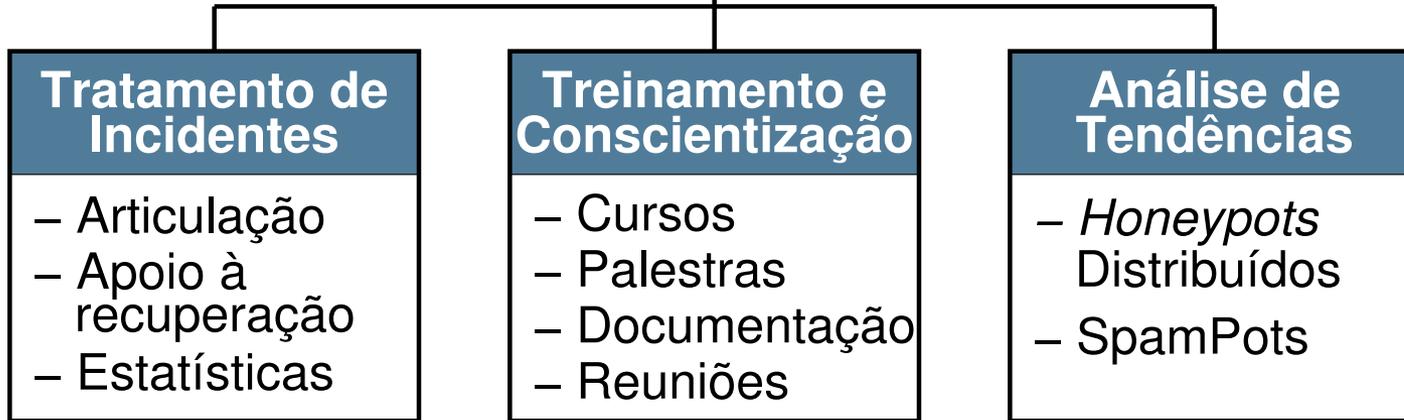nic.br cgi.br 20 anos cert.br

XII Semana da Informática
COTIL, Limeira, SP
04/09/17

IoT: Internet das coisas... Invadidas?

Marcus Vinícius Lahr Giraldi
marcus@cert.br

cert.br **nic.br** **cgi.br**

| **Tratamento de Incidentes**	**Treinamento e Conscientização**	**Análise de Tendências**
– Articulação – Apoio à recuperação – Estatísticas	– Cursos – Palestras – Documentação – Reuniões	– *Honeypots* Distribuídos – SpamPots

Criado em 1997 para:

– **Ser um ponto de contato nacional para notificação de incidentes**

– **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**

– **Estabelecer um trabalho colaborativo com outras entidades**

– **Aumentar a conscientização sobre a necessidade de segurança na Internet**

– **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Estrutura do CGI.br e NIC.br
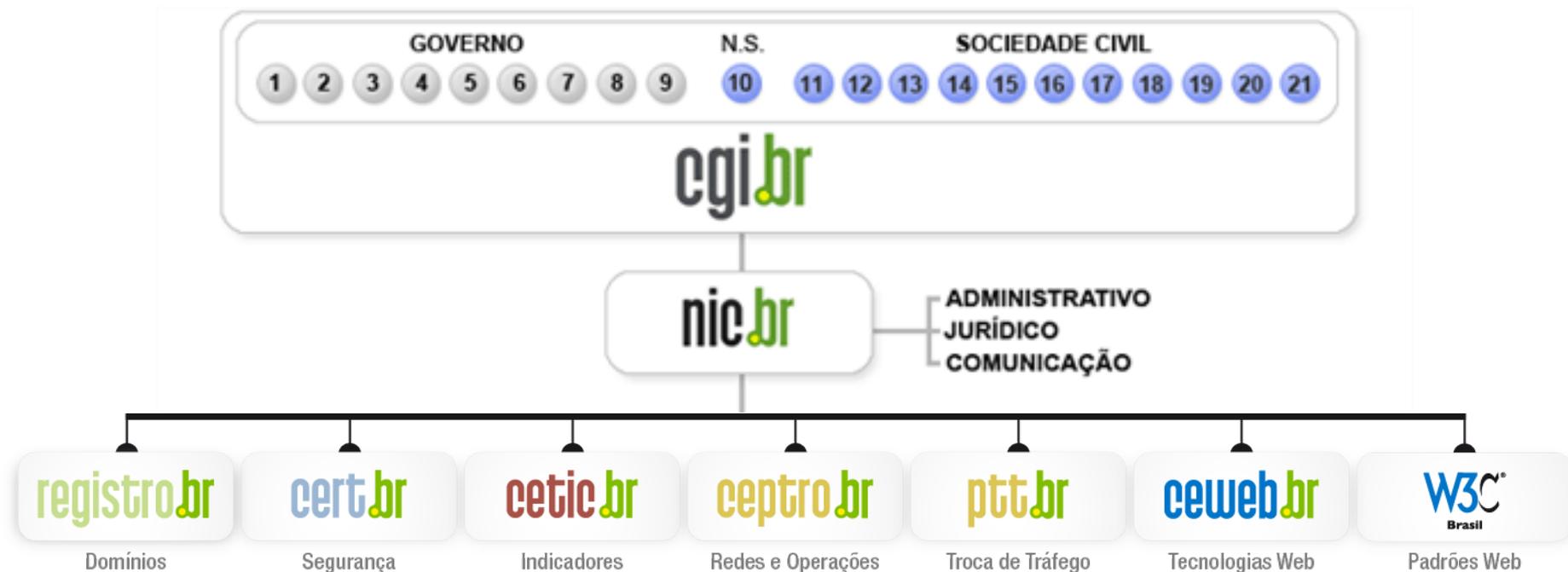
1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Agenda

- **Internet das Coisas**

- **Ataques atuais envolvendo IoT**

- **Problemas antigos**

- **Desafios**

Internet das Coisas
Nova tecnologia?

Computação Ubíqua

- **Mark Weiser, em 1988**

- **Oposto da "realidade virtual"**
  - pessoas colocadas em realidade gerada por computadores

- **Computador se integra a vida das pessoas**
  - utilizado sem ser notado, tecnologia "calma"
  - pano de fundo de nossas vidas

- **Ainda sem recursos disponíveis na época para ser usada**

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."

The Computer for the 21st Century

http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

Internet das Coisas – Surgimento

- ***Internet of Things* (IoT), *Internet of Everything* (IoE)**
- **Kevin Ashton, em 1999**
    - apresentação para executivos sobre como facilitar a logística da cadeia de produção usando RFID
- **Ainda com poucos recursos para ser usada**

"We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory."

That 'Internet of Things' Thing
In the real world, things matter more than ideas

*http://www.rfidjournal.com/articles/view?4986*

Internet das Coisas – Atualidade

"... is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity..."

Wikipedia

"...The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things..."
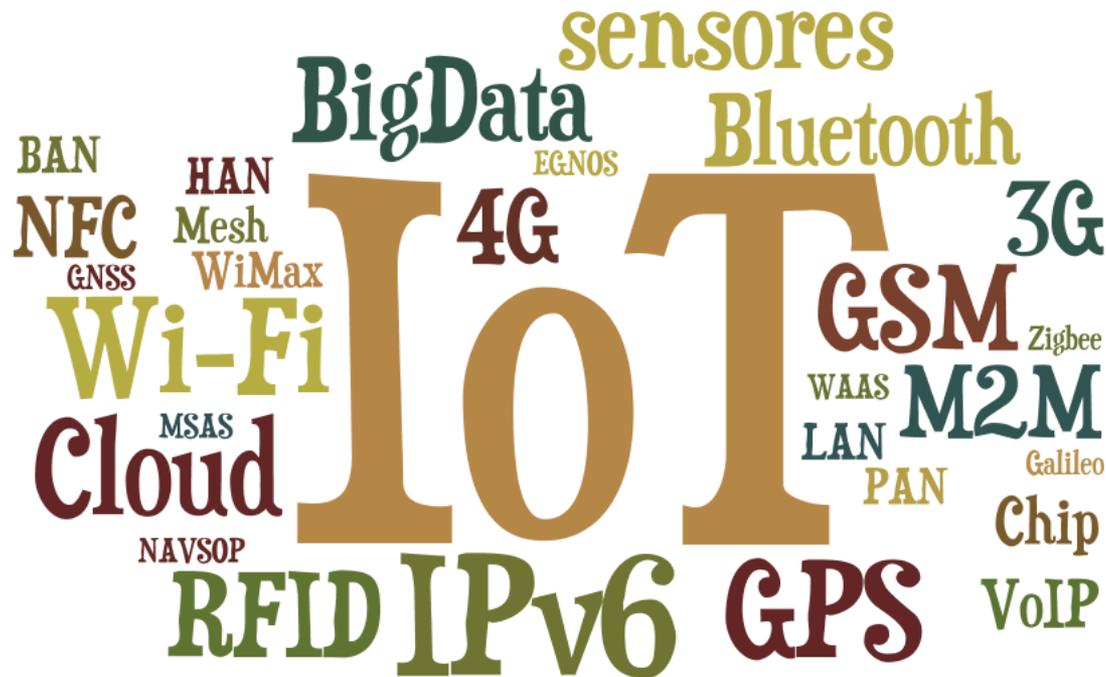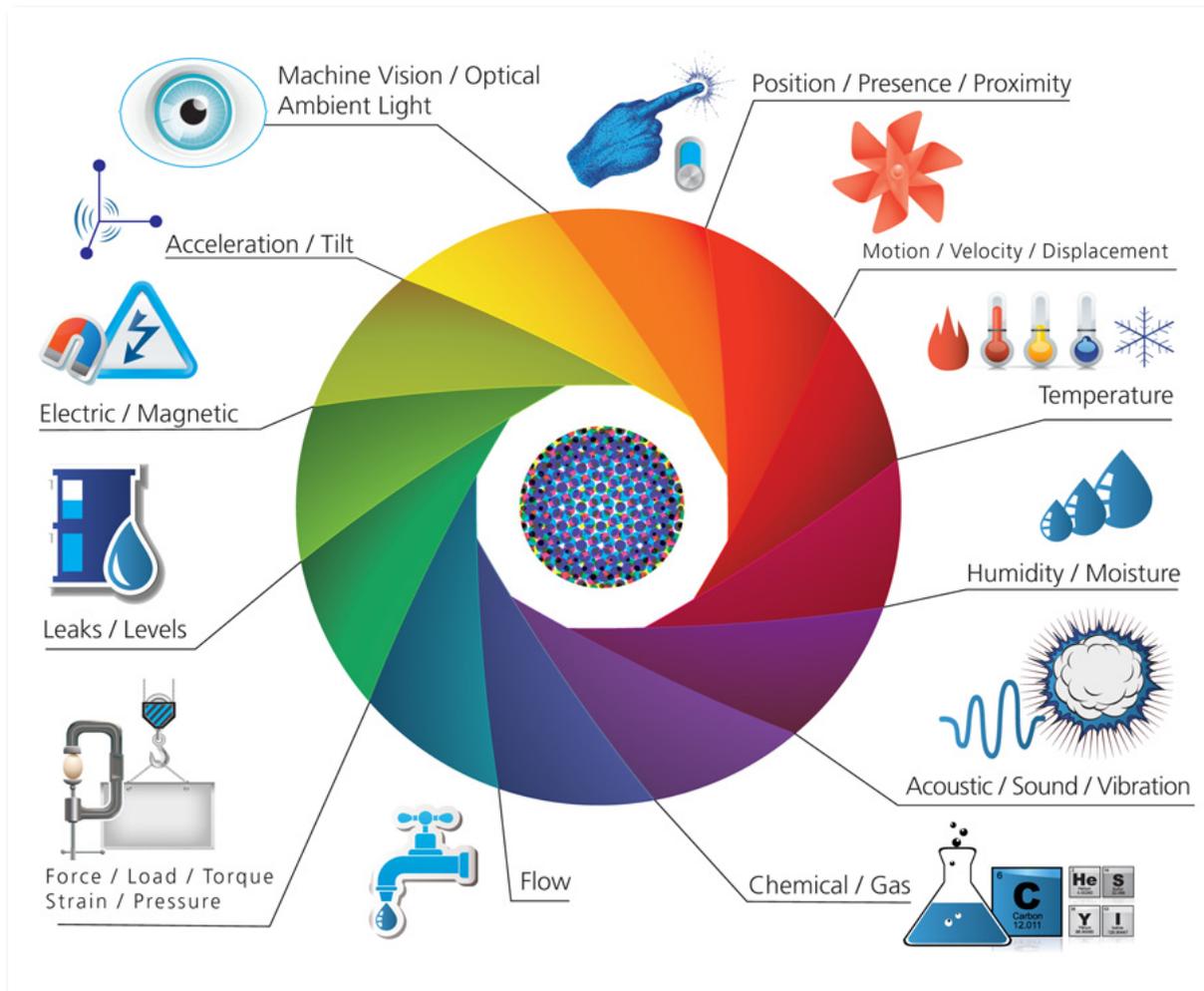
Webopedia
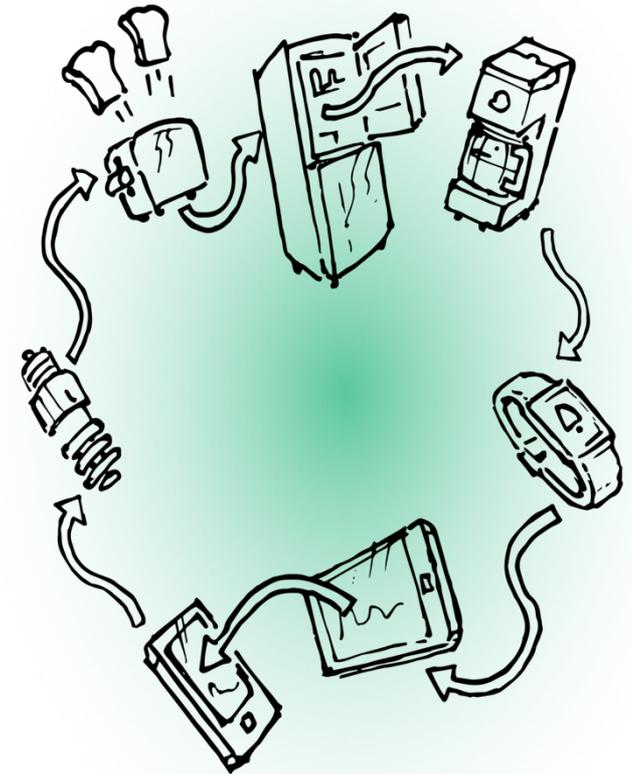
Internet das Coisas – Atualidade

- **As coisas já estão conectadas**
  - sistemas complexos e completos
    - sistema operacional, aplicações Web, permitem acesso remoto, etc
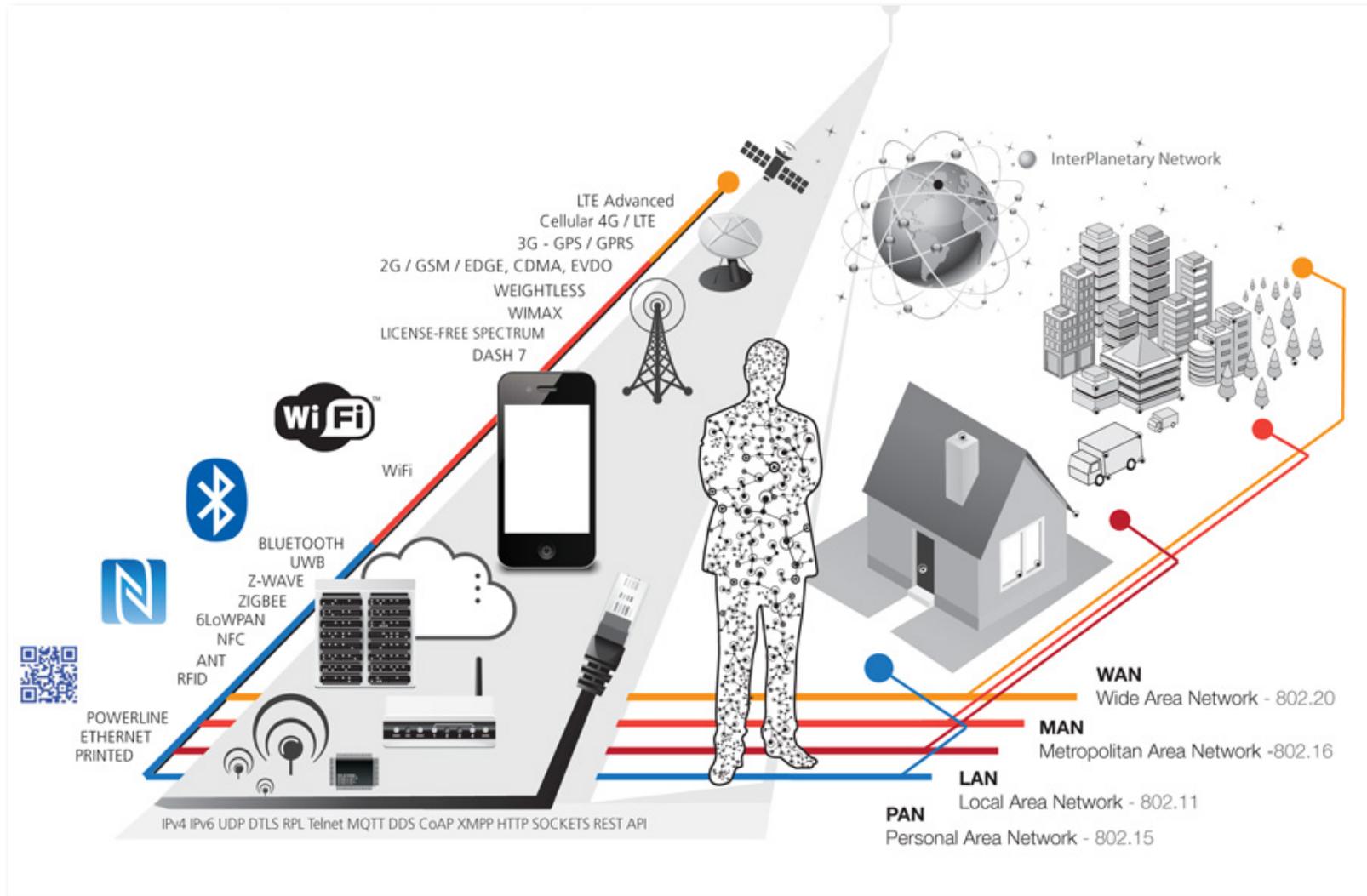   - múltiplas tecnologias

Internet das coisas - Sensores

Internet das coisas - Conectividade

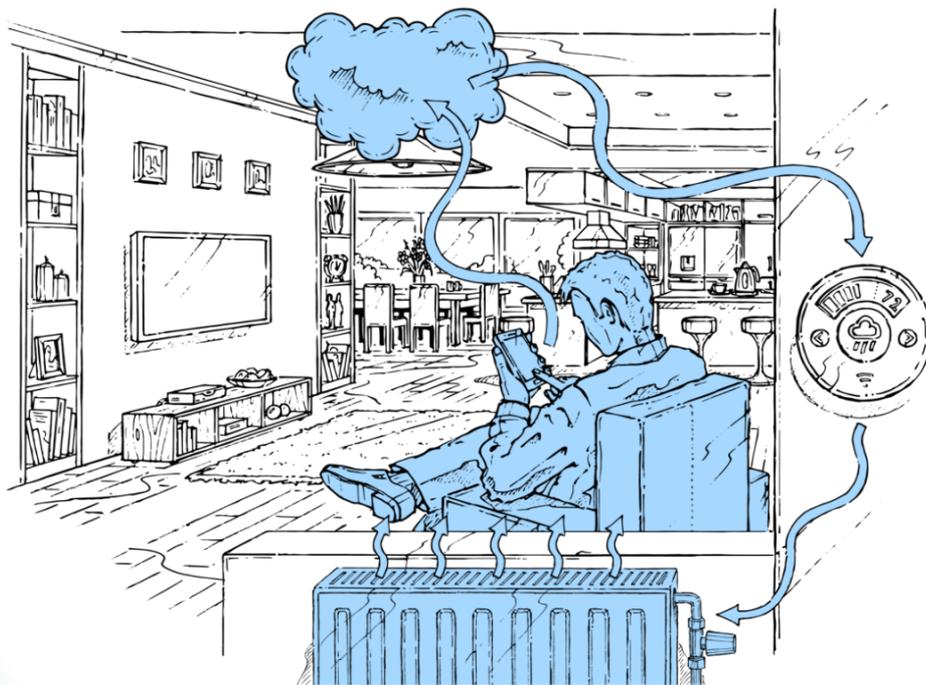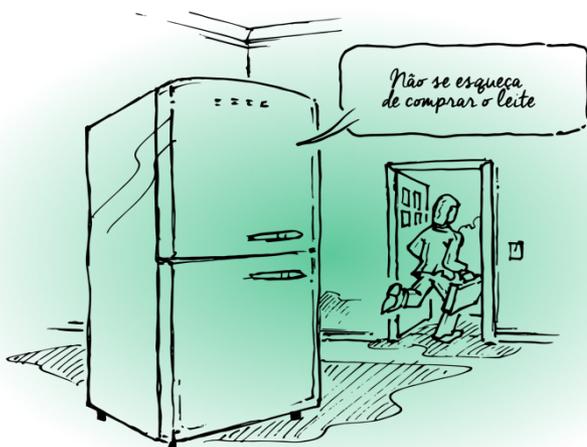http://www.visualcapitalist.com/what-is-internet-things/

Internet das coisas – Pessoas e Processos
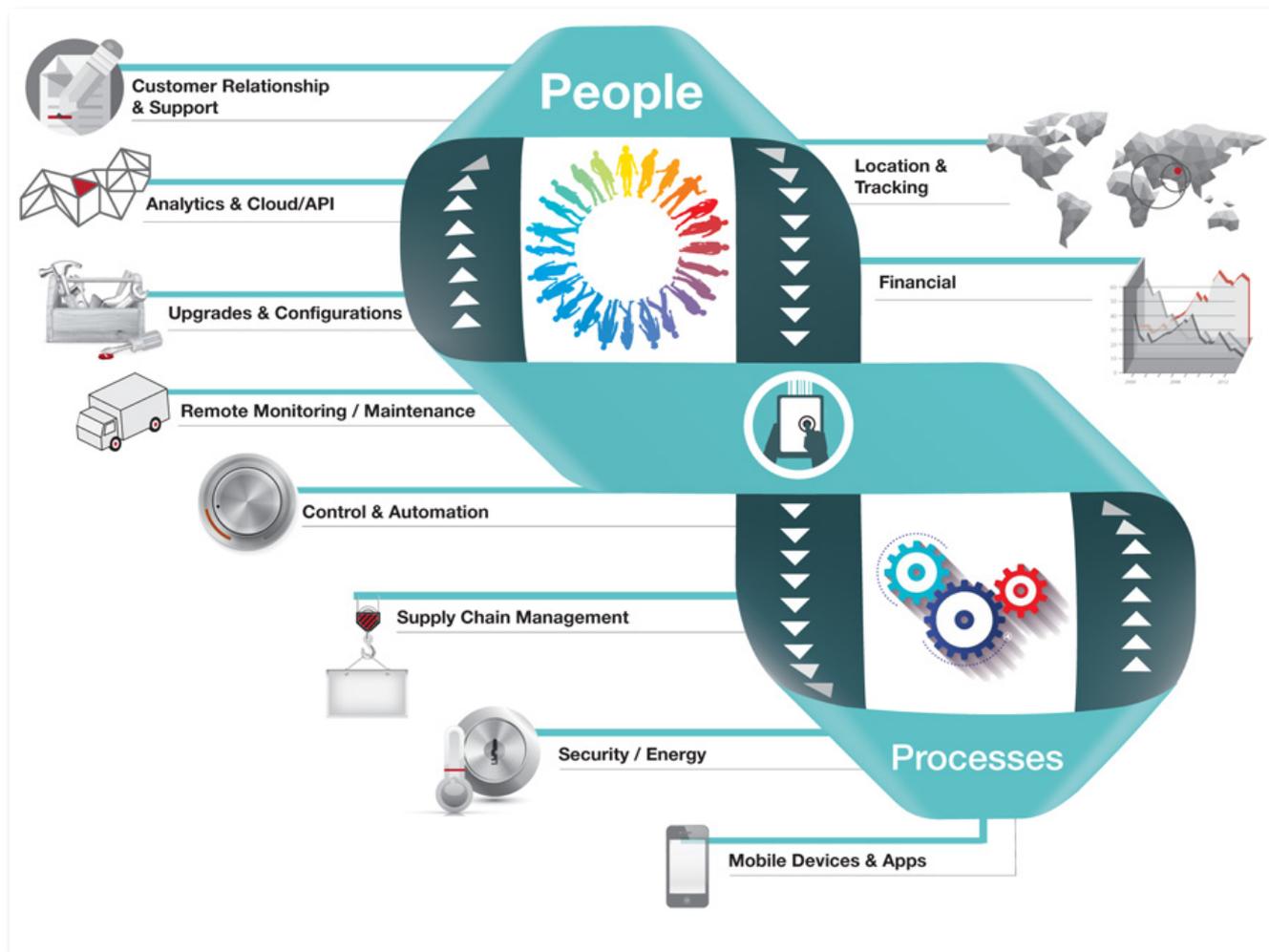
Internet das Coisas – Usos

- **Casas inteligentes**
- **Cidades inteligentes**
- **Carros conectados**
- **Equipamentos médicos**
- **Industria 4.0**
- ***Wearables***

Não se esqueça de comprar o leite

Libelium Smart World

Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.

Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.

Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.

Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.

Sportsmen Care
Vital signs monitoring in high performance centers and fields.

Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.

Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.

Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.

Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.

Electromagnetic Levels
Measurement of the energy radiated by cell stations and WiFi routers.

Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.

Smart Roads
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Smart Lighting
Intelligent and weather adaptive lighting in street lights.

Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.

Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.

Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.

Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.

Item Location
Search of individual items in big surfaces like warehouses or harbours.

Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.

Smart Parking
Monitoring of parking spaces availability in the city.

Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.

Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.
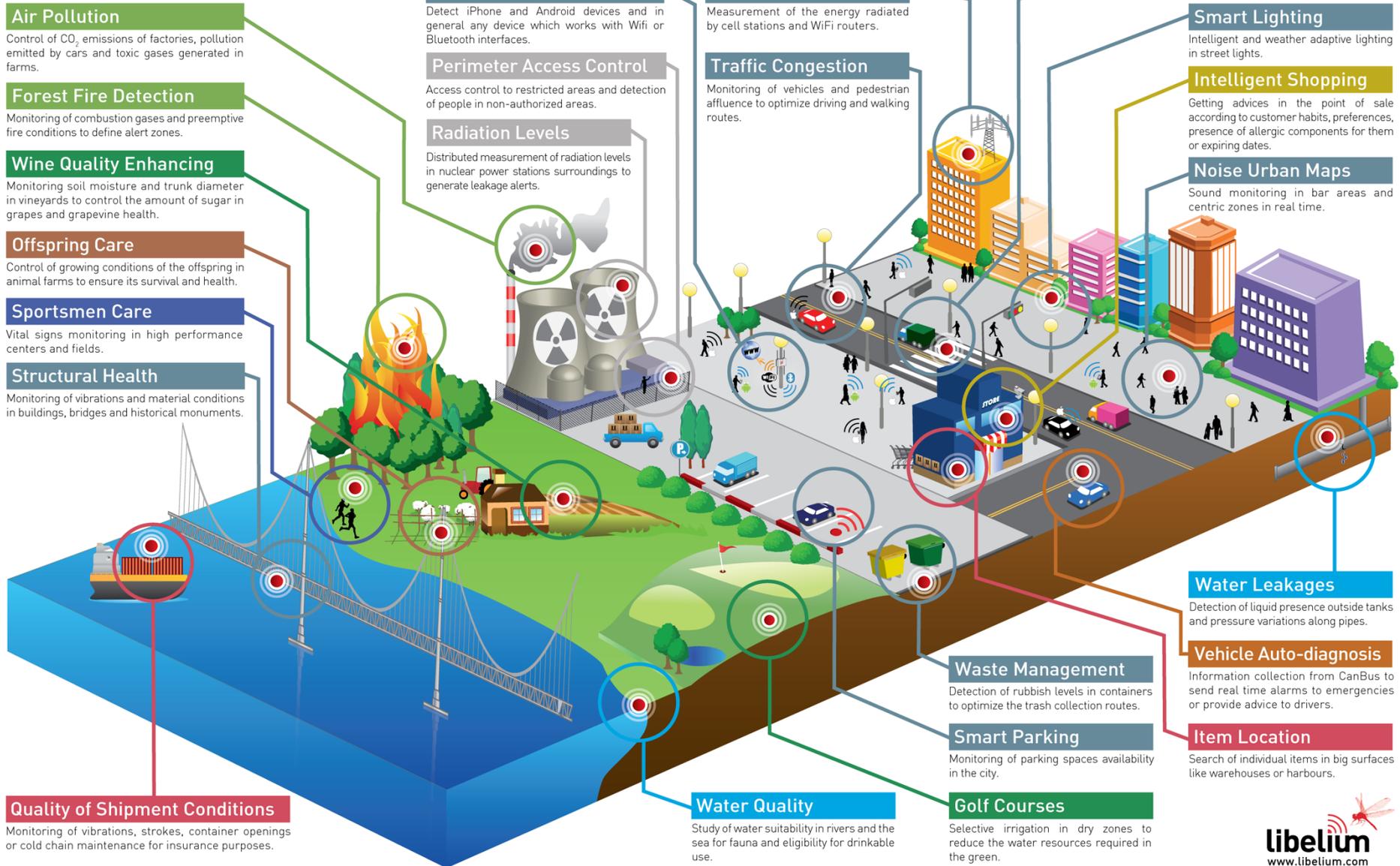
Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

libelium
www.libelium.com

cert.br   nic.br   cgi.br

My Signal

Published in: Case Studies, eHealth

MySi...
Domi...

May 10...

The Do...
materna...
which pr...

Libelium...
over the...
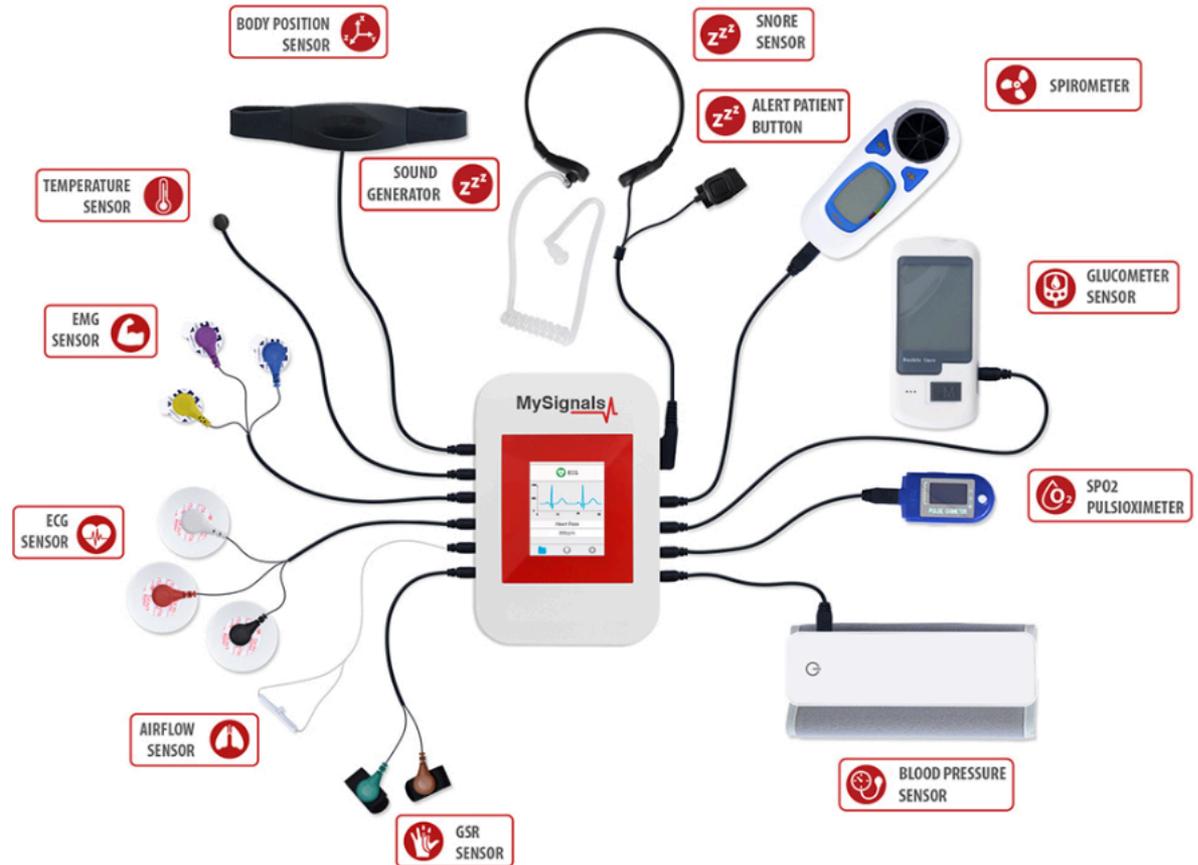
MySignals platform with 15 sensors

http://www.libelium.com/mysignals-helps-to-reduce-maternal-deaths-in-dominican-republic/

Irrigação inteligente

http://www.libelium.com/smart-irrigation-system-to-improve-kiwi-production-in-italy/
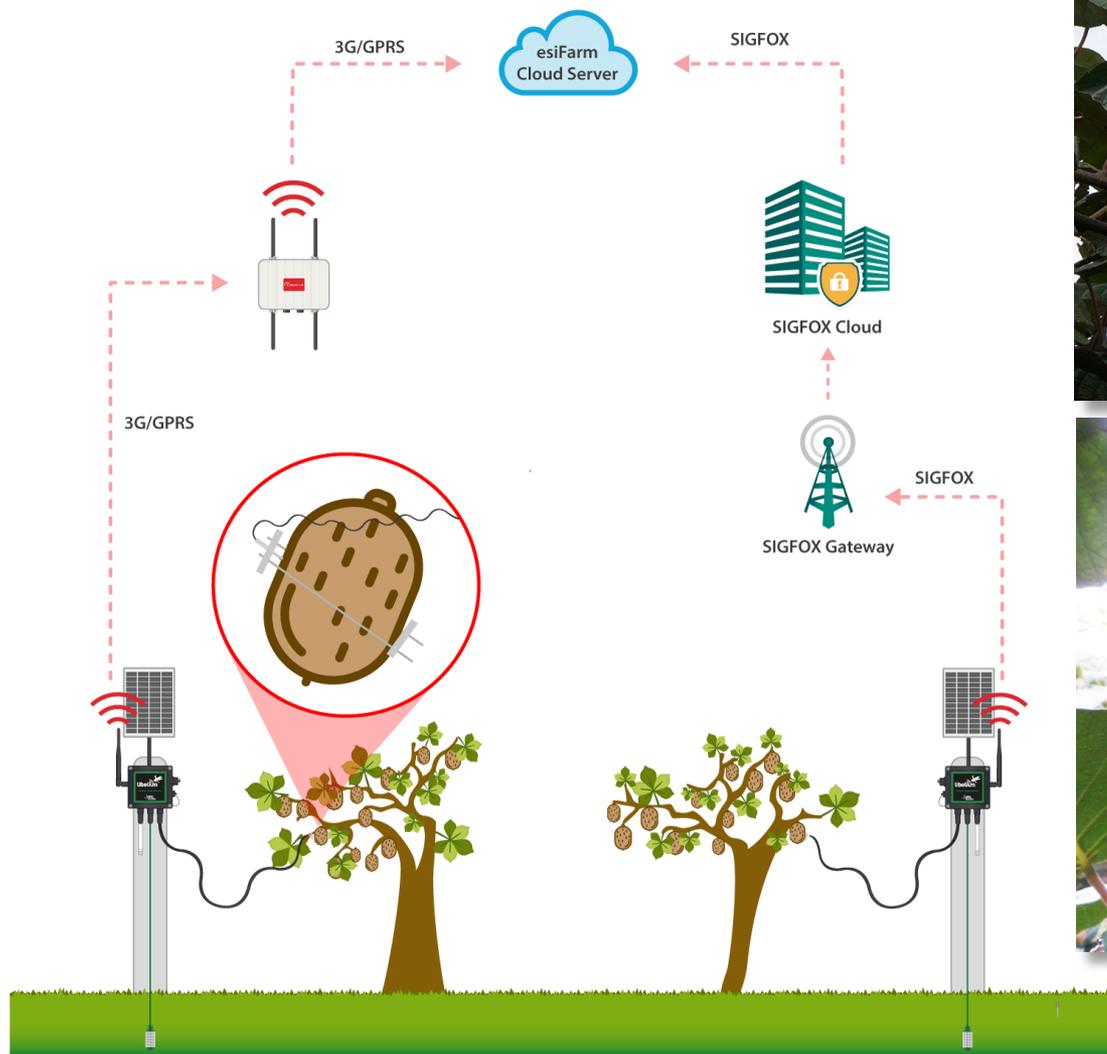
Novos riscos?

Atacantes

1. criminosos
2. espionagem industrial
3. governos
4. vândalos
5. pessoas que querem diversão

Vulnerabilidades

- **projeto sem levar em conta segurança**
- **sistemas desatualizados**
    - defasagem de tempo entre ser "fabricado" e chegar ao cliente
- **defeitos de *software/firmware***
- **falhas de configuração**
- **falta de proteção de dados**
- **uso inadequado**
- **contas:**
    - sem senhas
    - com senhas fracas ou *default*
    - de serviço (*backdoors*)
    - com acesso remoto

Riscos

- **violação de privacidade**
- **furto de dados**
- **perdas financeiras**
- **danos à imagem**
- **perda de confiança na tecnologia**
- **indisponibilidade de serviços críticos**
- **participação em golpes**
- **propagação de códigos maliciosos**
- **envio de *spam***
- **risco de morte**

Problema:
telnet e senhas fracas

IoT *botnets*

- **CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc**

- ***Malware* se propaga geralmente via telnet**

- **Explora senhas fracas ou padrão**
  - muitas vezes são "*backdoors*" dos fabricantes

- **Em nossos honeypots**
  - IPs de IoT infectados – 07/11/2016
    - Total: 581.917
    - BR: 76.187
  - Detecção:
    - número de sequência do pacote = endereço IP do destino

Notificações ao CERT.br:
Scans por porta em 2016

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2016

Scans reportados, por porta

Outras TCP/UDP/ICMP (10,61%)

5060/udp (0,70%)

161/udp (0,71%)

4028/tcp (0,91%)

multi/tcp (1,32%)

3389/tcp (2,34%)

53413/udp (2,68%)

21/tcp (2,78%)

22/tcp (20,33%)

25/tcp (30,10%)

23/tcp (27,52%)
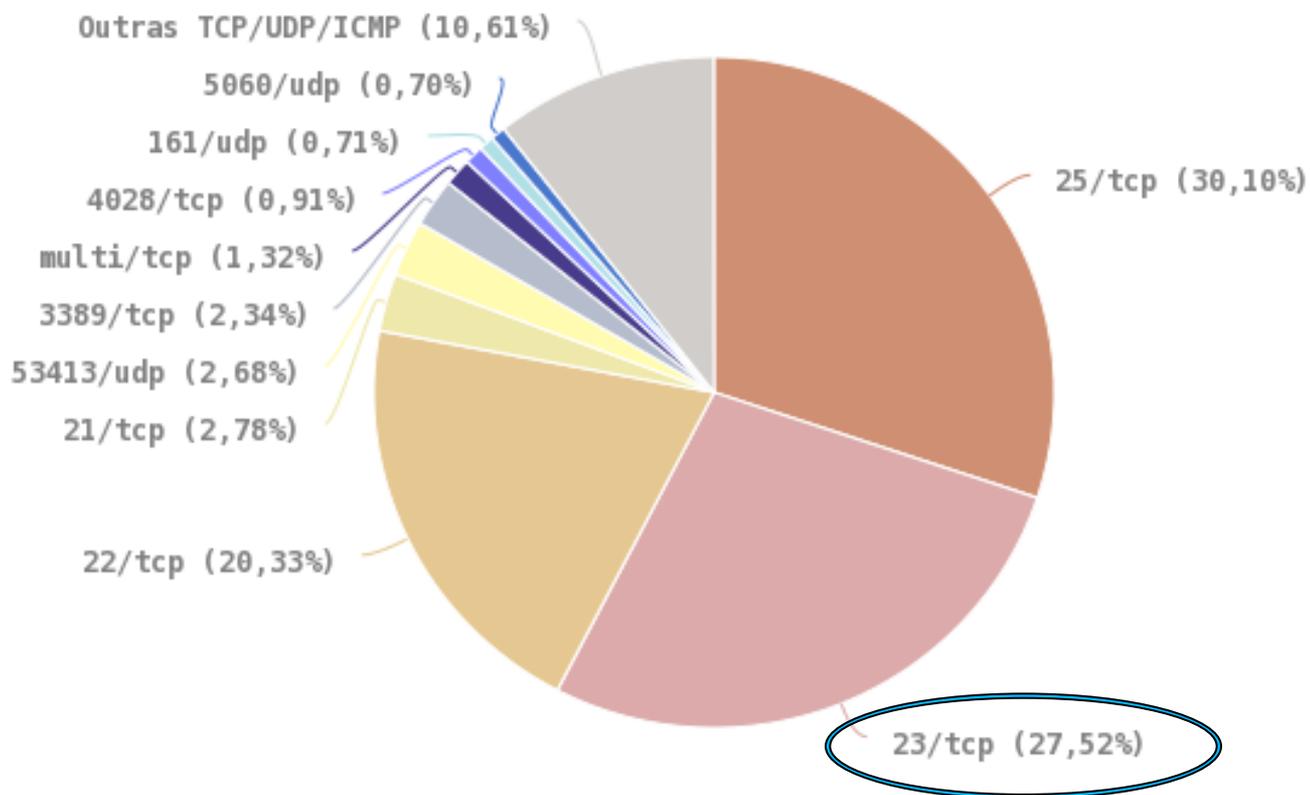
* Não inclui scans realizados por worms.

© CERT.br -- by Highcharts.com

Notificações ao CERT.br:
Scans por 23/TCP – 2013 a jun/2016

Varreduras por 23/TCP

Internet security experts have been warning for years that such devices are open to both data theft and remote control by a hacker. In 2007, Vice President Dick Cheney's cardiologist disabled the wireless functional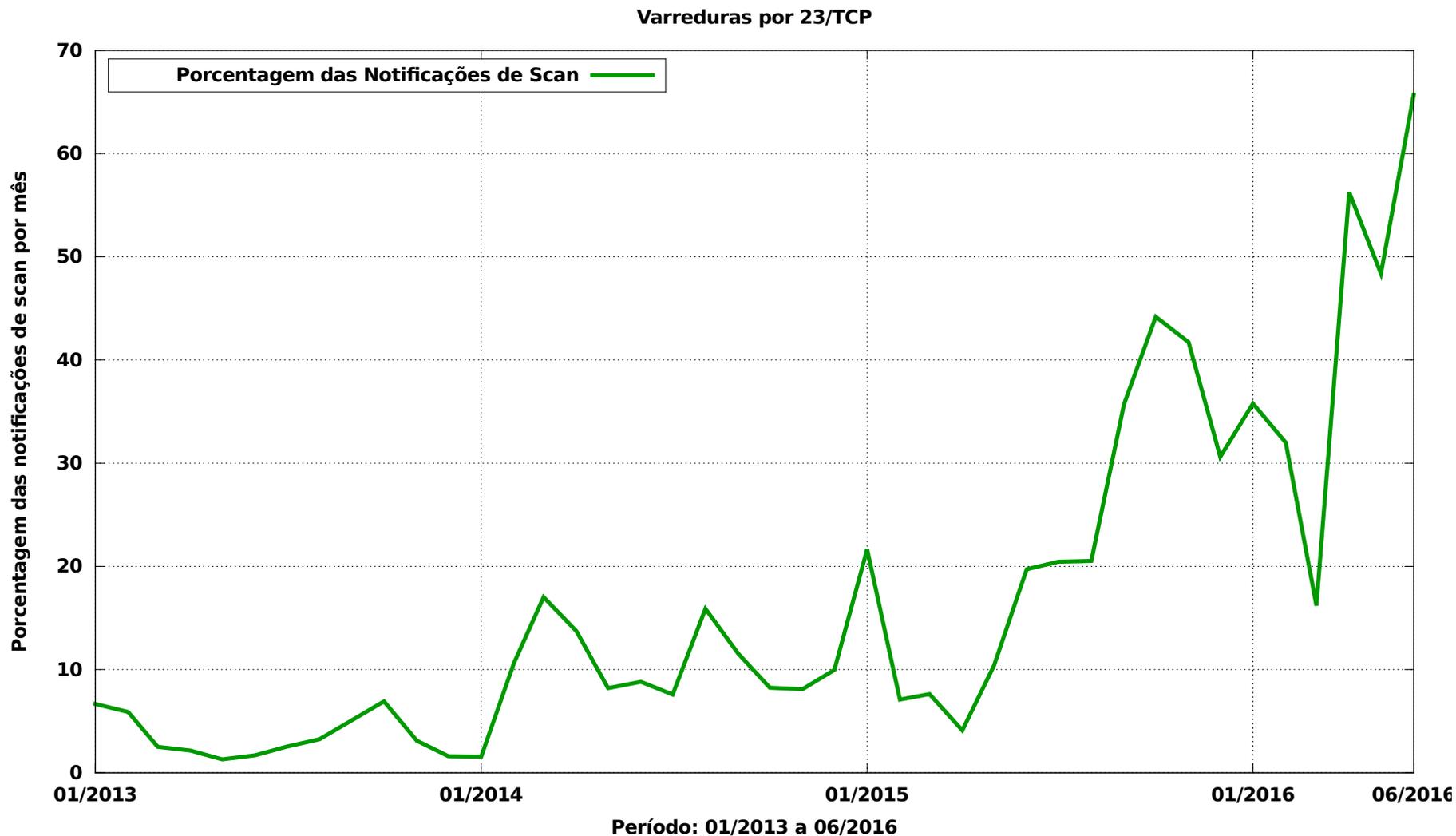ity of his pacemaker because of just that risk. "It seemed to me to be a bad idea for the vice president to have a device that maybe somebody on a rope line or in the next hotel room or downstairs might be able to get into—hack into," said the cardiologist, Jonathan Reiner of George Washington University Hospital in Washington, D.C., in a TV

Medical devices such as insulin pumps, continuous glucose monitors, and pacemakers or defibrillators have become increasingly small and wearable in recent years. They often connect with a hand-held controller over short distances using Bluetooth. Often, either the controller or

Medical devices don't get regular security updates, like smart phones and computers, because changes to their software could require recertification by regulators like the U.S. Food and Drug Administration (FDA). And FDA has focused on reliability, user safety, and ease of use—not on protecting against malicious attacks. In a Safety Communication in 2013, the agency said that it "is not aware of any patient injuries or deaths associated with these incidents nor do we have any indication that any specific devices or systems in clinical use have been purposely targeted at this time." FDA does say that it "expects medical device manufacturers to take appropriate steps" to protect devices. Manufacturers are starting to wake up to the issue and are employing security experts to tighten up their systems. But unless such steps become compulsory, it may take a fatal attack on a prominent person for the security gap to be closed.

http://www.sciencemag.org/news/2015/02/could-wireless-pacemaker-let-hackers-take-control-your-heart

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion and pain management pumps:

Contact Hospira

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Advisory (ICSA-15-161-01)

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base ~~score of 10.0 has been ass~~igned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

Thousands of medical devices are vulnerable to hacking, security researchers

The security flaws put patients' health

James Niccolai   Sep 29, 2015 5:50 PM
IDG News Service

Next time you go for an MRI scan, remember that the doctor might not be the only one who sees your results.

Thousands
infusion pur
security res

The same default passwords were used over and over for different models of a device, and in some cases a manufacturer warned customers that if they changed default passwords they might not be eligible for support. That's

cert.br nic.br cgi.br

Hackers Breach Casino After Compromising a Smart Fish Tank

Casino becomes vulnerable after connecting fish tank to the Internet, allowing hackers to break into the network

Jul 24, 2017 10:55 GMT · By Bogdan Popa 🐦 · Share: 🔴 🅵 f 🐦 g+

A casino in the United States was compromised after hackers managed to infiltrate into its network and steal undisclosed data after first breaking into a smart fish tank connected to the Internet

2. Check to make sure you have the Apex username and password correct (The username and password is not the same as Apex Fusion)

    1. Default username is '*admin*'

    2. Default password is '*1234*'

But it was this connection that exposed the fish tank, and eventually, the entire casino, to hackers, as an unnamed group of attackers managed to infiltrate into the network and

Now repeat step 7, and create another port forwarding rule to the telnet port, port 23 in your router. This port forwarding rule is for Neptune Systems should you ever have any problems or questions about your controller. You will have two port forwarding rules pointing towards your Apex's internal IP address when finished.

http://news.softpedia.com/news/hackers-breach-casino-after-compromising-a-smart-fish-tank-517134.shtml
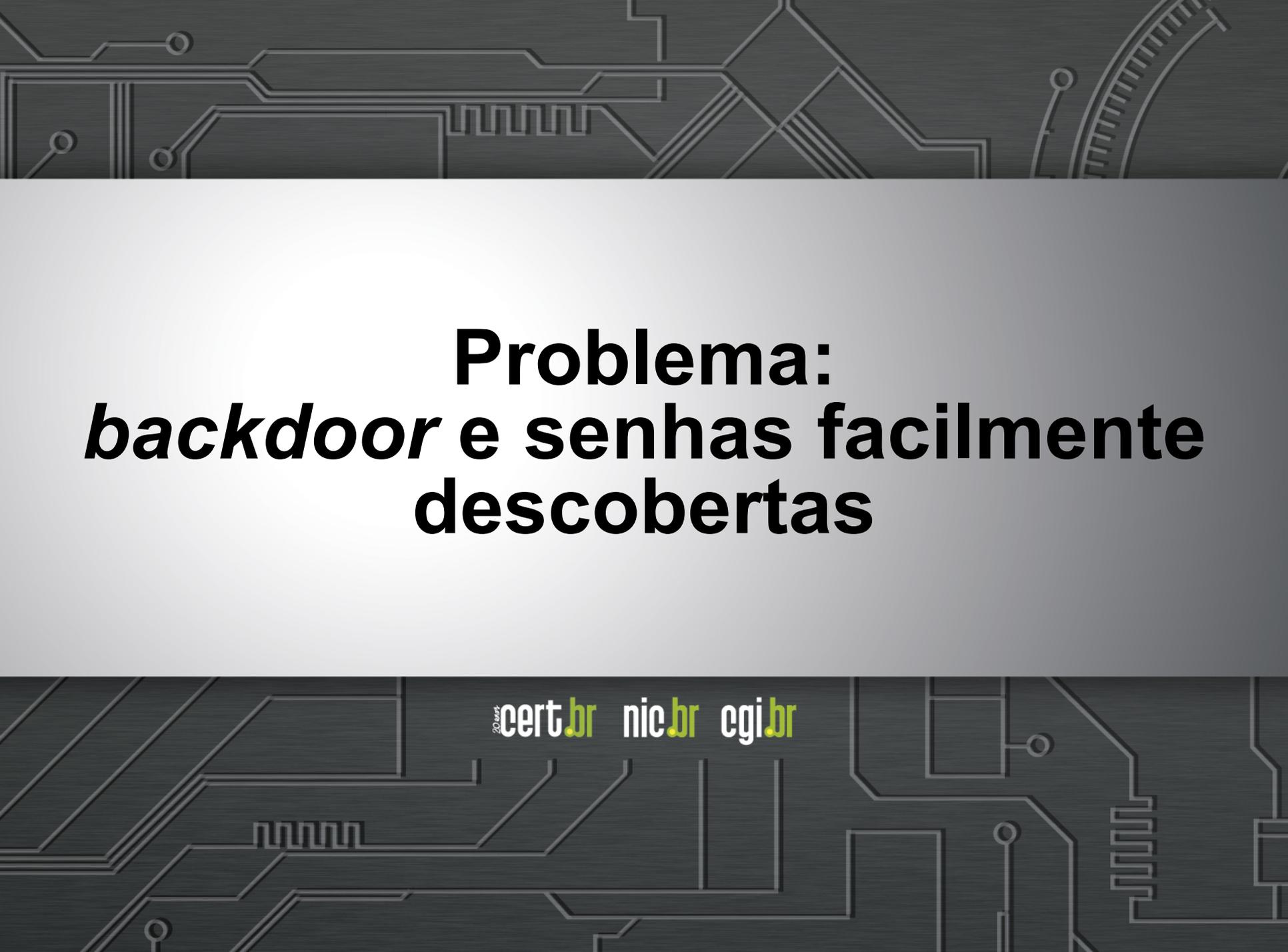
Problema:
backdoor e senhas facilmente descobertas

CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

CWE-798: Use of Hard-coded Credentials - CVE-2013-3612

All DVRs of the same series ship with the same default root password on a read-only partition. Therefore, the root password can only be changed by flashing the firmware. Additionally, a separate hard-coded remote backdoor account exists that can be used to control cameras and other system components remotely. It is only accessible if authorization is done through ActiveX or the stand-alone client. Additionally, a hash of the current date can be used as a master password to gain access to the system and reset the administrator's password.

Vulnerability Note VU#800094

Dahua Security DVRs contain multiple vulnerabilities

Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013

Print   Tweet   Send   Share

Overview

Digital video recorders (DVR) produced by Dahua Technology Co., Ltd. contain multiple vulnerabilities that could allow a remote attacker to gain privileged access to the devices.

Security researchers
forever altered the au
safety" in July when t
could remotely hack a
transmission and bral
issue an unprecedente
mailing out USB drive
infotainment systems
network that connect

Hackers can cut the brakes, shut down the engine, drive it off the road, or make all the electronics go haywire.

CNN **CNNMoney** ✔
@CNNMoney

🐦 Follow

Recall Alert: Fiat Chrysler is recalling 1.4 million hackable vehicles. Check affected cars: cnnmon.ie/1OrrqGv

9:59 PM - Jul 24, 2015

💬 ⟲ 48 ♡ 22

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Problema:
Falta de checagem na criptografia

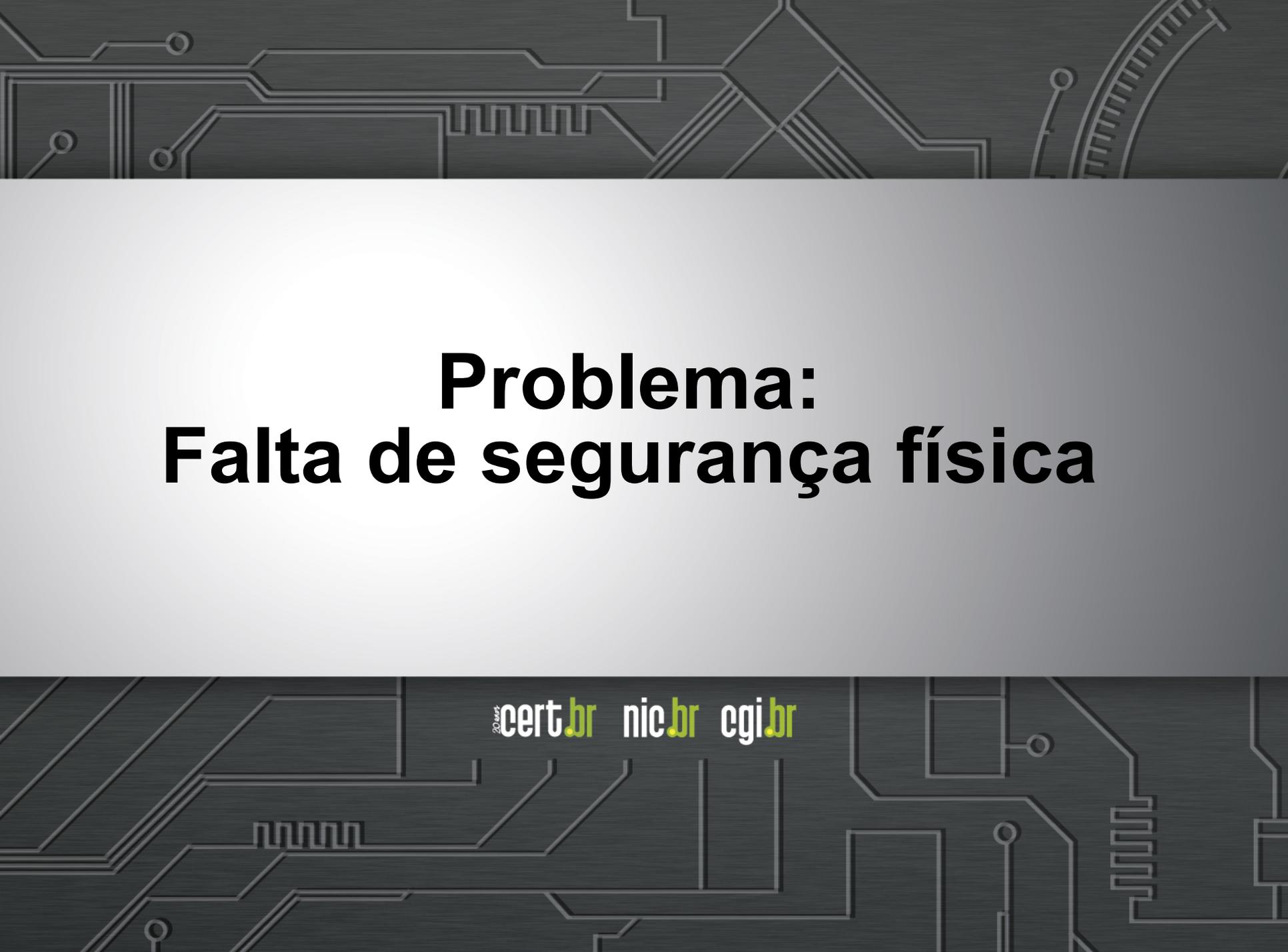# Hackers steal Gmail login details from Samsung smart fridge

By Anthony Cuthbertson

Updated

Hackers from Pen Test Partners extracted login details from the Samsung RF28HMELBSR smart fridge   (Samsung)

http://www.ibtimes.co.uk/samsung-rf28hmelbsr-hackers-steal-gmail-login-details-smart-fridge-1516940

Problema:
Falta de segurança física

BRINKS' SUPE
SAFES: NOT S(

BRINKS

BISHOP FOX

"Once you're able to plug into that USB port, you're able to access lots of things that you shouldn't normally be able to access," Petro told WIRED. "There is a full operating system...that you're able to...fully take over...and make [the safe] do whatever you want it to do."

The researchers created a malicious script that, once inserted into a safe on a USB stick, lets a thief automatically open the safe doors by emulating certain mouse and keyboard actions and bypassing standard application controls. "You plug in this little gizmo, wait about 60 seconds, and the door just pops open," says Petro.

https://www.wired.com/2015/07/brinks-super-secure-smart-safes-not-secure/

cert.br nic.br cgi.br

Hacked robots can be a deadly insider threat

eBook: Defending against crypto-ransomware

IOActive researchers have probed the security of a number of humanoid home and business robots as well industrial collaborative robots, and have found it seriously wanting.

> These robots usually have exposed connectivity ports that allow physically present users to fiddle with them (via special USB devices, Ethernet connections), but unfortunately there are also ways for remote attackers to interfere with the robots' safety features (collision detection and avoidance mechanisms), which can result in serious injuries.

https://www.helpnetsecurity.com/2017/08/22/hacked-robots-insider-threat/

Problema:
malware

Hackers Make the First-Ever Ransomware for Smart Thermostats

August 7, 2016 // 10:00 AM EST

One day, your thermostat will get hacked by some cybercriminal hundreds of miles away who will lock it with malware and demand a ransom to get it back to normal, leaving you literally in the cold until you pay up a few hundred dollars.

This has been a scenario that security experts have touted as one of the theoretical dangers of the rise of the Internet of Things, internet-connected devices that are often insecure. On Saturday, what sounds like a Mr. Robot plot line came one step closer to being reality, when two white hat hackers showed off the first-ever ransomware that works against a "smart" device, in this case a thermostat.
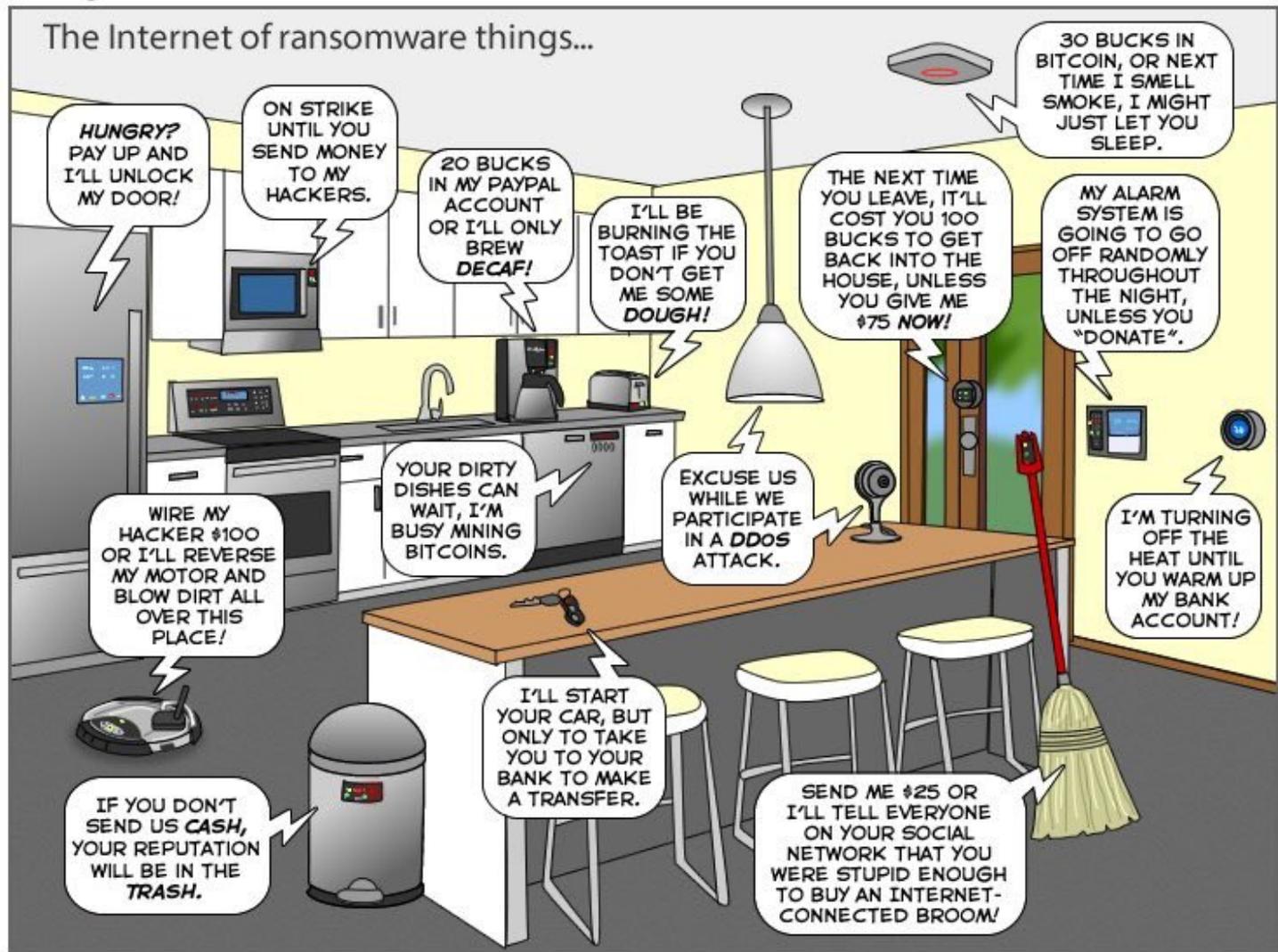
http://motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat

Why Light Bulbs May Be the Next Hacker Target

By JOHN MARKOFF   NOV. 3, 2016

Researchers report in a paper to be made public on Thursday that they have uncovered a flaw in a wireless technology that is often included in smart home devices like lights, switches, locks, thermostats and many of the components of the much-ballyhooed "smart home" of the future.

The researchers focused on the Philips Hue smart light bulb and found that the wireless flaw could allow hackers to take control of the light bulbs, according to researchers at the Weizmann Institute of Science near Tel Aviv and Dalhousie University in Halifax, Canada.

That may not sound like a big deal. But imagine thousands or even hundreds of thousands of internet-connected devices in close proximity. Malware created by hackers could be spread like a pathogen among the devices by compromising just one of them.

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten
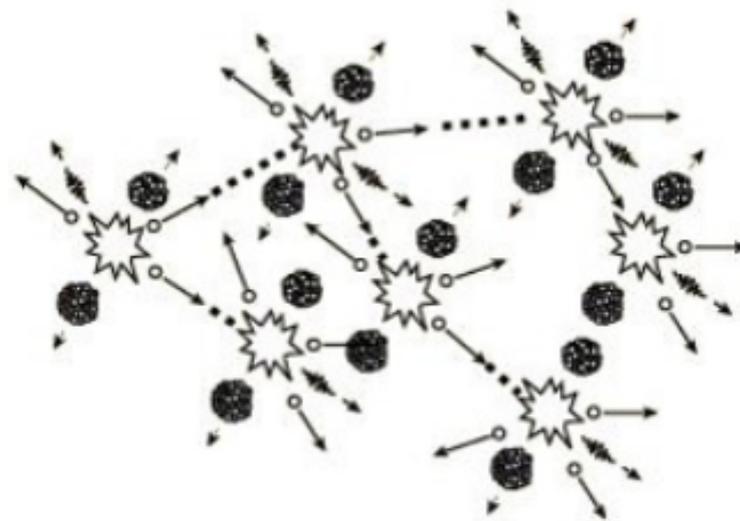
Creating an IoT worm

Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will spread explosively over large areas in a kind of nuclear chain reaction, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes, enabling the attacker to turn all the city lights on or off, permanently brick them, or exploit them in a massive DDOS attack. To demonstrate the risks involved, we use results from percolation theory to estimate the critical mass of installed devices for a typical city such as Paris whose area is about 105 square kilometers: The chain reaction will fizzle if there are fewer than about 15,000 randomly located smart

http://iotworm.eyalro.net

620Gbps contra o Blog do Brian Krebs

BBC NEWS

Massive web attack hits security blogger

22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

http://www.bbc.co.uk/news/amp/37439513

cert.br nic.br cgi.br

Record-breaking DDoS reportedly delivered by >145k hacked cameras

Once unthinkable, 1 terabit attacks may soon be the new normal.

RISK ASSESSMENT —

DAN GOODIN - 9/28/2016, 9:50 PM

Last week, security news site KrebsOnSecurity went dark for more than 24 hours following what was believed to be a record 620 gigabit-per-second denial of service attack brought on by an ensemble of routers, security cameras, or other so-called Internet of Things devices. Now, there's word of a similar attack on a French Web host that peaked at a staggering 1.1 terabits per second, more than 60 percent bigger.

The attacks were first reported on September 19 by Octave Klaba, the founder and CTO of OVH. The first one reached 1.1 Tbps while a follow-on was 901 Gbps. Then, last Friday, he reported more attacks that were in the same almost incomprehensible range. He said the distributed denial-of-service (DDoS) attacks were delivered through a collection of hacked Internet-connected cameras and digital video recorders. With each one having the ability to bombard targets with 1 Mbps to 30 Mbps, he estimated the botnet had a capacity of 1.5 Tbps.

http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Source code of Mirai botnet responsible for Krebs On Security DDoS released online

Now anyone can use the IoT-based botnet for their own destructive purposes.

By Charlie Osborne for Zero Day | October 3, 2016 -- 08:43 GMT (01:43 PDT) | Topic: Security

The source code for the botnet which disrupted Krebs On Security has been published online, leading to fears that the botnet will soon be used by practically anyone to flood the internet with powerful -- and expensive -- attacks.

This month, security expert Brian Krebs' blog, Krebs On Security, was struck with one of the largest distributed denial-of-service (DDoS) attacks on record.

At 620 Gbps, Akamai engineers were able to repel the attack, but the company -- which gave Krebs a home pro-bono -- was forced to let him go as a 'business decision' since keeping the blog and weathering more DDoS attacks could have ended up costing the business a fortune.

Europol

The botnet responsible is based on malware called Mirai. The malicious code utilizes vulnerable and compromised Internet of Things (IoT) devices to send a flood of traffic against a target.

In this case, the DDoS attack included SYN Floods, GET Floods, ACK Floods, POST Floods, and GRE Protocol Floods.

http://www.zdnet.com/article/source-code-of-mirai-botnet-responsible-for-krebs-on-security-ddos-released-online/

Hackers create more IoT botnets with Mirai source code

The total number of IoT devices infected with the Mirai malware has reached 493,000

By Michael Kan   FOLLOW

IDG News Service | Oct 18, 2016 2:04 PM PT

RELATED TOPICS

Security

Internet of Things

Malware & Vulnerabilities

3 COMMENTS

Malware that can build botnets out of IoT products has gone on to infect twice as many devices after its source code was publicly released.

The total number of IoT devices infected with the Mirai malware has reached 493,000, up from 213,000 bots before the source code was disclosed around Oct. 1, according to internet backbone provider Level 3 Communications.

http://www.computerworld.com/article/3132359/security/hackers-create-more-iot-botnets-with-mirai-source-code.html

cert.br nic.br cgi.br

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

Brad Chacos | @BradChacos   Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html

International Business Times.

Technology   CyberSecurity

Massive 'test' cyberattacks using Mirai botnet temporarily knock out Liberia's internet

A Mirai botnet was used to flood the target with fake traffic and cripple its servers.

By Hyacinth Mascarenhas

November 4, 2016 05:54 GMT

In October, a massive botnet powered by the Mirai malware targeted DNS provider Dyn to take down a portion of the internet in the US and parts of Europe (Credit: Reuters)

The same deadly malware behind the historic internet outage in the US in October seems to have been used to target the African nation of Liberia over the past week through a series of short attacks, temporarily taking the country offline . IT security researcher Kevin Beaumont wrote on Thursday (3 November) that these were distributed denial of service (DDoS) attacks. They harnessed a network of compromised computers to create a Mirai botnet, which was designed to flood its target with fake traffic and cripple its servers.

Desafios

Como melhorar o cenário

- **Solução depende de diversas camadas**
    - usuários
    - desenvolvedores
    - administradores
    - fabricantes

Usuários

- **Antes de comprar**
  - ser criterioso ao escolher o fabricante
    - verificar se possui política de atualização de *firmware*
    - verificar histórico de tratamento de vulnerabilidades

- **Assumir que os dispositivos virão com sérios problemas**
  - mantê-los atualizados
  - desabilitar o acesso remoto se não for necessário
  - alterar as senhas padrão
  - desabilitar serviços desnecessários (*hardening*)

Desenvolvedores

- **Não usar protocolos obsoletos**

- **Usar criptografia e autenticação forte**

- **Não ter senha do dia, senha padrão não documentada, *reset* de configuração via rede, etc**

- ***Defaults* seguros**

- **Atualização**
  - precisa ser possível
  - necessário prever algum mecanismo de autenticação

- **Usar práticas de desenvolvimento seguro**

Desenvolvedores

- **Segundo a *OWASP*, todos os elementos devem ser considerados**
  - O dispositivo *IoT*
  - O serviço de nuvem
  - A aplicação para celulares/*tablets*
  - A ligação com a rede
  - O software
  - Utilização de criptografia
  - Utilização de autenticação
  - Segurança física
  - Portas USB

Desenvolvedores
OWASP Top 10

	Applications - 2013	iot- 2014
1	Injection	Insecure Web Interface
2	Broken Authentication and Session Management	Insufficient Authentication/Authorization
3	Cross-Site Scripting (XSS)	Insecure Network Services
4	Insecure Direct Object References	Lack of Transport Encryption/Integrity Verification
5	Security Misconfiguration	Privacy Concerns
6	Sensitive Data Exposure	Insecure Cloud Interface
7	Missing Function Level Access Control	Insecure Mobile Interface
8	Cross-Site Request Forgery (CSRF)	Insufficient Security Configurability
9	Using Components with Known Vulnerabilities	Insecure Software/Firmware
10	Unvalidated Redirects and Forwards	Poor Physical Security

cert.br nic.br cgi.br

Administradores

- **Implementar boas práticas:**
  - BCP38/BCP84
  - filtrar pacotes com endereços "*spoofados*"
  - http://bcp.nic.br/entenda-o-antispoofing/

- **Manter os equipamentos atualizados**
  - sistema operacional e todos os serviços nele executados
  - serviço Web, SGBD, extensões, módulos e *plugins*

- **Desabilitar serviços desnecessários**

- **Ser cuidadoso ao usar e elaborar senhas**
  - se disponível, usar verificação em duas etapas

Fabricantes

- **Segurança deve ser nativa**
  - não deve ser opcional
  - requisitos de segurança devem ser considerados desde o projeto
- **Deve ser incluída na análise de risco das empresas**
  - danos à imagem
  - danos aos usuários
- **Como implementar segurança em larga escala**
- **Um equipamento -> diversos fabricantes**
  - recall????
  - Xiongmai Botnet
- **Ter grupo de resposta a incidentes preparado para lidar com os problemas**

Obrigado

www.cert.br

@ marcus@cert.br   @certbr

04 de setembro de 2017

nic.br cgi.br

www.nic.br | www.cgi.br