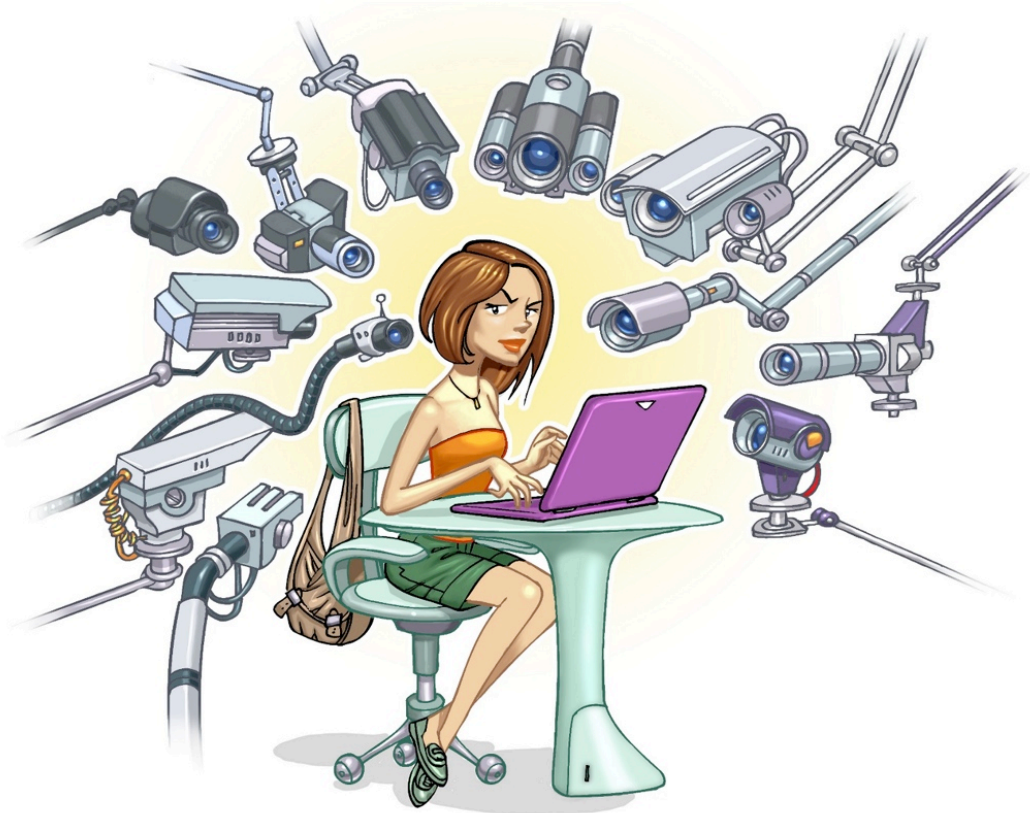
Privacidade e Segurança de Dados



Cristine Hoepers, D.Sc.
cristine@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

A privacidade e segurança dos dados dos cidadãos está cada vez mais nas mãos de terceiros

Privacidade com relação ao que está no computador e ao que se faz na Internet

- **dados armazenados**
- **acessos a sites e conteúdos**
  - **gostos, hábitos, opiniões**

Privacidade com relação a dados que precisam estar nos computadores de terceiros ou trafegar pela rede

- **depende destes terceiros manterem a confidencialidade**
- **serviços de *e-gov*, *e-health*, *e-commerce, e-**
  - **resultados *online* de exames, serviços de previdência, cartões de crédito, *sites* de nota fiscal, dados biométricos, RFIDs em carros e passaportes, preferências e histórico de compras, etc**

Estes dados estão protegidos?

- **exemplos crescentes de problemas nessa área...**

28 JUL 14

Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System

Three Israeli defense contractors responsible for building the "Iron Dome" missile shield currently protecting Israel from a barrage of rocket attacks were compromised by hackers and robbed of huge quantities of sensitive documents pertaining to the shield technology, KrebsOnSecurity has learned.

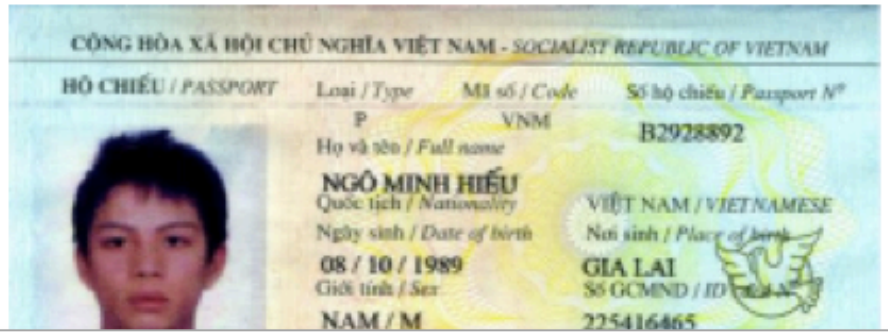
The never-before publicized intrusions, which occurred between 2011 and 2012, illustrate the continued challenges that defense contractors and other companies face in deterring organized cyber adversaries and preventing the theft of proprietary information.

According to CyberESI, IAI was initially breached on April 16, 2012 by a series of specially crafted email phishing attacks. Drissel said the attacks bore all of the hallmarks of the

Once inside the IAI's network, Comment Crew members spent the next four months in 2012 using their access to install various tools and trojan horse programs on systems throughout company's network and expanding their access to sensitive files, CyberESI said.

10 MAR 14 Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records

In October 2013, KrebsOnSecurity published an exclusive story detailing how a Vietnamese man running an online identity theft service bought personal and financial records on Americans directly from a company owned by **Experian**, one of the three major U.S. credit bureaus. Today's story looks deeper at the damage wrought in this colossal misstep by one of the nation's largest data brokers.



Last week, **Hieu Minh Ngo**, a 24-year-old Vietnamese national, pleaded guilty to running an identity theft service out of his home in Vietnam. Ngo was arrested last year in Guam by **U.S. Secret Service**

Experian came into the picture in March 2012, when it purchased Court Ventures (along with all of its customers — including Mr. Ngo). For almost ten months after Experian completed that acquisition, Ngo continued siphoning consumer data and making his wire transfers.

220 million records stolen, 16 arrested in massive South Korean data breach

by Lee Muns
FILED UNDER

Additionally, regulators fined three credit card companies and took away their card-issuing rights in February after 20 million residents had their data stolen by an IT contractor.

Then, in March, the government announced it was investigating another breach which had led to the compromise of 12 million names, resident registration numbers and bank account details from telecom company KT Corp.

South Kore
massive da
over half of

A group of hackers successfully compromised 220 million records containing personally identifiable information on 27 million people aged 15 to 65.

The breach came to light after 16 people were arrested following the theft of data from a number of online game and movie ticket sites.

The stolen records include real names, account names, passwords and resident registration numbers.

Hacker hijacks ISPs, steals $83,000 from Bitcoin mining pools | ZDNet

www.zdnet.com/hacker-hijacks-isps-steals-83000-from-bitcoin-mining

Reader

Hacker hijacks ISPs, steals $83,000 from Bitcoin mining pools

Summary: *Bitcoin exchanges and trading posts have been hacking targets over the past year, but now one hacker has taken on ISPs to loot Bitcoin from mining pools.*

By Charlie Osborne for Zero Day | August 8, 2014 -- 10:02 GMT (03:02 PDT)

Commer

A hijacker was able to use a fake Border Gateway Protocol (BGP) broadcast in order to compromise networks belonging to some of the biggest names in the field -- including Amazon, Digital Ocean, and OVH, among others -- between February and May 2014. According to the researchers, at least 51 networks were compromised from 19 different ISPs, and at least one hijacker was able to use this flaw to redirect cryptocurrency miners' connections to a hijacker-controlled mining pool, therefore collecting the miner's profit for themselves.


Point-of-sale malware has now infected over 1,000 companies in US | Ars Technica
arstechnica.com/security/2014/08/point-of-sale-malware-has-now-infected-over
Reader
MAIN MENU
MY STORIES: 25
FORUMS
SUBSCRIBE
JOBS
Point-of-sale malware has now infected over 1,000 companies in US
Program infects point-of-sale systems, steals credit-card details from businesses.
by Robert Lemos - Aug 25 2014, 2:29pm BRT
Share
Tweet
69
Critical crypto flaw in Facebook's WhatsApp for Android exposes chats | Ars Technica
arstechnica.com/security/2014/03/critical-crypto-flaw-in-facebooks-whatsapp-fo
Reader
MAIN MENU
MY STORIES: 25
FORUMS
SUBSCRIBE
JOBS
RISK ASSESSMENT / SECURITY & HACKTIVISM
Critical crypto flaw in Facebook's WhatsApp for Android exposes chats
Message history is wide open to theft and decryption by rogue apps, consultant says.
by Dan Goodin - Mar 12 2014, 2:30pm BRT
Share
Tweet
62

12 FEB 14 Email Attack on Vendor Set Up Breach at Target

The breach at **Target Corp.** that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation.

Last week, KrebsOnSecurity reported that investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to **Fazio Mechanical**, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of

US restaurant chain P.F. Chang's China Bistro plans to temporarily bring back manual credit card imprinting while it investigates a security breach that allowed hackers to steal customer payment card data from multiple stores.

P.F. Chang's turns to vintage 1970s tech after credit card breach

Restaurant chain goes old school as it investigates theft from multiple stores.

by **Dan Goodin** - June 13 2014, 1:47pm BRT

HACKING INTERNET CRIME 207

Consegue-se Quase Tudo no Mercado Negro

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale
http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

Russian Underground – Serviços Disponíveis

- **Pay-per-Install (global mix or specific country): $12–$550**
- **Bulletproof-hosting with DDoS protection: $2000 per month**
- **Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) $3000/month**
- **Programming: web server hacking $250; browser-in-the-middle $850; trojans $1300**
- **Windows rootkit (for installing malicious drivers): $292**
- **Linux rootkit: $500**
- **Hacking Facebook or Twitter account: $130**
- **Hacking Gmail account: $162**
- **Hacking corporate mailbox: $500**

"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per up

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

Fonte: Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**

Sistemas na Internet

Riscos

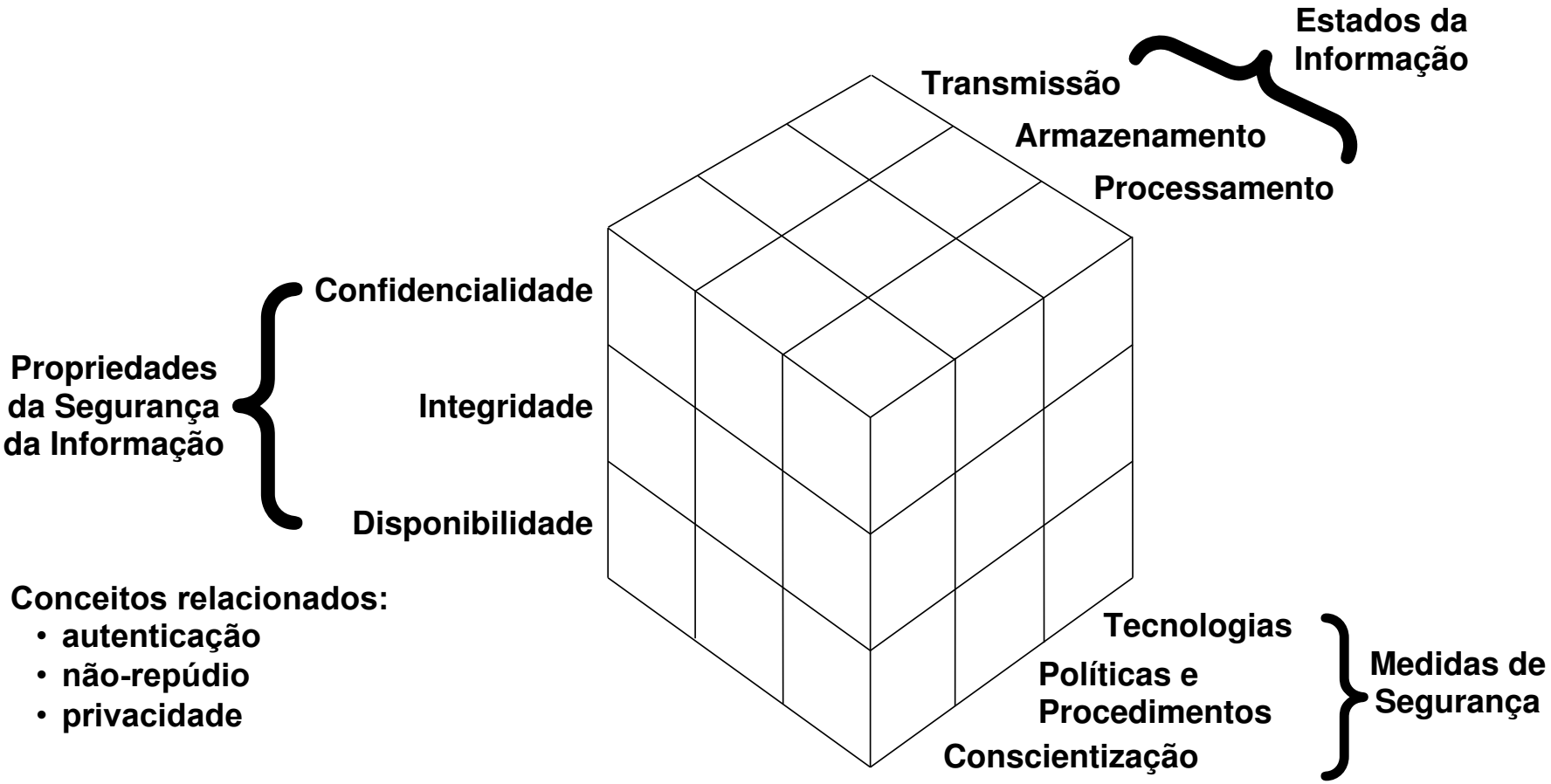
Ameaças

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

As informações estão em diversos locais e a segurança depende de múltiplos fatores



McCumber Information Security Model

http://www.ibm.com/developerworks/security/library/s-confnotes2/

Revendo Conceitos: Privacidade e Confidencialidade

- **Privacidade – habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.**

- **Confidencialidade – envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.**

Fonte: Security Engineering, 2nd Edition, 2008, Ross Anderson
http://www.cl.cam.ac.uk/~rja14/book.html

Privacidade é prejudicada com o cenário atual

Crescente demanda por serviços *online*

- Sistemas estão cada vez mais interconectados e interdependentes
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido

Segurança não é prioridade

- Impactos não são compreendidos
- Segurança não é parte do "*mindset*"
  - "alguém outro vai implementar"
- Dados tem muito valor para o crime organizado
  - bases de dados ("*big data*")
  - sistemas de e-gov
  - infraestruturas críticas
  - dados médicos

Desafios em aberto (1/3)

- **Privacidade não é só uma questão de evitar rastreamento**
  - **não são só hábitos de navegação que podem afetar a privacidade**
  - **não são só em *cookies* que estão informações que interessam à privacidade dos cidadãos**

- **Ir além do "*compliance*"**
  - **Seguir uma norma garante o mínimo de investimento de segurança**
  - **Maior parte das empresas com vazamentos de dados eram conformes**
    - **PCI/DSS, ISO 27000, SOX, etc**

- **Serviços Web estão construindo bases de dados massivas que já são alvo para**
  - **venda ou alteracão por atacantes internos**
  - **crime organizado**
  - **espionagem**

Desafios em aberto (2/3)

- **Não há "ferramenta de segurança" que consiga resolver os problemas**
  - **os sistemas precisam ficar online 100% do tempo**
  - **o tráfego com destino a eles não pode ser barrado**
- **Não é "só usar criptografia"**
  - **em algum momento os dados tem que estar disponíveis**
  - **crise de confiança nos padrões de criptografia**
    - **resultado das revelações de espionagem**
  - **já há um mercado negro de certificados digitais**
    - **há uma crise séria de confiança em sistemas de PKI/ICP**
- **Desenvolvimento seguro de *software* precisa se tornar parte da formação e do dia-a-dia de projetistas e desenvolvedores**
  - **desde a primeira disciplina e permeado em todas as disciplinas**
  - **inserido em todas as fases do ciclo de desenvolvimento**

Desafios em aberto (3/3)

- **Os serviços *online* (*e-mail*, redes sociais, *drives, *docs, buscas) não são gratuitos**
  - **pagamos com nossas informações, que valem muito**
  - **esse é o modelo de negócio, mas isto está claro para todos?**
- **Todos temos que fazer parte da solução para termos segurança e privacidade**
  - **todas as áreas de TI uma organização, principalmente**
    - **desenvolvedores de qualquer aplicação**
    - **administradores de redes**
    - **administradores de bancos de dados**
    - **webdesigners e webmasters**
  - **usuários de tecnologia**

Recomendação: Invista em Resiliência Operacional

Um sistema 100% seguro é muito difícil de atingir

Para conseguir uma segurança razoável é necessário:

- **Detectar comprometimentos o mais rápido possível**
  - **via novos métodos de *extrusion detection***
  - **atuando em notificações de incidentes**
  - **a tríade Firewall/IDS/Antivírus não é mais suficiente**
- **Diminuir o impacto**
  - **Conter, mitigar e recuperar o mais rápido possível**

Novo paradigma: Resiliência

- **Continuar funcionando mesmo na presença de falhas ou ataques**

Como Obter Resiliência

- Identificar o que é crítico e precisa ser mais protegido (Análise de Risco)
- Definir políticas (de uso aceitável, acesso, segurança, etc)
- Treinar profissionais para implementar as estratégias e políticas de segurança
- Treinar e conscientizar os usuários sobre os riscos e medidas de segurança necessários
- Implantar medidas de segurança que implementem as políticas e estratégias de segurança
  - como aplicar correções ou instalar ferramentas de segurança
- Formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes (CSIRTs)

Invista na Educação de seus Funcionários

Cartilha de Segurança para Internet

- Livro (PDF e ePub) e conteúdo no *site* (HTML5)
- Dica do dia no *site*, via *Twitter* e RSS
- http://cartilha.cert.br/

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Outros Materiais para Usuários Finais

Portal Internet Segura

- Reúne todas as iniciativas conhecidas de educação de usuários no Brasil

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/

Contatos

Cristine Hoepers, D.Sc.

cristine@cert.br

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