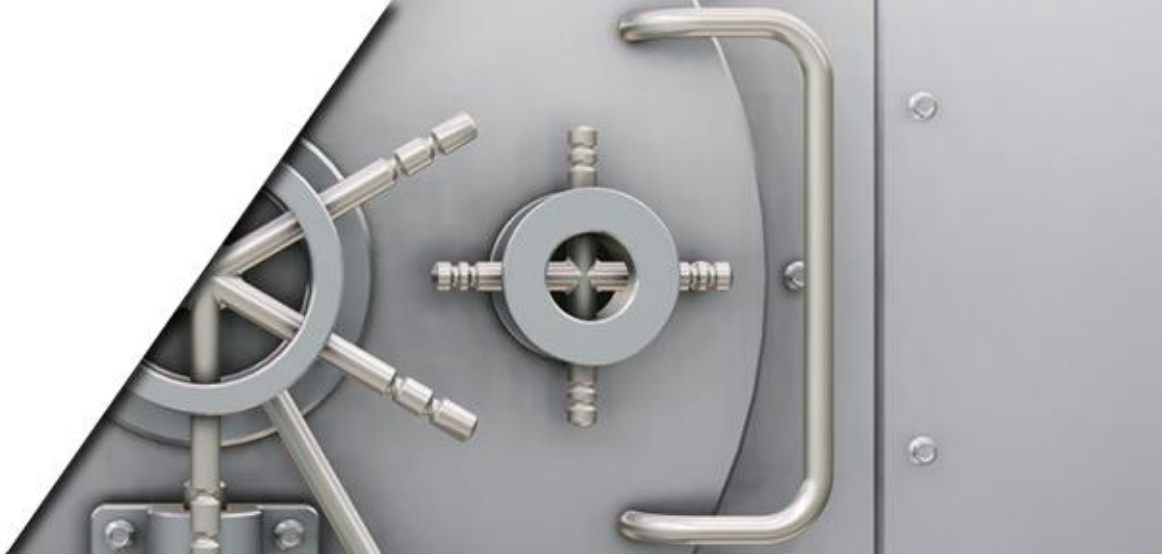
Associação Portuguesa para a Promoção da Segurança da Informação



Segurança da Informação
Desafios para o Diretor de Segurança

Jorge Pinto

Outubro 2016

proteger 2016
5ª CONFERÊNCIA DE SEGURANÇA

APSEI
ASSOCIAÇÃO PORTUGUESA DE SEGURANÇA

18 A 20 DE OUTUBRO
CENTRO DE CONGRESSOS DO ESTORIL

Apresentação – A AP2SI

- A AP2SI – Associação Portuguesa para a Promoção da Segurança da Informação é uma associação de direito próprio sem fins lucrativos criada em 2012, cujo objetivo é aumentar a consciencialização em Portugal para as questões da segurança da informação através da promoção de boas práticas, eventos de divulgação, conferências, entre outros.

- A AP2SI caracteriza-se por:
  - Abertura, podendo ser membros qualquer indivíduo interessados em participar nos fins propostos;
  - Enfoque, pela dedicação exclusiva ao seu objeto e missão;
  - Não concorrência com o mercado, pela ausência de pretensão de prestação de serviços;
  - Total independência, pela dissociação institucional e estatutária relativamente a organizações (comerciais ou outras), nacionais ou internacionais e pela autonomia financeira que manterá.

Mês Europeu da Ciber-segurança

- O Mês Europeu da Cibersegurança, que ocorre em Outubro, é uma iniciativa da União Europeia dinamizada pela ENISA (agência europeia para a segurança das redes e informação) que visa:
  - promover o tema da cibersegurança nos cidadãos europeus através de eventos, cursos, partilha de boas práticas entre outras iniciativas;
  - gerar conhecimento específico sobre Segurança nas Redes e Informação;
  - promover a utilização mais segura da Internet para todos;
  - aumentar o interesse dos *media* nacionais através da dimensão europeia e global do projeto;
  - melhorar a atenção e interesse no que diz respeito à segurança da informação.

MÊS EUROPEU DA CIBER-SEGURANÇA

STOP | THINK | CONNECT™

Desafios

Presidenciais EUA 2016

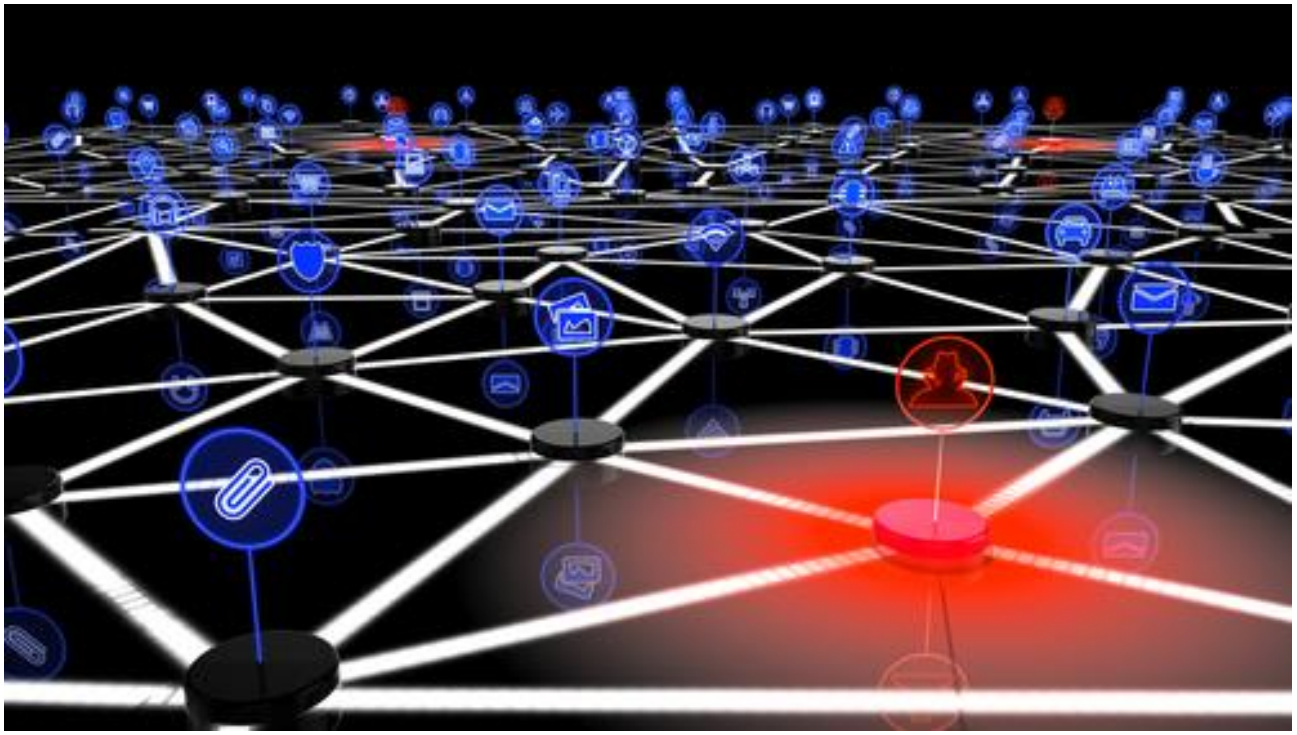
Presidential Debate Highlights | Clinton, Trump Debate Cybersecurity, Hacks

https://youtu.be/R9GSJUAuFfE

Yahoo – 500 Milhões de contas

http://www.express.co.uk/life-style/science-technology/713216/Yahoo-Confirm-MASSIVE-Data-Breach-200-Accounts-Hack

Botnet câmaras IP / DVR



Mais de 140,000 dispositivos comprometidos geraram cerca de 1,5 Terabytes por segundo

http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html

Desafios externos

- Atividades realizadas ou patrocinadas por atores estatais*
  - GhostNet, Red October e Stuxnet
    - http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/
    - http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide
    - http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
  - Mandiant Report sobre unidade chinesa de espionagem no ciberespaço
    - https://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/
  - Caso Snowden (agora em filme também)
    - http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
  - Ataques a SCI
    - https://www.wired.com/2015/01/german-steel-mill-hack-destruction/**

- ou não! Crime organizado e indivíduos também utilizam as mesmas ferramentas

** autoria não atribuída

Desafios externos

- Falhas de desenho generalizadas
  - Internet das Coisas
    - https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/
    - https://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/
    - https://www.rsaconference.com/writable/presentations/file_upload/ht-r08-how-hackers-are-outsmarting-smart-tvs-and-why-it-matters-to-you_copy1.pdf
  - Car Hacking
    - https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/
    - https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
  - Programas e aplicações
    - http://www.darkreading.com/vulnerabilities---threats/the-10-worst-vulnerabilities-of-the-last-10-years/d/d-id/1325425

- Crime organizado
  - Internet Organised Crime Threat Assessment
    - https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016
  - Silk Road
    - https://www.wired.com/2015/04/silk-road-1/

Desafios externos

- Hacktivismo
  - Anonymous
    - http://www.theguardian.com/world/2015/apr/07/anonymous-international-hackers-kremlin
  - Greenpeace - Let's go! Artic
    - http://arcticready.com/arctic (desligado)
      - http://www.luerzersarchive.com/en/features/digital/greenpeace-parodies-shell-with-arctic-ready-campaign-153.html
- Cadeia de fornecimento
  - Aplicações, sistemas e dispositivos
    - http://qz.com/213398/the-escalating-us-china-spying-war-is-mckinseys-loss-and-huaweis-gain/
  - Fornecedores externos / outsourcing / auditorias
    - http://www.bankinfosecurity.com/did-regulator-cause-data-breach-a-7685/op-1

Desafios externos

- Extração e publicação de informação
  - Yahoo (500 Milhões de contas)
    - http://arstechnica.com/business/2016/10/after-yahoo-data-breach-verizon-hints-that-it-could-pull-out-of-4-83b-deal/
  - Ashley Madison (36 milhões de contas)
    - http://www.theguardian.com/world/2015/apr/07/anonymous-international-hackers-kremlin
  - Target (dados financeiros de 40 milhões de cartões de crédito)
    - http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/
  - Panama Papers, Bahamas Leaks, Swiss Leaks, etc….
    - https://www.icij.org

- Legislação / Regulamentação
  - TJUE considera Safe Harbor inválido
    - http://www.computerworld.com.pt/2015/10/06/tuje-considera-safe-harbour-invalido/
  - Nova legislação europeia relativa à proteção de dados pessoais
    - http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN
  - Diretiva de Segurança em Redes
    - http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Desafios internos

- Organização, políticas, processos e procedimentos
  - Estrutura de segurança bem definida com responsabilidades claras
  - Documentação clara, aplicável e identificando ações monitorizáveis,
  - Com o compromisso e suporte da gestão de topo.
  - Relacionamento com a organização

- Controlo de acessos:
  - Para pessoas e aplicações
  - Alinhado com o tipo de informação que é acedido
  - Eficaz e tempestivo
  - Com geração de registos de históricos

- Monitorização e alarmística
  - Focada na deteção e reação rápida
  - Com suporte de *intelligence*

Desafios internos

- Auditoria interna
  - Assegurar formação e conhecimento necessários para criar valor
  - Assegurar a periodicidade das ações e alinhamento com referenciais. P.ex.:
    - Cobit (http://www.isaca.org/COBIT/Pages/COBIT-5-portuguese.aspx)
    - NP ISO/IEC 27001:2013 (http://www1.ipq.pt/PT/site/clientes/pages/Norma.aspx?docId=IPQDOC-185-107346)

- Novas formas de trabalhar a informação
  - Big Data
  - Cloud computing

- *Gap* geracional e aplicação de novos paradigmas
  - *Bring Your Own Device*
  - *Always on, everywhere*
  - *Internet of Things / Internet of Everything*

Desafios internos

- Segurança em dispositivos (cada vez mais) móveis
  - Tablets
  - Smartphones
  - Proteção das aplicações nestes dispositivos
  - Frigoríficos (http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/)
  - Ferros de engomar e chaleiras (http://www.ibtimes.com/russia-accuses-china-spying-imported-tea-kettles-irons-1450390)

- Reporte e comunicação
  - Conciso e claro com indicação de tendências
  - Com indicadores de *performance** (KPI) e risco (KRI) alinhados com orgãos de gestão. **Se não medimos não gerimos**.
  - Revisão periódica do reporte, alinhada com as alterações organizacionais ou do ambiente onde a organização desenvolve a actividade
  - Assegurar interação constante com partes interessadas relevantes (internas ou externas)

* *Performance* neste contexto relaciona-se com os objectivos da segurança e qual a eficiência e eficácia no seu atingimento

Desafios Internos

- Privacidade e proteção de dados pessoais
  - Conhecer as orientações da CNPD
  - Implementar mecanismos de proteção de dados pessoais que assegurem a privacidade das várias partes interessadas e garanta o cumprimento da legislação
  - Preparar a organização para os desafios futuros
  - Leitura:
    - http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52012DC0009&from=pt
    - http://tek.sapo.pt/noticias/computadores/cnpd_ha_um_numero_excessivo_de_elementos_exte_1436243.html
    - http://www.cnpd.pt/bin/decisoes/Delib/20_569_2015.pdf
    - http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN

- Preparar a organização para QUANDO algo acontecer
  - Educação, formação e sensibilização de todas as partes interessadas
  - Exercícios periódicos com o envolvimento de todas as partes interessadas
  - Respostas padrão alinhadas com cenários discutidos com o orgão de gestão

Recomendações finais

Recomendações finais (1/2)

- Assegurar a realização de auditorias às redes da empresa. Tenham conhecimento dos relatórios e saibam onde estão os equipamentos e redes de comunicações

- Assegurar a realização de auditorias periódicas aos equipamentos de segurança (redes IP de suporte a CCTV, controlo de acessos, intrusão, alarmística). Pressionem os fornecedores e a informática para correcção das falhas encontradas (porque elas existirão)

- Assegurar que a arquitectura de sistemas de informação de suporte à vossa actividades está definida e desenhada. Ter um plano de contingência para falha destes equipamentos

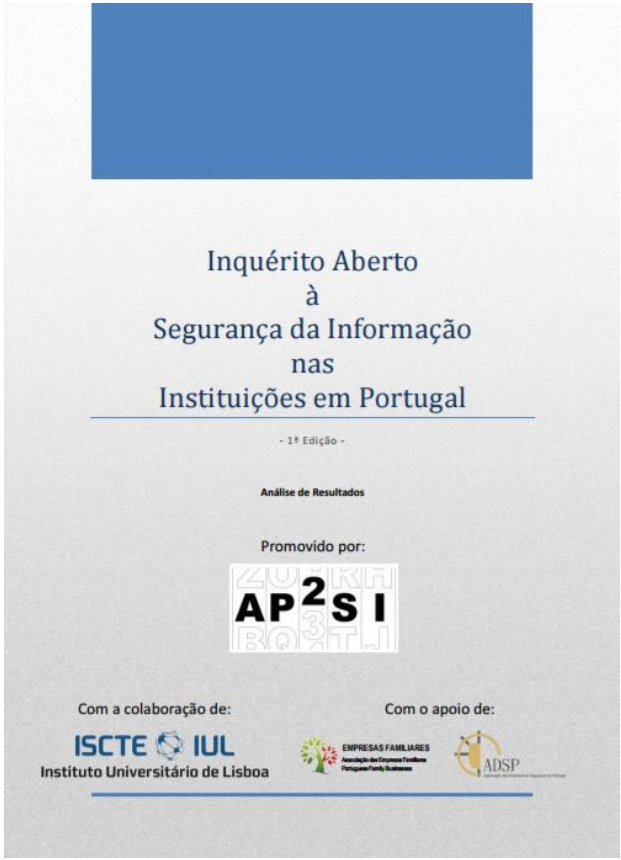
- Saibam onde estão os documentos das vossas infra-estruturas (*e dos vossos clientes*)

Recomendações finais (2/2)

- Atenção à informação que é disponibilizada pela vossa empresa na internet (nas redes sociais, nos comunicados de imprensa, entre outros)
- Utilizar práticas de *Intelligence* em benefício próprio
- Vistorias de segurança física aos computadores da organização
- Implementar uma política de mesa limpa.
- Os *smartphones/tablets* são computadores que permitem fazer chamadas e podem ser comprometidos como qualquer outro dispositivo.
- Adquiram a NP ISO/IEC 27001:2013 (*http://www.ipq.pt*)

Alguma literatura

- I Inquérito Aberto à Segurança da Informação nas Instituições em Portugal – https://ap2si.org/inquerito



Obrigado pelo vosso tempo

Questões?

Contactos

https:// ap2si.org

https://twitter.com/ap2si

geral@ap2si.org

https://facebook.com/ap2si

jorge.pinto@ap2si.org

https://linkedin.com/company/ap2si