *Anti-Vírus – 66%*
- *Cifra – 58%*
- *Autenticação por duas fases – 56%*
- *Detecção de Intrusões (IDS) – 50%*
- Segurança física – 49%
- Monitorização de tráfego – 46%
- Spyware/Adware – 43%
- ...
- Actualizações manuais – *26%*



Fonte: E-Crime Watch Survey – CSO magazine

Métricas

- **Medir o desempenho da SegInfo é fundamental.** Uma boa **métrica** para a função SegInfo deve procurar responder a questões como:
 - Qual a eficiência do meu processo de segurança?
 - Estou mais seguro do que estava há 1 ano atrás?
 - **Qual o meu nível de segurança face aos meus pares?**
 - O nível de investimento é adequado?
 - Quais são as minhas opções para gerir o risco?

4 Princípios básicos (Pfleeger)

- Princípio do ponto de penetração mais fácil
 - **Nem sempre óbvio ou espectável... mas mais fácil**
- Princípio do elo mais fraco
 - **A segurança é tão forte quanto o seu elo mais fraco**
- Princípio da proteção adequada
 - **Proteger os recursos até um grau consistente com o seu valor**
- Princípio da efetivação
 - **Controlos devem ser eficientes, "fáceis de usar", apropriados e... utilizados 😞**

Obrigado pela vossa atenção.
Questões?

