AP2SI

Associação Portuguesa
para a Promoção da
Segurança da Informação

Cibersegurança no Ambiente Escolar

Paulo Morgado

27-02-2016

Encontro Nacional SeguraNet
“Faz a tua parte por uma Internet melhor”
Escola Superior de Educação de Santarém

About me …

- Paulo Morgado
- Pai
- Formação em Engenharia
- https://www.linkedin.com/in/paulo-morgado-8272199
- https://twitter.com/pauljorg
- Direção AP2SI
- 21 anos experiência IT, 16 dos quais em Segurança
- IBM Portugal - Security & Risk Management
- paulo.morgado@ap2si.org

Disclaimer

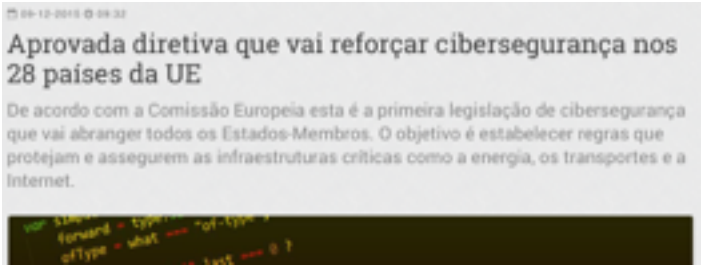
“Todas as opiniões expressas nesta apresentação são da responsabilidade estrita do autor e não refletem de forma alguma as posições da IBM Portuguesa.”

“O uso de material desta apresentação não necessitam de consentimento prévio do autor, mas agradece-se referência.”

Agenda

- Estado da ciber-“arte”
- Porquê ?
- Vectores de ataque ambiente educacional
- Como mitigar os riscos ? (ambiente escolar)
    - Pessoas / Processos / Tecnologia
- Exemplos
- Deep / Dark Web
- Conclusões

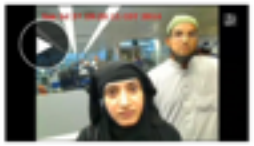
Estado da ciber-“arte”



Aprovada diretiva que vai reforçar cibersegurança nos 28 países da UE

De acordo com a Comissão Europeia esta é a primeira legislação de cibersegurança que vai abranger todos os Estados-Membros. O objetivo é estabelecer regras que protejam e assegurem as infraestruturas críticas como a energia, os transportes e a Internet.

http://tek.sapo.pt/noticias/internet/artigo/aprovada_diretiva_que_vai_reforcar_cibersegurança_nos_28_paises_da_ue-45344aox.html

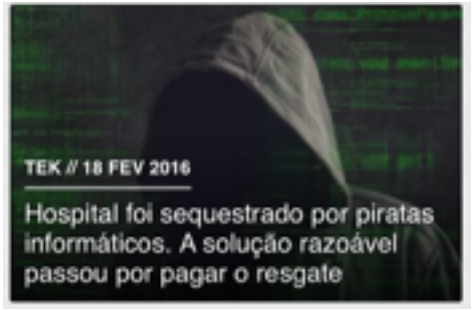


Apple recusa desbloquear iPhone de terrorista e alerta para implicações "arrepiantes"

ALEXANDRE MARTINS 17/02/2016

Empresa foi intimada a criar uma versão do seu sistema operativo para que o FBI possa vasculhar o telemóvel de um dos atiradores de San Bernardino. Mas avisa que esse programa poderia depois ser usado por organizações criminosas.

http://www.publico.pt/tecnologia/noticia/apple-desafia-ordem-de-tribunal-para-desbloquear-iphone-de-um-dos-atiradores-de-san-bernardino-1723566



http://tek.sapo.pt/noticias/computadores/artigo/hospital_foi_sequestrado_por_piratas_informaticos_a_solucao_razoavel_passou_por_-46276men.html

16-02-2016 10:25

Cibercriminalidade em segundo lugar nos crimes com mais inquéritos em Lisboa

http://tek.sapo.pt/noticias/computadores/artigo/cibercrime_em_segundo_lugar_na_investigacao_do_ministerio_publico_em_lisboa-46235xzo.html

Oito em cada dez jovens já bloquearam alguém na rede

INÊS MOREIRA CABRAL 21/01/2016

Estudo concluiu que os jovens portugueses têm um controlo activo das suas contas na Internet, e protegem os seus dados na rede: a maioria bloqueia desconhecidos e pede ajuda em situações sensíveis. Campanha de prevenção do Facebook arranca esta quinta-feira.

http://www.publico.pt/tecnologia/noticia/facebook-e-miudos-seguros-na-net-lancam-campanha-para-uso-responsavel-da-rede-1720888

12-02-2016 19:07

Polícia britânica terá detido hacker de 16 anos que entrou na conta de email do diretor da CIA

http://tek.sapo.pt/noticias/computadores/artigo/policia_britanica_tera_detido_hacker_de_16_anos_que_entrou_na_conta_de_email_do_-46209qjx.html

Ataque informático expõe dados de cinco milhões, incluindo crianças

PÚBLICO 01/12/2015

Base de dados de empresa de brinquedos electrónicos foi atacada e deixou expostas identidades e fotografias de menores.

http://www.publico.pt/tecnologia/noticia/ataque-informatico-expoe-dados-de-cinco-milhoes-de-pessoas-incluindo-criancas-1716139

Porquê ?

- Actualmente as nossas TI funcionam em rede
  - Não existem sistemas isolados, tudo está ligado a tudo (*IoT*)

- A Internet passou a ser uma *commodity* tal como a electricidade, a água, ou o carvão em séculos passados [(1)]
  - persistência: durabilidade de conteúdos *online*
  - visibilidade: maior potencial audiência alcançada
  - replicabilidade: facilidade da partilha de conteúdos
  - pesquisabilidade: possibilidade de encontrar conteúdos

- Falta de "ciber-literacia" dos utilizadores (escolares)
  - comportamento *online* diferente do comportamento físico
  - "esquecimento" de conceitos como Identidade/Privacidade
  - exposições elevadas aos perigos/ilegalidades digitais

Vectores de ataque ambiente educacional

- **Componente técnica:**
  - Várias redes informáticas escolares / universitárias (3)
  - "Computadores pessoais" estudantes / professores (*BYOD*)
  - Aplicações Web disponíveis 24x7x365
  - Sistemas de Controlo de Acessos Físicos / Lógicos
  - Sistemas de Video-Vigilância c/ tecnologia IP

Como se manifestam ?

- *Virus, Malware, Spyware, Adware, Ransomware, Botnets, Keylogers, Rootkit, APT (Advanced persistent threats), Backdoor, Brute force attack, Buffer overflow, XSS (Cross-site scripting), D-DoS (Distributed Denial-of-service), Spear phishing, Spoofing, SQL injection, 0-day exploits, Weak Authentication, Lack of encryption ou* (2)
  Acesso físico ao equipamento (*pen drive*)

Vectores de ataque ambiente educacional

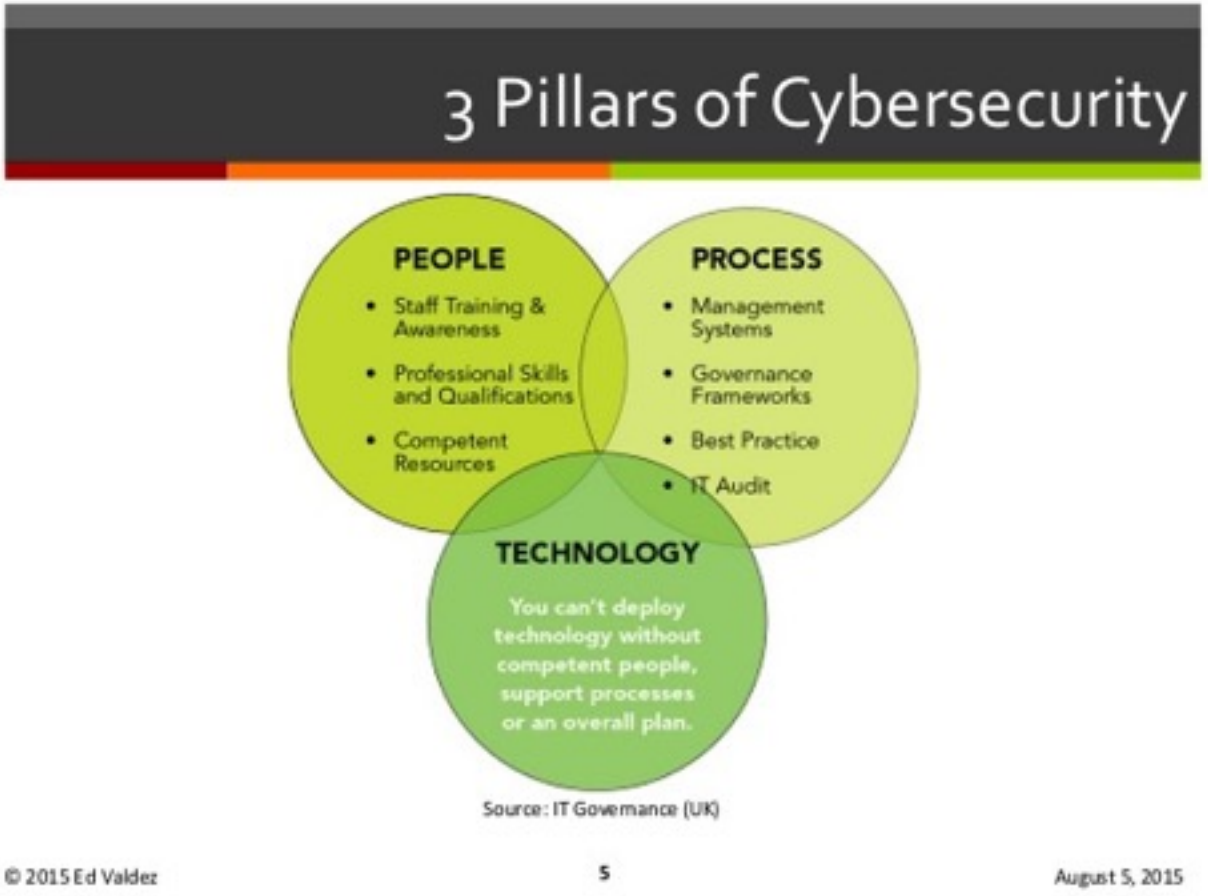
- **Componente humana:**
  - Fácil utilização da engenharia-social / passwords fracas
  - “só acontece aos outros”
  - Não há limites na publicação de conteúdos digitais
  - Narcisismo digital / pouco espirito critico *online*
  - O perigo do *click* / acesso instantâneo

Como se manifestam ?

- acessos indevidos
- roubo de identidade e fraude
- instalação de *backdoors* sem que se aperceba
- viciação digital (ao jogo ou a equipamentos)
- exposição direta à Internet de “sites” vulneráveis
- previsibilidade das pessoas

Como mitigar os riscos ?

Bruce Schneider "*Complexity is the worst enemy of security*"



Ambiente Escolar - Pessoas

- Estudantes
- Professores
- *Staff* escolar
- Administradores da rede informatica

Medidas para melhorar a segurança de informação;

- reactivar o conceito de Privacidade e Protecção de Dados (4)
- comunicação aberta entre Pais, Estudantes e Professores
- conhecer/evitar, e alertar, comportamentos de risco
- utilização de recursos on-line (p.ex. SeguraNet)
- formação especifica em segurança de informação para quem administra redes informáticas (p.ex. alterar as *pwds* iniciais dos equipamentos) / certificações (*CISSP*…)
- não ficar á espera que a tecnologia o proteja
- ser "cibercidadão" seguro e responsável (5)

Ambiente Escolar - Processos

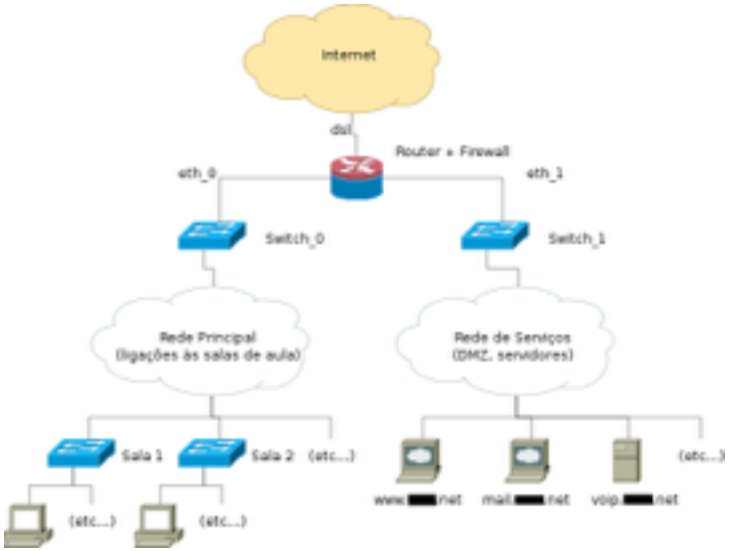
- Ter um **responsável** pela Segurança Informática, CISO - *Chief Information Security Officer*
  - sabe quem é o CISO ?

- Haver e **disponibilizar** as Normas e Regras de utilização de Sistemas de Informação alinhadas com; (7)
  - normativos internacionais (ISO27001, ISO27002) -> "Sistema de Gestão de Segurança da Informação" (6)
  - melhores práticas do mercado / orientações europeias
  - inclusão de segurança física

- Haver e **disponibilizar** procedimentos de Incidentes de Segurança / *Data Breaches*
  - A quem reportar ? O que fazer ? Como fazer ?

- **Avaliação** com auditorias periódicas (internas e/ou externas)

Ambiente Escolar - Tecnologia



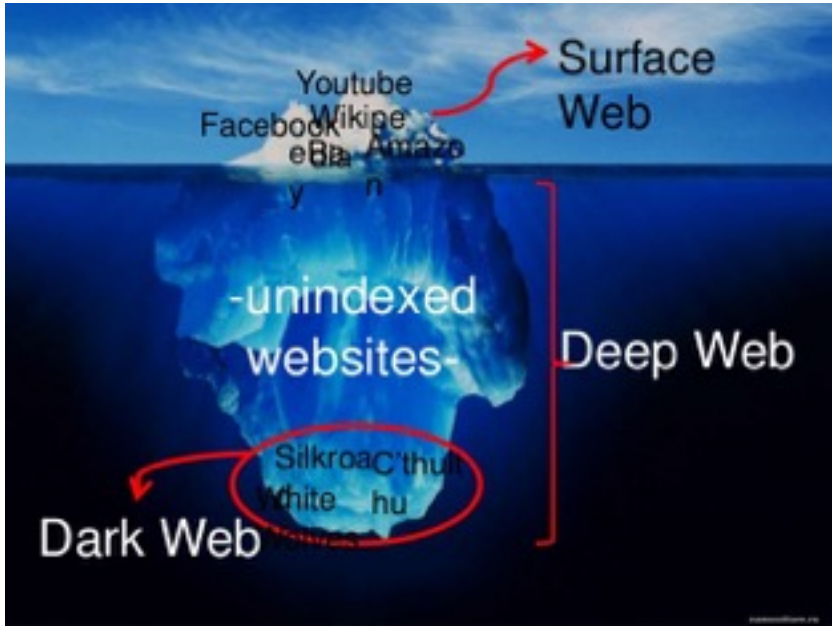
- Servidores, PCs, Anti-Virus, Smartphones, Tables, IPTVs
- Routers, Wireless Access Points, Switches, Balanceadores, CAS (Controls Access System)
- Firewalls, VPNs, IDS/IPS, Cloud
- Active Directory, Aplicações e Utilizadores

Como melhorar a segurança tecnológica ?

- manter actualizado os sistemas em todas as suas componentes (PC/Laptop/Smartphone/Tablet) e backups regulares
- uso de *passwords* complexas, altera-las frequentemente, e;
  - usar, se possível, "*2 Factor Authentication*"
  - usar aplicação "*password manager*"
- usar as funcionalidades de segurança dos equipamentos/aplicações
- se não usa *webcam* tape-a !!!
- controlar o acesso físico aos equipamentos
- utilização de arquiteturas de redes seguras
- segmentação de privilégios dos utilizadores
- armazenados remotamente dos *logs* dos sistemas
- monitoria constante da rede
- manter imagens de PCs partilhados

Exemplos (bons e “menos-bons”)

Deep / Dark Web



- A *Dark Web* (lado negro da net) é uma rede cifrada, privada e com acesso directo a pedofilia, tráfico de drogas (silk road), armas, pessoas ou *Snuff* vídeos
- Cybercrime ou terrorismo
- O desconhecimento deste lado negro da net pode ser tão, ou mais grave, que as outras ameaças mais "correntes"

- Estima-se que 96% de toda a Internet esteja na *Deep Web* (net invisível)
- Acede-se via *TOR Browser* (anónimo com um conjunto ligações aleatórias até ao seu destino) a um conjunto de conteúdo não indexado por motores de busca convencionais
  - cuidados especiais na navegação na *Deep Web*
  - venda de identidades
  - moeda é Bitcoin
  - usada por jornalistas em países com forte censura da Internet
  - usado por quem pretende estar “fora dos radares” dos controlos da Internet

Dark Web - Conclusões de um investigador

"I never look at people the same. Throughout taking this research-oriented trip through the dark web, my view on humanity has been changed. Every video I watched in the name of research chinked away at my emotions, often left me crying. Curiosity broke me, and it has been nearly a **year** since I have full **recovered**.
Now before you launch Tor and find these sites, please know. There is nothing enjoyable, entertaining, or at all suitable content on this network. You will be left in tears, you will be scarred, and worst of all... you will never view others again.
Please refrain from PM'ing me about this subject unless you have certain details or past experiences you would like to privately share."

Conclusões

- O ciberespaço tem que ser encarado como uma extensão do espaço físico onde a **segurança** não poderá ser menosprezada

- A formação académica (**desde o ensino básico**) nesta área vai ser fundamental nas próximas décadas para a competitividade de Portugal (ciber-smart[8])

- O novo Regulamento Geral da UE sobre a Protecção de Dados vai uniformizar e mudar o **paradigma** nos 28 estados membros em *Data Privacy* [9]

- As plataformas *mobile* e *IoT* estão em larga expansão entre os jovens sendo necessário encara-las como desafios **explicando** os benefícios e riscos inerentes á plataforma

Obrigado pelo vosso tempo

Questões?

Referências / Bibliografia

- *IOT* - Internet Of Things (Internet das Coisas)
- *BYOD* - Bring Your Own Device (Utilização de Aparelho Próprio)
- *CISSP - Certified Information Systems Security Professional*
- http://www.binarionet.com.br/blog/educacao-lidera-ameacas-a-ciberseguranca-por-que-e-como-reagir/
- http://www.anacom.pt/streaming/Jose_Alegria.pdf?contentId=1176122&field=ATTACHED_FILE
- www.schneier.com

1. "É Complicado - As Vidas Socias dos Adolescentes em Rede" de Danah Boyd, Relógio D'Água Editores
2. https://www.linkedin.com/pulse/cyber-security-attack-vectors-tansel-akyuz-cissp-pmp
3. "Educação lidera ameaças a cibersegurança. Por que e como reagir?" http://www.binarionet.com.br/blog/educacao-lidera-ameacas-a-ciberseguranca-por-que-e-como-reagir/
4. http://empreend.pt/web/wp-content/uploads/desafios-do-marketing-vs-dados-pessoais.pdf
5. http://cybersmart.org/assets/files/NCSA_K-12_TIPS.pdf
6. https://web.fe.up.pt/~jmcruz/seginf/seginf.1314/trabs-als/final/G4-ISO.27000.final.pdf
7. REGULAMENTO DE UTILIZAÇÃO DA REDE LOCAL, RECURSOS INFORMÁTICOS E MULTIMÉDIA_Agrupamento de Escolas Dr. José Leite de Vasconcelos
8. http://www.cybersmart.gov.au/~/media/Cybersmart/Documents/Documents/Parents_guide_to_online_safety.pdf
9. http://www.consilium.europa.eu/pt/policies/data-protection-reform/data-protection-regulation/

Contactos

ap2si.org


geral@ap2si.org


twitter.com/ap2si


facebook.com/ap2si