Cibersegurança da Saúde em Portugal: Estamos em risco?

Miguel Pupo Correia

GO CLINIdATA® - Lisboa, 16 de Maio de 2017

Estrutura

- Motivação
- Estudo: riscos na Saúde em Portugal
- Conclusões

2

MOTIVAÇÃO

3

12 de Maio de 2017: WannaCry 2

Empresas e bancos alvos de ataque informático

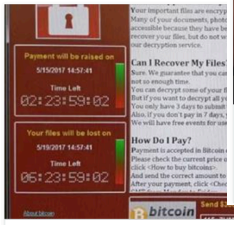
Na PT, trabalhadores receberam ordem para desligar as máquinas e e ser mandados para casa. Veja a mensagem recebida pelos trabalhad PT

TVI24.IOL.PT

Ataque informático. O que foi, como se espalhou, quem o travou

Um poderoso vírus entrou por uma falha do Windows e alastrou na rede. Criou o caos em hospitais e empresas de todo o mundo.

OBSERVADOR.PT



NHS hit by massive ransomware attack, many hospitals and clinics offline

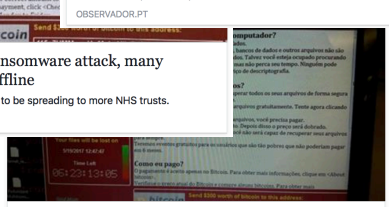
The ransomware attack appears to be spreading to more NHS trusts.

ARSTECHNICA.CO.UK

Portugal Telecom alvo de ataque informático internacional

A Portugal Telecom é um dos alvos do ataque informático que afetou várias empresas em Portugal, Espanha e Alemanha. A espanhola Telefónica é outr...

OBSERVADOR.PT



Ataque informático mundial: empresas portuguesas afetadas

Vírus afeta apenas os utilizadores que tenham sistema operativo da Microsoft

DN.PT | POR DIÁRIO DE NOTÍCIAS

4

Como funciona o ataque?

colaborador da empresa recebe *mail* infetado (anexo .zip)

colaborador abre anexo que contamina o PC com o malware WannaCry 2

malware invade outros computadores da empresa (vulnerabilidade no Windows/SMB)

malware cifra os ficheiros, apaga *backups* e pede resgate (ransomware)

5

Saúde afetada?

- In the UK, many hospitals fell victim and some health organisations diverted ambulances and cancelled non-essential services (…)
- Why has the NHS been hit so hard?
- (...) it is a huge organisation supported by a massive IT infrastructure. It also has lots of partners and suppliers that connect to its core network.

BBC NEWS

Cyber-attack: Is my computer at risk?

By Zoe Kleinman
Technology reporter, BBC News

6

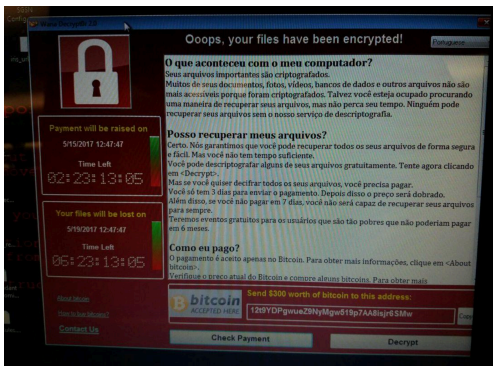
Ataque avançado?

- Sim:
  - Impacto elevado (milhares de empresas, 150 países)
  - Dois vetores de ataque
- Não:
  - Vulnerabilidade corrigida há 2 meses; foi afetado quem falhou 3 atualizações do Windows (!)
  - Falta de preparação dos colaboradores, problema conhecido
  - Ransomware crítico há ~2 anos; solução conhecida (cópias de segurança desligadas da rede)

7

Vai voltar a acontecer?

- Provavelm.: lucrativo, malware costuma ter variantes
- Muitos beneficiários: hackers, tradutores, mulas,...



8

Foi a primeira vez?

- Nesta escala sim, mas de resto não:

MENU ÚLTIMAS SOL

ECONOMIA POLÍTICA OPINIÃO

SOCIEDADE 18 de fevereiro 2017

Piratas informáticos atacam hospital Garcia de Orta

Ministério Público está a investigar ciberataque contra o hospital de Almada. Situação foi detetada no final de 2016 e afetou banco de exames médicos. Nenhuma imagem foi roubada, garantiu ao SOL a administração hospitalar.

Expresso

INTERNACIONAL

Hackers atacam hospital americano e exigem €3 milhões para desbloquear sistemas

16.02.2016 às 10h07

9

Podia ter sido pior?

- Computadores afetados foram PCs administrativos
  - Disrupção na operação dos serviços
- Há outros computadores na área da Saúde?
  - Aparelhos de raio-X
  - Aparelhos para cirurgia remota
  - Pacemakers
  - Neuro-estimuladores (Parkinson)
  - ...
  - Consequências?

10

ESTUDO: RISCOS NA SAÚDE EM PORTUGAL

O estudo

- Objetivo: aumentar o nível de alerta sobre cibersegurança na área da saúde em Portugal
- Como: top 10 de riscos => análise de risco
- Grupo de trabalho da APDSI
- Ivo Pinto, "*Security Risks in Healthcare*", Dissertação de Mestrado, Instituto Superior Técnico, Fev. 2017

Metodologia

- Entrevistas preliminares
  - para validar a metodologia
- Definição do escopo
  - Ativos, ameaças, vulnerabilidades, ataques
- Análise de risco
  - metodologia da OWASP, com adaptações à Saúde
- Criação do Top 10
- Validação
  - questionários a profissionais

13

Definição do escopo: Ativos

- Técnicos
  - Computadores administrativos
  - Dispositivos médicos eletrónicos
  - Aplicações de software
  - Disponibilidade de serviço
- Pessoas
  - Profissionais do setor
  - Saúde dos pacientes
- Dados
  - Dados dos pacientes (p.ex., registos médicos)
  - Informação da unidade de saúde (p.ex., hospital)
- Outros
  - Reputação
  - Finanças

14

Análise de risco

Risco = Impacto x Probabilidade

- Impacto
  - técnico: perda de confidencialidade, integridade e disponibilidade
  - no negócio: dano financeiro, dano à reputação, perda de *compliance*, violação de privacidade
  - na saúde de pacientes
- Probabilidade
  - fatores de ameaça: competência, motivo, oportunidade, dimensão
  - fatores de vulnerabilidade: facilidade de descoberta, de ataque, conhecimento, deteção

15

Exemplo: avaliação do risco de *vulnerabilidades no software*

Impacto

Technical impact				**Business impact**				**Patient safety**
Loss of confidentiality	Loss of integrity	Loss of availability		Financial damage	Reputation damage	Non-compliance	Privacy violation	Patient health
8	3	7		3	5	5	6	7
Overall technical impact:		6		Overall business impact:		4.75		
				Overall impact:	6.2			

Probabilidade

Threat agent factors					**Vulnerability factors**			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
9	7	7	9		9	5	4	9
Overall threat:		8			Overall vulnerability:		6.75	
		Overall likelihood:		7.4				

16

Top 10

1

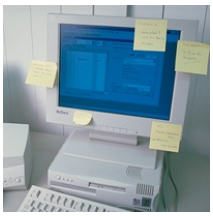
Vulnerabilidades no software

Exemplo: caso de 12/05/2017 deveu-se a vulnerabilidade no Windows

2

Acesso não autorizado a sistemas

Exemplo: *passwords* partilhadas ou mal guardadas



17

Top 10

3

Falta de medidas ativas de proteção

Contra-exemplo: auditoria (*pen* testing) descobriu dados médicos visíveis (Índia)

4

Falta de pessoal qualificado em cibersegurança

Contra-exemplo: Boston Children's Hospital ameaçado em 2014 mas ataque falhou devido à intervenção da equipa de cibersegurança

Boston Children's Hospital
Until every child is well™

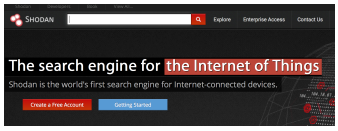
18

Top 10

5

Comprometimento de dispositivos médicos eletrónicos

Exemplos: investigador ligou-se a aparelho de ressonância magnética de um hospital encontrado no Shodan (2016); outro consegui interferir com bomba de insulina



6

Negação de serviço

Exemplos: caso de 12/05/2017;

o Hollywood Presbyterian Medical Center foi infetado por ransomware e teve de pagar 17 mil dólares de resgate (2016)

19

Top 10

7

Vulnerabilidades de rede

Exemplo: casos de servidores de ficheiros em rede comprometidos e dados privados roubados

8

Engenharia social

Exemplos: funcionário abre anexo de *mail* e malware acede a dados médicos de 90 mil pacientes no UW Medicine (2013); caso de 12/05/2017

20

Top 10

9

Acesso físico a servidores

Exemplo: servidor contendo informação médica de 40 mil pessoas roubado ao *Silicon Valley Eyecare Optometry and Contact Lenses* (2010)

10

Dispositivos móveis

Exemplos: dois portáteis contendo informação de 1,2 milhões de pacientes roubados à AvMed (2010); estudo mostra que Apps de saúde contêm inúmeras vulnerabilidades (2014)

AvMed Embrace better health.

21

CONCLUSÕES

22

Conclusões

- Estamos em risco? Sim, sem dúvida
- Soluções:
  - Entidades do setor devem levar o tema a sério
  - Danos para a saúde dos pacientes (indireta e diretamente) e financeiros são riscos reais (reg. privacidade EU, 2016)
  - Entidades do setor devem ter equipa de cibersegurança e aceitarem que há custos associados
- Desafios:
  - Paradoxo da Informática ter impacto na Saúde
  - Cibersegurança não cura, mas sua ausência pode matar

23

U LISBOA | UNIVERSIDADE DE LISBOA

Muito obrigado

miguel.p.correia@tecnico.ulisboa.pt

This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2013 (INESC-ID)

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

TÉCNICO LISBOA

inesc id lisboa