



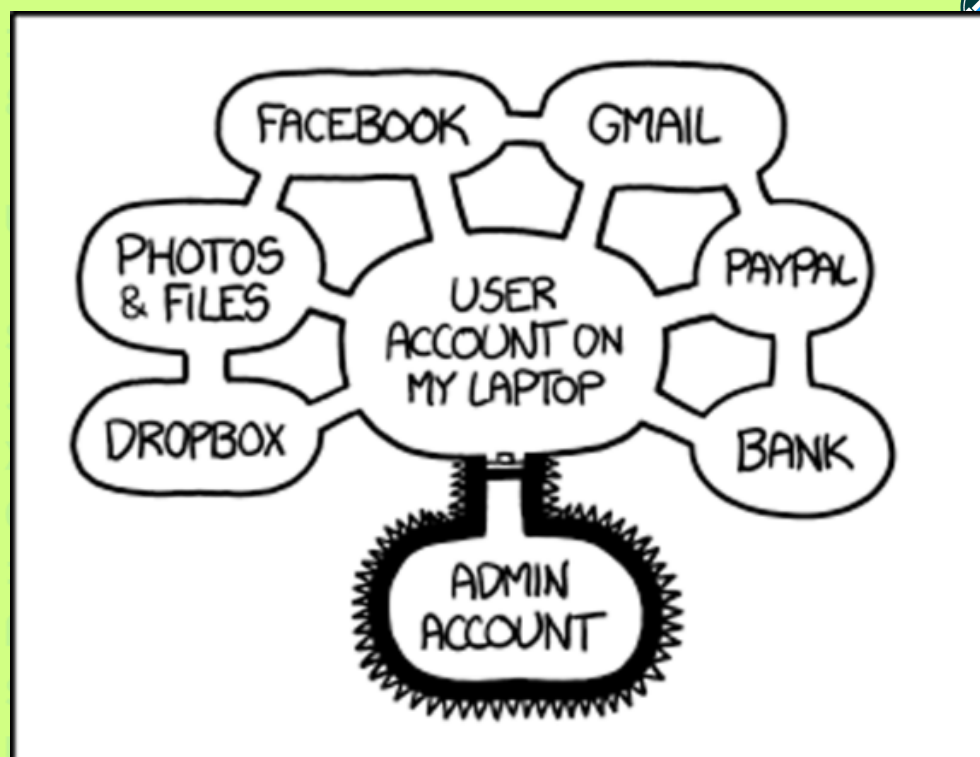
ROADSEC

**O Maior evento de Hacking e
Segurança da Informação do Brasil**

Fomos atacados, e agora?

Prof. Marcelo Caiado

M.Sc., CISSP, GCFA, GCIH, EnCE



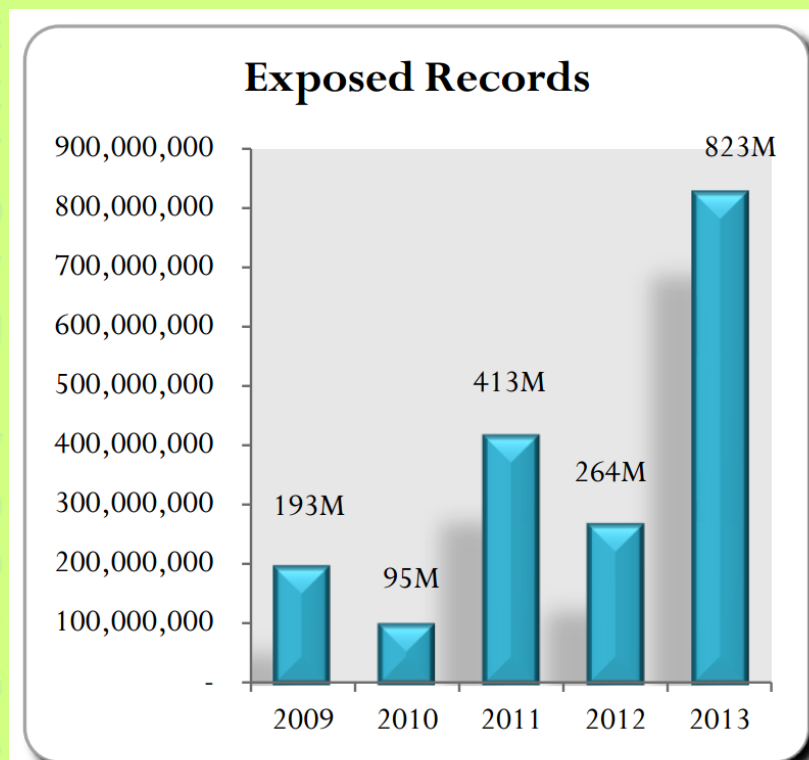
O início

IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS, BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Fonte: XKCD

2013 – Uma odisséia no vazamento de dados

Foram 2.164 incidentes relatados somente em 2013, que expuseram **822 milhões** de registros.



2013 – Uma odisséia no vazamento de dados

Breach Type	Number of Incidents	Percent of Total Incidents	Number of Records Exposed	Percent of Total Records Exposed
Fraud/Social Engineering	152	7.02%	102,21,936	1.24%
Hacking	1293	59.75%	592,596,691	72.05%
Unknown	66	3.05%	9,732,565	1.18%
Missing/Lost/Stolen Drive	30	1.39%	764,970	0.09%
Web	103	4.76%	138,648,221	16.86%
eMail	69	3.19%	730,924	0.09%
Government Seizure	1	0.05%	60,000,000	7.29%
Snail Mail	46	2.13%	318,678	0.04%
Other	78	3.60%	234,576	0.03%
Lost/Stolen/Missing Documents	62	2.87%	70,508	0.01%
Stolen Laptop	106	4.90%	1,996,320	0.24%
Stolen Computer	30	1.39%	4,189,553	0.51%
Skimming	34	1.57%	982	0.00%
Virus	29	1.34%	2,680,753	0.33%
Improper Disposal	65	3.00%	322,886	0.04%
Total	2164	100.00%	822,509,563	100.00%

2013 – Uma odisséia no vazamento de dados

- λ Mobile malware
- λ Cyber espionagem
- λ Ransomware
- λ Watering Hole
- λ APTs
- λ •••



EMERGÊNCIA

**EM CASO DE
EMERGÊNCIA
QUEBRE O VIDRO**

MAZ.COM.BR

Em caso de invasão

- ① Demitir o Diretor de Seginfo (CSO)
- ② Demitir o Diretor de T.I. (CIO)
- ③ Demitir o Presidente (CEO)
- ④ Demitir os membros do conselho
- ⑤ Fechar as portas da empresa...

Target is overhauling its information security practices, Gregg Steinhafel, the company's chairman, president and CEO, said in a statement. Target is searching for an interim CIO to help guide the company "through this transformation," he said.

In addition, Target is elevating its CISO role and hiring for that position and for a chief compliance officer, he added. The company has hired Promontory Financial Group "to help us evaluate our technology, structure, processes and talent as a part of this transformation," he said.

Target Expects \$148 Million Loss from Data Breach

Dan Kedney | Aug. 6, 2014



The bill comes due for one of the largest security breaches in retail history

Target estimates that losses from a 2013 data breach that compromised credit cards and account information for 40 million shoppers could cost upwards of \$148 million, the company said Tuesday.

The announcement came in advance of Target's second quarter earnings report, which would detail the losses incurred from claims placed by payment card networks



Customers walk outside a Target store August 14, 2013 in Springfield, Virginia.

Alex Wong/Getty Images

Target CIO Beth Jacob resigns in breach aftermath

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com

Do it!

Don't show me this again X

by Lisa Vaas on March 6, 2014 | 24 Comments
FILED UNDER: Data loss, Featured

Following its recent epic breach, Target has announced that it's putting its technology through the wringer.

Its CIO, Beth Jacob, has already gone down the drain.

The beleaguered US retailer announced on Wednesday that it's going to overhaul its information security practices.

At the same time, Target announced that Jacob has resigned - the first high-level executive to leave following a breach over the Christmas holiday shopping season.

That breach led to the theft of some 40 million credit and debit card records, along with another 70 million customer records.

That's a total of at least 70 million records, given that some of the two data sets may be duplicates. Naked Security took no pleasure in doing it, but given the likely size of the breach, we ushered Target into the "100 million plus" club, along with Adobe and Sony.

Target told Reuters in an email on Wednesday that it plans to replace Jacob with an external hire.

In January, Target admitted that there was malware on its point-of-sale (PoS) registers - what Naked Security's Paul Ducklin has assumed is a specialized botnet, designed to hook together Target's PoS registers into a network of data-stealing Trojans under criminal control.

Jacob had her hands on the reins during a time when, it turns out, a thorough security review had been advised by at least one analyst just months before the breach, prior to Target's planned upgrade of its payment system.

We don't know if the review actually happened, or whether it was lost in the cacophony of warnings security teams and government agencies constantly put forth.

But the buck, apparently, stopped at Jacob's desk.

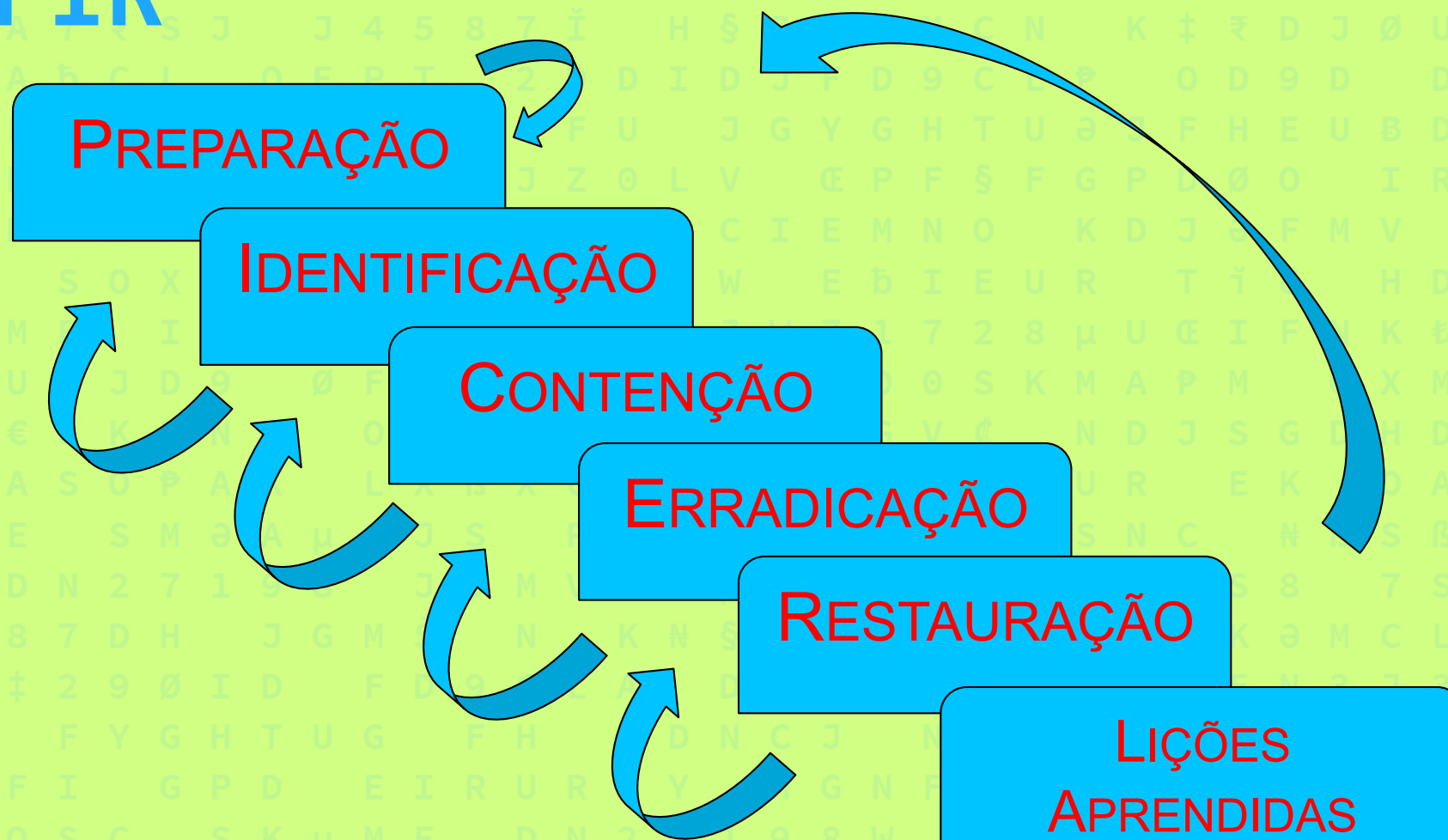




ADSEC

Atirar no que não se vê só tem efeito em um lugar : Hollywood.

DFIR



Cybersecurity Skills Crisis

Too Many Threats

 **62%**
INCREASE
IN BREACHES
IN 2013¹

1 IN 5 
ORGANIZATIONS
HAVE **EXPERIENCED**
AN APT ATTACK⁴

US \$3
TRILLION
TOTAL GLOBAL
IMPACT OF
CYBERCRIME³


 **8 MONTHS**
IS THE AVERAGE TIME
AN ADVANCED THREAT
GOES UNNOTICED ON
VICTIM'S NETWORK²

2.5
BILLION 
EXPOSED RECORDS AS
A RESULT OF A DATA BREACH
IN THE PAST 5 YEARS⁵

Too Few Professionals

 **62%**
OF ORGANIZATIONS
HAVE NOT INCREASED
SECURITY TRAINING
IN 2014⁶

 **1 OUT OF 3**
SECURITY PROS ARE
NOT FAMILIAR WITH
ADVANCED PERSISTENT
THREATS⁷

 **<2.4%**
GRADUATING STUDENTS
HOLD COMPUTER
SCIENCE DEGREES⁸

 **1 MILLION**
UNFILLED SECURITY
JOBS WORLDWIDE⁹

83% 
OF ENTERPRISES CURRENTLY
LACK THE RIGHT SKILLS AND
HUMAN RESOURCES TO PROTECT
THEIR IT ASSETS¹⁰

Enterprises are under siege from
a rising volume of cyberattacks.

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

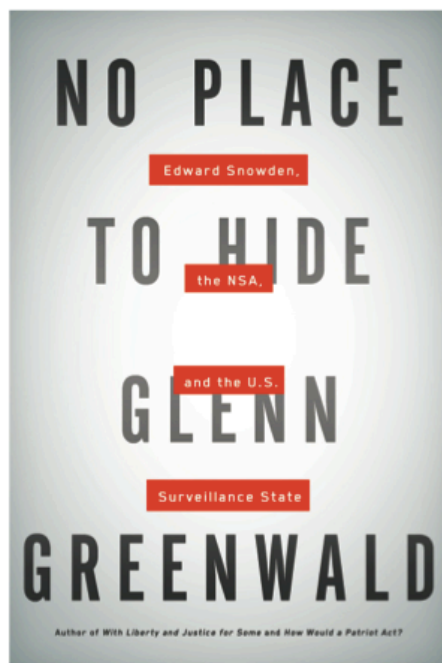
SOURCES: **1.** Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; **2.** M-Trends 2013: Attack the Security Gap, Mandiant, March 2013; **3.** Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; **4.** ISACA's 2014 APT Study, ISACA, April 2014; **5.** Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; **6.** ISACA's 2014 APT Study, ISACA, April 2013; **7.** ISACA's 2014 APT Study, ISACA, April 2014; **8.** Code.org, February 2014; **9.** 2014 Cisco Annual Security Report; **10.** Cybersecurity Skills Haves and Have Nots, ESG, March 2014



Obrigado Snowden!

DOCUMENTS FROM *NO PLACE TO HIDE*

Glenn Greenwald's *No Place to Hide* includes the following documents from the Snowden archive.
For discussion of these documents, please see the book at the page numbers indicated.



Page 120

OLYMPIA & THE CASE STUDY



CSEC's Network Knowledge Engine

Various data sources
Chained enrichments
Automated analysis

Brazilian Ministry of Mines and Energy (MME)

New target to develop
Limited access/target knowledge

Advanced Network Tradecraft - CSEC

TOP SECRET // SI

O quê fazer?



- ✓ Manter a cadeia de custódia
- ✓ Obter as evidências (memória, hds, pen drives, logs, etc)
- ✓ Não alertar o atacante
- ✓ Decidir se irá notificar (clientes, parceiros, imprensa, polícia, etc)

Os cinco W's

Quando?

When?

Quem?

Who?

Aonde?

Where?

O quê?

What?

Por quê?

Why?

Como?

How?

Fontes confiáveis

Unusual Log Entries

Check your logs for suspicious events, such as:

"Event log service was stopped."

"Windows File Protection is not active on this system."

"The protected System file [file name] was not restored to its original, valid version because the Windows File Protection..."

"The MS Telnet Service has started successfully."

Look for large number of failed logon attempts or locked out accounts.

To do this using the GUI, run the Windows event viewer:

```
C:\> eventvwr.msc
```

Using the command prompt:

```
C:\> eventquery.vbs | more
```

Or, to focus on a particular event log:

```
C:\> eventquery.vbs /L security
```

Other Unusual Items

Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager → Process and Performance tabs

Additional Supporting Tools

The following tools are not built into Windows operating system but can be used to analyze security issues in more detail. Each is available for free download at the listed web site.

DISCLAIMER: The SANS Institute is not responsible for creating, distributing, warranting, or supporting any of the following tools.

Tools for mapping listening TCP/UDP ports to the program listening on those ports:

Fport – command-line tool at www.foundstone.com

TCPView – GUI tool at www.microsoft.com/technet/sysinternals

Additional Process Analysis Tools:

Process Explorer – GUI tool at www.microsoft.com/technet/sysinternals
TaskMan+ -- GUI tool at <http://www.diamondcs.com.au>

The Center for Internet Security has released various Windows security templates and security scoring tools for free at www.cisecurity.org.

SANS
INSTITUTE

Intrusion Discovery

Cheat Sheet v2.0

Windows XP Pro /
2003 Server / Vista
POCKET REFERENCE GUIDE

SANS Institute

www.sans.org and isc.sans.org

Download the latest version of this sheet from
<http://www.sans.org/resources/winsacheatsheet.pdf>

Purpose

System Administrators are often on the front lines of computer security. This guide aims to support System Administrators in finding indications of a system compromise.

How To Use This Sheet

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Unusual Processes and Services
- Unusual Files and Reg Keys
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- Other Unusual Items
- Additional Supporting Tools

If you spot anomalous behavior: DO NOT PANIC!
Your system may or may not have come under attack. Please contact the Incident Handling Team immediately to report the activities and get further

Programas gratuitos (*)

Overview Why OpenIOC? Schema Tools OpenIOC FAQ Resources

Get The Tools

IOC Editor

Following MANDIANT's long tradition of providing free tools, MANDIANT has created the **IOC Editor**, which allows users to create, edit and compare Indicators of Compromise in XML format.

[Download](#)

Redline

Redline enables users to conduct investigations and search for Indicators of Compromise on a single host, allowing for everything from testing to finding evil during the course of actual investigations.

[Download](#)

Frequently Asked Questions

What is OpenIOC?

- Anti-Malware Tools
- Assessment Utilities
- Forensic Tools
- Foundstone SASS Tools
- Intrusion Detection Tools

Attacker v3.0
Attacker v3.0 - A TCP/UDP port listener.

Carbonite
Carbonite v1.0 - A Linux Kernel Module to aid in RootKit detection.

FileWatch
FileWatch v1.0 - A file change monitor. Used with BlackICE Defender.

FPort
FPort v2.0 - Identify unknown open ports and their associated applications.

IPv4Trace
IPv4Trace v1.0 - A Win32 C++ programming library port of the OpenBSD 2.8 kernel-land IPv4 fragment reassembly implementation.

Windows Sysinternals

The Sysinternals web site was created in 1996 by [Mark Russinovich](#) and Bryce Cogswell to host their advanced you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose.

Get up to speed fast!

- Read the official guide to the Sysinternals tools, [The Windows Sysinternals Administrator's Reference](#)
- Watch Mark's top-rated [Case-of-the-Unexplained](#) troubleshooting presentations and other webcasts
- Read [Mark's Blog](#) which highlight use of the tools to solve real problems
- Check out the Sysinternals [Learning Resources](#) page
- Post your questions in the [Sysinternals Forum](#)

DECRYPTION PRODUCTS

FTK IMAGER

FTK Imager version 3.2.0 [Download](#) Release Date: J

MD5: 966b626b872561fdee4ca01976cda42d

[Release Notes](#)
[User Guide](#)

FTK Imager Lite version 3.1.1 [Download](#) Release Date: Oc

COMMAND LINE VERSIONS OF FTK IMAGER

UTILITIES

LICENSE MANAGER

Contenção

- ✓Prevenir o atacante de obter outros acessos
- ✓Estabelecer salvaguardas e evitar profiliação
- ✓Considerar criticidade, sensibilidade e categorias



Erradicação

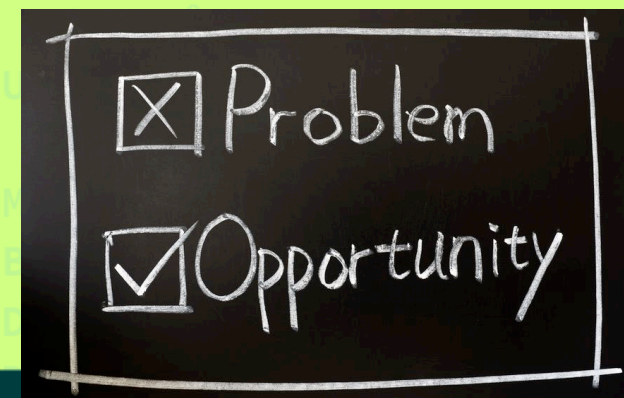
- ✓ Remover definitivamente artefatos utilizados pelo atacante
- ✓ Determinar causas e sintomas do incidente
- ✓ Melhorar as defesas

Restauração

- ✓ (Re)colocar os sistemas em produção
- ✓ Validar os sistemas
- ✓ Monitorar possíveis reinfecções, bem como malware ainda não identificado

Lições Aprendidas

- ✓ Documentar e melhorar processos e capacidades
- ✓ Aplicar correções PPT: pessoas, processos e tecnologia



Cadeia de custódia

✓ Processo que garante a integridade dos dados:

- ✓ Tal que não sejam contaminados ou perdidos
- ✓ É composto por documentação e testemunho
- ✓ Armazenamento em local seguro
- ✓ Pode-se fazer uso de Ata Notarial



Engajamento jurídico

“Computação Forense é coleta e análise de dados de uma forma tão livre de distorção ou viés quanto possível, para reconstruir os dados ou o que aconteceu no passado em um sistema” –
Farmer & Venema, 1999

Engajamento jurídico



CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988

TÍTULO II

Dos Direitos e Garantias Fundamentais

CAPÍTULO I

DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS

Art. 5º Todos são iguais perante a lei (...)

**LVI - são inadmissíveis, no processo, as
provas obtidas por meios ilícitos;**

Legislação



✓Brasil

- ✓Constituição Federal
- ✓Leis 8.112, 9.504, 9.605, 10.703, 12.527, 12.737, 12.965, etc
- ✓Decretos 2.556, 3.294, 3.505, 7.724, 7.845, 8.135, 8.159, etc
- ✓Lei Geral das Telecomunicações
- ✓Código de Defesa do Consumidor
- ✓CPC – Artigos 145-147 e 420 e seguintes

✓Mundo

- ✓Clientes e fornecedores fora do Brasil
- ✓Regulamentações específicas internacionais

Desafios

- ✓Efeito CSI
- ✓Restrições orçamentárias: hardware, software, treinamento, certificações, pessoal
- ✓Falta de pessoal qualificado, de uma equipe formal de resposta a incidentes e de estratégias
- ✓Falta de comprometimento da alta adm.
- ✓Computação em nuvem
- ✓APTs
- ✓Backlogs
- ✓Incremento dos crimes cibernéticos
- ✓Utilização de criptografia e anti-forense
- ✓Capacidade das mídias de armazenamento
- ✓Novas mídias
- ✓MOM
- ✓Questões legais

Links úteis

- ✓ DFIR – <http://dfir.com.br>
- ✓ HTCIA Brasilia –
<http://www.facebook.com/HTCIABrasilia>
- ✓ Schneier on Security –
<https://www.schneier.com/>
- ✓ Krebs on Security – <http://krebsonsecurity.com/>
- ✓ SANS Institute Blogs –
<http://www.sans.org/security-resources/blogs>



ROADSEC

“Existem apenas dois tipos de empresas: as que foram hackeadas, e aquelas que serão. Mesmo isto está se fundindo em uma única categoria: as que foram hackeadas e serão novamente.”

ROBERT MUELLER – Diretor do FBI



ROADSEC

Obrigado!

@mbcaiado