

Ameaças à segurança de redes de comunicação

CCNA Security - Ch. 1 - Modern Network Security Threats



Objectivos:

1. Sensibilização para o tema da segurança da informação
2. Descrever a perspectiva histórica da segurança em redes
3. Descrever as principais organizações envolvidas na segurança
4. Descrever os domínios da segurança de informação
5. Descrever o que são políticas de segurança
6. Descrever vírus, vermes e cavalos de Tróia
7. Descrever como mitigar vírus, vermes e cavalos de Tróia
8. Descrever como os ataques de rede podem ser categorizados
9. Descrever ataques de reconhecimento, acesso e DoS
10. Descrever como mitigar ataques de rede

Tópicos

1. Motivação
2. Enquadramento histórico;
3. Princípios Fundamentais da Segurança da Informação
4. Instituições
5. Gestão de Segurança da Informação
6. Ciber-ameaças & Mitigação
7. Metodologias de ataques em rede
8. Mitigação de ataques em rede

Motivação

DEIS

Motivação

- Será o uso de um cadeado adequado?



- Depende do “bem seguro”.
 - O valor do bem seguro é subjetivo. A segurança é um sentimento.
- Depende de quanto tempo e como fica o cadeado exposto.
 - A segurança não é absoluta nem definitiva. O contexto (tempo, espaço, envolvente social, ...) influencia amplamente a segurança.

Motivação

- Será esta uma boa estratégia?



In <http://www.seguranca24.pt/>

SEGURANÇA É UMA ARTE NÃO É UM "KIT".

O nosso conceito de fazer segurança.

Para que um sistema de segurança seja realmente seguro, o intruso não deve "saber" como este funciona. Por esse motivo os sistemas de

In <http://www.nist.org/>

*"System security
should not depend on
the secrecy of the
implementation or its
components."*

- “Segurança por ocultação” (*security by obscurity*) é uma estratégia possível mas limitada, perigosa e desencorajadora.

- No entanto, divulgar as estratégias publicamente pode também revelar-se um problema ... (Até ao ano 2000 a legislação americana equiparou sistemas de encriptação com chaves de 40 ou mais bits a “armamento” para efeitos de limitação à exportação. Porquê? Porque esta tecnologia poderia dificultar acções de violação de privacidade que poderiam interessar ao Estado.)

Motivação

- E, já que falamos dos EUA, ...

[NSA Planted Stuxnet-Type Malware Deep Within Hard Drive Firmware](#)



The U.S. National Security Agency (NSA) may be hiding highly-sophisticated hacking payloads in the firmware of consumer hard drives over the last 15 to 20 years in a campaign, giving the agency the means to eavesdrop on thousands of targets' computers, according to an analysis by Kaspersky labs and subsequent reports.

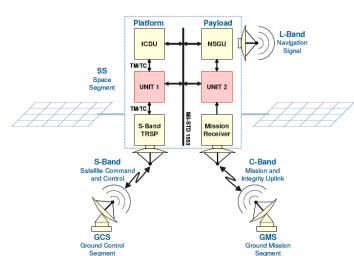
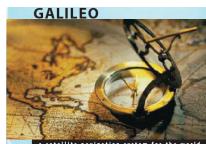
<http://thehackernews.com/2015/02/hard-drive-firmware-hacking.html>

The U.S. **National Security Agency (NSA)** may be hiding highly-sophisticated hacking payloads in the firmware of consumer hard drives over the last 15 to 20 years in a campaign, giving the agency the means to eavesdrop on thousands of targets' computers, according to an analysis by Kaspersky labs and subsequent reports.

Samsung, Western Digital, Seagate, Maxtor, Toshiba and Hitachi.

Motivação

- A segurança começa na concepção



Pedro
Pereira

Motivação

Primeiros dois satélites do GPS europeu são lançados quinta-feira

19.10.2011 - 21:29 Por Nicolau Ferreira

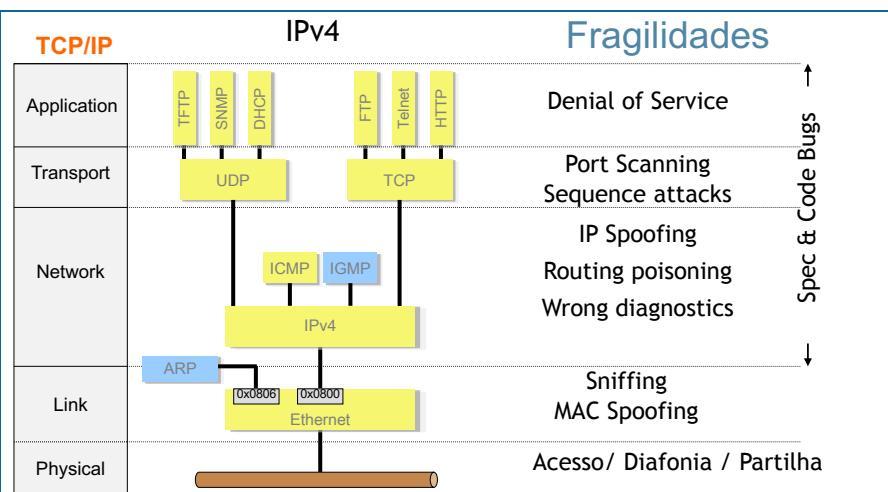
Votar ★★★★★ | 4 votos ★★★★

5 de 5 notícias em Ciências « anterior

Os dois primeiros satélites do sistema Galileu vão ser lançados quinta-feira, a partir da Guiana Francesa, na América do Sul, às 11h34 (hora de Lisboa). Os aparelhos integram o sistema de posicionamento geográfico, uma espécie de GPS europeu e serão transportados por um Soiuz – uma estreia na parceria entre russos e europeus que fez com que pela primeira vez um foguetão russo seja lançado fora dos dois cosmódromos utilizados por Moscou.



Motivação



Motivação

- A fragilidade do TCP/IP justifica muitas notícias como esta ...
Daily Telegraph, 12-Set-2008

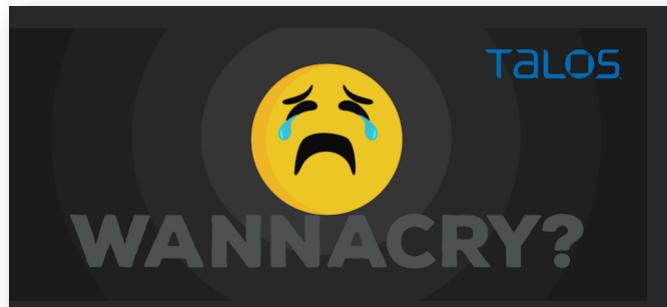


Maior acelerador do mundo sofreu ataque de “hackers” durante experiência

As primeiras partículas estavam a circular no Grande Acelerador de Hadrões, perto de Genebra, onde nasceu a World Wide Web, quando um grupo de “hackers” grego invadiu o sistema com o único objectivo de mostrar a sua fragilidade. Ao que parece, se o regresso ao “Big Bang” foi um sucesso, os piratas informáticos também foram bem sucedidos no seu objectivo: mostrar aos cientistas que estes não passavam de “um bando de miúdos da escola”, segundo noticia o jornal britânico “Daily Telegraph”.

Motivação

- **WannaCry Ransomware Attack (FRIDAY, MAY 12, 2017)**



Os clientes da PT ficaram sem acesso ao email até dia 13 à noite e ficaram com duas mailboxes.

<http://blog.talosintelligence.com/2017/05/wannacry.html>

A major ransomware attack has affected many organizations across the world reportedly including [Telefonica](#) in Spain, the [National Health Service](#) in the UK, and [FedEx](#) in the US. The malware responsible for this attack is a ransomware variant known as 'WannaCry'.

Motivação

- E esta ...

Google hack raises serious concerns, U.S. says

Secretary of State Hillary Clinton asks the Chinese government for an explanation

By Robert McMillan IDG News Service

January 13, 2010 01:41 AM ET

[Share/Email](#) [Tweet This](#) [1 Comment](#) [Print](#) [Newsletter Sign-Up](#)

A coordinated hacking campaign targeting Google, Adobe Systems and more than 30 other companies raises serious concerns, U.S. Secretary of State Hillary Clinton said Tuesday.

[Data breaches in the past 12 months](#)

In a [statement](#) released late Tuesday night, Clinton said that the U.S. government is taking the attack -- which [Google](#) said came from China -- very seriously. "We have been briefed by Google on these allegations, which raise very serious concerns and questions," she said. "We look to the Chinese government for an explanation."

Sources familiar with the situation say that more than 30 U.S. companies, including [Adobe Systems](#), were hit by this targeted attack, which Google first discovered in mid-December. Using an attack that exploited an unpatched bug in widely used software, the attackers were able to gain footholds in these companies and siphon out valuable intellectual property.

Related Content

- Google's 10 toughest rivals/a>
- GOOGLE SUBNET: Blogs, videos, giveaways for Google

In Google's case the attackers also gained access information about the e-mail accounts of Chinese dissidents.



Google desafia governo chinês e admite poder vir a ser forçada a sair do país

08-04-PUBLICO
A gigante de Internet Google está em rota de colisão com o governo chinês e já admittiu poder vir a ser forçada a sair do país.

Motivação

- E esta ...

Critical NASA network was open to Internet attack

Network is used to run Space Shuttle, International Space Station and Hubble Telescope missions

By Tim Greene, Network World
March 23, 2011 01:49 PM ET

[Comment](#) [Print](#) [Recommend](#) 42 people recommend this.

Six [NASA](#) servers exposed to the Internet had critical vulnerabilities that could have endangered Space Shuttle, [International Space Station](#) and [Hubble Telescope](#) missions -- flaws that would have been found by a [security](#) oversight program the agency agreed to last year but hasn't yet implemented, according to a [report by the agency's inspector general](#).

NASA's CIO [Linda Cureton](#) says she has patched the vulnerabilities, but IG Paul Martin found that NASA still has no ongoing program for spotting and correcting similar problems as they arise and is giving itself until the end of September just to come up with a plan, according to the report titled "Inadequate Security Practices Expose Key NASA Network to Cyber Attack." The deadline for the plan is Sept. 30.

MORE ON SPACE: [Gigantic changes keep space technology hot](#)

The six vulnerable servers were associated with IT projects that control spacecraft or contain critical NASA information, the report says. The audit also found other servers that exposed encryption keys, encrypted passwords and user-account information, all of which could enable attackers to gain unauthorized network access. The report didn't assess the agencywide network that isn't directly used for missions.

Motivação

- E esta ...

Hackers roubaram dados de jogadores da PlayStation

26.04.2011 - 23:05 Por PÚBLICO

Votar ★★★★★ | 3 votos ★★★★☆

5 de 5 notícias em Tecnologia < anterior

A Sony emitiu um comunicado em que avisa os utilizadores da plataforma online da PlayStation de que um *hacker* roubou dados pessoais, que podem incluir cartões de crédito.



A Sony está a investigar o caso. (Foto: Reprodução)

Motivação

- E esta ... Após greve geral **Hackers divulgam dados pessoais de 107 polícias de Lisboa e ameaçam toda a PSP**

29.11.2011 - 08:10 Por José Bento Amaro

Votar  | 46 votos 

1 de 30 notícias em Sociedade [seguinte »](#)

Um grupo intitulado Lulzsec Portugal terá acedido ilegalmente aos computadores do Ministério da Administração Interna (MAI), copiado e divulgado os dados pessoais de mais de uma centena de efectivos da PSP a trabalharem em três esquadras de Lisboa. Num texto resumido, acompanhado do endereço onde os dados pessoais podem ser consultados, os *hackers* ameaçam vir a divulgar os elementos de todo o efectivo da PSP, argumentando que tal acontece como represália pelos actos de violência que terão sido praticados contra pessoas que, no dia 24, participaram, em frente à Assembleia da Repúblíca, no protesto da greve geral.



Hackers acederam a dados pessoais de polícias, guardas e

bombeiros (Foto: Patricia de Melo Moreira/AFP)

Motivação

- E esta ...

Site do Parlamento em baixo na sequência de ataque

29.11.2011 - 22:08 Por João Pedro Pereira

Votar  | 13 votos 

15 de 16 notícias em Política [« anterior](#) [seguinte »](#)

O site do Parlamento ficou inacessível, pouco tempo depois de o grupo LulzSec Portugal ter anunciado no Twitter que este seria o próximo alvo de um ataque.



O ataque ao site do Parlamento foi anunciado no Twitter (Nuno Ferreira Santos)

Motivação

- E tb se investiga ...

Criador do Tugaleaks detido por ataque informático à Procuradoria de Lisboa

EM ACTUALIZAÇÃO PEDRO SALES DIAS & MARIANA OLIVEIRA 26/02/2015 - 12:24

Mais seis pessoas foram detidas em 24 buscas realizadas em Lisboa e Porto. Detidos estarão ligados aos Anonymous.



Motivação

- E se contra-ataca

Hackers voltam a atacar e exigem libertação de membros dos Anonymous

CLAUDIA BANCALERO 27/02/2015 - 12:40

Ataque a site do ICS. Ação acontece um dia depois de operação da Polícia Judiciária ter levado à detenção de sete pessoas.



Motivação

- E esta ...

TeamPoison preparam "Operação Robin Hood"

Hackers divulgam palavras-passe de e-mails da ONU

29.11.2011 - 21:00 Por Hugo Torres

Votar ★★★★★ | 6 votos ★★★★★

4 de 5 notícias em Tecnologia « anterior seguinte »

As Nações Unidas são o mais recente alvo dos TeamPoison, grupo de *hackers* que publicou online os nomes de utilizador e as respectivas palavras-chave de mais de um milhar de e-mails de funcionários das Nações Unidas, da Organização de Cooperação e de Desenvolvimento Económico e da Organização Mundial de Saúde.



O Programa das Nações Unidas para o Desenvolvimento é o mais afectado (Reuters)

Motivação

- E esta ...

A partir do quarto, jovem argentino desvia mais de 37 mil euros por mês

PÚBLICO 14/09/2013 - 18:38

Um argentino de 19 anos foi detido por suspeita de liderar um esquema de fraude informática através da qual desviava mensalmente cerca de 50 mil dólares por mês (37.600 euros). O jovem, que já foi apelidado pela polícia argentina de “superhacker”, era investigado há mais de um ano.

...

Na última sexta-feira, dia da detenção, a polícia ordenou que fosse cortado o abastecimento de electricidade na zona da residência do suspeito em San Cristóbal, um bairro em Buenos Aires, para impedir que este destruísse provas que pudesse levar à sua acusação.

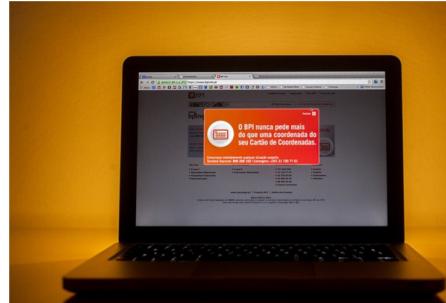
Motivação

- E quem paga, quem é?

Supremo condena BPI num caso em que empresa foi vítima de ataque informático

ANA HENRIQUES 20/01/2014 - 07:18

Acórdão defende que riscos de burla dos sistemas informáticos de *homebanking* têm de correr por conta dos bancos.



"Por conta" dos bancos

Quando, naquele dia da Primavera de 2008, Ana Bela Fernandes entrou no BPI Net para verificar se um cheque que havia passado a um fornecedor já tinha sido descontado, ainda o banco Lehman Brothers não se tinha tornado à escala planetária o rosto de uma crise financeira sem precedentes. Ana Bela usava o serviço centenas de vezes sem problemas, e dessa vez também não notou nada de especial, embora não tivesse conseguido entrar no sistema à primeira. Só três dias depois, ao fazer uma consulta no BPI Net pela última vez haviam voado 13 mil euros da sua firma, a Trading XXI, para uma conta desconhecida. Ainda tentou que o seu banco cancelasse a transferência, mas sem sucesso. "Entrou no que pensou ser a página do banco para efectuar as suas operações, sem se dar conta que estava afinal numa página clonada", descreve o acórdão de Dezembro do Supremo Tribunal de Justiça. E quando forneceu os códigos de segurança para poder aceder à conta da empresa estava, na realidade, a entregá-los aos burlões. A sócia-gerente e o banco foram **vítimas de pharming**, uma modalidade sofisticada de **phishing**.

Motivação

- Como fazer dinheiro de modo lícito com a insegurança?
Microsoft will pay you to successfully hack Windows

June 26, 2013

 By Brian Fagioli | Published 1 month ago | [Follow @brianfagioli](#)

 9 Comments

 Like 52  Share 8  +1 31  Tweet 26

Typically, a company frowns upon having its products hacked. However, Microsoft is inviting people to do just that. The tech company announces that it will be offering direct cash payments "in exchange for reporting certain types of vulnerabilities and exploitation techniques". No, Microsoft has not gone crazy (at least I hope). Companies usually offer such bounty programs for sane reasons -- security and publicity.



From a security standpoint, it makes sense for Microsoft to invite people to hack its products. When a bug or exploit is found, it can be patched. The tech company's products can only get more secure as a result. Heck, maybe Microsoft can even hire the successful hackers!

From a publicity standpoint, Microsoft can't lose. There are essentially two outcomes -- products get hacked or they don't. If no one is successful in hacking Windows, the company can tout its product's security. However, if a product *is* hacked, Microsoft can get positive press from its relationship with the security community and the paying of cash prizes.

<http://beta.news.com/2013/06/20/microsoft-will-pay-you-to-successfully-hack-windows/>

Motivação

- Até que ponto é lícito a NSA ser um *Man-In-the-Middle*?

NSA violou regras de espionagem milhares de vezes

PÚBLICO | 16/08/2013 - 08:43
Auditória revelada por Edward Snowden diz que agência americana não seguiu as normas e espiou sem autorização.



<http://www.publico.pt/mundo/noticia/nsa-violou-regras-de-espionagem-milhares-de-vezes-1603213>

Motivação

- Até que ponto é lícito a NSA ser um *Man-In-the-Middle*?

Edward Joseph Snowden¹ (*Elizabeth City, 21 de junho de 1983*) é um ex-analista de inteligência americano² que tornou públicos detalhes de várias programas altamente confidenciais de vigilância eletrônica dos governos de Estados Unidos e Reino Unido.^{3 4} Snowden era um colaborador terceirizado da Agência de Segurança Nacional (NSA) e foi também funcionário da Central Intelligence Agency (CIA).

A revelação deu-se através dos jornais *The Guardian* e *The Washington Post*, dando detalhes da vigilância de comunicações e tráfego de informações executada pelo programa de vigilância PRISM dos Estados Unidos.^{5 6 7 8} Em reação às revelações, o Governo dos Estados Unidos acusou-o de roubo de propriedade do governo, comunicação não autorizada de informações de defesa nacional e comunicação intencional de informações classificadas como de inteligência para pessoa não autorizada.⁹

Edward Snowden	
Nome completo	Edward Joseph Snowden
Conhecido(a) por	Revelar detalhes dos programas de vigilância do governo dos Estados Unidos
Nascimento	1983 (30 anos) Elizabeth City, Carolina do Norte, EUA
Residência	desconhecido/território desconhecido
Nacionalidade	norte-americano
Ocupação	Administrador de sistemas
Prémios	Indicado ao Prémio Nobel da Paz de 2014
Empregador	Baillie Allen Hamton (até 10 de junho de 2013)
Cargo	Analista de segurança da informação
Salário	US\$ 122.000,00 por ano

http://pt.wikipedia.org/wiki/Edward_Snowden

Motivação

- Citizenfour: documentário que retrata a trajetória de Edward Snowden durante as revelações de junho de 2013



Monsieur, je ne sais même pas votre nom ! Oh, pardon, je m'appelle Edward Snowden, ou "Ed"

<https://pt.wikipedia.org/wiki/Citizenfour>

Motivação

- Até que ponto é lícito a NSA ser um *Man-In-the-Middle*?

EUA acusaram formalmente ex-espião que divulgou programas da Agência Nacional de Segurança

PÚBLICO 22/06/2013 - 10:10

Edward Snowden está refugiado em Hong Kong desde 20 de Maio e foi agora acusado de espionagem, roubo e uso inapropriado de informações do Governo.



Muitos consideram Snowden um herói mas também há quem o considere um terrorista (Foto: TAUAN/AP)

TÓPICOS >
Hong Kong
China

Os Estados Unidos já acusaram formalmente Edward Snowden, um ex-funcionário da Agência Nacional de Segurança (NSA) dos EUA e que divulgou vários dados sobre o rolo de espionagem norte americana. Foi já enviada uma ordem de detenção para Hong Kong, onde o ex-espião se encontra refugiado desde 20 de Maio.

União Europeia é um dos principais alvos da espionagem norte americana

AGÊNCIA FRANCESA DE PRESSE

Revista alemã Der Spiegel revela novos documentos recolhidos pelo analista informático Edward Snowden.



Ou seja, os EUA dão especial atenção à política externa, comércio internacional e estabilidade económica (Foto: DPA)

TÓPICOS >
Europa
Alemanha

A União Europeia é um dos principais alvos dos programas de espionagem dos Estados Unidos, de acordo com documentos confidenciais recolhidos pelo analista informático Edward Snowden e divulgados neste sábado pelo site da revista alemã Der Spiegel.

<http://www.publico.pt/ultimas/internacional/5098980/atores-na-mira-da-nsa-na-europa>

Motivação

- Até que ponto é lícito a NSA ser um *Man-In-the-Middle*?

Programa da NSA recolhe "quase tudo o que um utilizador comum faz na Internet"

ALEXANDRE MARTINS 31/07/2013 - 22:31

Jornal britânico *The Guardian* revela documentos facultados por Edward Snowden sobre o programa XKeyscore.



O XKeyscore permite o acesso a mensagens privadas do Facebook, por exemplo MICHAEL CALDERREUTERS

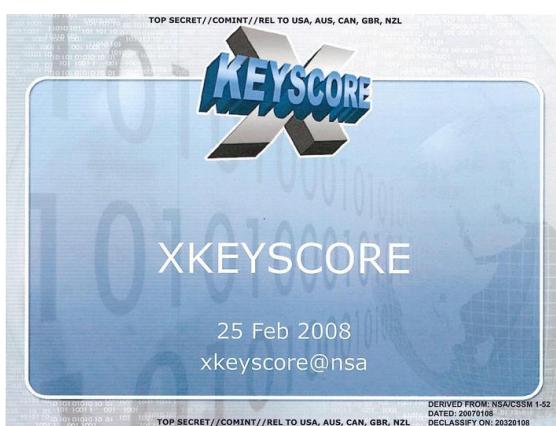
A Agência de Segurança Nacional dos Estados Unidos usa um programa para recolha de dados em larga escala que lhe permite aceder a "quase tudo o que um utilizador comum faz na Internet", incluindo o conteúdo de emails, mensagens privadas trocadas no Facebook e o histórico da navegação de sites, revela o jornal *The Guardian*.

O programa, chamado XKeyscore, já tinha sido referido de uma forma superficial pela revista alemã *Der Spiegel*, no início da semana passada, mas o jornal britânico publicou nesta quarta-feira [uma apresentação interna](#) da Agência de Segurança Nacional (NSA, na sigla em inglês), facultada pelo analista informático Edward Snowden.

<http://www.guardian.co.uk/world/2013/jul/31/nsa-xkeyscore-programme>

Motivação

- O front-end da rede de sondas de atividade on-line



<http://www.wired.com/gadgets/reviews/xkeyscore-control-panel.html>

Motivação

- Até que ponto é lícito a NSA ser um *Man-In-the-Middle*?

Alemanha cancela acordo de espionagem com EUA e Reino Unido

PÚBLICO 02/09/2013 - 08:09

Fim do pacto, assinado na década de 1960, é visto como uma medida para acalmar debate sobre espionagem no país.



Os alemães debatem a privacidade online a poucas semanas das eleições THOMAS PETER/REUTERS

Estados Unidos espiaram Dilma Rousseff

PÚBLICO 02/09/2013 - 13:48

Ministro da Justiça brasileiro vai a Washington pedir explicações. Actual Presidente do México também foi escutado pela NSA.



Dilma tem uma visita aos EUA marcada para Outubro. JESSICA MARCEL/REUTERS

Motivação

- Até que ponto é lícito a NSA ser um *Man-In-the-Middle*?

Gigantes da Internet formam grupo para mudar regras de vigilância da NSA

PÚBLICO 09/12/2013 - 08:59

Facebook, Google, Microsoft, Apple são algumas das empresas que assinam carta comum que pede mais responsabilização, transparência e limite à autoridade dos governos para recolher a informação depois do caso lançado por Edward Snowden.

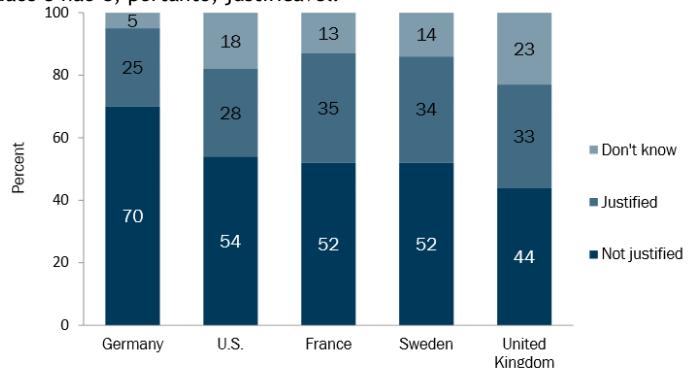


Acha que há justificação para que o seu Governo recolha dados de telefones e da Internet dos seus cidadãos como parte dos esforços para proteger a segurança nacional, ou acha que essa actividade vai longe de mais na violação da privacidade dos cidadãos e não é, portanto, justificável?

[http://www.aljazeera.com/indepth/interviews/2013/09/090909-interview-with-edward-snowden.html](http://www.aljazeera.com/indepth/interviews/2013/09/09/090909-interview-with-edward-snowden.html)

Motivação

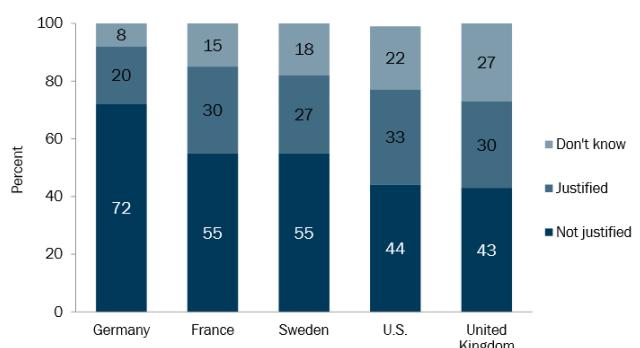
- Entende que há justificação para que o seu Governo recolha dados de telefones e da Internet dos seus cidadãos como parte dos esforços para proteger a segurança nacional, ou acha que essa actividade vai longe de mais na violação da privacidade dos cidadãos e não é, portanto, justificável?



[http://www.esri.com/news/2013/11/11/11/Best-Domestic-Surveillance-Holiday.pdf](http://www.esri.com/news/2013/11/11/Best-Domestic-Surveillance-Holiday.pdf)

Motivação

- E quanto à recolha de informação sobre de cidadãos residentes noutros países aliados, como perspetiva esta atuação?



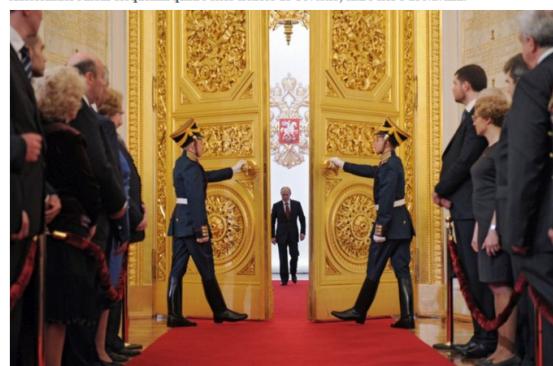
[http://www.esri.com/news/2013/11/11/11/Best-Domestic-Surveillance-Holiday.pdf](http://www.esri.com/news/2013/11/11/Best-Domestic-Surveillance-Holiday.pdf)

Motivação

Kremlin diz que o seu site está debaixo de um "poderoso ataque" informático

PÚBLICO 14/3/2014 - 11:28

Autoridades russas bloqueiam quatro sites críticos do Governo, entre eles o de Navalni.



O site da presidência russa está debaixo de um "poderoso ataque" informático, anunciou o Kremlin revelando que piratas informáticos também bloquearam o acesso ao site do banco central russo.

...
O banco central da Rússia, em comunicado, confirmou que também está com problemas no seu sistema informático devido a um ataque de *hackers*. Estava prevista, para a manhã desta sexta-feira, uma revisão das taxas de juro, prevendo-se uma baixa depois de várias semanas em que os números subiram. Mas a actualização das taxas não pôde ser feita devido a este ataque.

<http://www.adfoco.pt/noticias/actualidade/politica/putin-anuncia-que-site-do-governo-russo-e-debaixo-de-ataque-informatico-169253>

Motivação

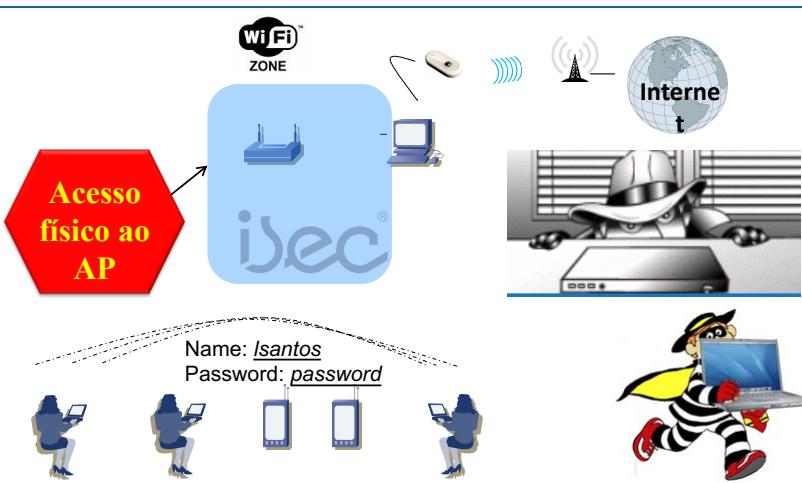


Name: lsantos
Password: password

Motivação



Motivação



Motivação

Chapter 3: Getting to Know the Wireless-N Router with Storage Link

The Back Panel

The Router's ports, where the cables are connected, and **Reset** button are located on the back panel.

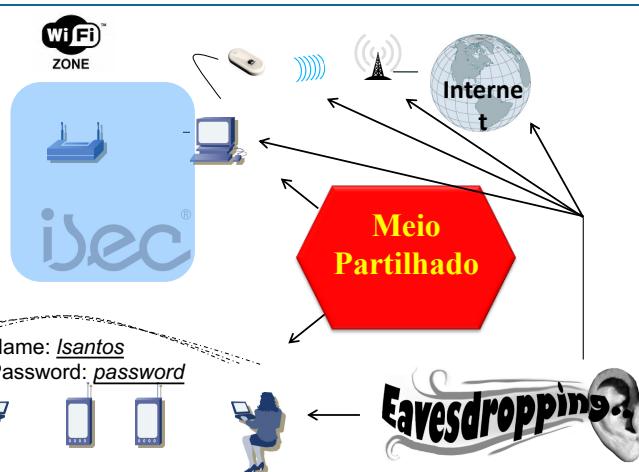


Figure 3-1: The Router's Back Panel

ISB	1
INTERNET	1
Ethernet 1, 2, 3, 4	1
Reset Button	1
Power	1

IMPORTANT: Resetting the Router will erase all of your settings (Internet connection, wireless security, and other settings) and replace them with the factory defaults. Do not reset the Router if you want to retain these settings.

Motivação



Motivação

- WiFi
 - 1997: IEEE 802.11
 - 1999: WEP (*Wired Equivalent Privacy*)
 - 2005: Freeware que quebra o WEP em minutos



http://www.youtube.com/watch?v=A88XB7_Jz7s

Motivação

- WiFi
 - 2006: WPA (*Wi-Fi Protected Access*)
 - 2008: WPA cracked ☹

Computer & Internet Security News
06 November 2008

WPA cracked for the first time

By Robert McMillan, IDG News Service

Security researchers have cracked the Wi-Fi Protected Access (WPA) encryption standard used to protect data on many wireless network according to a presentation at next week's PacSec conference in Tokyo.

There, researcher Erik Tews will show how he was able to crack WPA encryption, in order to read data being sent from a router to a laptop computer. The attack could also be used to send bogus information to a client connected to the router.

To do this, Tews and his co-researcher Martin Beck found a way to break the Temporal Key Integrity Protocol (TKIP) key, used by WPA, in just 12 to 15 minutes, according to Dragos Ruiu, the conference's organiser.

Motivação

New attack cracks common Wi-Fi encryption in a minute

Attack works on older WPA systems that use the TKIP algorithm

By Robert McMillan, IDG News Service, 08/27/2009

[Share/Email](#) [Tweet This](#) [18 Comments](#) [Print](#)

[Newsletter Sign-Up](#)

Computer scientists in Japan say they've developed a way to break the WPA encryption system used in wireless routers in about one minute.

The attack gives hackers a way to read encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system. The attack was developed by Toshihiro Ohigashi of Hiroshima University and Masakatu Morii of Kobe University, who plan to discuss further details at a [technical conference](#) set for Sept. 25 in Hiroshima.

Last November, security researchers first showed how WPA could be broken, but the Japanese researchers have taken the attack to a new level, according to Dragos Ruiu, organizer of the PacSec security conference where the first WPA hack was demonstrated. "They took this stuff which was fairly theoretical and they've made it much more practical," he said.

They Japanese researchers discuss their attack in a [paper](#) presented at the [Joint Workshop on Information Security](#), held in Kaohsiung, Taiwan earlier this month.

Compromisso

Um mecanismo de segurança só é útil se for prático de usar. Porém “ser prático” normalmente implica abdicar de parte da robustez.

Motivação

- GSM

Tecnologia GSM
Telemóveis: “Hacker” alemão decifra código de segurança que encripta chamadas telefónicas

29.12.2009 - 16:33 Por Agências

Votar  | 3 votos 

2 de 3 notícias em Tecnologia [« anterior](#) [seguinte »](#)

Albert Gea/Reuters

Karsten Nohl, um engenheiro alemão de 28 anos, conseguiu decifrar com sucesso o código de segurança que encripta 80 por cento das chamadas realizadas hoje a partir de telemóveis. O objectivo desta acção foi alertar para as falhas de segurança da tecnologia GSM, a mais popular e usada praticamente por todos os quatro mil milhões de utilizadores de telemóveis em todo o mundo.



A Associação GSM, que desenvolveu o algoritmo e que impulsionou a adopção da tecnologia em todo o mundo, indicou que o trabalho de Karsten Nohl seria considerado ilegal em muitos países

[64-bit A5/1 encryption](#)

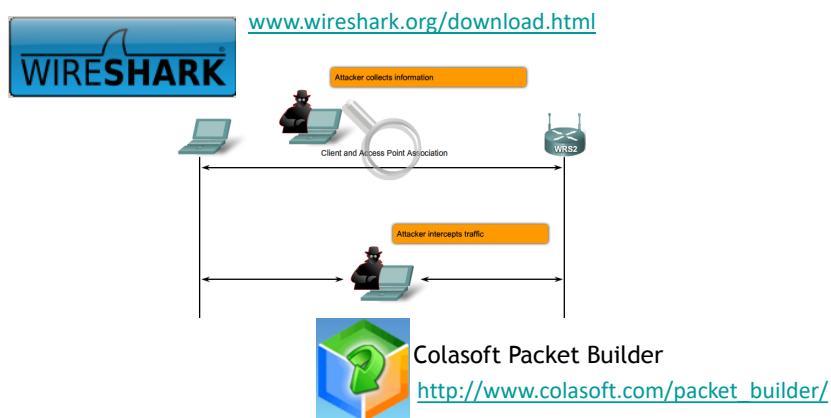
Motivação

- Confias no teu ISP?
- E no ISP do teu ISP?
- E no ISP do ISP do teu ISP?
- ...
 - <http://www.yougetsignal.com/tools/visual-tracert/>
 - [tracert https://www.bpinet.pt/](https://www.bpinet.pt/)
- Confias no *Hotspot “lsantos”*?
 - Ataques *Man-in-The-Middle* (MITM)



Motivação

- *Man-in-the-Middle* (≡ ataques por interposição)



Motivação

- Será que os ISP são verdadeiramente inimputáveis?

NSA recolhe milhões de listas de contactos a partir de e-mails e mensagens

PÚBLICO 15/10/2013 - 09:13

Dados obtidos permitem estabelecer mapas de relações. São conseguidos fora dos EUA, contornando a proibição de interceptar comunicações de norte-americanos.



BILLINGTON CyberSecurity

A intercepção é feita a partir de pontos de acesso “um pouco por todo o mundo”, mas não nos Estados Unidos, o que permite à NSA contornar a proibição de interceptar comunicações de norte-americanos no território do país — segundo os dois responsáveis contactados.

O jornal escreve que a recolha de dados beneficia de acordos secretos com empresas de telecomunicações estrangeiras ou serviços de informações de países aliados.

Motivação

- A segurança não é um estado mas um processo de gestão do risco subjacente.

Tecnologias



Enquadramento Histórico

DEIS

Segurança de Rede

- *Network security is the protection of information and systems and hardware that use, store, and transmit that information.*
- *Network security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resources.*

National Security Telecommunications and
Information Systems Security Committee
(NSTISSC)



Dos primeiros receios ao risco global

Year	1960s	1970s	Early 1980s
Events	Phone Freaks (Phreaks)	Phone Freaks (Phreaks)	Wardialing

Year	1988	1993
Events	First Internet Worm	First Def Con Hacking Conference

Year	1994
Events	First 5-Year Federal Prison Sentence for Hacking

- **1960:** *phone freaking* (= phreaking). Clientes da AT&T começaram a explorar a comutação automática injetando vários tons para fazer chamadas inter-hurbanas pelo preço de chamadas locais.

- **Wardialing:** Busca, com um modem, de números locais ligados cuja linha telefônica servia computadores. Depois aplicavam-se utilitários para quebra de passwords.

Dos primeiros receios ao risco global

Year	1995	September 1997	1997
Events	Kevin Mitnick Begins 4 Years in Prison for Hacking Credit Card Accounts	Nmap Published	First Malicious Scripts Released and Used by Less Educated Hackers (Script Kiddies).

Year	Late 1990s	2002
Events	Wardriving	Melissa Virus Creator Gets 20 Months in Federal Prison

Timeline:

- 1978 - First Spam on ARPAnet
- 1988 - The Morris Internet Virus
- 1999 - Melissa Email Virus
- 2000 - MafiaBoy DoS Attack, Love Bug Worm, LophiCrack password cracker released
- 2001 - Code Red DoS Attack
- 2004 - Botnet hits U.S. Military Systems
- 2007 - Storm botnet, TJX Credit Card Data Breach
- 2008 - Société Générale Stock Fraud

- **Wardriving:** Com um automóvel e um portátil ou PDA os utilizadores tentam detectar e comprometer redes wireless.

Dos primeiros receios ao risco global

- Code-Red Worm (Jul 2001, 0m 28s)



Dos primeiros receios ao risco global

- A Internet hoje é verdadeiramente global

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	825,094,396	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	475,069,448	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	63,240,946	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	266,224,500	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	204,689,836	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	21,263,990	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7 %	444.8 %	100.0 %

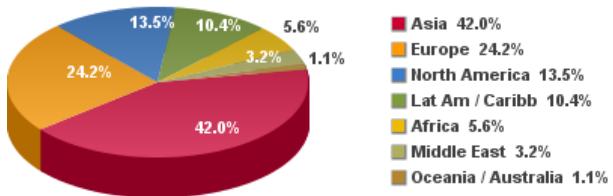
NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2010. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the [US Census Bureau](#). (4) Internet usage information comes from data published by [Nielsen Online](#), by the [International Telecommunications Union](#), by [GfK](#), local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the [Site Surfing Guide](#). (6) Information in this site may be cited, giving the due credit to [www.internetworldstats.com](#). Copyright © 2000 - 2010, Miniwatts Marketing Group. All rights reserved worldwide.

<http://www.internetworldstats.com/>

Dos primeiros receios ao risco global

- Mesmo nos continentes adormecidos ...

**Internet Users in the World
Distribution by World Regions - 2010**



Source: Internet World Stats - www.internetworldstats.com/stats.htm

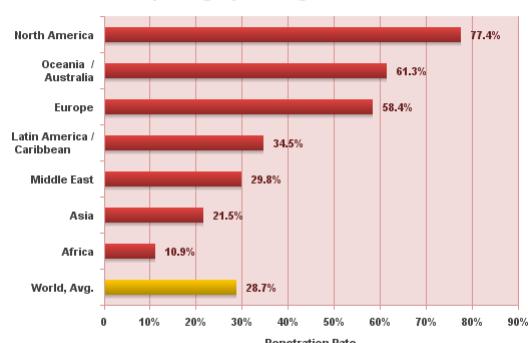
Basis: 1,966,514,816 Internet users on June 30, 2010

Copyright © 2010, Miniwatts Marketing Group

Dos primeiros receios ao risco global

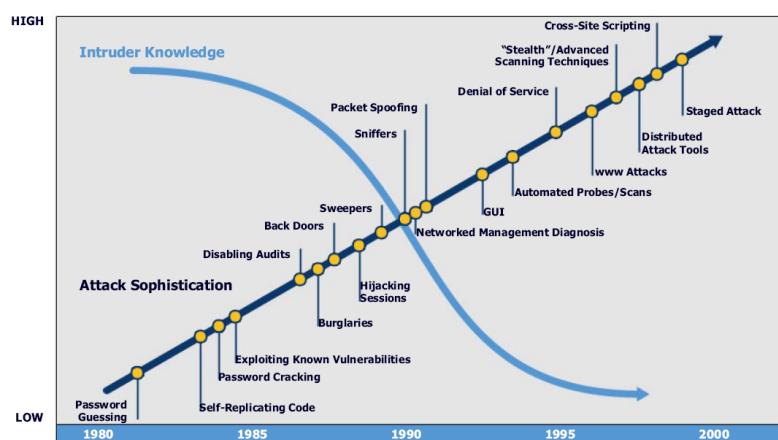
- Os servidores e serviços *on-line* encontram-se hoje à distância de um clique para um terço da população mundial.

**World Internet Penetration Rates
by Geographic Regions - 2010**



Source: InternetWorld Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 6,845,609,960 and 1,966,514,816 estimated Internet users on June 30, 2010.
Copyright © 2010, Miniwatts Marketing Group

A sofisticação das ferramentas de ataque tem banalizado as actividades ilegítimas



Source: Julia H. Allen, *CERT Guide to System and Network Security Practices*, Addison-Wesley, 2001

A sofisticação da defesa é igualmente progressiva

Year	1984	Late 1988	1989
Security Technology	First IDS for ARPAnet (SRI International IDES)	DEC Packet Filter Firewall	AT&T Bell Labs Stateful Firewall

Year	1991	1994	1995
Security Technology	DEC SEAL Application Layer Firewall	Check Point Firewall	NetRanger IDS



Firewall



Cisco Centri Firewall



Cisco IOS Firewall



Router - with Firewall

- **1984:** Uma das primeiras ferramentas de defesa foi um **IDS (intrusion detection system)** – Permitem detecção rápida.
- **1988:** DEC produz a primeira **firewall stateless** na forma de um filtro de pacotes IP
- **1989:** A AT&T produz a primeira **firewall stateful**.

A sofisticação da defesa é igualmente progressiva

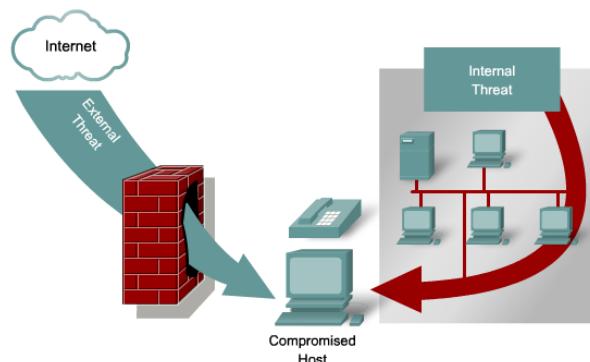
Year	August, 1997	1998	Late 1999	2006
Security Technology	RealSecure IDS	Snort IDS	First IPS	Cisco Zone-Based Policy Firewall

- **1990s:** As IDS começaram a ser substituídas por **IPS (intrusion prevention systems/sensors)** – Ao contrário dos IDS, os IPS são reactivos.

Year	1998	2000	2003
Security Technology	Mitigating MAC Address Spoofing Attacks Mitigating MAC Address Table Overflow Attacks Mitigating LAN Storm	Mitigating Root Bridge Spoofing Mitigating VLAN Attacks	Mitigating ARP Spoofing Attacks

Ameaças externas vs. internas

- As ameaças internas apenas começaram a ser mitigadas 20 anos depois de se dar atenção às ameaças externas



Ameaças externas vs. internas



*Hackers,
intruso
ou
atacante*

Equipa de segurança



Princípios Fundamentais da Segurança da Informação

DEIS

Objectivos típicos da segurança de informação

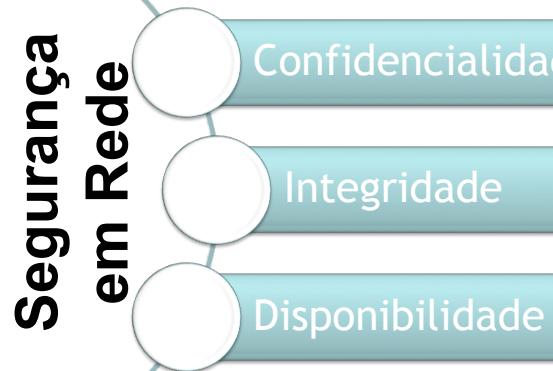
- A segurança da informação manifesta-se de múltiplas formas, em função da situação e requisitos específicos da entidade ou entidades envolvidas na sua transacção.

in Handbook of Applied Cryptography

privacy or confidentiality	keeping information secret from all but those who are authorized to see it.
data integrity	ensuring information has not been altered by unauthorized or unknown means.
entity authentication or identification	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
message authentication	corroborating the source of information; also known as data origin authentication.
signature	a means to bind information to an entity.
authorization	conveyance, to another entity, of official sanction to do or be something.
validation	a means to provide timeliness of authorization to use or manipulate information or resources.
access control	restricting access to resources to privileged entities.
certification	endorsement of information by a trusted entity.
timestamping	recording the time of creation or existence of information.
witnessing	verifying the creation or existence of information by an entity other than the creator.
receipt	acknowledgement that information has been received.
confirmation	acknowledgement that services have been provided.
ownership	a means to provide an entity with the legal right to use or transfer a resource to others.
anonymity	concealing the identity of an entity involved in some process.
non-repudiation	preventing the denial of previous commitments or actions.
revocation	retraction of certification or authorization.

Os três atributos fundamentais

Atributos == propriedades, objetivos, aspectos fundamentais, critérios, *building blocks*, etc..



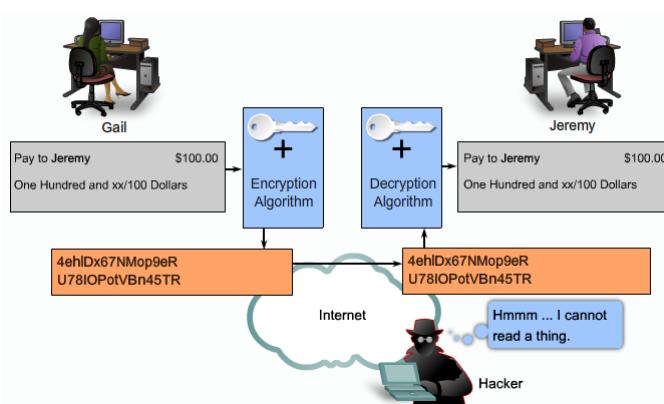
Confidencialidade (*Confidentiality/Privacy/Secrecy*)

- Objectivo: Assegurar que o conteúdo da informação apenas está acessível às entidades autorizadas.
- Como pode tal ser assegurado?
 - Ex.1: Através da protecção física



Confidencialidade (*Confidentiality/Privacy/Secrecy*)

- Ex. 2: Através de algoritmos matemáticos



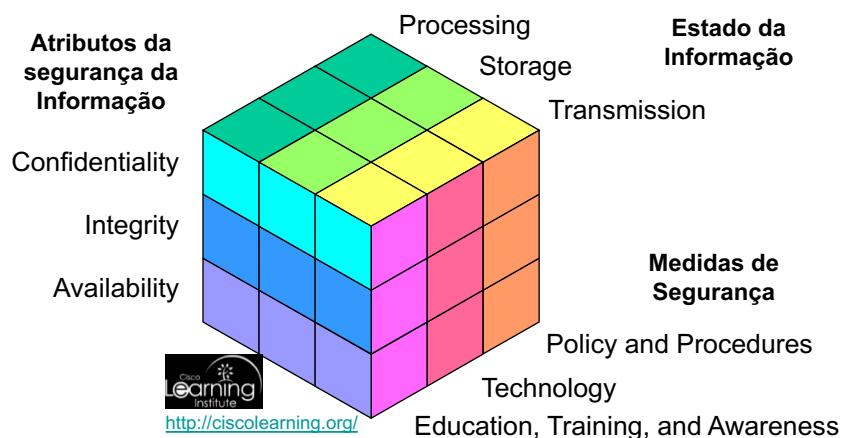
Integridade (*Integrity*)

- Objectivo: assegurar que o conteúdo da informação apenas é alterado por entidades autorizadas.
- Para assegurar a integridade da informação são necessários mecanismos que possibilitem detectar a manipulação (adição, alteração, remoção) indevida de todo ou parte do conteúdo de forma intencional (fraude) ou accidental (negligência).
- Exemplos de violações de integridade:
 - Alteração não solicitada da aparência de um *web site*
 - Interceptar e modificar uma transacção de *e-commerce*
 - Alterar o conteúdo de uma ficha de informação num servidor

Disponibilidade (*Availability*)

- Objectivo: assegurar que os sistemas de informação e as respetivas infraestruturas permitem o acesso à informação na qualidade esperável quando este é solicitado.
- A disponibilidade é uma medida da acessibilidade da informação.
 - Ex. Se um serviço fica *off-line* apenas 5 minutos por ano possui uma disponibilidade de 99.999 % (5 noves).
- Violações de disponibilidade
 - O suporte digital da informação danifica-se (e.g., *head crash*)
 - Uma ligação de acesso ao servidor fica saturada
 - Um *bug* na codificação do servidor, estimulado natural ou maliciosamente, torna inacessível o serviço

Modelo de segurança da informação



Modelo de segurança da informação

- A suficiência dos três atributos fundamentais têm sido posta em causa diversas vezes.
- Em 2002 Donn Parker propôs estender a seis a lista de princípios básicos de segurança:
 - Confidencialidade
 - Integridade
 - Disponibilidade
 - Autenticidade (*authenticity*)
 - Titularidade (*possession*)
 - Utilidade (*Utility*), i.e. valor relativo da informação
- Não há consenso ...

Modelo de segurança da informação

- Em 2013 foi proposto um conjunto mais extenso de atributos base que se provou ser mais completo:
 - Confidentiality
 - Integrity
 - Availability
 - Accountability
 - Auditability
 - Authenticity/Trustworthiness
 - Non-repudiation
 - Privacy

http://en.wikipedia.org/wiki/Information_security



Instituições

Instituições relevantes



www.first.org



www.mitre.org



www.cert.org



www.infosyssec.com



www.sans.org



www.cisecurity.org



www.isc2.org

Instituições relevantes

- *Computer Emergency Response Team Coordination Center - CERT/CC (<http://www.cert.org/>)*
 - 1988/CMU (reacção do DARPA ao worm Morris)
 - *Software assurance, secure systems, organizational security, coordinated response, education and training.*
 - Conceito tem hoje cobertura global
 - <http://cert.pt/> (Av. do Brasil 101 1700-066 Lisboa)
 - O CERT.PT tem como missão contribuir para o esforço de cibersegurança nacional, nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal.



www.cert.org

Instituições relevantes

- *Computer Security Training, Network Research & Resources*
[\(http://www.sans.org/\)](http://www.sans.org/)
 - Instituição criada em 1989
 - Ensino de diversos cursos
 - Certificações globais
 - *Global Information Assurance Certification (GIAC)*
 - Serviço de alertas gratuito
 - *Internet Storm Center*
 - Resumos semanais das ameaças mais relevantes



www.sans.org

Instituições relevantes

- International Information Systems Security Certification Consortium, Inc., (ISC)² (<https://www.isc2.org/>)
- Instituição sem fins lucrativos de carácter global
- Missão: *We make society safer by improving productivity, efficiency and resilience of information-dependent economies through information security education and certification.*
- (ISC)² Common Body of Knowledge (CBK)
 - Compêndio de tópicos sobre segurança da informação
 - Actualizado anualmente
 - Base das várias certificações em segurança do (ISC)²



www.isc2.org

Instituições relevantes

• Certificações (ISC)²



Systems Security Certified Practitioner (SSCP®)

Certified Authorization Professional (CAP®)

Certified Secure Software Lifecycle Professional (CSSLP®)

Certified Information Systems Security Professional (CISSP®)



www.isc2.org

- As certificações são *vendor-neutral*
- A *Certified Information Systems Security Professional (CISSP)* é das certificações de segurança com maior reconhecimento.



Information Systems Security Architecture Professional (CISSP-ISSAP®)

Information Systems Security Engineering Professional (CISSP-ISSEP®)

Information Systems Security Management Professional (CISSP-ISSMP®)

Instituições relevantes

SSCP® (Systems Security Certification Practitioner) CBK

- Controles de acesso
- Análise e monitoramento
- Criptografia
- Código malicioso
- Redes e telecomunicações
- Risco, resposta e recuperação
- Operações e administração de segurança

CSSLP® (Certified Secure Software Lifecycle Professional)

- Conceitos de Software Seguro
- Requisitos de Software Seguro
- Design de Software Seguro
- Implementação/Codificação de Software Seguro
- Teste de Software Seguro
- Aceitação de Software
- Implantação, Operações, Manutenção e Alienação de Software

CISSP® (Certified Information Systems Security Professional) CBK

- Controle de acesso
- Segurança da aplicação
- Planejamento de continuidade do negócio e recuperação de desastres
- Criptografia
- Gerenciamento de segurança da informação e de riscos
- Jurídico, regulamentos, conformidade e investigações
- Segurança de operações
- Segurança (ambiental) física
- Arquitetura e design de segurança
- Segurança das telecomunicações e da rede



CISSP-ISSAP® (Information Systems Security Architecture Professional)

- Sistemas e metodologia de controle de acesso
- Criptografia
- Integração de segurança física
- Análise das necessidades e padrões, diretrizes e critérios de segurança
- Tecnologia relacionada ao BCP (Business Continuity Planning, Planejamento de Continuidade dos Negócios) e DRP (Disaster Recovery Planning, Planejamento de Recuperação de Desastres)
- Segurança das telecomunicações e de rede

CISSP-ISSEP® (Information Systems Security Engineering Professional – Profissional de engenharia de segurança dos sistemas de informações)

- Certificação e permissão
- Engenharia de segurança dos sistemas
- Gerenciamento técnico
- Regulamentações de segurança de informações do governo dos EUA

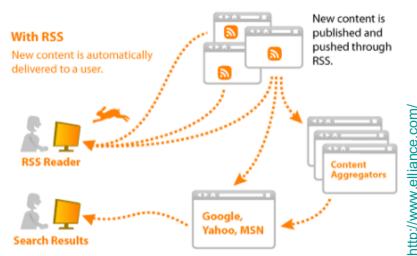
CISSP-ISSMP® (Information Systems Security Management Professional – Profissional de gerenciamento de segurança do sistema de informações)

- Práticas de gerenciamento de segurança da empresa
- Segurança de desenvolvimento do sistema de toda empresa
- Lei, investigações, criminal e ética
- Conformidade de fiscalização da segurança das operações
- Entendimento do BCP (Business Continuity Planning, Planejamento de continuidade dos negócios), DRP (Disaster Recovery Planning, Planejamento de recuperação de desastres) e COOP (Continuity of Operations Planning, Planejamento de continuidade de operações)

Instituições relevantes

- Divulgação de alertas críticos

- A tecnologia RSS (*Really Simple Syndication*) é normalmente a preferencial para alojar feeds
- Capacidade de notificação activa (assíncrona)
- Capacidade de agregação local ou remota



Gestão de Segurança da Informação

DEIS

Normas publicadas

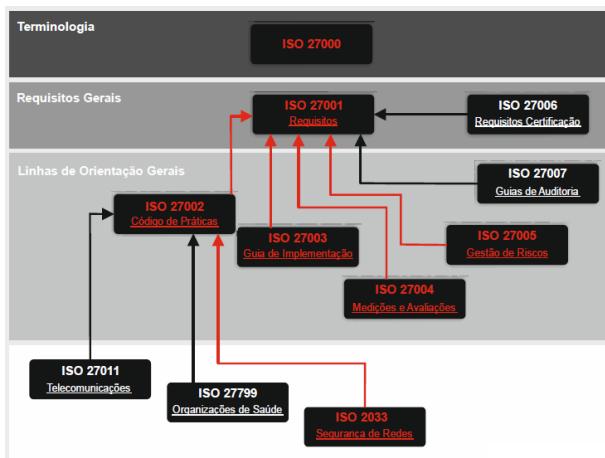
- Série ISO/IEC 27000 - Information Security Standards
 - ISO/IEC 27000: Overview and vocabulary
 - ISO/IEC 27001: Requirements  **Até 2007 denominava-se ISO/IEC 17799**
(Antes BS7799 – UK)
 - ➡ - ISO/IEC 27002: Code of practice for information security management
 - ISO/IEC 27003: Implementation guidance
 - ISO/IEC 27004: Information security management – Measurement
 - ISO/IEC 27005: Information security risk management
 - ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems
 - ISO/IEC 27011: Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
 - ➡ - ISO/IEC 27033-1: Network security overview and concepts
 - ISO 27799: Information security management in health using ISO/IEC 27002

Normas em preparação

- Série ISO/IEC 27000 - Information Security Standards
 - ISO/IEC 27007: Guidelines for information security management systems auditing
 - ISO/IEC 27008: Guidance for auditors on ISMS controls
 - ISO/IEC 27013: Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
 - ISO/IEC 27014: Information security governance framework
 - ISO/IEC 27015: Information security management guidelines for the finance and insurance sectors
 - ISO/IEC 27031: Guideline for ICT readiness for business continuity
 - ➡ - ISO/IEC 27032: Guideline for cybersecurity
 - ISO/IEC 27033: IT network security, a multi-part standard based on ISO/IEC 18028:2006
 - ISO/IEC 27034: Guideline for application security
 - ISO/IEC 27035: Security incident management
 - ➡ - ISO/IEC 27036: Guidelines for security of outsourcing
 - ➡ - ISO/IEC 27037: Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Normas em preparação

- Organização



Série ISO 27000. Abordagem normalizada de segurança para PMEs, 2011 / 2014,
António Manuel dos Santos Simões. Rui Jorge Lopes Martins

Domínios de gestão da segurança da informação

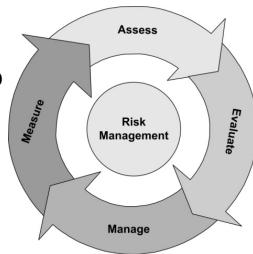
- A ISO/IEC 27002 organiza em 12 domínios os inúmeros aspectos relativos à segurança da informação
 - Trata-se de um modelo de referência que nos ajuda a enquadrar qualquer discussão sobre a temática da Segurança
 - Paralelo com o CISSP

Risk Assessment
Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Access Control
Information Systems Acquisition, Development and Maintenance
Information Security Incident Management
Business Continuity Management
Compliance

Risk Assessment (Avaliação do risco)

4 RISK ASSESSMENT AND TREATMENT	5
4.1 ASSESSING SECURITY RISKS	5
4.2 TREATING SECURITY RISKS.....	5

- Primeira etapa do processo de gestão do risco
 - Afere o valor quantitativo e qualitativo do risco relacionado com determinada situação específica ou ameaça identificada.
 - Pressuposto: o risco pode ser mitigado mas nunca evitado
 - Estabelecesse um nível aceitável de risco para a organização



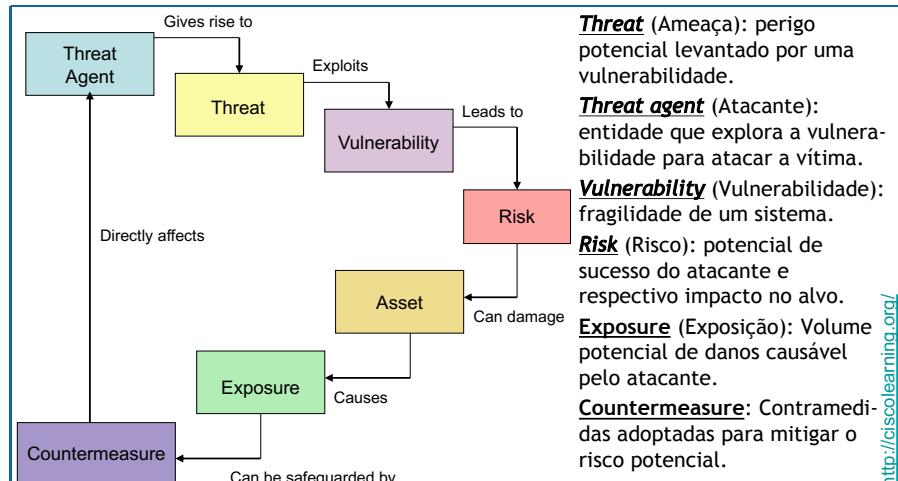
<http://ciscolearning.org/>

Risk Assessment (Avaliação do risco)

- Categorias dos bens
 - Bens de Informação: pessoas, hardware, software, sistemas
 - Bens de Suporte: infra-estruturas, serviços,
 - Bens Críticos: qualquer um dos mencionados atrás
- Compilação dos atributos de cada bem identificado
- Determinação do valor relativo de cada bem
 - Quanto retorno/lucro gera?
 - Qual o custo de substituição associado?
 - Quão difícil é a sua substituição?
 - Quão rápido pode ser substituído?
- Ameaças
 - Falhas de equipamentos, ataques estruturados, desastres naturais, vírus, e outros eventos causadores de danos

<http://ciscolearning.org/>

Risk Assessment (Avaliação do risco)



Risk Assessment (Avaliação do risco)

- Análise qualitativa do Risco
 - Os valores da Exposição ao risco servem para priorizar a atenção dada a cada ameaça

Ameaça	Probabilidade	Severidade	Exposição
Um novo worm	7	7	49
Sistema de armazenamento central avaria	2	10	20
Sistema de protecção contra incêndio inunda o datacenter	1	10	10

Risk Assessment (Avaliação do risco)

- Análise quantitativa do Risco
 - Qual o impacto anual, em unidades monetárias, previsto.
- Decisão

Tomar consciência de que o risco existe mas aceitá-lo sem qualquer medida.

Aplicar medidas de protecção que diminuam a exposição ao risco do bem em causa.



Entregar a terceiros a responsabilidade de gerir o risco.

Eliminar o bem do conjunto de bens da instituição ou eliminar a exposição ao risco do mesmo.

<http://ciscolearning.org/>

Security Policy (Política de segurança)

5 SECURITY POLICY	7
5.1 INFORMATION SECURITY POLICY	7
5.1.1 Information security policy document	7
5.1.2 Review of the information security policy.....	8

- Trata-se de um documento formal que clarifica como é que uma instituição planeia proteger os seus bens
 - Define objectivos para a empresa, regras de comportamento para os utilizadores e requisitos para os sistemas, os quais colectivamente asseguram os níveis de segurança adequados.
- Exemplos:
 - Todos os utilizadores devem possuir um par ID/password únicos em conformidade com a política de passwords local
 - A solução de antivírus da empresa para laptops deve efectuar actualizações diárias. <http://www.sans.org/security-resources/policies/>

Security Policy (Política de segurança)

1. What do you have that others want?
2. What processes, data, or information systems are critical to you, your company, or your organization?
3. What would stop your company or organization from doing business or fulfilling its mission?

The security policy should protect the assets of your organization by answering several security questions.



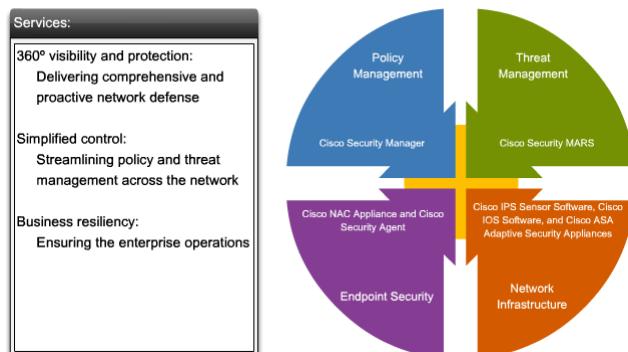
Security Policy (Política de segurança)

Subsection	6.1 PERSONNEL SECURITY	Change Control #: 1.0
Policy	6.1.3 Confidentiality Agreements	Approved by: SMH
Objectives	Confidentiality of organizational data is a key tenet of our information security program. In support of this goal, ABC Co will require signed confidentiality agreements of all authorized users of information systems. This agreement shall conform to all federal, state, regulatory, and union requirements.	
Purpose	The purpose of this policy is to protect the assets of the organization by clearly informing staff of their roles and responsibilities for keeping the organization's information confidential.	
Audience	ABC Co confidentiality agreement policy applies equally to all individuals granted access privileges to an ABC Co Information resources	
Policy	This policy requires that staff sign a confidentiality policy agreement prior to being granted access to any sensitive information or systems. Agreements will be reviewed with the staff member when there is any change to the employment or contract, or prior to leaving the organization. The agreements will be provided to the employees by the Human Resource Dept.	
Exceptions	At the discretion of the Information Security Officer, third parties whose contracts include a confidentiality clause may be exempted from signing individual confidentiality agreements.	
Disciplinary Actions	Violation of this policy may result in disciplinary actions, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to civil and criminal prosecution.	

Security Policy (Política de segurança)

- Os maiores *players* (e.g. Cisco) possuem soluções ajustadas à implementação das políticas de segurança mais vulgares

Cisco Self-Defending Network



Organization of Information Security (Organização da segurança de informação)

6 ORGANIZATION OF INFORMATION SECURITY	9
6.1 INTERNAL ORGANIZATION	9
6.1.1 <i>Management commitment to information security.....</i>	9
6.1.2 <i>Information security co-ordination.....</i>	10
6.1.3 <i>Allocation of information security responsibilities.....</i>	10
6.1.4 <i>Authorization process for information processing facilities.....</i>	11
6.1.5 <i>Confidentiality agreements.....</i>	11
6.1.6 <i>Contact with authorities</i>	12
6.1.7 <i>Contact with special interest groups</i>	12
6.1.8 <i>Independent review of information security</i>	13
6.2 EXTERNAL PARTIES	14
6.2.1 <i>Identification of risks related to external parties.....</i>	14
6.2.2 <i>Addressing security when dealing with customers</i>	15
6.2.3 <i>Addressing security in third party agreements</i>	16

- Procedimentos genéricos de base à segurança de informação que envolvem quer as políticas internas de coordenação da mesma quer as políticas externas de relacionamento

Asset Management (Gestão de bens)

7 ASSET MANAGEMENT.....	19
7.1 RESPONSIBILITY FOR ASSETS.....	19
7.1.1 <i>Inventory of assets</i>	19
7.1.2 <i>Ownership of assets</i>	20
7.1.3 <i>Acceptable use of assets</i>	20
7.2 INFORMATION CLASSIFICATION.....	21
7.2.1 <i>Classification guidelines</i>	21
7.2.2 <i>Information labeling and handling</i>	21

- Inventariação e classificação dos bens segurados, identificação dos seus legítimos proprietários e usufruto aceitável.

Human Resources Security (Equipa técnica responsável pela Segurança)

8 HUMAN RESOURCES SECURITY	23
8.1 PRIOR TO EMPLOYMENT	23
8.1.1 <i>Roles and responsibilities</i>	23
8.1.2 <i>Screening</i>	23
8.1.3 <i>Terms and conditions of employment</i>	24
8.2 DURING EMPLOYMENT	25
8.2.1 <i>Management responsibilities</i>	25
8.2.2 <i>Information security awareness, education, and training</i>	26
8.2.3 <i>Disciplinary process</i>	26
8.3 TERMINATION OR CHANGE OF EMPLOYMENT.....	27
8.3.1 <i>Termination responsibilities</i>	27
8.3.2 <i>Return of assets</i>	27
8.3.3 <i>Removal of access rights</i>	28

- Procedimentos de segurança relacionados com a admissão, manutenção e abandono de colaboradores.

Physical and Environment Security (Segurança física e ambiental)

9.1	SECURE AREAS	29
9.1.1	Physical security perimeter	29
9.1.2	Physical entry controls	30
9.1.3	Securing offices, rooms, and facilities	30
9.1.4	Protecting against external and environmental threats	31
9.1.5	Working in secure areas	31
9.1.6	Public access, delivery, and loading areas.....	32
9.2	EQUIPMENT SECURITY	32
9.2.1	Equipment siting and protection.....	32
9.2.2	Supporting utilities	33
9.2.3	Cabling security.....	34
9.2.4	Equipment maintenance.....	34
9.2.5	Security of equipment off-premises.....	35
9.2.6	Secure disposal or re-use of equipment.....	35
9.2.7	Removal of property	36

- Segurança física da instituição, matriz de liberdade de acesso físico a locais e equipamento bem como políticas de reutilização do mesmo.

Communications and Operations Management (Gestão de operações e comunicação)

10.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES	37
10.1.1	Documented operating procedures.....	37
10.1.2	Change management	37
10.1.3	Segregation of duties	38
10.1.4	Separation of development, test, and operational facilities.....	38
10.2	THIRD PARTY SERVICE DELIVERY MANAGEMENT	39
10.2.1	Service delivery.....	39
10.2.2	Monitoring and review of third party services.....	40
10.2.3	Managing changes to third party services.....	40
10.3	SYSTEM PLANNING AND ACCEPTANCE.....	41
10.3.1	Capacity management	41
10.3.2	System acceptance	41
10.4	PROTECTION AGAINST MALICIOUS AND MOBILE CODE.....	42
10.4.1	Controls against malicious code.....	42
10.4.2	Controls against mobile code	43
10.5	BACK-UP	44
10.5.1	Information back-up	44
10.6	NETWORK SECURITY MANAGEMENT.....	45
10.6.1	Network controls.....	45
	10.6.2 Security of network services	46

Communications and Operations Management (Gestão de operações e comunicação)

10.7	MEDIA HANDLING	46
10.7.1	Management of removable media.....	46
10.7.2	Disposal of media	47
10.7.3	Information handling procedures	47
10.7.4	Security of system documentation.....	48
10.8	EXCHANGE OF INFORMATION	48
10.8.1	Information exchange policies and procedures.....	49
10.8.2	Exchange agreements	50
10.8.3	Physical media in transit	51
10.8.4	Electronic messaging.....	52
10.8.5	Business information systems	52
10.9	ELECTRONIC COMMERCE SERVICES	53
10.9.1	Electronic commerce	53
10.9.2	On-Line Transactions	54
10.9.3	Publicly available information	55
10.10	MONITORING	55
10.10.1	Audit logging	55
10.10.2	Monitoring system use	56
10.10.3	Protection of log information	57
10.10.4	Administrator and operator logs	58
10.10.5	Fault logging	58
10.10.6	Clock synchronization	58

Access Control (Controlo de acesso)

11.1	BUSINESS REQUIREMENT FOR ACCESS CONTROL	60
11.1.1	Access control policy.....	60
11.2	USER ACCESS MANAGEMENT.....	61
11.2.1	User registration.....	61
11.2.2	Privilege management	62
11.2.3	User password management.....	62
11.2.4	Review of user access rights	63
11.3	USER RESPONSIBILITIES.....	63
11.3.1	Password use	64
11.3.2	Unattended user equipment	64
11.3.3	Clear desk and clear screen policy.....	65
11.4	NETWORK ACCESS CONTROL	65
11.4.1	Policy on use of network services	66
11.4.2	User authentication for external connections	66
11.4.3	Equipment identification in networks	67
11.4.4	Remote diagnostic and configuration port protection	67
11.4.5	Segregation in networks	68
11.4.6	Network connection control.....	68
11.4.7	Network routing control	69

Access Control (Controlo de acesso)

11.5 OPERATING SYSTEM ACCESS CONTROL.....	69
11.5.1 Secure log-on procedures.....	69
11.5.2 User identification and authentication	70
11.5.3 Password management system.....	71
11.5.4 Use of system utilities	72
11.5.5 Session time-out.....	72
11.5.6 Limitation of connection time	72
11.6 APPLICATION AND INFORMATION ACCESS CONTROL	73
11.6.1 Information access restriction	73
11.6.2 Sensitive system isolation	74
11.7 MOBILE COMPUTING AND TELEWORKING.....	74
11.7.1 Mobile computing and communications	74
11.7.2 Teleworking.....	75

- Direitos de acesso a redes, sistemas, aplicações, dados e funções por parte de cada entidade/colaborador.

Information systems Aquisition, Development and Maintenance (Integração de segurança nas aplicações)

12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS.....	77
12.1.1 Security requirements analysis and specification.....	77
12.2 CORRECT PROCESSING IN APPLICATIONS	78
12.2.1 Input data validation.....	78
12.2.2 Control of internal processing.....	78
12.2.3 Message integrity.....	79
12.2.4 Output data validation.....	79
12.3 CRYPTOGRAPHIC CONTROLS	80
12.3.1 Policy on the use of cryptographic controls	80
12.3.2 Key management.....	81
12.4 SECURITY OF SYSTEM FILES.....	83
12.4.1 Control of operational software	83
12.4.2 Protection of system test data	84
12.4.3 Access control to program source code.....	84
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	85
12.5.1 Change control procedures	85
12.5.2 Technical review of applications after operating system changes.....	86
12.5.3 Restrictions on changes to software packages.....	86
12.5.4 Information leakage.....	87
12.5.5 Outsourced software development.....	87
12.6 TECHNICAL VULNERABILITY MANAGEMENT	88
12.6.1 Control of technical vulnerabilities	88

Information Security Incident Management (Gestão de incidentes de segurança)

13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES	90
13.1.1 Reporting information security events.....	90
13.1.2 Reporting security weaknesses	91
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	91
13.2.1 Responsibilities and procedures	92
13.2.2 Learning from information security incidents	93
13.2.3 Collection of evidence.....	93

- Descrição de como antecipar e responder a cenários de insegurança manifestados (previstos ou não)

Business Continuity Management (Gestão da ininterruptão de serviços)

14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	95
14.1.1 Including information security in the business continuity management process.....	95
14.1.2 Business continuity and risk assessment.....	96
14.1.3 Developing and implementing continuity plans including information security	96
14.1.4 Business continuity planning framework.....	97
14.1.5 Testing, maintaining and re-assessing business continuity plans.....	98

- Descrição de como proteger, manter e retomar processos e sistemas críticos ao negócios (*disaster recover plans*).

Compliance (Conformidade)

15.1 COMPLIANCE WITH LEGAL REQUIREMENTS	100
15.1.1 Identification of applicable legislation	100
15.1.2 Intellectual property rights (IPR)	100
15.1.3 Protection of organizational records.....	101
15.1.4 Data protection and privacy of personal information	102
15.1.5 Prevention of misuse of information processing facilities	102
15.1.6 Regulation of cryptographic controls.....	103
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	103
15.2.1 Compliance with security policies and standards.....	104
15.2.2 Technical compliance checking.....	104
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS	105
15.3.1 Information systems audit controls.....	105
15.3.2 Protection of information systems audit tools	105

- Respeita aos cuidados de conformidade entre as medidas internamente adoptadas e as disposições legais e normativas em vigor na zona geo-política em causa.

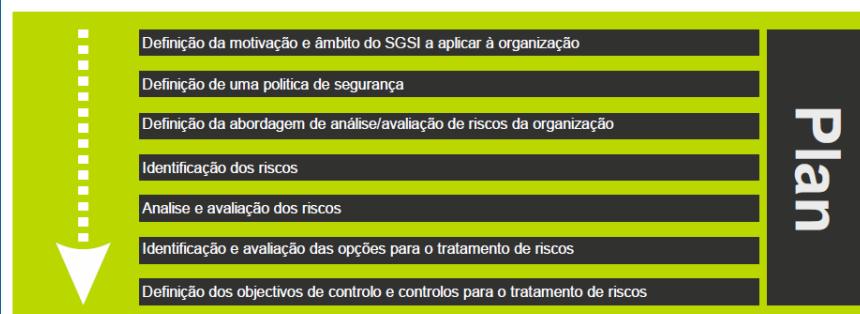
ISO 27000: Metodologia de Implementação

- Ciclo PDCA



ISO 27000: Metodologia de Implementação

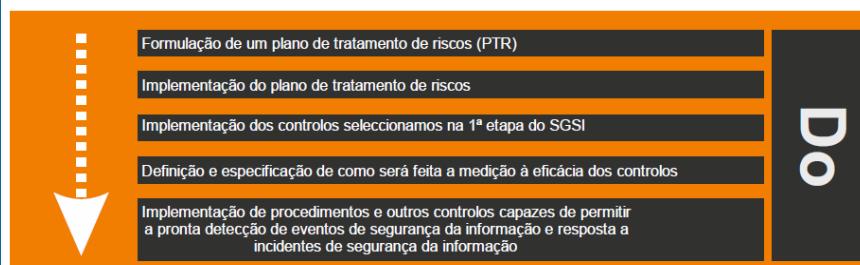
- PLAN: Sistemas de Gestão de Segurança da Informação



Série ISO 27000, Abordagem normalizada de segurança para PMEs, 2011 /2014,
António Manuel dos Santos Simões, Rui Jorge Lopes Martins

ISO 27000: Metodologia de Implementação

- DO: Sistemas de Gestão de Segurança da Informação



Série ISO 27000, Abordagem normalizada de segurança para PMEs, 2011 /2014,
António Manuel dos Santos Simões, Rui Jorge Lopes Martins

ISO 27000: Metodologia de Implementação

- **CHECK:** Sistemas de Gestão de Segurança da Informação



- Estabelecer procedimentos de monitorização/análise crítica
- Realização de análises críticas regulares à eficácia do SGSI
- Medição da eficácia dos controlos para verificar se os requisitos de segurança da informação foram atendidos
- Analisar criticamente as avaliações de risco, riscos residuais e níveis de riscos aceitáveis
- Conduzir auditorias internas do SGSI em intervalos planeados
- Atualizar os planos de segurança da informação
- Registar acções e eventos que possam ter impacto na eficácia ou no desempenho do SGSI

Check

Série ISO 27000, Abordagem normalizada de segurança para PMEs, 2011 /2014,
António Manuel dos Santos Simões, Rui Jorge Lopes Martins

ISO 27000: Metodologia de Implementação

- **ACT:** Sistemas de Gestão de Segurança da Informação

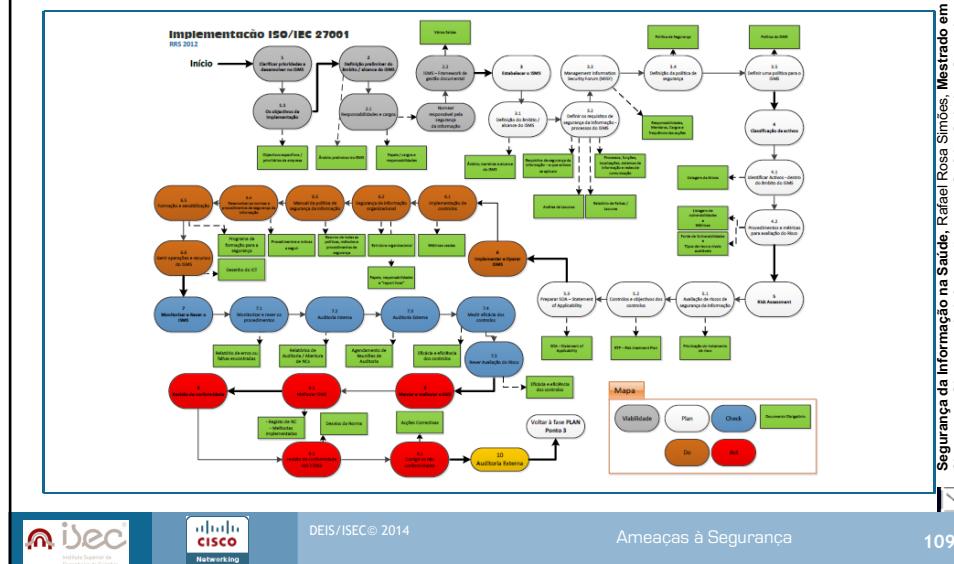


- Implementar as melhorias identificadas no SGSI.
- Executar as ações preventivas e corretivas apropriadas
- Comunicar as ações e melhorias a todas as partes interessadas
- Assegurar-se de que as melhorias atinjam os objetivos pretendidos

Act

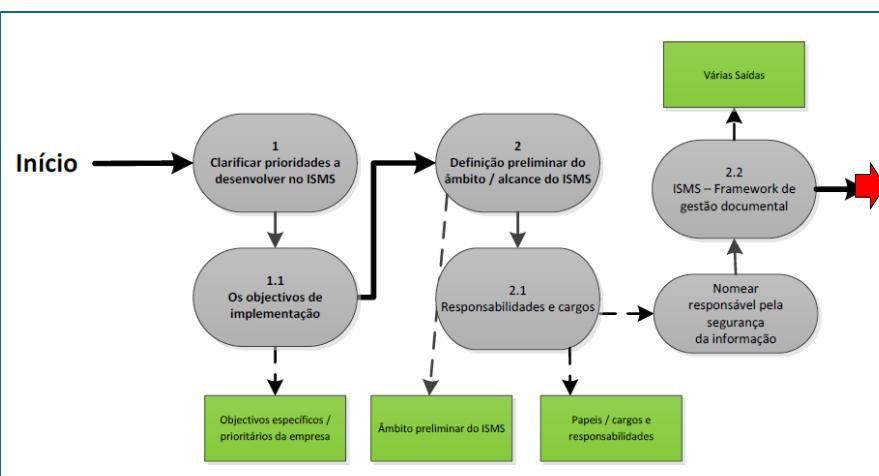
Série ISO 27000, Abordagem normalizada de segurança para PMEs, 2011 /2014,
António Manuel dos Santos Simões, Rui Jorge Lopes Martins

ISO 27000: Metodologia de Implementação



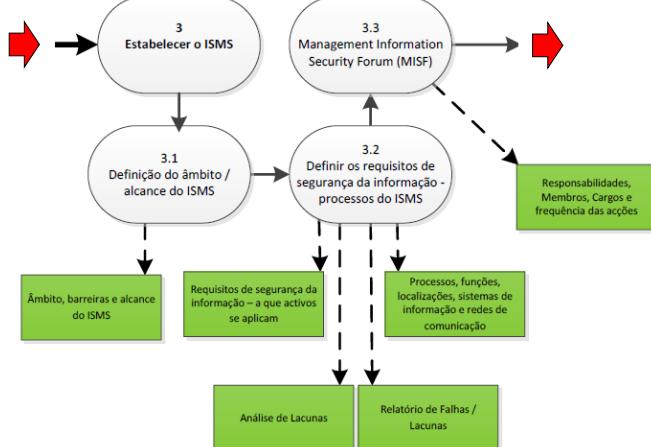
Segurança da Informação na Saúde, Ráfael Rosa Simões, Mestrado em Sistemas e Sistemas da Informação para a Saúde, Coimbra, Setembro, 2014

ISO 27000: Metodologia de Implementação

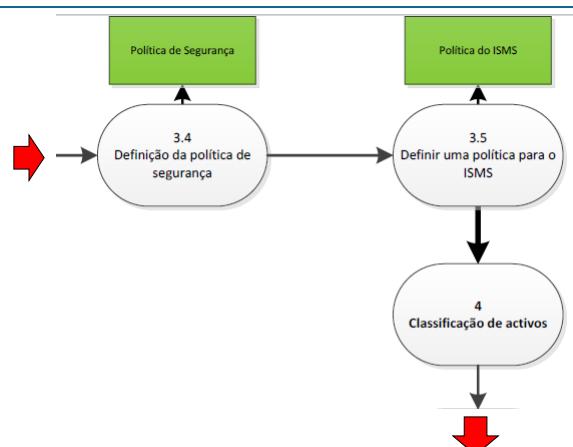


Segurança da Informação na Saúde, Rafael Rosa Simões, Mestrado em Sistemas e Sistemas da Informação para a Saúde, Coimbra, Setembro, 2014

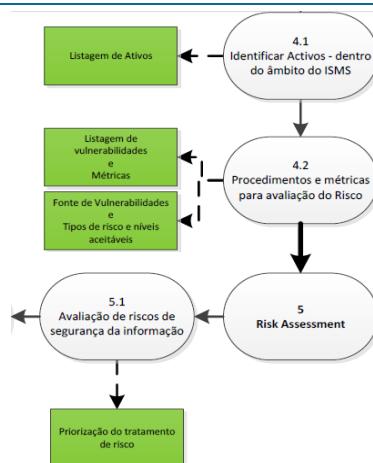
ISO 27000: Metodologia de Implementação



ISO 27000: Metodologia de Implementação



ISO 27000: Metodologia de Implementação



ISO 27000: Metodologia de Implementação

- Implementação

Ciber-Ameaças

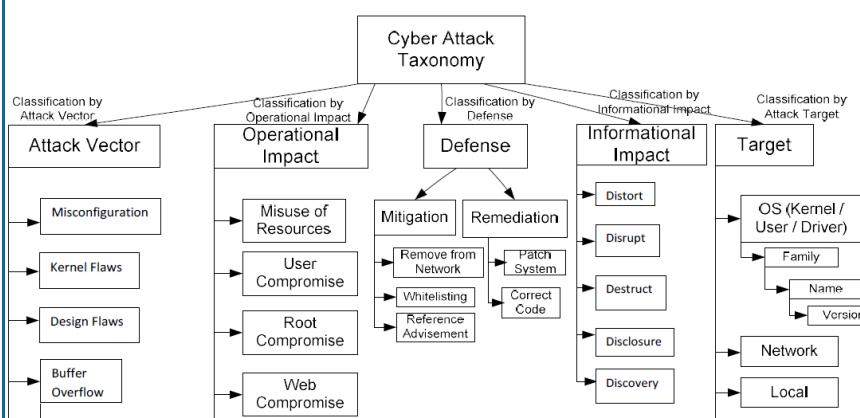
&

Mitigação

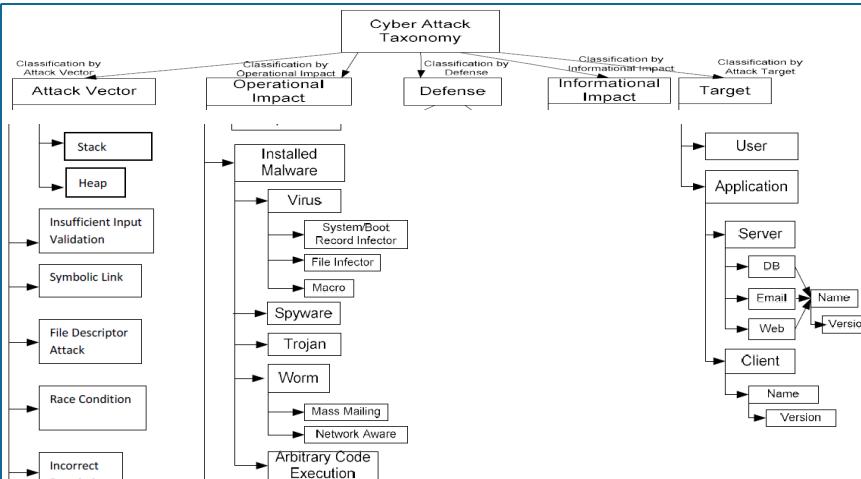
DEIS

Uma taxonomia possível para as ciber-ameaças

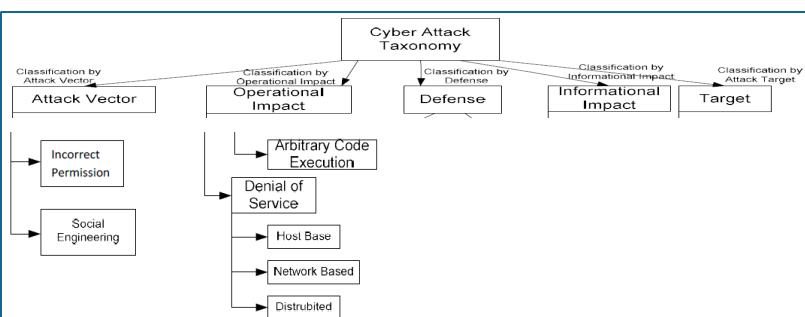
- AVOIDIT: A Cyber Attack Taxonomy (2009/University of Memphis)



Uma taxonomia possível para as ciber-ameaças



Uma taxonomia possível para as ciber-ameaças

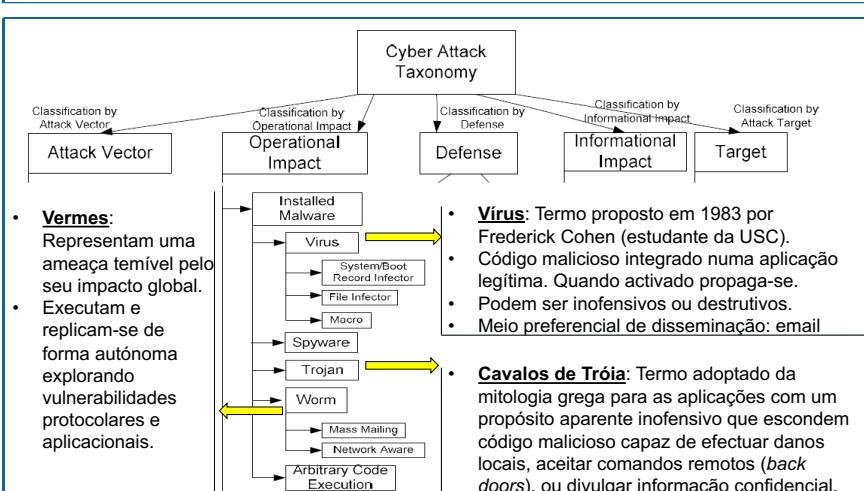


Uma taxonomia possível para as ciber-ameaças

- Exemplo de aplicação

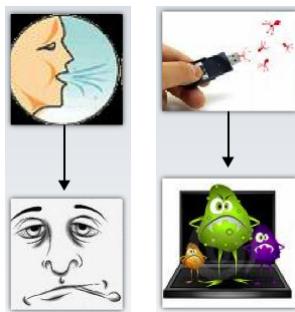
Name	Attack Vector	Operational Impact	Informational Impact	Defense	Target
MS RPC Stack Overflow	Buffer Overflow: Stack	Installed Malware: ACE	Distort	Mitigation: Reference Advisement VU#827267 Remediation: Patch System	OS: Windows Server
Gimmiv.A	Buffer Overflow: Stack	Installed Malware: Trojan	Disclosure	Mitigation: Reference Advisement Microsoft Remediation: Patch System	OS: Windows Server
Conficker	Buffer Overflow: Stack	Installed Malware: Worm	Disrupt	Mitigation: Reference Advisement Microsoft Remediation: Patch System	OS: Windows Server, 2000, XP

As ameaças com efeitos mais nefastos



Vírus (Virus)

- Vírus biológico é um organismo infeccioso que requer uma célula hospedeira para crescer e multiplicar-se.

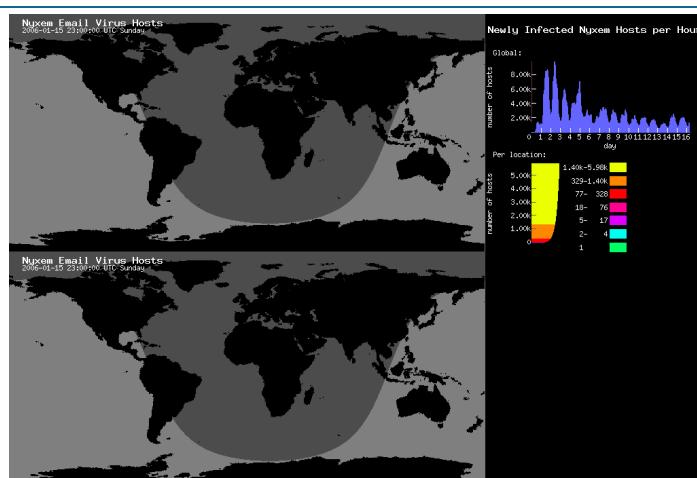


Viruses that have created problems across the Internet:

- Creeper Virus on ARPANet - early 1970's
- Rabbit Virus - 1974
- ANIMAL Virus - 1975
- Elk Cloner Virus - 1982
- Term "Computer Virus" Coined - 1983
- Brain Boot Sector Virus - 1986
- Ghostball Virus - 1989
- Michelangelo Virus - 1991
- Concept Macro Virus - 1995
- Melissa Virus - 1999
- Simile Multi-OS Virus - 2001

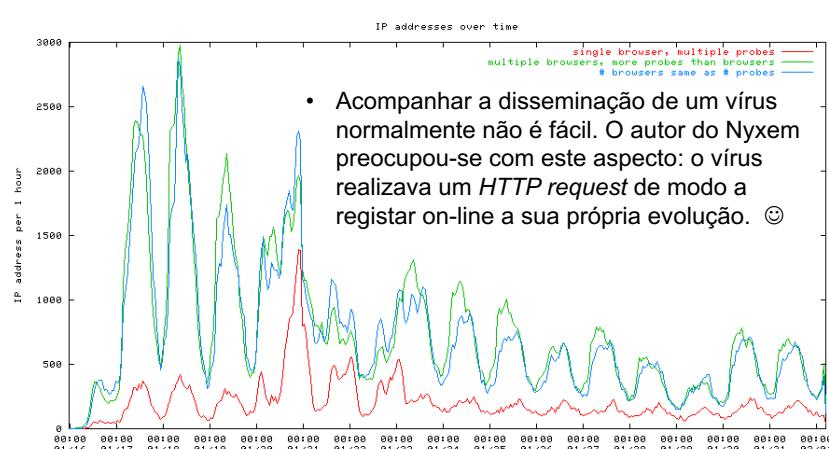


Vírus (Virus) - Nyxem Virus (Jan 2006, 0m 39s)



<http://www.caida.org/research/security/blackworm/>

Vírus (*Virus*) - Nyxem Virus (Jan 2006, 0m 39s)



<http://www.caida.org/research/security/blackworm/>

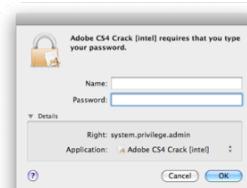
Cavalos de Tróia (*Trojan Horses*)

- Apesar de não criarem réplicas de si próprios são de muito fácil elaboração (*script kids*) e operam em cliente/servidor.
- Em regra são de difícil detecção e por vezes auto-des-troem-se para impossibilitar/dificultar a detecção.
 - Ex. *Keylogger*, *Backdoor* , *Spammers*, ...



Trojan Horses that have created problems across the Internet:

- NetBus – March 1998
- Back Orifice – August 1998
- Sub7 – 1999
- ProRat – 2003
- Vundo – 2004
- SpySheriff – 2005
- Zlob – 2005
- Storm – 2007



Cavalos de Tróia (*Trojan Horses*)

- Tipos comuns

- Remote-access Trojan Horse
- Data sending Trojan Horse
- Destructive Trojan Horse
- Proxy Trojan Horse
- FTP Trojan Horse
- Security software disabler
- Trojan Horse
- Denial of Service Trojan Horse



Cavalos de Tróia (*Trojan Horses*)

Dois milhões de utilizadores instalaram versão infectada do programa de limpeza CCleaner

Algumas versões da ferramenta da empresa de cibersegurança Avast estavam infectadas com ficheiros maliciosos desde Julho.

KARLA PEQUININO - 19 de setembro de 2017, 15:28

0 PARTILHAS



Cavalos de Tróia (*Trojan Horses*)

Judiciária detecta fraude informática em 250 farmácias portuguesas



Os dados informáticos em causa, transmitidos a empresas nacionais e internacionais, envolvem tanto histórias clínicas dos doentes como actividade das farmácia, bem como informação sobre o receituário dos médicos.

19-03-2012 18:14 por Dara Pires

Algumas farmácias podem ter colaborado em burla informática



Caso envolve o comércio de dados pessoais dos utentes, bem como dados sobre o receituário dos médicos.
19-03-2012 18:55

PJ detecta burla informática em 250 farmácias

A Polícia Judiciária (PJ) revelou ontem os resultados de uma operação de burla informática nos computadores de 250 farmácias em todo o País.

A informação era recolhida por uma empresa multinacional do sector farmacêutico e transmitida a outras empresas além-fronteiras, com o objectivo de controlar a concorrência, segundo uma informação avançada ontem pela Rádio Renascença (RR). Os dados em causa

envolvem tanto dados clínicos dos doentes como actividade das farmácias e também informação sobre a prescrição dos médicos, apurou ainda a RR.

De acordo com uma nota publicada no site da PJ, da investigação em curso foi possível recolher indícios que apontam para a prática dos crimes de burla informática, sabotagem informática, dano relativo a programas ou outros dados infor-

máticos, acesso ilegítimo, acesso indevido e tratamento transfronteiriço de dados pessoais.

A operação, a que a PJ chamou de "relax", tem vindo a desenvolver-se nos últimos seis meses, e levou à apreensão de "dados informáticos relevantes para a investigação e que agora vão ser analisados ao detalhe, por forma a circunscrever os factos praticados e a determinar responsabilidades criminais concretas". ■ C.D.

Vermes (*Worms*) - Fases de propagação



- Muitos vermes caracterizam-se por explorar determinada vulnerabilidade, possuir um mecanismo de propagação em rede específico e um payload onde é alojado o código ofensivo (e.g., uma backdoor)

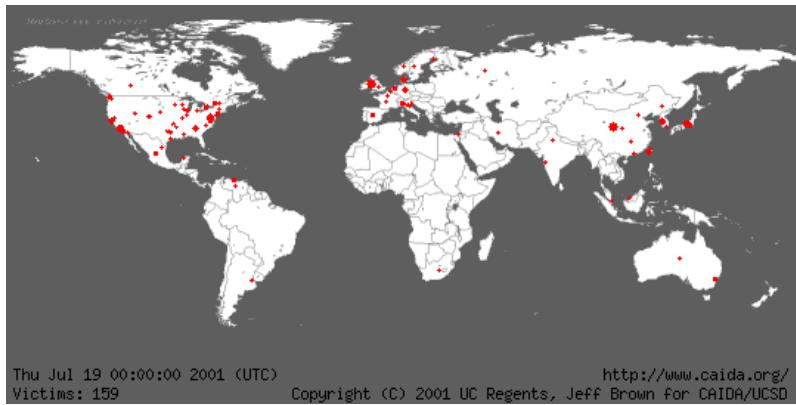
Worm and Virus – Exploit Comparison (~20 Yrs)

	Morris 1988	Love Bug 2000	Code Red 2001	Slammer 2003	MyDoom 2004	Zotob 2005	MS RPC DNS 0day 2007
Probe	Scans for finger	N/A	Scans for IIS	N/A	N/A	Scans for MS directory services	Scans for endpoint Mapper query
Penetrate	Causes buffer overflow in finger	Arrives as email attachment	Causes buffer overflow in IIS	Causes buffer overflow in SQL and MSDE	Arrives as email attachment	Causes buffer overflow in UPnP service	Causes buffer overflow in RPC service
Persist	Executes script to download code	Creates executables and edits the registry	Executes script to download code	N/A	Creates executables and edits the registry	Creates executables and edits the registry, download code	Executes payload to download code
Propagate	Looks for addresses and spreads to new victims	Opens address book and emails copies of itself to new victims	Picks new addresses and spreads to new victims	Picks new addresses and spreads to new victims	Opens address book and email copies of itself to new victims	Starts FTP and TFTP services, looks for addresses and spreads to new victims	Looks for addresses and spreads to new victims
Paralyze	Spawns many processes which slow the system	Worm spreads	Spawns many threads which slow the system	Generates many packets which slows the network	Worm spreads	Deletes registry keys and files, and terminates processes	Worm spreads

Vermes (Worms)



- Code-Red Worm (Jul 2001, 0m 28s)

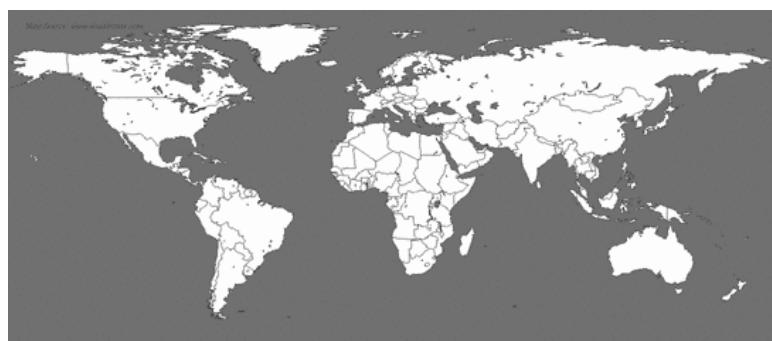


<http://www.caida.org/research/security/code-red/>

Vermes (Worms)



- Sapphire Worm (a.k.a. SQL/Slammer)(Jan 2003, 0m 2s)



<http://www.caida.org/research/security/sapphire/>

Vermes (Worms)



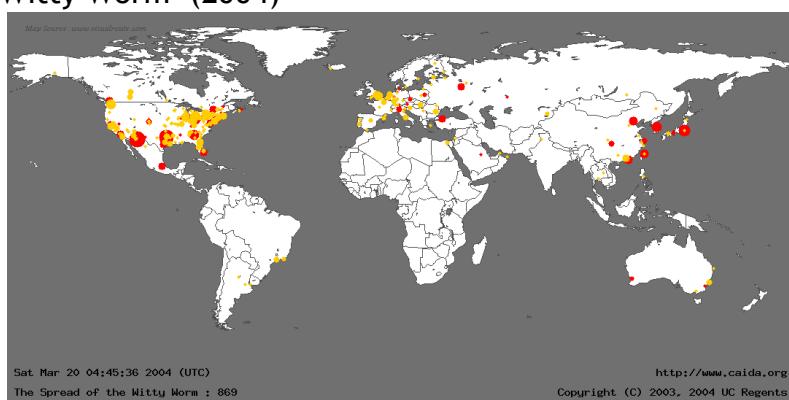
- Sapphire Worm (a.k.a. SQL/Slammer)(Jan 2003, 0m 2s)
 - Um dos vermes de mais rápida propagação da história
 - 90% dos servidores SQL na Internet infectados em 10 min.
 - Provocou a quebra total, entre outros:
 - Das redes de comunicação móvel na Coreia do Sul
 - Da rede de terminais ATM do Bank of America
 - De 5 *root servers* DNS mundiais
 - Da bilheteira da Continental Airlines
 - Em Portugal, 300.000 clientes ficaram privados, durante 12h, do serviço de Internet por cabo.

<http://www.caida.org/research/security/sapphire/>

Vermes (Worms)



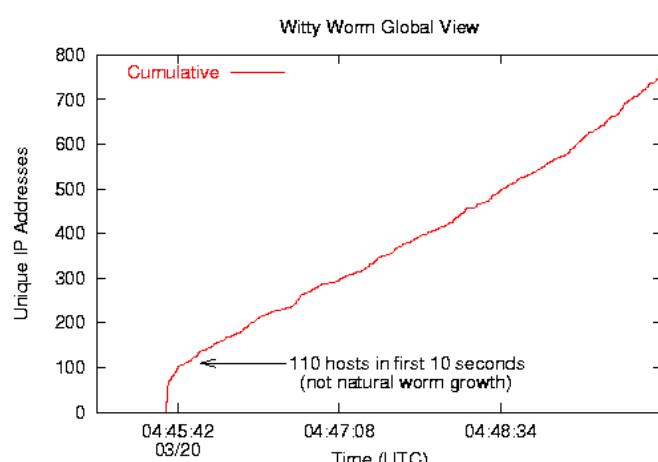
- Witty Worm (2004)



<http://www.caida.org/research/security/witty/>

Vermes (Worms)

- Witty Worm (2004)



<http://www.caida.org/research/security/witty/>

Vermes (Worms)

"The Moon" worm infects Linksys routers

Self-replicating worm program infects Linksys routers by exploiting an authentication bypass vulnerability

By Lucian Constantin

February 14, 2014 09:07 AM ET [Add a comment](#)

[Share](#) [Twitter](#) [G+](#) [StumbleUpon](#) [Email](#) [More](#)

IDG News Service - A self-replicating program is infecting Linksys routers by exploiting an authentication bypass vulnerability in various models from the vendor's E-Series product line.

Researchers from SANS Institute's Internet Storm Center (ISC) [issued an alert](#) Wednesday about incidents where Linksys E1000 and E1200 routers had been compromised and were scanning other IP (Internet Protocol) address ranges on ports 80 and 8080. On Thursday the ISC researchers reported that [they managed to capture the malware](#) responsible for the scanning activity in one of their honeypots -- systems intentionally left exposed to be attacked.

<http://www.computerworld.com/article/2626444/the-moon-worm-infects-linksys-routers.html>

Vulnerabilidade típica: *buffer overflows*

- Cerca de um terço das vulnerabilidades do software dizem respeito a *buffer overflows* (CERT)
- *Buffer* é uma zona de memória reservada por uma aplicação para armazenar dados temporários
 - Aplicações deficientes podem aceitar guardar dados de volume superior ao que na verdade suportam, corrompendo zonas de memória contíguas com outros dados ou código.
 - Os Vírus e os Cavalos de Tróia tendem a explorar *root buffers* locais (espaços de endereçamento privilegiados)
 - Vermes como o SQL Slammer e o Code Red exploraram *root buffers* remotos (i.e., não necessitaram de utilizadores locais nem dos seus privilégios para aceder a esses buffers)

Vulnerabilidade típica: *buffer overflows*

- <http://www.phenoelit.org/ultimaratio/index.html>
- (documentar aqui um ataque ao IOS)

Malware como ciberarma

De acordo com o "The Washington Post"
EUA e Israel foram os criadores do vírus Flame

20.06.2012 - 10:06 Por Susana Almeida Ribeiro

Votar ★★★★★ | 4 votos ★★★★★ 0 Gosto 3 de 8 notícias em Mundo « anterior seguinte

EUA e Israel desenvolveram em conjunto o sofisticado vírus informático Flame, detectado recentemente e considerado uma "ciberarma" global, com o intuito de conduzir uma ciber-sabotagem à capacidade iraniana de desenvolver armas nucleares, avança hoje o "The Washington Post", que cita "responsáveis ocidentais com conhecimentos acerca desse esforço".

```
if not _params.STD then
    assert(loadstring(config.get("LUA_LIBS.STD")))
if not _params.table_ext then
    assert(loadstring(config.get("LUA_LIBS.table_ext")))
end
if not _params.LIB_FLAME_PROPS_LOADED... then
    LIB_FLAME_PROPS_LOADED... = true
    Flame_props = {}
    Flame_props.FLAME_ID_CONFIG_KEY = "MANAGER_FLAME_ID"
    Flame_props.FLAME_TIME_CONFIG_KEY = "TIMER_NUM_OF_SECS"
    Flame_props.FLAME_LOGGING_PERCENTAGE_KEY = "FLAME_LOGGING_PERCENTAGE"
    Flame_props.FLAME_VERSION_CONFIG_KEY = "FLAME_VERSION_NUMBER"
    Flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR_INTERNET_CHECK"
    Flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    Flame_props.BPS_CONFIG = "GATOR_LINK_BANDWIDTH_CALCULATOR.BPS_QUEUE"
    Flame_props.BPS_KEY = "BPS"
    Flame_props.GATOR_PROXY_SERVER_KEY = "GATOR_PROXY_DATA_PROXY_SERVER"
    Flame_props.gatormethod = function()
        if config.haskey(Flame_props.FLAME_ID_CONFIG_KEY) then
            local l_1_0 = config.get
            local l_1_1 = Flame_props.FLAME_ID_CONFIG_KEY
            return l_1_0(l_1_1)
        end
        return nil
    end
end
```

Stuxnet

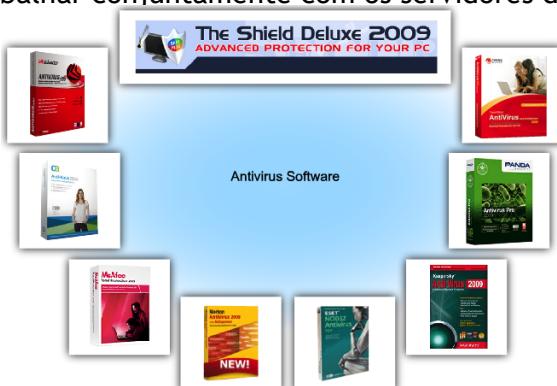
Zero Days covers the phenomenon surrounding the [Stuxnet](#) computer virus and the development of the malware software known as "[Olympic Games](#)".



https://en.wikipedia.org/wiki/Zero_Days

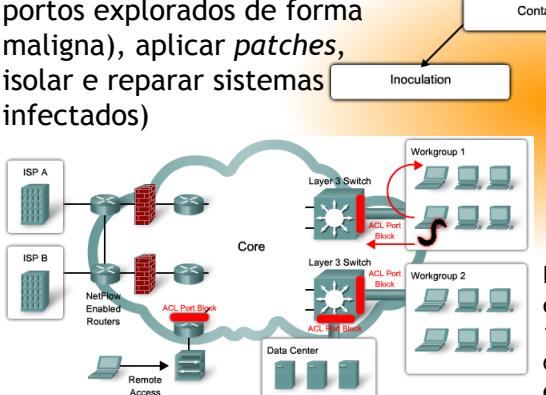
Mitigação

- Vírus e Cavalos de Tróia: antivírus locais e antivírus preparados para trabalhar conjuntamente com os servidores de email



Mitigação

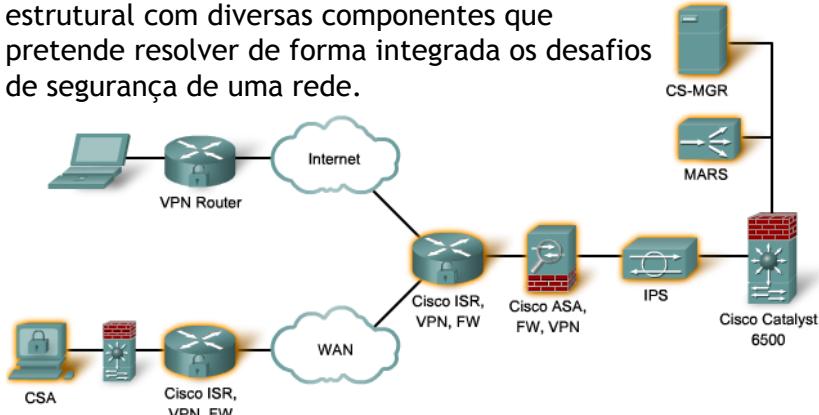
- Vermes: Contenção (fechar portos explorados de forma maligna), aplicar *patches*, isolar e reparar sistemas infectados



Ex. O SQL Slammer explorou a porta UDP 1434, porta esta que devia estar fechada ao exterior.

Mitigação

- *Cisco Self-Defending Network* é uma solução estrutural com diversas componentes que pretende resolver de forma integrada os desafios de segurança de uma rede.



Mitigação

- **Cisco Security Agent (CSA)**: Um HIPS (*host-based intrusion prevention system*) integrável com um qualquer antivírus
- **Cisco Network Admission Control (NAC)**: um dispositivo que restringe as admissões à rede a dispositivos que possuam um perfil de segurança adequado
- **Cisco Security Monitoring, Analysis, and Response System (MARS)**: reporta eventos relevantes.

Products available for the Cisco Self-Defending Network

Cisco IOS platforms with integrated IPS, VPN, and stateful FW

Cisco PIX 500 Series Security Appliances with integrated VPN

Integrated network IDS and IPS

Security modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

Cisco ASA 5500 Series Adaptive Security Appliances (ASA) with integrated VPN

Appliance-based network intrusion detection system (IDS) and intrusion prevention system (IPS)

Cisco Secure ACS

Cisco Security Agent endpoint protection software

Cisco Security Manager, Cisco Security MARS, Cisco Router and Security Device Manager (SDM), and other GUI-based device managers

*NOTE: Each product can be deployed independently or as part of an integrated security design.

Outra taxonomia possível

- Ataques Estruturados

- Oriundos de hackers competentes e profundos conhecedores das vulnerabilidades, capazes de desenvolver ferramentas para o efeito. Tipicamente são movidos pelo intuito de realizar algum tipo de ilícito.

- Ataques não Estruturados

- Realizados por indivíduos inexperientes que possuem apenas a curiosidade de experimentar ferramentas existentes. Podem no entanto causar graves prejuízos.

Outra taxonomia possível

- Ataques Externos

- Realizados por indivíduos estranhos à organização e conduzidos tipicamente de forma remota.

- Ataques Internos

- Perpetrados por indivíduos com acesso autorizado à infra-estrutura de comunicação da empresa. Constituem entre 60 a 80% dos ataques. As motivações são diversas mas normalmente estão relacionadas com a insatisfação dos seus autores.

Outra taxonomia possível

- Ataques Passivos

- Captura e análise/interpretação/divulgação de conteúdo sensível presente tráfego.
- Normalmente este tipo de ataque tem pouca visibilidade mas é usado na preparação de ataques activos.

- Ataques Activos

- Entrar em sistemas através de credenciais obtidas de forma fraudulenta (obtidas por ataques passivos).
- Modificação de mensagens (MITM)
- DoS, ...

Taxonomia Evento/Efeito

Event Vector

Threat Agent	Motivation	Objective	Method	Technique
Malicious Individual Organizations Foreign Government	Service Theft	Information Corruption	System Compromise	Targeted Exploit of System Vulnerability
			Protocol Compromise	Targeted Exploit of Social Vulnerability
	Sabotage	Information Fabrication	System Compromise	Targeted Exploit of System Vulnerability
			Protocol Compromise	Targeted Exploit of Social Vulnerability
	Information Destruction	System Compromise	System Compromise	Targeted Exploit of System Vulnerability
			Resource Exhaustion	Overload Network Resources
	Intelligence Gathering	Information Disclosure	Hardware Failure	Physical Damage
			Software Crash	Targeted Exploit of System Vulnerability
	Extortion	System Subversion	System Compromise	Targeted Exploit of System Vulnerability
			Hardware Failure	Targeted Exploit of Social Vulnerability
	Zombie Propagation	Information Corruption	Hardware Failure	Physical Damage
	Widespread Destruction	Information Disclosure	System Compromise	Targeted Exploit of System Vulnerability
		Information Discovery	System Compromise	Targeted Exploit of Social Vulnerability
	Identity Theft	System Subversion	System Compromise	Targeted Exploit of System Vulnerability
		Information Destruction	Autonomous Self Propagating Malware	Targeted Exploit of Social Vulnerability
	Nature Human Error	None	Information Disclosure	Autonomous Self Propagating Malware
			Information Corruption	Autonomous Self Propagating Malware
			System Compromise	Autonomous Self Propagating Malware
			Hardware Failure	Physical Damage
			Software Crash	Unintentional Exploit of System Vulnerability

Taxonomia Evento/Efeito

Effect Vector

Cause	Service Affected	Disruption Impact		Evaluation Metrics
		Economic Impact	% Revenue Lost, %GDP Lost	
Cyber Event within Service	Energy	Population Impact	% Population Denied Access	
Cascade Disruption from <Service>	Telecommunications	Government Impact	% Government Effectiveness Reduced	
	Finance	Population Impact	% Population denied access to service	
	Water Supply	Economic Impact	% Revenue Lost, %GDP Lost	
	Healthcare	Population Impact	% Population Denied Access	
	Transportation	Population Impact	% Population Denied Access	
	Law Enforcement	Population Impact	% Population Denied Access	
	Emergency and Fire Response	Government Impact	% Government Effectiveness Reduced	
	Govt. Administration	Population Impact	% Population Denied Access	
	Shipping	Government Impact	% Government Effectiveness Reduced	
	Agriculture	Economic Impact	% Revenue Lost, %GDP Lost	
	Commercial Facilities	Population Impact	% Revenue Lost, %GDP Lost	
	Critical Manufacturing	Economic Impact	% Population Denied Access	
		Economic Impact	% Revenue Lost, %GDP Lost	

Taxonomia Evento/Efeito

Event Vector (1)

Community	Threat Agent	Motivation	Objective	Method	Technique
San Jose/San Carlos	Unknown	Sabotage	Service Disruption	Hardware Failure	Physical Damage

Effect Vector (1)

Cause	Service Affected	Impact	Evaluation Metrics
Cyber Event within Service	Telecommunications	Population Impact	Unknown Percentage of Population
Cascade Disruption from Telecommunications	Finance	Population Impact	Unknown Percentage of Population
Cascade Disruption from Telecommunications	Emergency and Fire Response	Economic Impact	Unknown Revenue, GDP Lost
Cascade Disruption from Telecommunications	Healthcare	Population Impact	Unknown Percentage of Population

Event Vector (2)

Community	Threat Agent	Motivation	Objective	Method	Technique
Brazil	Organized Crime	Extortion	System Subversion	System Compromise	Targeted Exploit of System Vulnerability

Effect Vector (2)

Cause	Service Affected	Impact	Evaluation Metrics
Cyber Event within Service	Energy	Economic Impact	Unknown Revenue, GDP Lost

Event Vector (3)

Community	Threat Agent	Motivation	Objective	Method	Technique
Houston	Unknown	Zombie Propagation	System Subversion	System Compromise	Autonomous Self Propagating Malware

Effect Vector (3)

Cause	Service Affected	Impact	Evaluation Metrics
Cyber Event within Service	Law Enforcement	Government Impact	Unknown Reduction in Government Efficiency

Metodologias de ataques em rede

DEIS

Metodologias de ataque

- Categorização (CCNA Security):
 - Ataques por reconhecimento (*Reconnaissance Attacks*)
 - Descoberta não autorizada de sistemas, serviços e vulnerabilidades. Ferramentas: *sniffers* e *port scanners*.
 - Ataques de acesso a informação (*Access Attacks*)
 - Exploração de vulnerabilidades de autenticação conhecidas em serviços disponíveis com o objectivo de aceder de forma ilegítima a informação sensível. Tipicamente usam-se ataques por força bruta apoiados por dicionários.
 - Ataques de impedimento de prestação de serviço (*Denial of Service Attacks - DoS*)
 - Este tipo de ataques visa consumir uma fracção significativa de recursos (de servidores ou da rede) com prejuízos graves para o normal desempenho de serviços.

Ataques por reconhecimento

- Precedem normalmente ataques de acesso ou DoS.
- Estratégia simples: *ping sweep* (ICMP Echo Req/Repl).
- *Internet Information queries*
 - Descoberta de espaços de endereçamento (DNS/Whois)
- Para cada sistema descoberto inventariar os serviços alojados (e.g., Nmap).
- Para cada serviço identificar “assinaturas” (OS, version ...)
- *Packet sniffers* (e.g. Wireshark)
 - Em modo promíscuo podem capturar todo o tráfego *broadcast* e por vezes *multicast*
 - Nas redes comutadas (*switches*) o isolamento é apenas aparente quando comparado com a sua inexistência em segmentos partilhados (*collision domain*).
- Sistema de prevenção de intrusões (IPS) disparam alarmes a sinalizar alguns destes ataques (e.g., IOS de *routers Cisco ISR*).

Ataques de acesso

- **Ataques a passwords (password attacks)**
 - Métodos: Ataques por força bruta (com ou sem apoio de dicionários), cavalos de Tróia (*keyloggers*), ou *sniffers*.
- **Abuso de confiança (Trust exploitation)**
 - Exploram-se privilégios atribuídos indevidamente.
- **Redireccionamento de portos (port redirection)**
 - É um tipo específico de ataque por abuso de confiança em que uma terceira máquina comprometida é usada como medidora do ilícito (por, por exemplo, usufruir de privilégios na firewall).
 - Sistemas *host-based IDS* e antivirus ajudam na prevenção.
- **Ataques por interposição (Man-in-the-middle attack-MITM)**
 - Tipicamente alteram conteúdo de mensagens que circulam entre um par de entidades legítimas.

Ataques de acesso

Cisco IP Phones Vulnerable To Remote Eavesdropping

Monday, March 23, 2015 by Swati Khandelwal

8:1 | 166 | Like | 2.2k | Share | 1461 | Tweet | 291 | Reddit | 315 | Share | 32 | ShareThis | 2264



A critical vulnerability in the firmware of Cisco small business phones lets an unauthenticated attacker to remotely eavesdrop on private conversation and make phone calls from vulnerable devices without needing to authenticate, Cisco warned.

LISTEN AND MAKE PHONE CALLS REMOTELY

The vulnerability (CVE-2015-0670) actually resides in the default configuration of certain Cisco IP phones is due to "*improper authentication*", which allows hackers to remotely eavesdrop on the affected devices by sending specially crafted XML request.
Demands LAN access.

<http://thehacknews.com/2015/03/cisco-ip-phones-hacking.html>

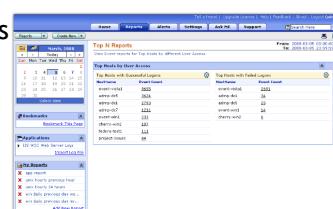
Ataques de acesso

• Buffer overflow

- [VNC Buffer Overflow](#)

• Detecção

- Inspecção de *logs* de acessos negados
- Ferramentas possíveis:
 - ManageEngine EventLog Analyzer
 - Cisco Secure Access Control Server
 - ...
- MITM
 - Aumento anormal da actividade de rede pode ser um indício uma vez que normalmente há duplicação de tráfego.



Ataques de acesso

**O FALSO BRUNO DE CARVALHO,
UM ELEVADOR E UMA
FUNCIONÁRIA DO SPORTING...**

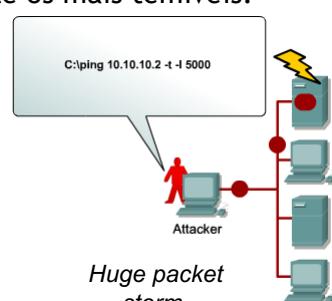


Uma

funcionária do Sporting Clube de Portugal, foi a "vítima" de uma brincadeira do humorista, Luís Franco Bastos, e acreditou num telefonema, em que o presidente do clube "Leonino" estava supostamente preso num elevador em Alvalade...

Ataques DoS

- Trata-se de um tipo de ataque de rede que pretende diminuir a disponibilidade de determinado serviço prestado a pessoas (e.g., sites web), equipamentos ou aplicações.
- São ataques simples mas tipicamente os mais temíveis.
- Vulnerabilidades exploradas:
 - Tratamento deficiente de determinada formatação específica de uma mensagem protocolar (e.g., *Ping of Death*)
 - Limites dos recursos disponíveis nos próprios serviços (RAM/ CPU/ etc.) ou nas redes e equipamentos de acesso ao mesmo.



Ataques DoS: Exemplos

- *Ping of Death*

- Envio de um pacote IP maior que o tamanho máximo (65,535 bytes). A sua construção é possível através do envio de fragmentos. Bastavam 65,536 bytes para causar um *buffer overflow* na pilha do receptor e respectivo *crash*.

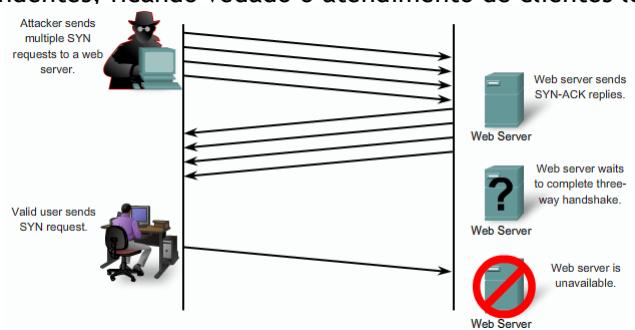
- *Smurf Attack*

- O atacante envia uma quantidade elevada de *ICMP Echo Requests* para o endereço de *broadcast* dirigido de uma rede, forjando o *source address* com endereços *unicast* locais.
- A rede destino rapidamente satura
- Hoje grande parte dos *routers* e dos sistemas operativos dos terminais já estão por omissão preparados para evitar ser alvos deste tipo de ataque.

Ataques DoS: Exemplos

- *TCP SYN Flood*

- Envio de muitos pacotes TCP SYN, tipicamente com o endereço SA forjado. Deste modo satura-se rapidamente o nº de sessões pendentes, ficando vedado o atendimento de clientes legítimos



Ataques DoS: Exemplos

- **Teardrop**

- Envio de pacotes IP fragmentados com os campos protocolares usados no processo de reagrupamento povoados com valores fraudulentos de modo a provocar comportamentos erróneos no sistema atacado.

Another DoS attack!



Ataques DoS: Consequências & Sintomas

- Consequências directas comuns

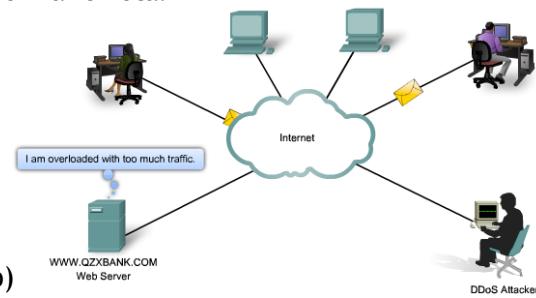
- Consumo excessivo de recursos como largura de banda, espaço em disco, ou tempo de processador
- Danos na informação de configuração (e.g., encaminhamento)
- Danos na informação de estado (e.g., resets de sessões TCP)
- Danos em equipamentos físicos
- Impedimento de comunicação legítima com o sistema alvo.

- Sintomas possíveis

- Desempenho de rede abaixo do normal
- Indisponibilidade de determinado web site
- Indisponibilidade de todos os web sites
- Aumento desmesurado de spam (*mail bombs*)

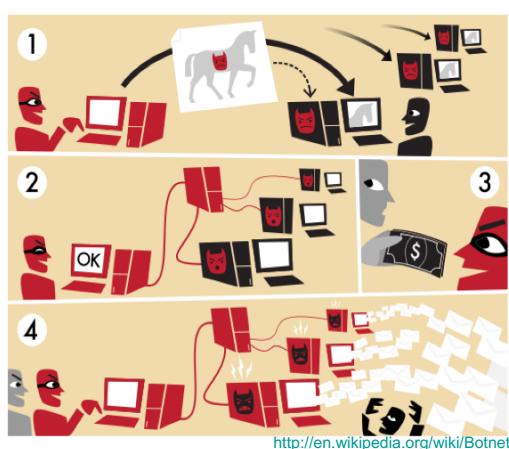
Ataques *Distributed DoS* (DDoS)

- Semelhante ao DoS sendo no entanto que o tráfego malicioso é injectado a partir de múltiplos sistemas da rede
 - Objectivo alcançado através da distribuição prévia de zombies (por vírus, vermes ou cavalos de tróia) que o atacante instrui posteriormente de forma remota.
- Em alternativa o ataque pode ser acordado através de redes sociais por grupos que partilham um mesmo objectivo (normalmente ideológico ou político)



Botnets: Cibercrime & mercado negro

- O atacante compromete (através de vírus, vermes, cavalos de Tróia, etc.) um conjunto alargado de nós (denominados zombies), instalando nestes um robot.
- A rede (net) de bots, denominada botnet, aguarda de modo passivo por ordens/comandos emanados a partir do controlador central (*command-and-control (C&C) server*).
- O potencial do botnet é então alugado para os mais diversos efeitos: envio de SPAM, DDOS (web sites e DNS root servers, extorsão por chantagem, etc.

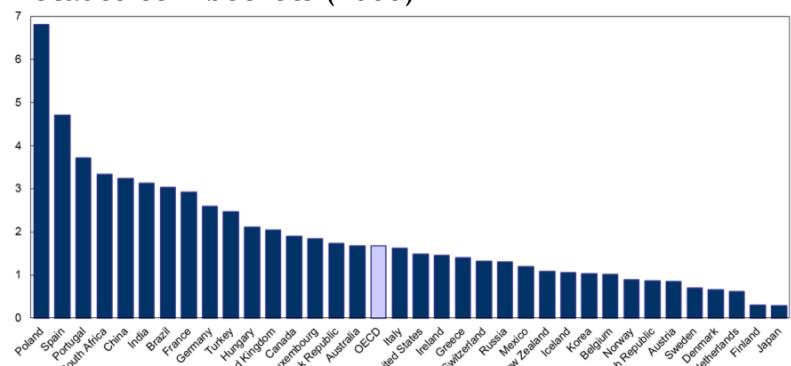


Botnets: Cibercrime & mercado negro

- Estima-se que um em cada quatro computadores da Internet integrem um ou mais *botnets*.
- Os *bots* tipicamente recorrem a infra-estruturas de comunicação populares como o IRC, o *twitter* ou *Instant Messenger* para melhor camuflarem a comunicação com os *Command & Control servers*.
- As instâncias mais recentes têm evoluído para arquitecturas *peer-to-peer* (P2P).
- Os botnets mais modestos albergam 10.000 a 20.000 nós. Os maiores chegam a integrar vários milhões de terminais.

Botnets: Cibercrime & mercado negro

- Percentagem de computadores servidos por banda larga infetados com botnets (2006)



<http://www.oecd.org/sti/broadband/oecdbroadbandporta1.htm>

Botnets: Cibercrime & mercado negro

Date created	Name	Estimated no. of bots	Spam capacity	Aliases
2009 (May)	BredoLab	30,000,000 ^[12]	3.6 billion/day	Oficia
2008 (around)	Mariposa	12,000,000 ^[13]	?	
?	Conficker	10,500,000+ ^[14]	10 billion/day	DownUp, DownAndUp, DownAdUp, Kido
?	Zeus	3,600,000 (US Only) ^[15]	n/a	Zbot, PRG, Wsnpoem, Gorhax, Kneber
2007 (Around)	Cutwail	1,500,000 ^[16]	74 billion/day	Pandex, Mutant (related to: Wigon, Pushdo)

- Em Julho de 2010 o FBI capturou um esloveno de 23 anos responsável por comandar, junto com dois parceiros, o botnet Mariposa (12.7 milhões de PCs Windows em 190 países).
- O botnet havia sido desmantelado a 23 de Dezembro de 2009 num trabalho conjunto do FBI, da Guarda Civil Espanhola e das empresas Panda Security e Defence Intelligence.

http://www.theregister.co.uk/2010/03/03/mariposa_botnet_bust_analysis/



Botnets: Cibercrime & mercado negro

- Polícia espanhola desmantela organização de pirataria informática Anonymous (10.06.2011) Paula Torres**
- Com a detenção de três dirigentes do grupo Anonymous, a Polícia Nacional espanhola desmantelou a cúpula do grupo de piratas informáticos que já fora considerado uma "ameaça".
- Na casa de um deles, organizaram ataques às páginas da Playstation, BBVA, Bankia, Enel e às dos governos do Egípto, Argélia, Líbia, Irão, Chile, Colômbia e Nova Zelândia.
- ... Os detidos que a NATO considerou uma ameaça à "aliança militar" podem agora incorrer em crimes de associação criminosa puníveis de dois a três anos de prisão.



http://www.publico.pt/Sociedade/policia-espanhola-desmantela-organizacao-de-pirataria-informatica-anonymous_1498341

“missilenets”

Grupo da Universidade do Texas alerta para perigos associados aos aviões não tripulados
Investigadores norte-americanos piratearam um “drone” em pleno voo

29.06.2012 - 16:58 Por Isabel Gorjão Santos

Votar ★★★★★ | 2 votos ★★★★  4 |  132

6 de 9 notícias em Mundo « anterior | seguinte »

Um grupo de investigadores da Universidade de Austin, no Texas, conseguiram assumir o controlo de um “drone” durante o voo e demonstrar o risco de utilizar este tipo de aparelhos.

- **Spoofing por GPS (envio de sinais mais potentes)**
- **Em 2013 prevêem-se 30.000 (uso comercial)**



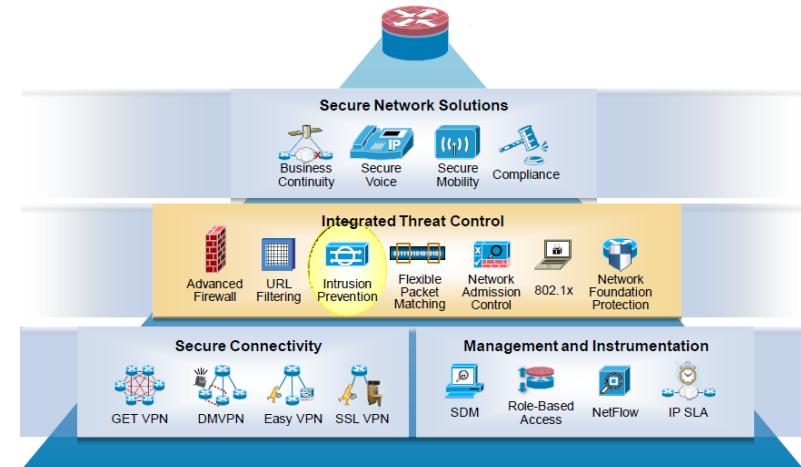
Os “drones” são habitualmente usados em operações militares, mas a sua segurança tem sido posta em causa. (Reuters)

<http://www.publico.pt/Mundo/investigadores-norteamericanos-piratearam-um-drone-em-pleno-voo-1552659>

Mitigação de ataques em rede

DEIS

O IOS oferece protecção no acesso à WAN



Mitigação de ataques de reconhecimento

- Defesas contra *packet sniffers*
 - Mecanismos de autenticação robustos
 - E.g., One-Time Password (OTP) recorre a autenticação de factor duplo (e.g., ATM: cartão + PIN)
 - Encriptação da comunicação
 - Adopção de infra-estrutura comutada (ajuda apenas)
 - *Antisniffer software* (*delays/CPU times* anormais)
- Defesas contra *Port scanning*
 - Não existe forma de mitigar estes ataques
 - Os IPS e as *firewalls* podem limitar em muito a descoberta
 - Os *ping sweeps* podem ser evitados filtrando tráfego ICMP na periferia da rede. Ainda assim é possível fazer *port scanning!*

Mitigação de ataques de reconhecimento

- Os IPS (*network e host-based*) podem alertar o administrador para a realização de um ataque de reconhecimento
 - O administrador pode tomar algumas medidas (e.g., alertar o ISP para a origem desses ataques)

Techniques Available for Reconnaissance Attack Mitigation Include:

- Implement authentication to ensure proper access.
- Use encryption to render packet sniffer attacks useless.
- Use anti-sniffer tools to detect packet sniffer attacks.
- Implement a switched infrastructure.
- Use a firewall and IPS.

Mitigação de ataques de acesso

- Ataques por *brute force* podem ser desencorajados
 - Desactivando contas após tentativas consecutivas falhadas.
 - Por adopção de política de escolha de passwords robustas.
 - Usando OTPs ou passwords encriptadas
- A rede deve adoptar o princípio da confiança mínima (*minimum trust*): um servidor seguro não deve confiar num servidor não seguro.
- Acessos remotos e tráfego de encaminhamento deve ser encriptado

Techniques Available for Access Attack Mitigation Include:

- Strong password security
- Principle of minimum trust
- Cryptography
- Applying operating system and application patches

Mitigação de ataques DoS

- Ataques DoS

- A adopção de técnicas simples de protecção *anti-spoofing* no perímetro da rede elimina uma grande percentagem
- Firewalls e IPSs são das soluções mais efectivas, disponibilizando uma série de técnicas para o efeito (*DHCP snooping*, *IP Source Guard*, *Dynamic ARP Inspection*, ACLs.)

- Ataques DDoS

- A sua mitigação requer a cooperação com ISPs
- Mecanismo de *Quality of Service* (QoS) podem dar uma ajuda (limitada)

The Primary Means of Mitigating DoS Attacks Include:

- IPS and firewalls (Cisco ASAs and ISRs)
- Anti-spoofing technologies
- Quality of Service – traffic policing

Boas práticas

1. Manter os sistemas actualizados diariamente (*patches*)
2. Desactivar serviços e portos desnecessários
3. Usar passwords robustas e alterá-las com frequência
4. Controlar o acesso físico aos sistemas
5. Limitar ao estritamente necessário o input dos serviços de acesso remoto
6. Realizar e testar backups com regularidade
7. Educar os colaboradores para os riscos da engenharia social e desenvolver estratégias de apoio à validação de identidades através do telefone, email ou contacto pessoal

Boas práticas

8. Proteger com passwords e encriptação dados sensíveis
9. Adoptar soluções tecnológicas de apoio (firewalls, IPS, VPNs, antivírus, etc.)
10. Redigir uma política de segurança para a empresa.



Referências

- CCNA Security - Ch. 1 - Modern Network Security Threats
- ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management, 2005
- Information Security Policy, University of Princeton, April 2008
- S. Shiva, C. Simmons, C. Ellis, D. Dasgupta, S. Roy, Q. Wu. [AVOIDIT: A cyber attack taxonomy.](#) Technical Report: CS-09-003, University of Memphis. August, 2009.
- K. Harrison , G. White, A Taxonomy of Cyber Events Affecting Communities, [2014 44th Hawaii International Conference on System Sciences](#)
- Malware Security report: protecting your Business, customers, and the bottom line, VeriSign, 2010

Obrigado pela atenção. Alguma dúvida?

