nic.br cgi.br

20 anos cert.br

GTS 30
São Paulo, SP
07 de dezembro de 2017

Conscientização como uma Ferramenta para Diminuir a Efetividade de *Spear Phishing* e *Insider Threats*

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/
http://politica.estadao.com.br/noticias/geral,hackers-atacam-sistema-de-e-mails-e-de-leitura-de-documentos-do-itamaraty,1172332
http://www.eweek.com/security/rsa-s-securid-breach-started-with-phishing-email
http://www.eweek.com/security/rsa-s-securid-breach-started-with-phishing-email
https://www.helpnetsecurity.com/2017/09/13/phishers-linkedin-hijacked-accounts/
http://mspmentor.net/security/office-365-users-increasingly-targeted-credential-stealing-phishing-campaigns

Cenário atual (1/2)

- **Ataques a usuários finais:**
  - visando serviços de autenticação
  - com foco em grandes corporações
  - levando a grandes vazamento de dados
  - repositórios de credenciais sendo confundidos com invasão de BD

- **Fruto da mudança de enfoque dos atacantes**
  - é mais fácil e “rentável” atacar um usuário
  - usuários com acesso a muitas e valiosas informações

Cenário atual (2/2)

- **Ataques cada vez mais convincentes, explorando**
  - grande quantidade de informações expostas na Internet
  - a confiança cega que as pessoas têm em contatos conhecidos
  - “estupidez” ou falhas humanas (engenharia social)
    - mecanismos de convencimento / persuasão:
      - princípio do tempo, obediência à autoridade, mentalidade de manada, distração, desejo, desonestidade, orgulho, caridade / gentileza / vontade ser útil, ganância, curiosidade, preguiça
- **Credenciais com alto valor no mercado negro**

Underground Hacker Markets	
Large U.S. Airline Points Account varies based on amount	*Price based on points in account 1,500,000 - $450 / 200,000 - $60*
Large International Hotel Chain Points Account	*Price based on points in account 1,000,000 - $200 / 200,000 - $40*
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	*$129*
Popular U.S. Social Media Accounts	*$129*
Corporate email accounts	*$ 500 per mailbox*
Remote Access Trojans (RATs)	*$5 – $10*
High Quality Bank Accounts with Verified Large Balances of $70,000 – $150,000	*6% of the balance of the account*
Hacking Website (stealing data)	*$350*
Full business dossiers on companies located within the Russian Federation	*$547 - $822*

Underground Hacker Markets – Annual Report – April 2016 SecureWorks
https://www.secureworks.com/~/media/Files/US/Reports/SecureWorksSECO2123NUndergroundHackerMarketplace.ashx

Underground Hacker Markets
Hacking Email Accounts

"No prepayments, you pay only for visible results — we will present the necessary proof."

"Complete Confidentiality— the victim will not even notice that their email account has been hacked."

"Burglary of the email account will be carried out without changing the password, the victim, will access their email account noticing no suspicious activity."

"Access to all the websites registered by the owner of the email account."

Underground Hacker Markets – Annual Report – April 2016 SecureWorks
https://www.secureworks.com/~/media/Files/US/Reports/SecureWorksSECO2123NUndergroundHackerMarketplace.ashx

Como são obtidas as credenciais

- **Informadas pelos próprios usuários (*insider threats*)**
  - forma intencional ou não intencional
- **Uso de protocolos sem criptografia**
- **Instalação de *malware***
- **Ataques de força bruta**
- **Falhas em sistemas**
- ***Phishing***

Phishing

- **Tradicional:**
  - *e-mails* enviados de forma massificada
  - tentam induzir o usuário a executar ações e fornecer dados
- **Em cascata:**
  - uso de conta forjada/genérica para envio de *e-mails* aos funcionários
  - uso de conta invadida para envio de *e-mails* a funcionários específicos
    - burlar sistemas de reputação (como SPF/DKIM)
    - responder conversas em andamento, incluindo *links*
    - usuários acreditam em contatos conhecidos (mesmo com conteúdo "estranho")
- ***Spear phishing:*** direcionados a grupos específicos
- ***Whaling:*** direcionados a alvos chave das organizações
- ***Watering hole attacks:*** direcionados a *sites* acessados pelos alvos reais
- ***SMiShing*:** direcionados a usuários de dispositivos móveis

Security

Prison hacker who tried to free friend now likely to join him inside

But he got oh so close

By Iain Thomson in San Francisco 4 Dec 2017 at 21:00 24 SHARE ▼

In a sustained campaign, Voits managed to get the login details and passwords for 1,600 county employees, including for the Xjail computer system that is used to track inmates. By March he had the logins to the prison management system and tried to amend the records of one inmate to arrange their early release.

https://www.theregister.co.uk/2017/12/04/prison_hacker_pleads_guilty/

EMPRESAS ALEMÃS PERDEM MILHÕES DE EUROS EM “FRAUDE DO CEO”

JUL 10, 2017 *ROBERTO CHU* *AMEAÇAS DIGITAIS* *NO COMMENTS YET*

Empresas alemãs perderam milhões de euros para o crime organizado em um golpe apelidado de "fraude do CEO" que usa falsos memorandos de altos executivos para convencer funcionários de contabilidade à transferir fundos, disse nesta segunda-feira a agência federal de segurança cibernética da Alemanha (BSI).

A agência BSI disse que as autoridades que investigam a nova fraude receberam uma lista de 5 mil alvos potenciais, e notificaram as empresas envolvidas.

Organizações criminosas estão usando informações que conseguem em redes sociais, sites corporativos, sites de empregos e até ligações para as companhias para falsificar as informações de contato de altos executivos.

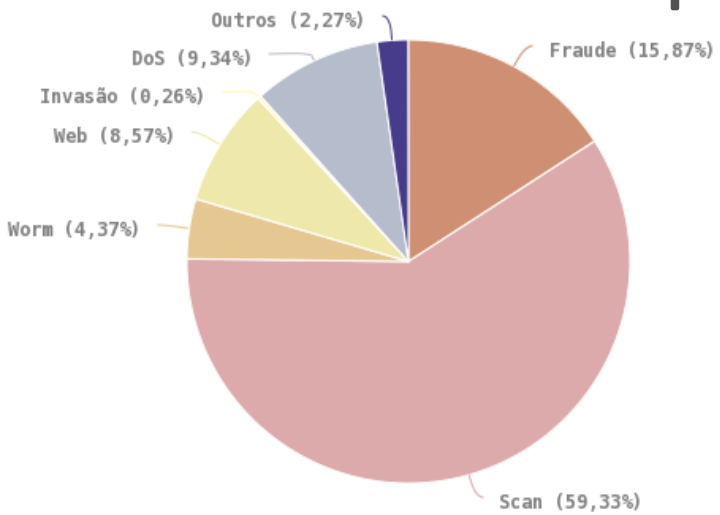
A BSI disse que a Polícia Federal Criminal alemã estimou que o golpe já custou milhões de euros a empresas nos últimos meses.

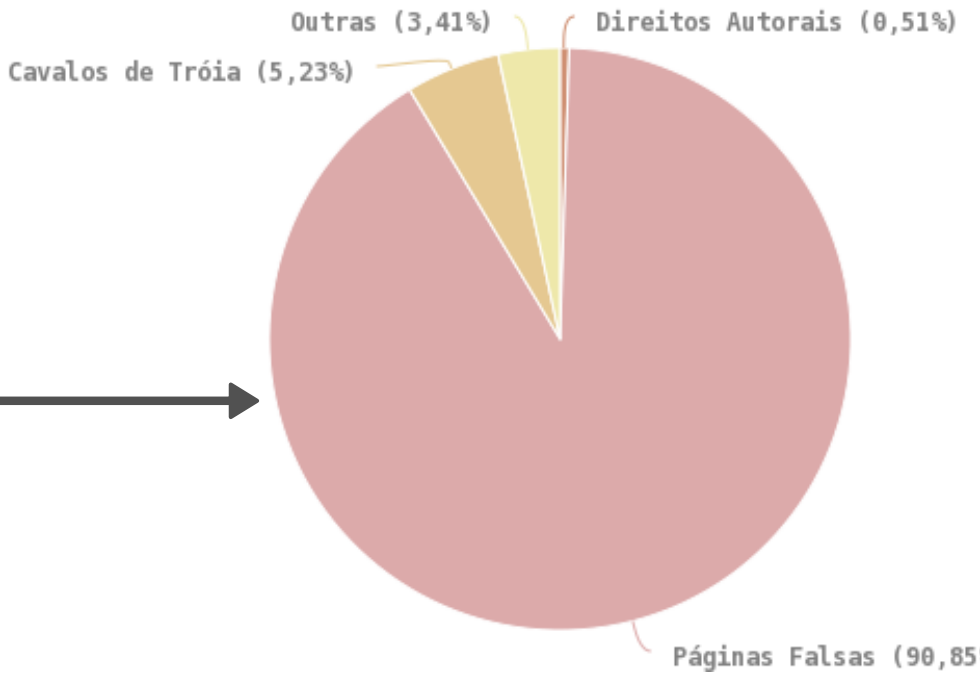
A fraude visa funcionários dos departamentos de contabilidade e auditoria de uma companhia que foi autorizada a transferir dinheiro, muitas vezes usando pressão de tempo e avisos sobre um suposto "projeto secreto" para manipulá-los à realizar os falsos pagamentos.

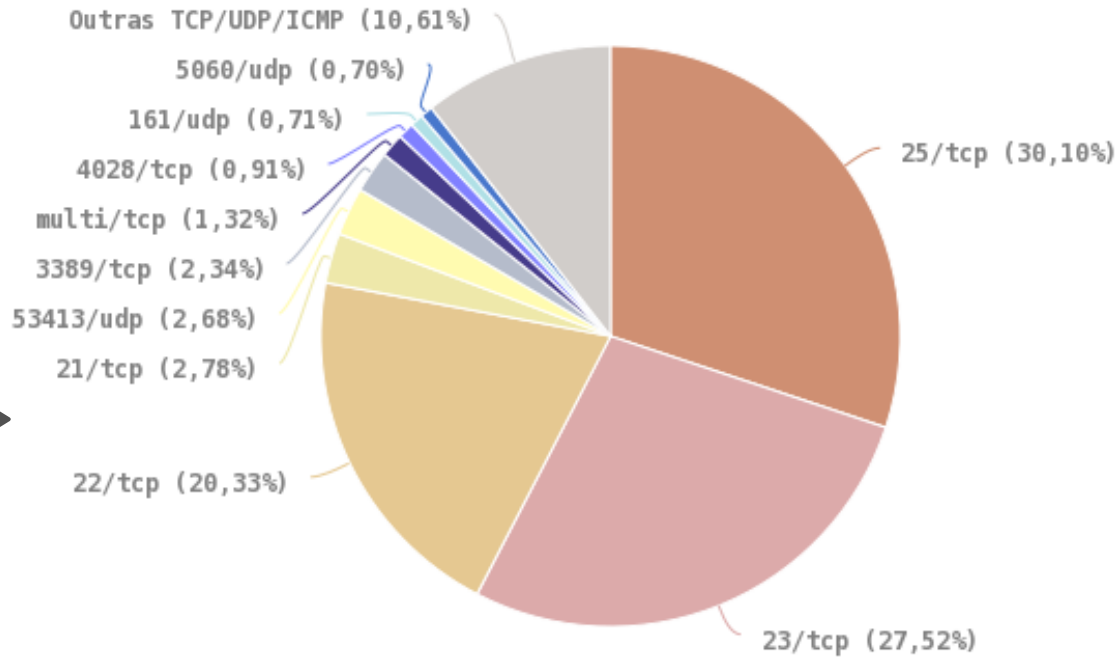
http://www.e-guardian.com.br/ameacas/empresas-alemas-perdem-milhoes-de-euros-em-fraude-do-ceo

http://edition.cnn.com/2017/07/31/politics/white-house-officials-tricked-by-email-prankster/index.html

Estatísticas 2016







*Insider Threat** (1/2)

Potencial de um
(ex) funcionário, parceiro, prestador de serviços,
que tem (teve) acesso aos sistemas da organização,
de usar esse acesso,
com intuito malicioso ou não intencional,
de forma a colocar a organização em risco

Baseado na definição do CERT-CC
https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

Insider Threat (2/2)

- **Por que agem/não agem?**
  - não intencionais
    - ocorrem por erros humanos, displicência, preguiça, desconhecimento
  - intencionais
    - predisposição associada a oportunidade e motivo
    - geralmente difíceis de serem detectados
      - utilizam acessos legítimos
    - estão um passo à frente dos atacantes externos
    - conhecem as joias da coroa
      - e principalmente as fraquezas
      - ex-funcionários conseguem persuadir mais facilmente os atuais

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

POLICY —

Former Energy Department employee admits trying to spear phish coworkers

Feds say campaign was part of a plot to hack computers storing nuclear secrets.

DAN GOODIN - 2/3/2016, 7:33 PM

Wikipedia

This carp was not paranoid enough. (The person pictured has nothing to do with the case reported in this post.)

A former Department of Energy employee has pleaded guilty to federal charges that he attempted to infect 80 current DOE employees with malware so foreign hackers could take control of computer systems that held sensitive information

https://arstechnica.com/tech-policy/2016/02/former-energy-department-employee-admits-trying-to-spear-phish-coworkers/

One out of five employees is willing to sell work email passwords

0

By Kavita Iyer on MARCH 23, 2016 — Security news, Technology

Scaring survey finds that one out five employees would sell corporate passwords, some for less than $1000

According to the 2016 Market Pulse Survey, sponsored by an Austin-based security company, SailPoint Technologies, the biggest threat to a company's digital security seems to be its employees. The survey says that one in five employees would be willing to sell their work passwords to another organization, which is up from one in seven last year.

The data comes from a survey of 1,000 office workers at private organizations (with at least 1,000 employees) across the US, UK, Germany, France, the Netherlands and Australia.

The survey shows that one third (32 percent) of respondents said they share their passwords with their co-workers, and nearly two thirds (65 percent) said they only use a single password across multiple applications.

However, the most shocking revelation is that one in five employees globally said they would sell their passwords to an outsider. Of those who would sell their passwords, 44 percent would do it for less than $1,000, and some for less than $100.

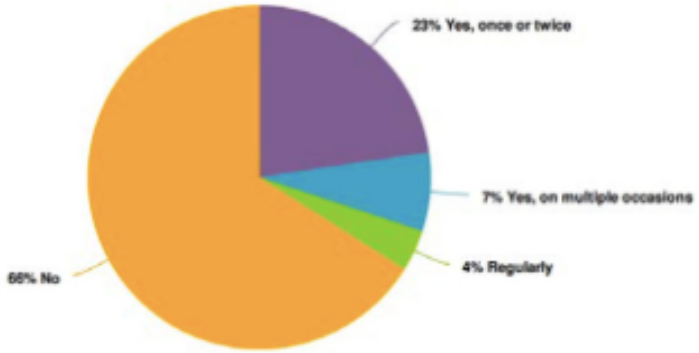
https://www.techworm.net/2016/03/one-five-employees-willing-sell-work-email-passwords.html

Poor security habits are the ideal recipe for a breach

[New eBook] Defending against ransomware. Read it now.

A Preempt survey of more than 200 employees (management level or above) from enterprise companies of 1000 or more people, found that businesses are left exposed by employees who have more access to sensitive resources than they should and who follow poor security habits.

Have you ever "bent the rules" or found a security workaround in order to get something done at work?



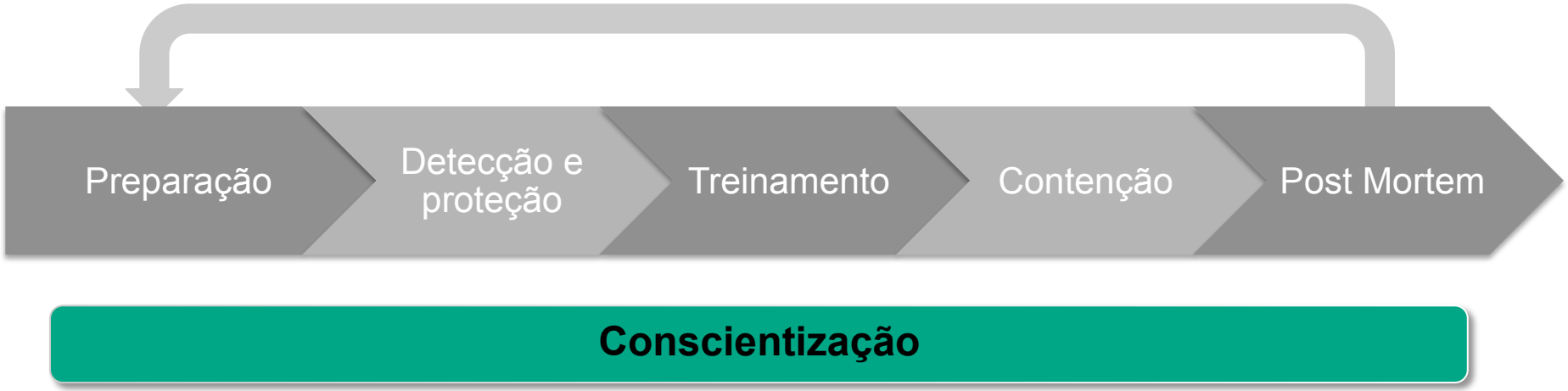
With nearly 41 percent of employees using the same password for both personal and work accounts, and 20 percent of employees aware that their passwords were compromised in a breach, it is concerning to find that 63 percent claim they only changed their passwords for the account that was breached, proving they are not aware of the full consequences of a password leak.

https://www.helpnetsecurity.com/2017/11/17/poor-security-habits/

Como melhorar o cenário

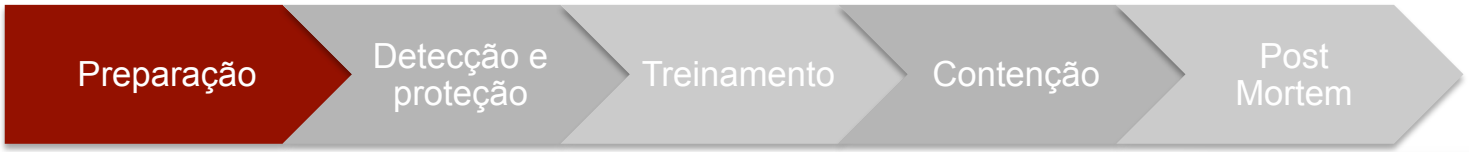
Com melhorar o cenário

- **Conscientização**
  - processo constante e contínuo
  - não basta estar em conformidade com normas e certificações
  - aplicado a todos os níveis organizacionais



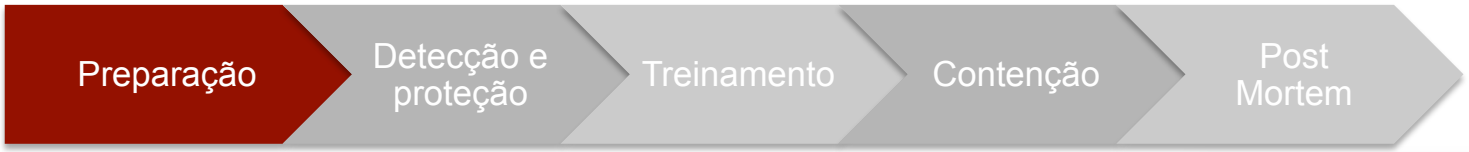
Preparação (1/2)

- **Conhecer a organização**
  - identificar o *baseline*
    - conhecer o que é o “normal” da rede e dos usuários
  - fazer análise de risco, considerando
    - quais serviços, sistemas e dados são mais críticos
    - quais são os usuários chave
- **Criar um CSIRT**
- **Preparar funcionários para dar treinamentos**
  - conhecimento multidisciplinar



Preparação (2/2)

- **Definir políticas**
  - segurança
    - contas
      - privilégio mínimo
      - senhas
      - 2FA, incluindo o uso de chaves de segurança para posições chave
    - uso de equipamentos
      - BYOD
  - proteção de dados
    - *backup* / engenharia social / confidencialidade (uso de redes sociais)
  - contratação e demissão



Detecção e proteção

- **Implementar boas práticas**
  - impedir que as mensagens cheguem aos usuários
    - monitoramento de rede (mudanças de padrão)
    - bloquear arquivos em anexo
    - implementar sistemas de combate a spam
      - listas de bloqueio, filtros de conteúdo, *greylisting*, SPF, DKIM, DMARC
  - proteger os equipamentos dos usuários
    - manter os sistemas atualizados
    - usar mecanismos de segurança
      - *firewall*, antivírus, antispam, *antiphishing*, extensões (NoScript)
  - implementar filtros de saída (*extrusion detection*)
    - netflow, DNS passivo, *data feeds*
    - gerência de porta 25
  - bcp.nic.br

Treinamento (1/6)

- **Considerar que as barreiras serão burladas**
- **Investir em pessoas**
  - usuários essenciais para preservar a segurança da organização
- **Benefícios:**
  - criar cultura de segurança na organização
    - casos não intencionais
      - reduzir e minimizar os problemas
    - casos intencionais
      - detectar os problemas
      - conhecer as consequências

Treinamento (2/6)

- **Para quem (público alvo)**
  - geral
  - segmentado por áreas da organização
  - dedicado a funcionários:
    - área gerencial
    - com acesso privilegiado
    - com acesso a dados críticos

Treinamento (3/6)

- **Com qual periodicidade**
  - prazo estipulado pela empresa (anual, semestral, etc)
  - quando os casos estiverem aumentando
  - quando um usuário solicitar ajuda
  - quando funcionário começar a trabalhar na organização
  - contínuo

- **Com qual nível de dificuldade**
  - um único e grande módulo
  - gradual – dividido em pequenos módulos

Treinamento (4/6)

- **Explicar de forma clara o porquê do treinamento (engajamento)**
  - qual é o problema
    - obtenção de credenciais/dados pessoais e financeiros
  - qual é a importância
    - pessoas como algo de ataques
  - quais são as consequências:
    - para a empresa (perdas financeiras/vazamento de dados, etc.)
    - para o usuário (invasão de privacidade/furto de identidade/perda do emprego, etc.)

Treinamento (5/6)

- **Mostrar os benefícios (motivação)**
  - conhecimento aplicado a vida pessoal
    - não é apenas “coisa da empresa”
  - estimular o uso seguro também nos equipamentos pessoais

- **Apresentar soluções**
  - o que o usuário deve fazer para se prevenir
  - a quem recorrer em caso de problemas

Treinamento (6/6)

- **Métodos que podem ser usados**
  - um a um (quando o funcionário reportar algo)
  - cartazes espelhados pela organização
  - palestras (exemplos concretos / *storytelling*)
  - simulações anunciadas
  - simulações não anunciadas
    - ajudam na retenção
    - exploram a maior receptividade em momentos de aprendizagem (“*landing page*”)
  - *gamification* / *active feedback*
    - participação voluntária
      - incentivo por meio de recompensas

http://phish-education.apwg.org/r/en/index.htm

Game on: UNSW team develops cyber security education app

17 NOV 2017 | SUSANNA SMITH

A team from across UNSW has used a 1980s retro-style arcade game to develop an app that educates students about cyber security.

A.L.I.C.E. has been developed to educate students and staff about cyber security.

UNSW Sydney students, employees and alumni have collaborated to develop an app designed to educate people about cyber security.

A.L.I.C.E. (Artificial Learning Intelligence for Centralised Education) uses a 1980s retro-style arcade theme to take players through a range of cyber security scenarios with the aim of recovering their stolen identity. Along the way they navigate "the network", using their wits to outsmart evil viruses, beat attacking malware

https://newsroom.unsw.edu.au/news/science-tech/game-unsw-team-develops-cyber-security-education-app

Cartilha de Segurança para Internet / Guias Internet Segura

https://cartilha.cert.br/
http://internetsegura.br/

Contenção (1/2)

- **Pro-atividade como forma de combate**
  - "*if you see something, say somehting*"
  - "*see phishing, report phishing*"*
- **Quanto antes a empresa souber**
  - mais rápido poderá atuar
  - mais eficiente poderá ser a contenção
  - menores serão os danos
    - evitar outros casos
      - reutilização de senhas
      - propagação de *malware*

* https://apwg.org//report-phishing/

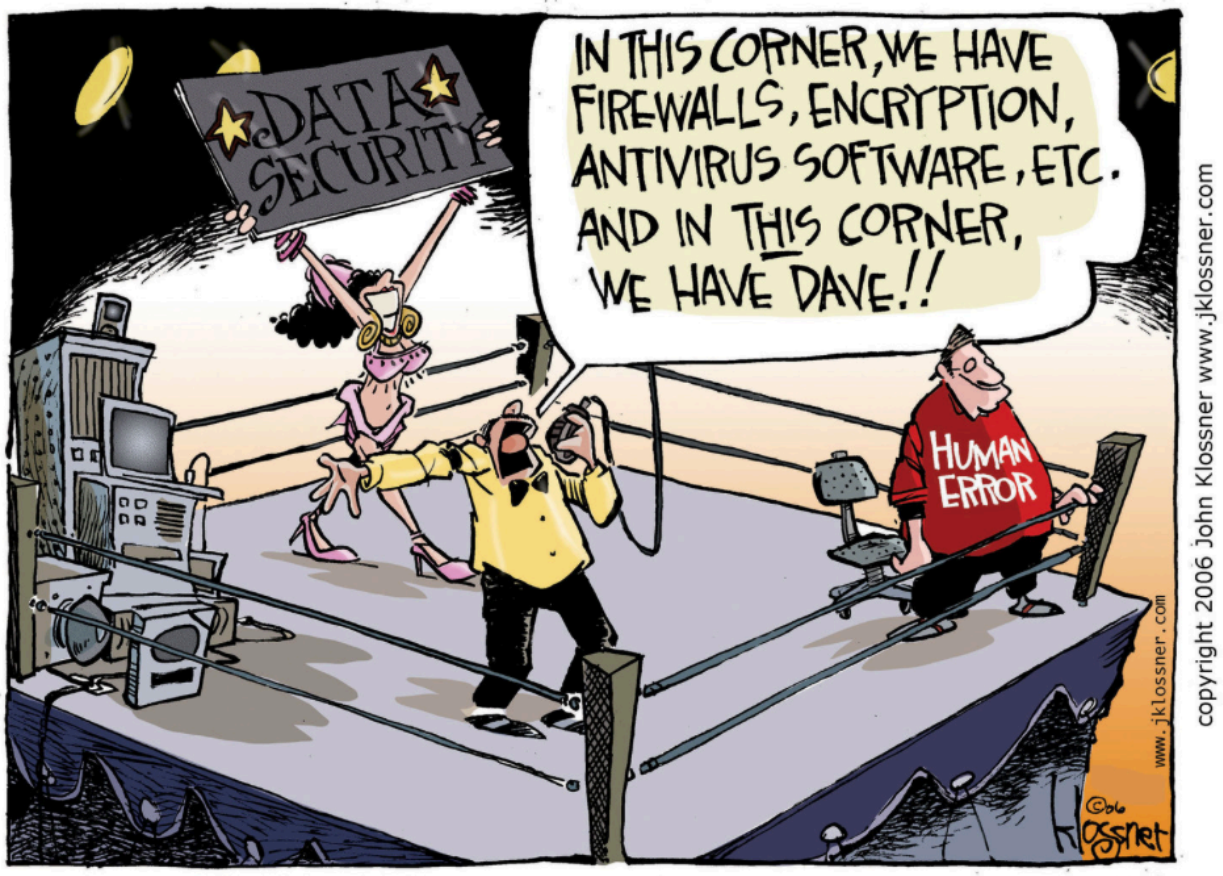
Contenção (2/2)

- **Funcionários devem ser incentivados a reportar**
  - quando suspeitarem:
    - que tenham instalado *malware*
    - que tenham caído em *phishing*
    - que o equipamento pode ter sido invadido
    - de algum comportamento ou situação estranha/suspeita
- **CSIRT pode ser o caminho para receber as notificações**
  - deve ser de fácil acesso e amigável
  - garantir a confidencialidade
    - implementar canais anônimos

Post Mortem

- **Analisar métricas**
  - considerar que decisões humanas são subjetivas e dependem do momento e das técnicas de persuasão usadas
- **Usar reforço positivo para os casos que foram notificados**
  - falsos positivos são bem vindos
- **Verificar o que deu errado em cada caso e usar isso para melhorar todo o processo**
  - refinar controles / customizar ferramentas
- **Rever as etapas anteriores**

Considerações finais



Se o usuário é o elo mais fraco da segurança, o que fazer para torná-lo um aliado?

Se a segurança é em camadas, não estaria a camada do usuário sobrecarregada?

O que podemos fazer ou o que deveríamos estar fazendo para auxiliá-los?

Referências

Advanced Persistent Training:

Take Your Security Awareness Programme to the Next Level, Jordan Schroeder

Insider Threat he CERT Division

http://www.cert.org/insider-threat/

Common Sense Guide to Mitigating Insider Threats, Fifth Edition

http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Obrigada

www.cert.br

miriam@cert.br

certbr

07 de dezembro de 2017

nic.br cgi.br

www.nic.br | www.cgi.br