Insider Threats

Estamos convidando os inimigos a entrar?

Miriam von Zuben

miriam@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

Agenda

- Introdução
- Problemas causados
- Exemplos
- Categorias
- Detecção e prevenção
- Leituras recomendadas

Introdução

O que é um *insider threat?*

Insider threat **(atacante interno) é um:**

- **funcionário ou ex-funcionário**
- **prestador de serviço, parceiro ou funcionário terceirizado**

- **que possui/possuiu acesso a dados, sistemas ou rede de uma organização**
- **que de forma intencional ou não intencional:**
  - **excede**
  - **mal utiliza**
  - **não utiliza esse acesso**
- **ocasionando no prejuízo ou na possibilidade de prejuízo de informações e sistemas desta empresa**

http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

Principais características (1/2)

- *Insider*s possuem direito de acesso a:
  - informações, sistemas, bases de dados
- Estão um passo a frente em relação aos atacantes externos
  - conhecem as "jóias da coroa"
- Podem contornar mecanismos de segurança
  - acessos legítimos
  - difíceis de serem detectados
    - envolvem fatores humanos
    - como saber se uma empresa já teve problema ou não?
    - como saber se algo não foi detectado?
- Ataques externos X internos:
  - externos: maior quantidade
  - internos: causam mais danos

Principais características (2/2)

- **Motivação:**
  - **financeiras**
    - **extorsão**
  - **vingança**
  - **expectativas não atendidas**
  - **ideológicas**
  - **conluio com *underground* ou crime organizado**
  - **falta de conhecimento, ingenuidade (não intencional)**

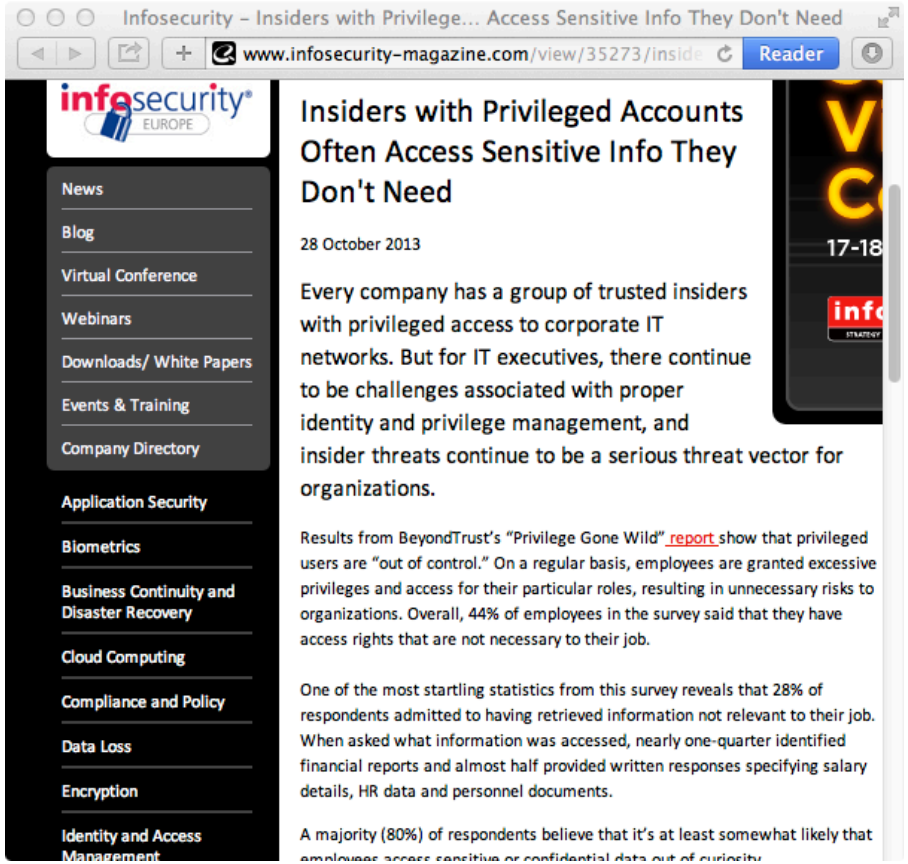
Problemas causados

Problemas causados por *insider threats* (1/4)

- **2013 US State of Cybercrime Survey**
  - **53% tiveram problemas com *insider threats***
  - **53% tiveram problemas mais graves com *insider threats* do que com ataques externos**
  - **incidentes mais comuns**
    - **Exposição não intencional de dados privados ou sensíveis – 34%**
    - **Furto de propriedade intelectual – 34%**
    - **Acesso não autorizado a informações, sistemas e redes – 30%**
    - **Furto de informações de clientes ou financeiras – 31%**
  - **82% resolveram os problemas internamente**

http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml
http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

Problemas causados por *insider threats* (2/4)

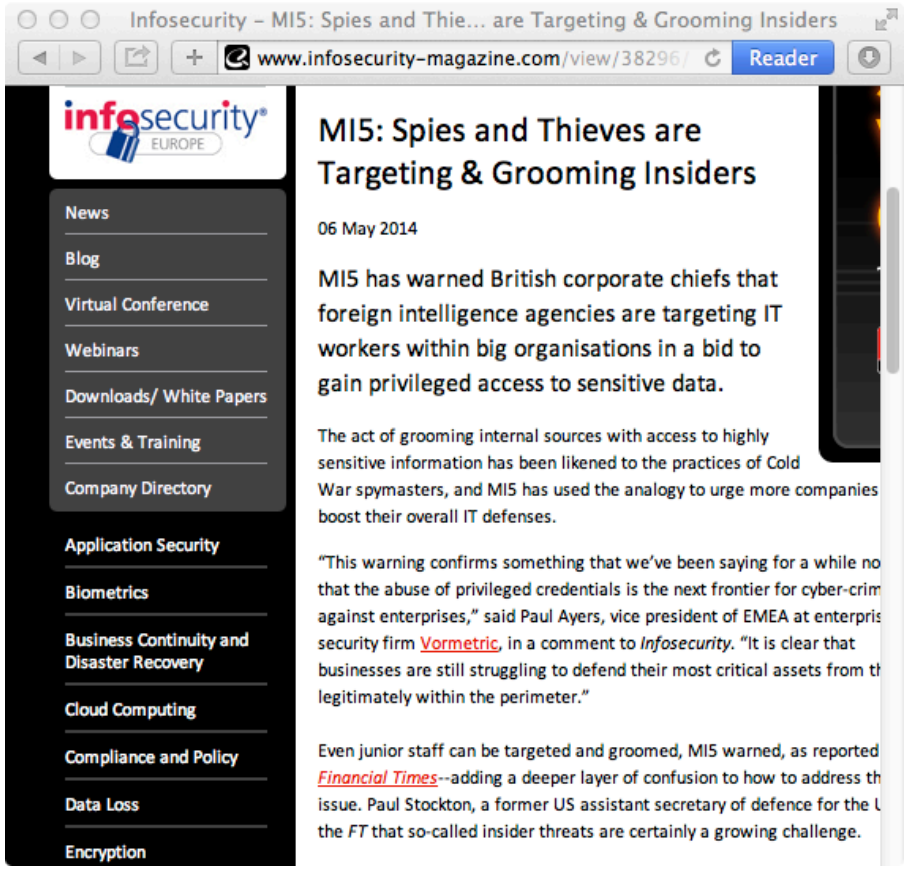


2013

- ***Privilege Gone Wild Report – BeyondTrust***
  - **28% acessaram informações não relevantes ao trabalho**
    - **relatórios financeiros, salários, RH, docs pessoais**
  - **65% das empresas possuem mecanismos de controle**
    - **54% sabem como despistá-los**
  - **44% possuem acessos desnecessários**

http://www.infosecurity-magazine.com/view/35273/insiders-with-privileged-accounts-often-access-sensitive-info-they-dont-need/

Problemas causados por *insider threats* (3/4)



2014

- **Reporte do MI5**
  - **empresas estrangeiras de inteligência visando profissionais de TI para obter dados sensíveis**
  - **"the abuse of privileged credentials is the next frontier for cyber-crime against enterprises" – Paul Ayers, vice presidente da EMEA**

http://www.infosecurity-magazine.com/view/38296/mi5-spies-and-thieves-are-target

Problemas causados por *insider threats* (4/4)

- ***Cloud Computing***
- ***The Notorious Nine - Cloud Computing Top Threats in 2013 –***
  - **Acesso de informações**
    - **quem possuiu acesso?**
    - **informações criptografadas?**
    - **quem possui acesso às chaves?**

https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Exemplos

Exemplos de *insider threats* (1/6)

- **Difíceis de serem achados**
- **Organizações não tornam casos públicos**
  - **problemas são tratados internamente**
    - **falta de evidências e provas**
    - **dano insuficiente**
    - **dificuldade de identificar o(s) autor(es)**
    - **preocupação com publicidade negativa**
- **EUA: leis obrigando empresas a notificarem vazamento de informações de identificação pessoal**

Exemplos de *insider threats* (2/6)

Planalto se cala sobre espião preso...as – Política – Correio Braziliense

www.correiobraziliense.com.br/app/noticia/ Reader

Planalto se cala sobre espião preso após roubar informações dos colegas – Politic...

Planalto se cala sobre espião preso após roubar informações dos colegas

João Valadares
Publicação: 21/09/2012 07:46 Atualização:

Prisão do funcionário que invadiu e-mails da agência de informações irritou o governo, que trata o assunto com sigilo

O episódio da prisão em flagrante W.T.N., de 35 anos, servidor da Agência Brasileira de Inteligência (Abin) que conseguiu "hackear" 238 senhas de investigadores do órgão, está sendo tratado pela Presidência da República com absoluto sigilo. Um dia depois de o Correio revelar que o oficial técnico de inteligência foi preso em flagrante, dentro de sua sala na própria instituição, o Gabinete de Segurança Institucional (GSI) se fechou para não expor ainda mais a fragilidade da proteção de informações sigilosas. Ontem, o ministro chefe do GSI, general José Elito Carvalho, tratou do assunto em várias reuniões. Para auxiliares, o ministro demonstrou grande insatisfação com a divulgação do caso.

Leia mais notícias em Política

O Correio apurou que o espião W.T.N. foi

2009

- **Funcionário da Abin**
- **238 senhas *hackeadas***
- **detectado por um "fluxo atípico de dados em uma estação de trabalho"**

http://www.correiobraziliense.com.br/app/noticia/politica/2012/09/21/interna_politica,323675/planalto-se-cala-sobre-espiao-preso-apos-roubar-informacoes-dos-colegas.shtml

Exemplos de *insider threats* (3/6)

G1 – Detran-AM descobre programa espiã... estagiários – notícias em Trânsito AM

G1 – Detran-AM descobre programa espião em sistema e afasta estagiários – notícias em Trânsito AM

25/02/2014 22h25 - Atualizado em 25/02/2014 22h25

Detran-AM descobre programa espião em sistema e afasta estagiários

Software espião foi instalado em computadores do órgão, diz Detran.
Três estagiários são suspeitos de receberem R$ 500 por ação realizada.

Marcos Dantas e Leandro Tapajós
Do G1 AM

3 comentários Tweetar 31 Recomendar 62

Leonel Feitoza confirmou o descobrimento da fraude (Foto: Reprodução/TV Amazonas)

Três estagiários, dos cursos de direito e tecnologia da informação, que atuavam no Departamento de Trânsito do Estado do **Amazonas** (Detran/AM) são suspeitos de participarem de um esquema de fraudes. Segundo informações do órgão, o trio teria implantado um software 'espião' que permitia realizar alterações em processos. Eles supostamente recebiam cerca de R$ 500 por ação realizada, entre elas a retirada de pontos de Carteiras Nacionais de Habilitação (CNHs). O esquema foi descoberto no fim de janeiro. Os suspeitos foram indiciados nessa segunda-feira (24) e devem responder por corrupção passiva. As informações sobre a fraude foram divulgadas à imprensa nesta terça-feira (25).

2014

- **Detran – AM**
- **Instalação de *spyware***
- **Fraude:**
  - **retirada de pontos de CNH**

http://g1.globo.com/am/amazonas/transito/noticia/2014/02/detran-am-descobre-programa-espiao-em-sistema-e-afasta-estagiarios.html

Exemplos de *insider threats* (4/6)

Navy Systems Admin. Faces Hacking Charge – GovInfoSecurity

www.govinfosecurity.com/navy-systems-admin-faces-hacking-c

Reader

Navy Systems Admin. Faces Hacking Charge

Allegedly Hacked Computer Systems of 30 Organizations

By Jeffrey Roman, May 6, 2014. Follow Jeffrey @gen_sec

Credit Eligible | Email | Tweet | Like | Share | Get Permission

A former systems administrator in the nuclear reactor department of an aircraft carrier is one of two individuals charged with hacking U.S. Navy computer systems and those at dozens of other government and commercial organizations.

The U.S. Attorney's Office for the Northern District of Oklahoma alleges that Nicholas Paul Knight of Chantilly, Va., and Daniel Trenton Krueger of Salem, Ill, conspired to hack computers and systems as part of a plan to steal identities, obstruct justice and damage a protected computer.

At the time of the hacking attacks, Knight was assigned to the nuclear aircraft carrier USS Harry S. Truman as a systems administrator in the nuclear reactor department. Krueger was a student at an Illinois community college where he studied network administration, prosecutors say.

Knight and Krueger were members of the hacking group Team Digi7al, the U.S. attorney's office alleges. Knight allegedly served as the group's self-proclaimed leader and publicist.

In June 2012, the Naval Criminal Investigative Service detected a breach of the Navy's Smart Web Move database. The database manages transfers for service members of all branches of the military, storing sensitive personal records, including Social Security numbers, names and dates of birth, for approximately 220,000 service members.

2014

- **Administrador de redes**
- **Alvo: Marinha americana e diversas empresas**
- **Objetivo:**
  - **furtar dados pessoais**
  - **danificar computador protegido**
- **Informações coletadas postadas via Twitter**
- **Membro do grupo *hacker* Team Digi7al**

http://www.govinfosecurity.com/navy-systems-admin-faces-hacking-charge-a-6816

Exemplos de *insider threats* (5/6)

2013

- Edward Snowden
  - vazamento de informações
  - uso de senhas de colegas de trabalho

http://www.govinfosecurity.com/navy-systems-admin-faces-hacking-charge-a-6816

Exemplos de *insider threats* (6/6)

San Francisco's Mayor Gets Back Keys to the Network | PCWorld

www.pcworld.com/article/148787/network.html Reader

SEARCH

PCWorld

SECURITY
business security, networking, storage & networking, network security, security

BUSINESS READY

San Francisco's Mayor Gets Back Keys to the Network

By Robert McMillan and Paul Venezia, IDG News Service, IDG News ServiceJul 23, 2008 1:30 AM

San Francisco Mayor Gavin Newsom met with jailed IT administrator Terry Childs Monday, convincing him to hand over the administrative passwords to the city's multimillion dollar wide area network.

Childs made headlines last week when he was arrested and charged with four counts of computer tampering, after he refused to give over passwords to the Cisco Systems switches and routers used on the city's FiberWAN network, which carries about 60 percent of the municipal government's network traffic. Childs, who managed the network before his arrest, has been locked up in the county jail since July 13.

On Monday afternoon, he handed the passwords over to Mayor Newsom, who was "the only person he felt he could trust," according to a declaration filed in court by his attorney, Erin Crane. Newsom is ultimately responsible for the Department of Telecommunications and Information Services (DTIS) where Childs worked for the past five years

2008

- **Administrador era o único a possuir a senha de acesso ao roteador**
- **insubordinação**

http://www.govinfosecurity.com/navy-systems-admin-faces-hacking-charge-a-6816

Categorias

Fonte: The CERT Guide to Insider Threats
http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310

Categorias (1/5)

Sabotagem

- **Causar danos à organização**
- **Perfil:**
  - **posições técnicas: administradores de redes, sistemas e dados**
  - **motivações:**
    - **descontentamento, falta de reconhecimento, sentir-se injustiçado**
  - **costumam ocorrer logo após a demissão**
    - **mas podem ter sido preparados há muito tempo**
- **Forma:**
  - **implantação de bombas lógicas (*logic bomb*)**
  - **inclusão de *backdoors* e outros *malware***
  - **mudança de senhas**
  - **exploração de vulnerabilidades**
  - **instalação de ferramentas maliciosas, de acesso remoto**
  - **desativação de *logs* e antivírus**
  - **extorsão**

Categorias (2/5)

Fraude

- Manipulação de dados para ganhos próprios
- Vazamento de dados
- Perfil:
  - funcionários ativos
  - durante horário de trabalho
  - conluio com atacantes externos
- Pode ficar muito tempo até ser detectado
- Quanto mais alto o cargo maiores podem ser os danos

Espionagem

- Entre países e empresas

Categorias (3/5)

Furto de propriedade intelectual

- **Espionagem industrial**
- **Informações furtadas para:**
  - **conseguir novo emprego**
  - **abrir negócio próprio**
  - **vender para outras empresas**
- **Envio de informações**
  - ***e-mail*, *pen-drive*, CDs**
  - **acessos indevidos**
  - ***notebooks*, dispositivos móveis**
  - **ssh, ftp, telnet**

Categorias (4/5)

Não intencionais

- **Causadas por uma ação:**
  - **uso de engenharia social**
  - **exemplos:**
    - **vazamento de informações**
    - **instalação de códigos maliciosos**
      - **APT, *malware*, *phishing***
    - **descarte de discos, *pen-drives*, papéis**
    - **perda de equipamentos**

Categorias (5/5)

Não intencionais

- **Causadas por falta de ação**
  - **omissão, desleixo, falta de comprometimento**
    - **NÃO instalação de correções de segurança**
    - **NÃO fazer *backups***
    - **NÃO utilizar criptografia**
    - **NÃO utilizar técnicas de programação segura**
    - **NÃO configurar os sistemas corretamente**
    - **NÃO usar senhas fortes**
    - **NÃO bloquear estação de trabalho**

- **BYOD, pode facilitar:**
  - **vazamento de dados**
  - **perda de dados**
  - **propagação de *malware***

Detecção e Prevenção

Fonte: The CERT Guide to Insider Threats
http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310

Detecção e prevenção (1/4)

- Empresas com dificuldade em perceber a extensão do problema
  - preocupadas mais com ameaças externas que internas
- Difíceis de serem prevenidos
  - atacantes exercendo ações autorizadas
  - possuem acesso legítimo a dados, sistemas e equipamentos
  - possuem conhecimento sobre sistemas, computadores, topologia, infra-estrutura, etc.
- Apenas indicadores técnicos são insuficientes
  - precisam ser combinados com indicadores comportamentais
- Criar grupo multidepartamental para lidar com esses casos
  - TI, RH, jurídico, etc
  - antecipar comportamentos negativos

Detecção e prevenção (2/4)

- **Modo de operação:**
  - **a partir do momento que um atacante externo possui acesso interno a uma rede/sistema pode agir da mesma forma que um atacante interno**
  - **proteção contra atacantes internos também previnem contra atacantes externos**
- **Devem ser incluídos na análise de risco**
- **Definição de políticas**
  - **separação de tarefas, privilégio mínimo**
  - **desligamento de funcionários**
  - ***backup* e recuperação de dados**
  - **BYOD**
- **Acordos claros com serviços de *cloud computing***

Detecção e prevenção (3/4)

- Gerenciamento de contas e senhas
  - controle de acesso restrito a usuários com acessos privilegiados
- Uso de ferramentas de correlação de *logs*
- Estabelecer o que é um comportamento "normal" de rede
- Controle e monitoração
  - *logs*, auditorias, *firewall*
  - acessos remotos
  - detecção pode ocorrer via relato de outros funcionários
    - desconfiança, mudanças comportamentais
- Ficar a atento a:
  - redes sociais
  - *data exfiltration (pen-drives*, HDs, CDs)

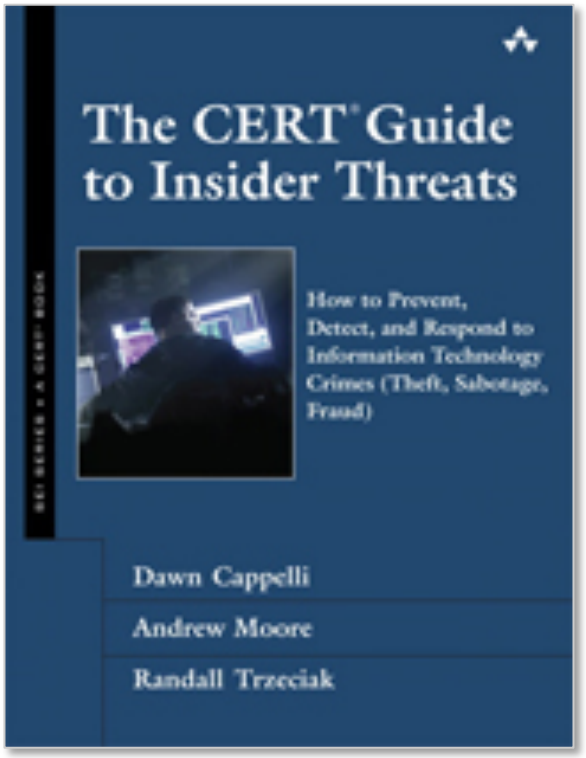
Detecção e prevenção (4/4)

- **Não intencionais:**
  - **treinamento constante contra:**
    - **engenharia social**
    - ***malware*, *phishing***
    - **proteção de informações**
  - **custos com treinamento e conscientização de usuários podem ser baixos se comparados com os danos que podem causados**

Leituras Recomendadas

The CERT Guide to Insider Threats

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



Perguntas?

Miriam von Zuben.
miriam@cert.br

- CGI.br – Comitê Gestor da Internet no Brasil
  http://www.cgi.br/
- NIC.br – Núcleo de Informação e Coordenação do .br
  http://www.nic.br/
- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  http://www.cert.br/
- Cartilha de Segurança para Internet
  http://cartilha.cert.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil