nic.br cgi.br

20 anos cert.br

INFOESTE 2018

Presidente Prudente, SP

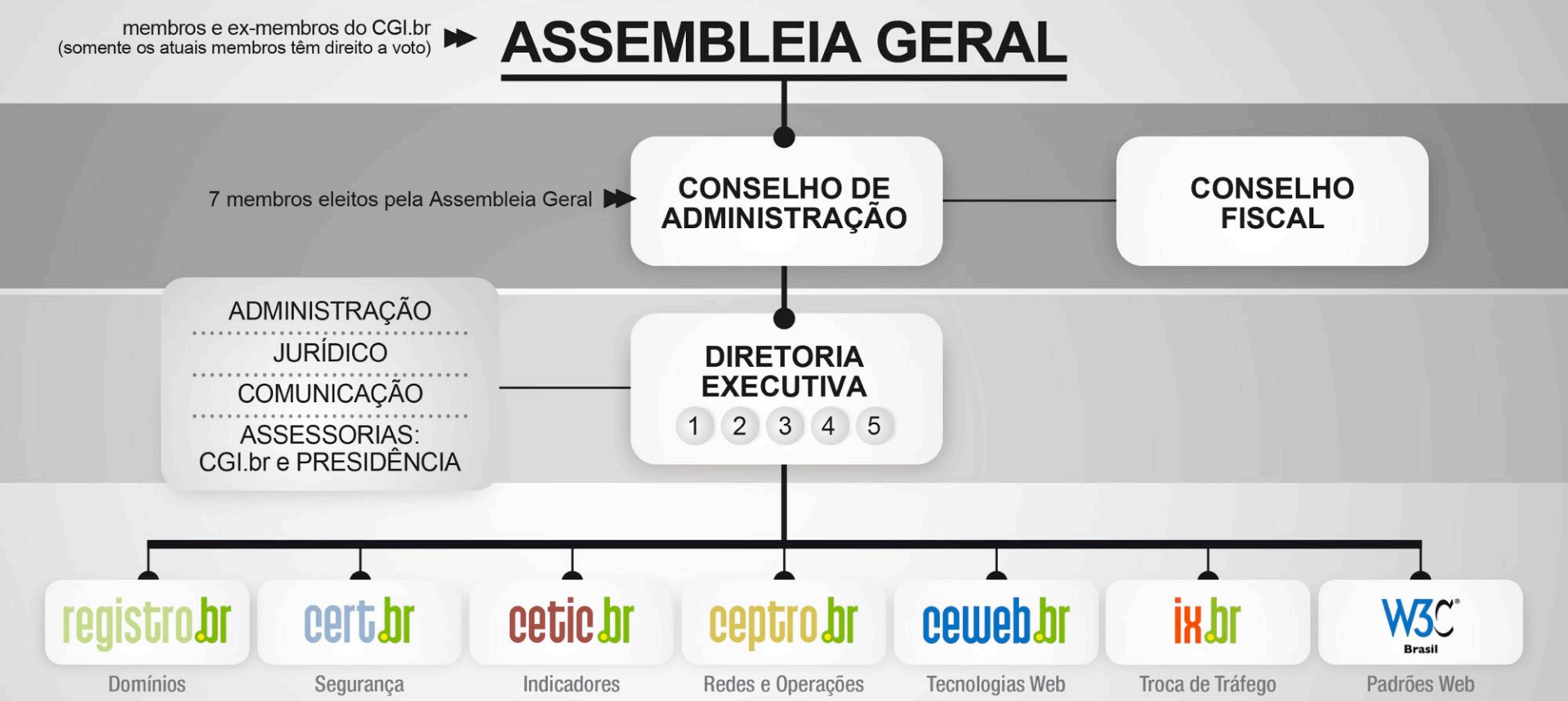
17 de maio de 2018

[In]Segurança na Internet das Coisas

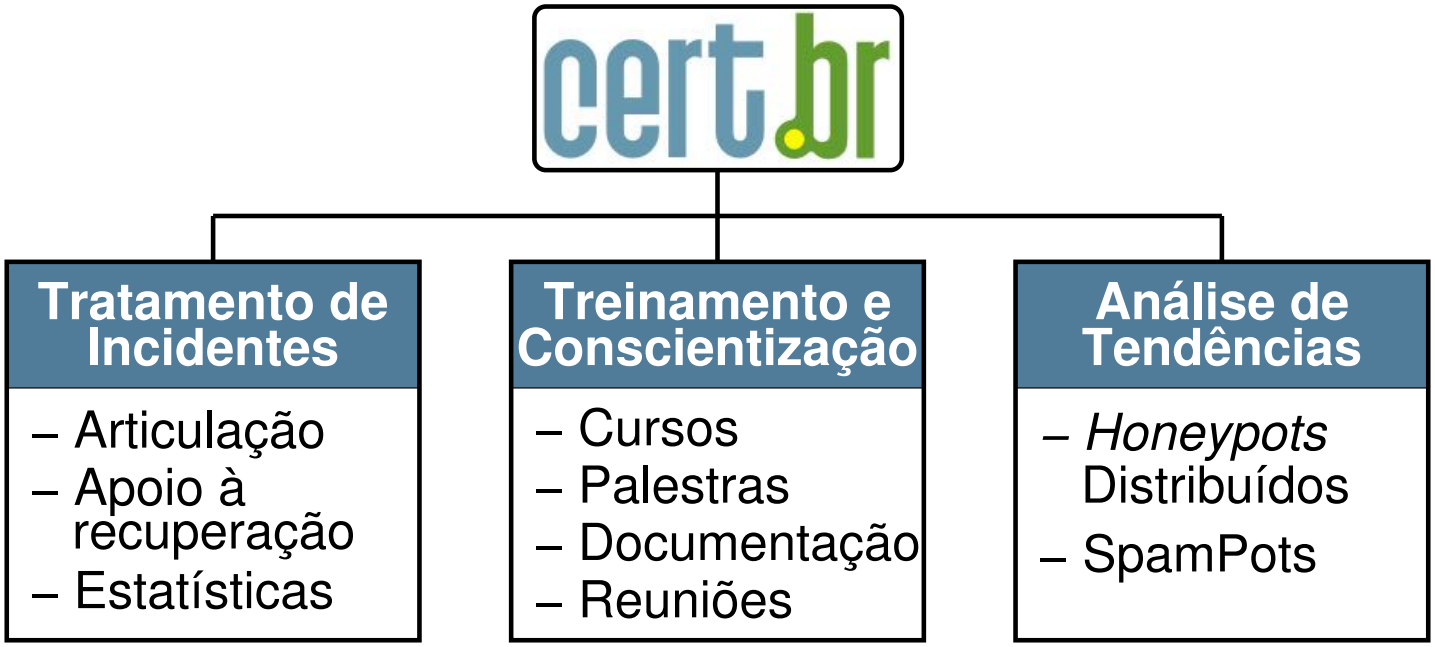
Marcus Vinícius Lahr Giraldi
marcus@cert.br

cert.br nic.br cgi.br

Estrutura do NIC.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet
PROJECT

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**

IoT

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."

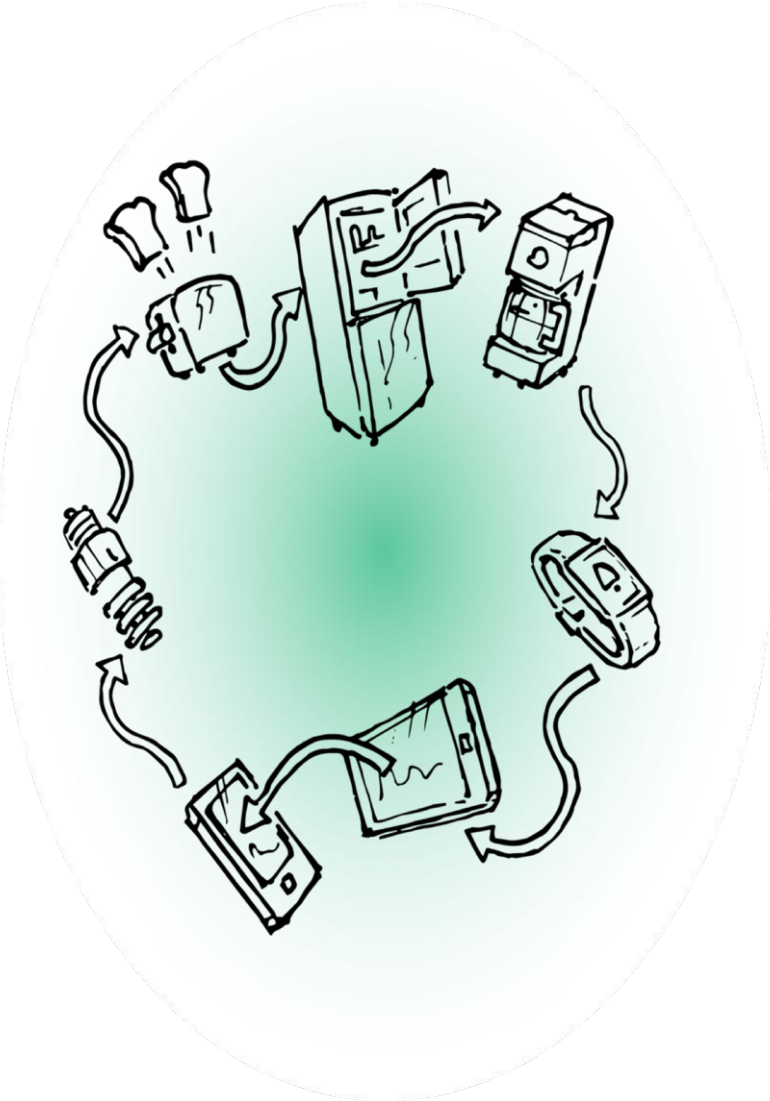
That 'Internet of Things' Thing
In the real world, things matter more than ideas

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

Definição IoT

“... é uma rede de objetos físicos, veículos, prédios e outros que possuem tecnologia embarcada, sensores e conexão com rede capaz de coletar e transmitir dados.”

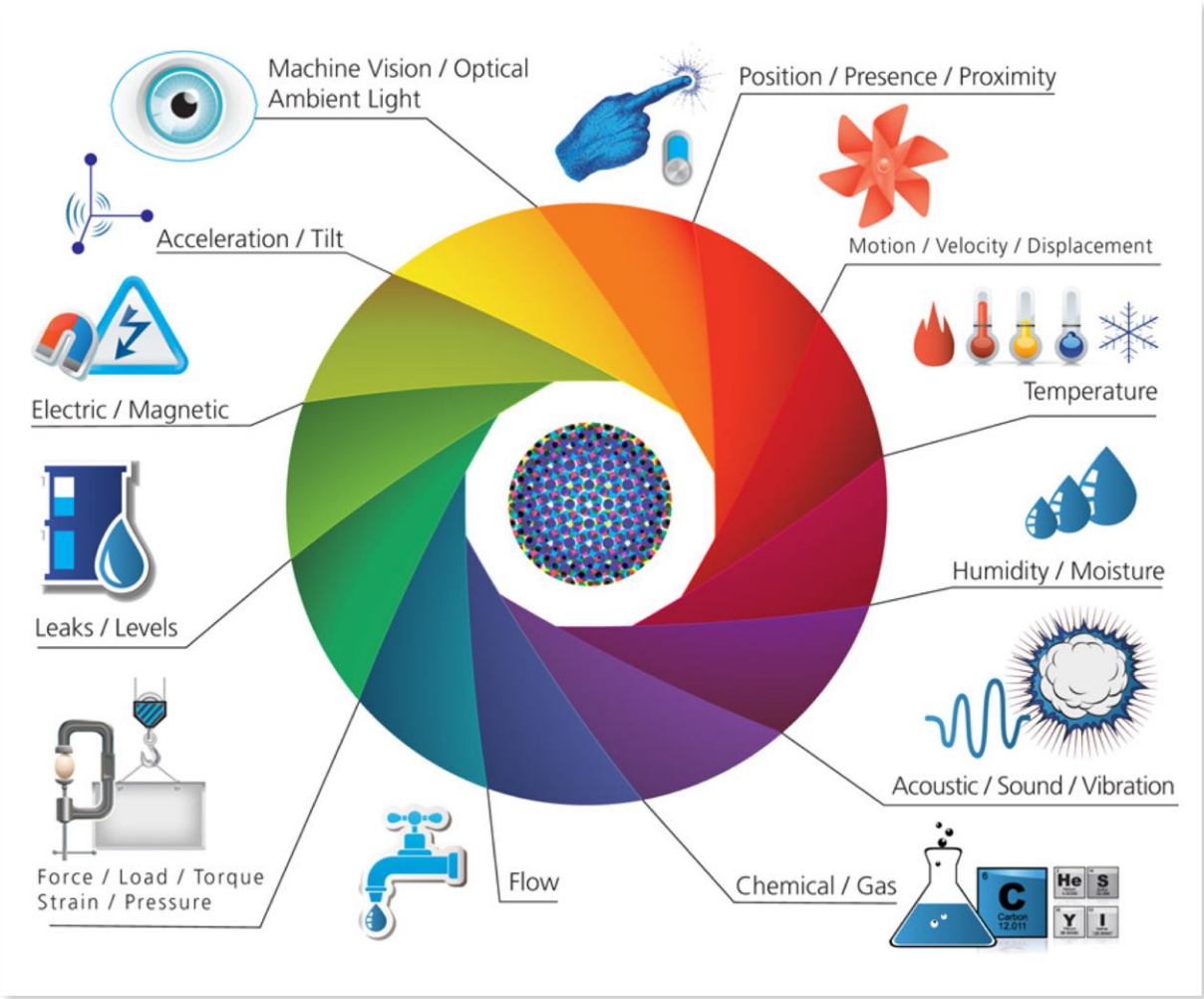
Wikipedia



Internet das Coisas – Atualidade

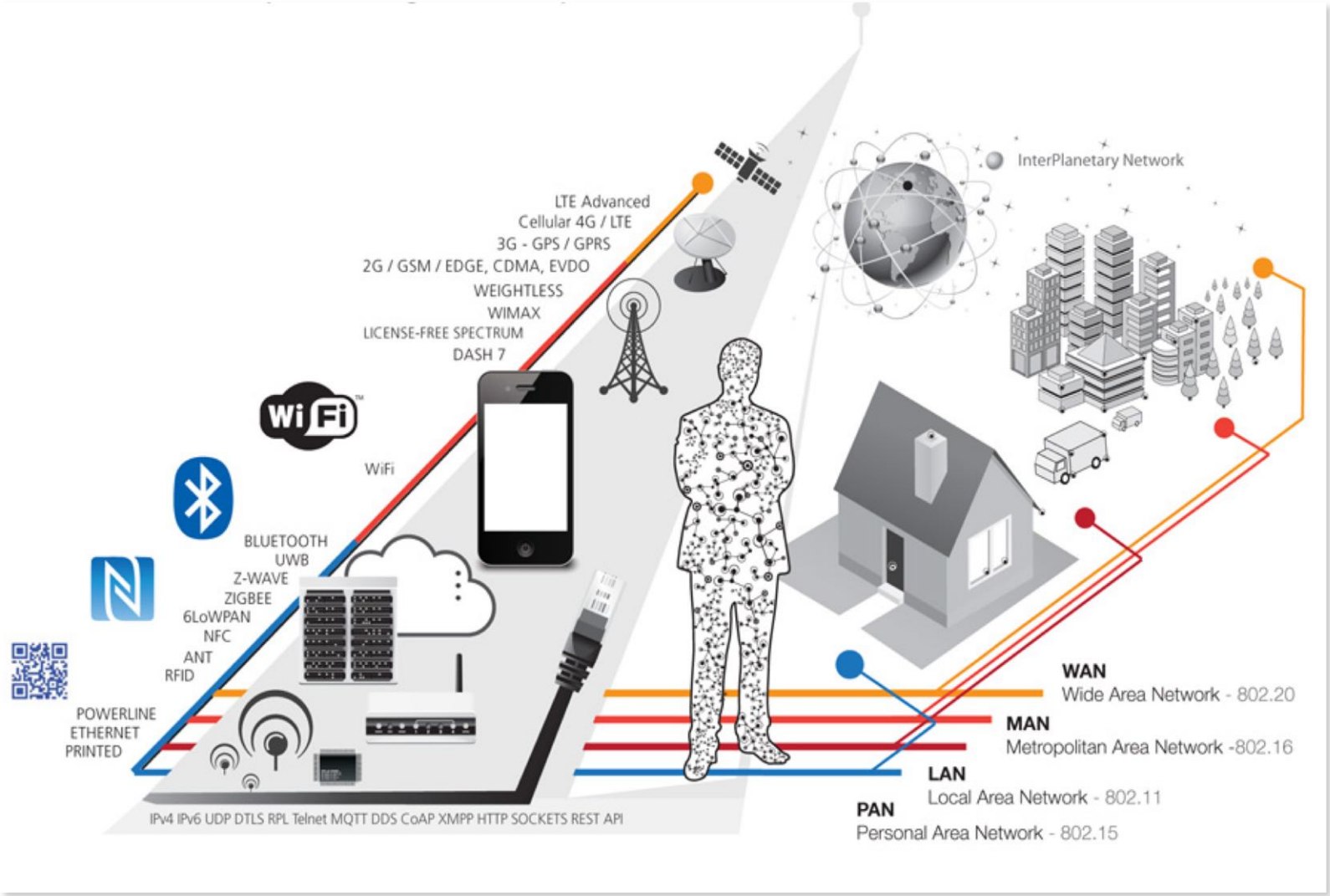
- **As coisas já estão conectadas**
  - sistemas complexos e completos
    - sistema operacional, aplicações Web, permitem acesso remoto, etc
    - múltiplas tecnologias

Internet das coisas - Sensores



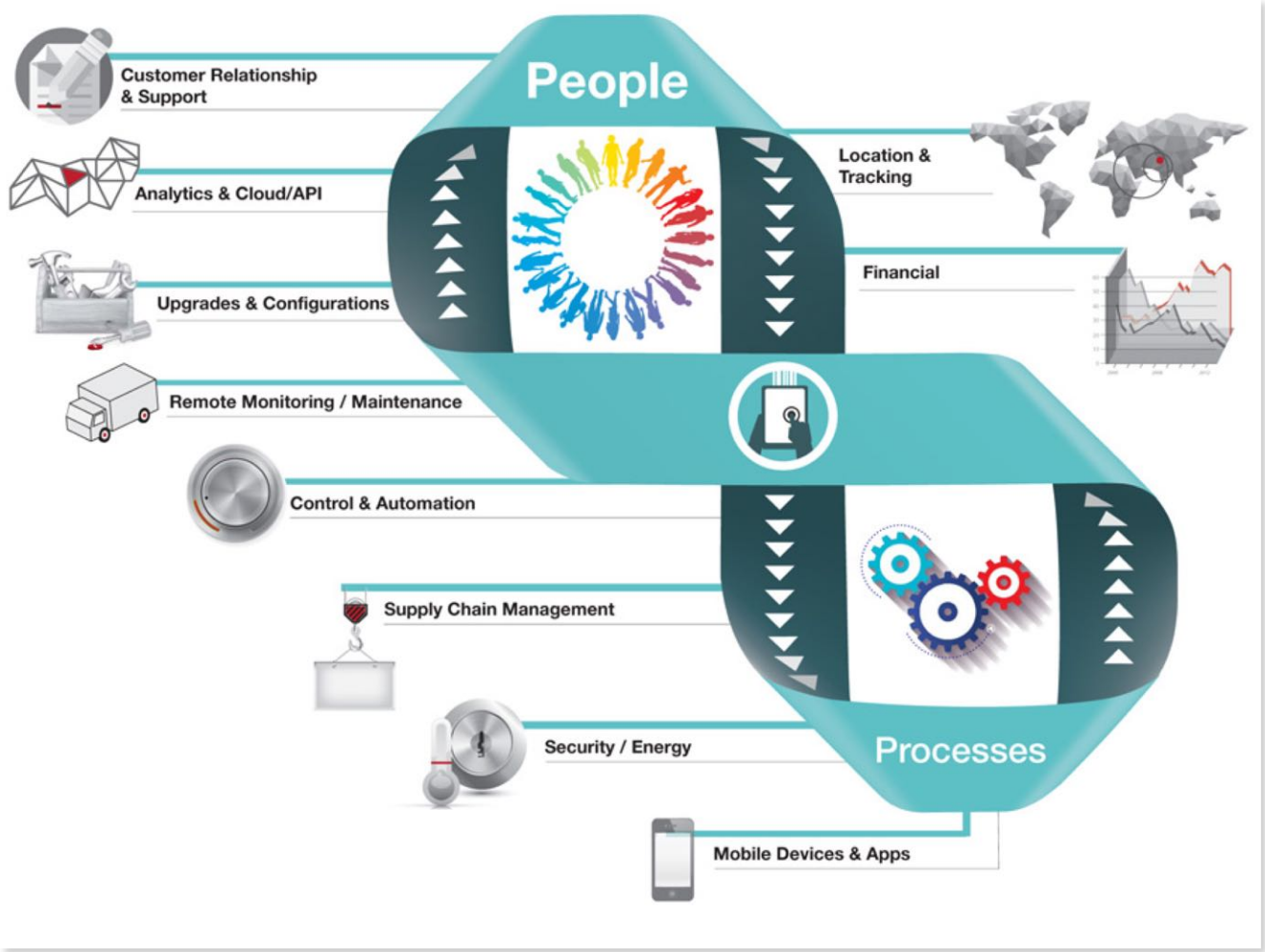
http://www.visualcapitalist.com/what-is-internet-things/

Internet das coisas - Conectividade



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

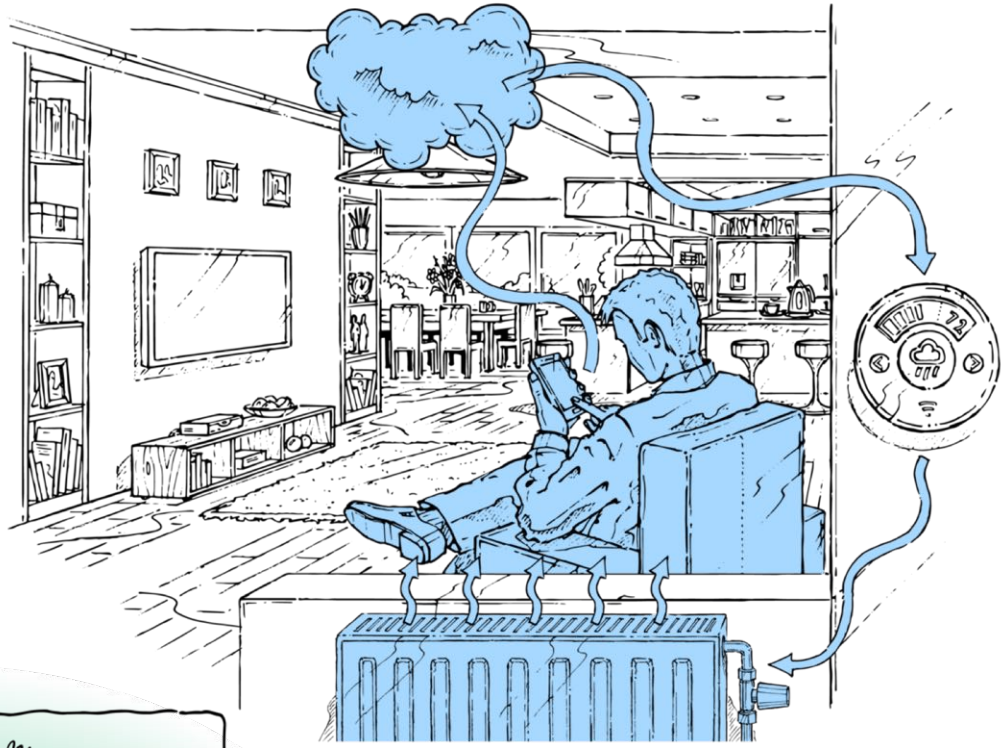
Internet das coisas – Pessoas e Processos



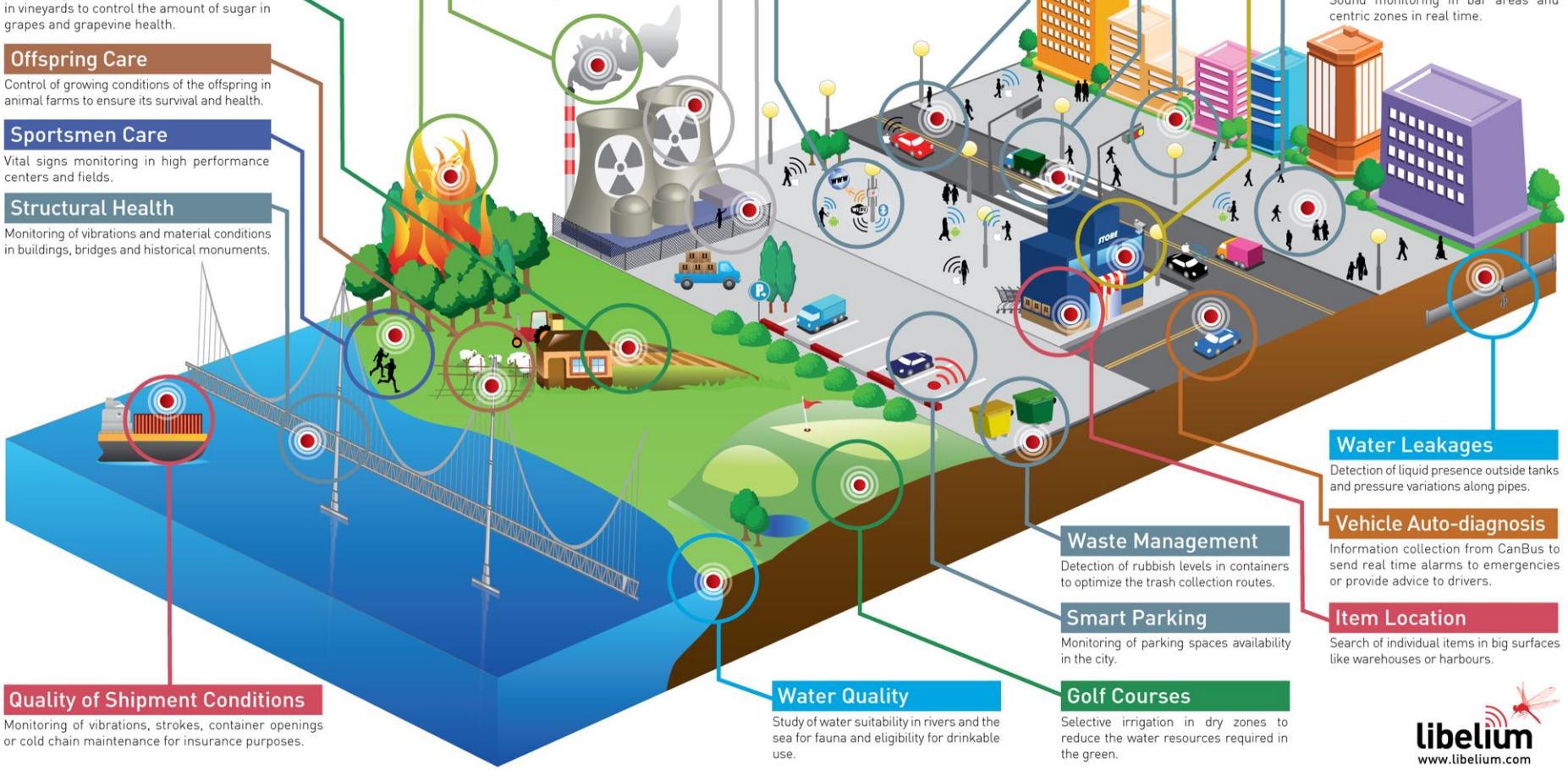
http://www.visualcapitalist.com/what-is-internet-things/

Usos

- **Casas inteligentes**
- **Cidades inteligentes**
- **Carros conectados**
- **Equipamentos médicos**
- **Agropecuária**
- **Indústria 4.0**
- ***Wearables***



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.

Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.

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.

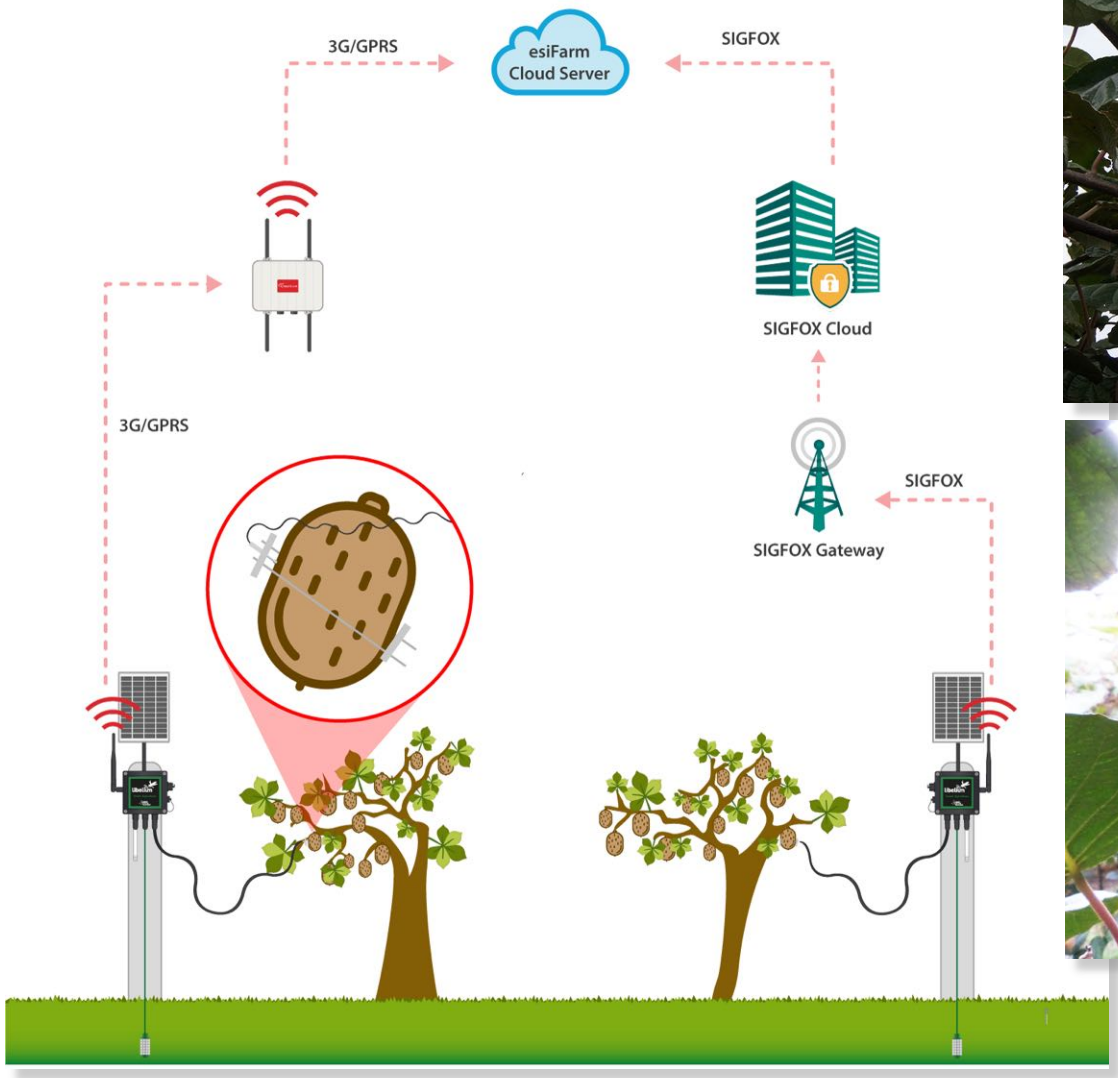
Smart Parking
Monitoring of parking spaces availability in the city.

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.

libelium
www.libelium.com

Irrigação inteligente



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

My Signal

› Libelium World:

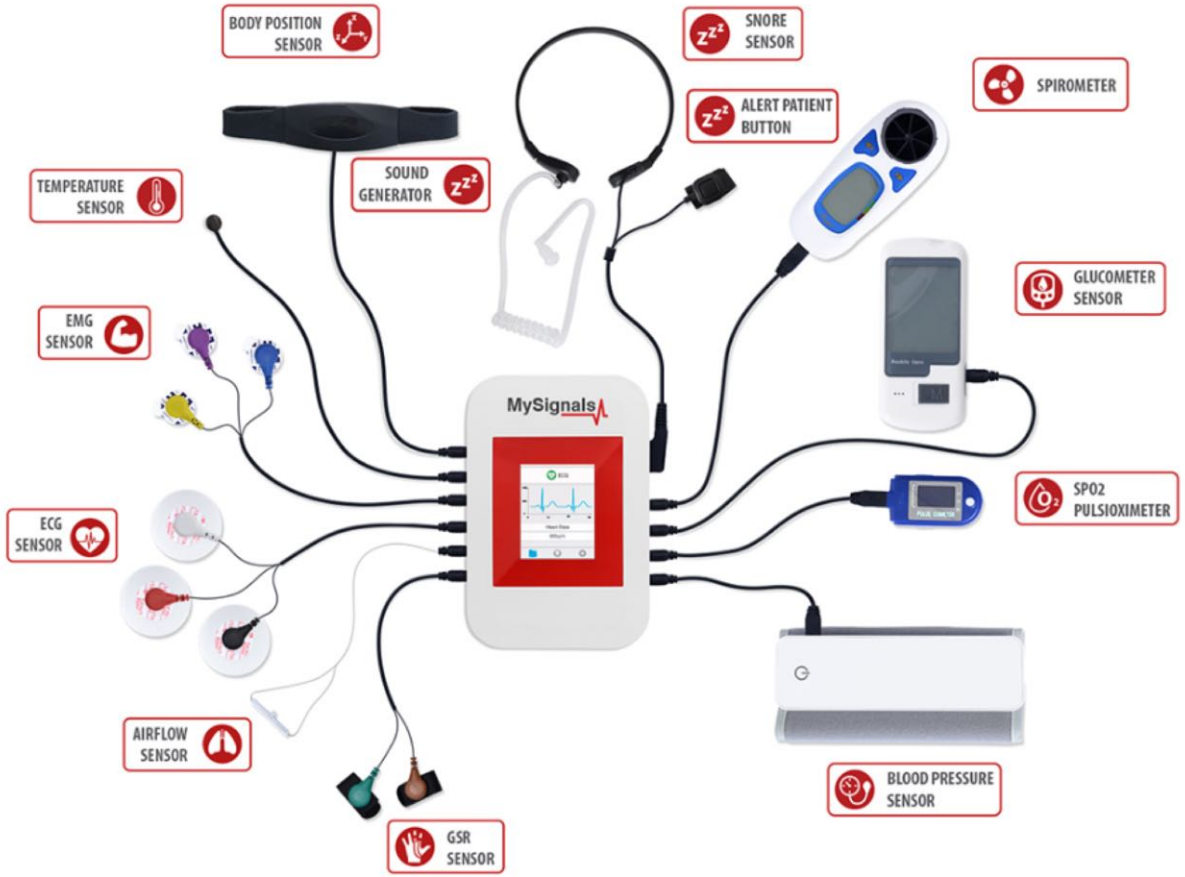
Published in: Case Studies, eHealth

MySi
Domi

May 10

The Do
materna
which pr

Libelium
over the



MySignals platform with 15 sensors

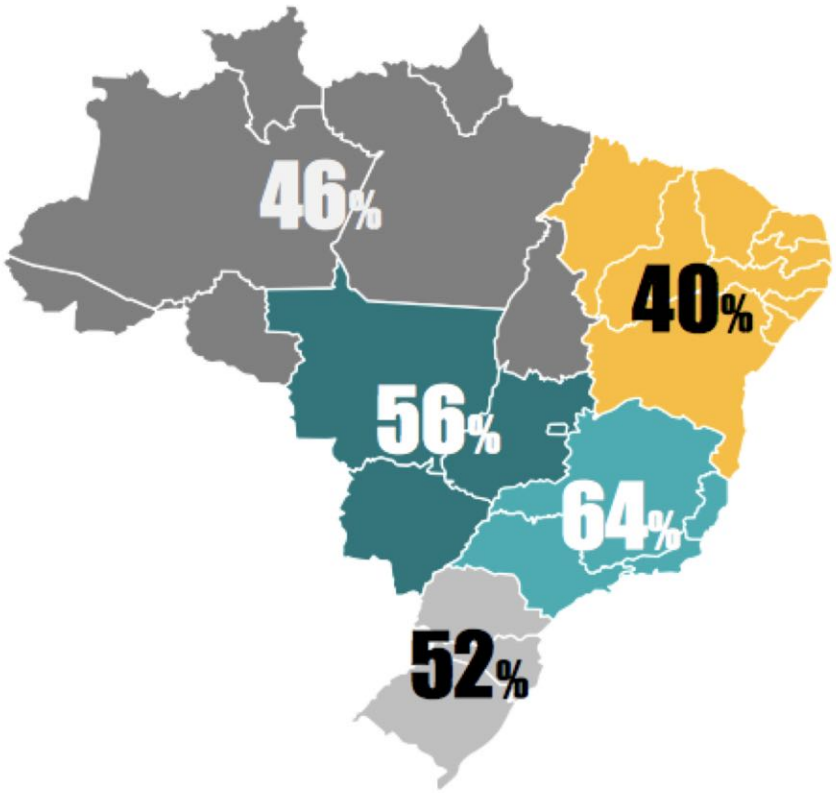
http://www.libelium.com/mysignals-helps-to-reduce-maternal-deaths-in-dominican-republic/

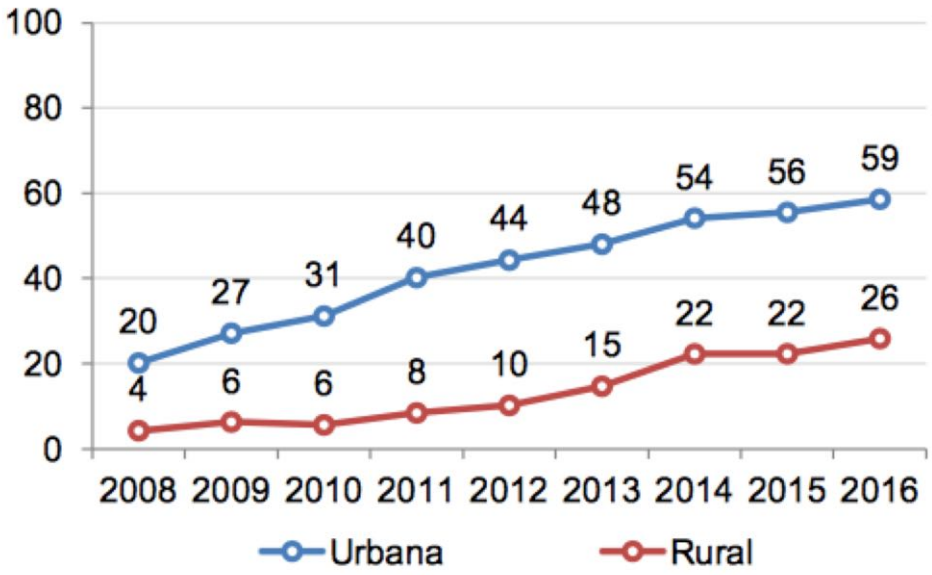
Desafios

Principais Desafios

- **Infraestrutura**
- **Privacidade**
- **Segurança**

Infraestrutura - TIC Domicílios 2016
Domicílios com acesso à Internet





http://cetic.br/pesquisa/domicilios/

Privacidade

- **Proteção de dados**
  - responsabilidades
  - assimetria de acesso entre empresas e consumidores
    - planos de saúde
    - seguradoras de veículos
    - compras em geral
- **Difícil adquirir equipamentos sem essas tecnologias**
  - tudo tem que estar conectado
  - porque é possível conectar não significa que tem que estar

Privacidade

News > Technology News

‘My Friend Cayla’ Doll Records Children’s Speech, Is Vulnerable to Hackers

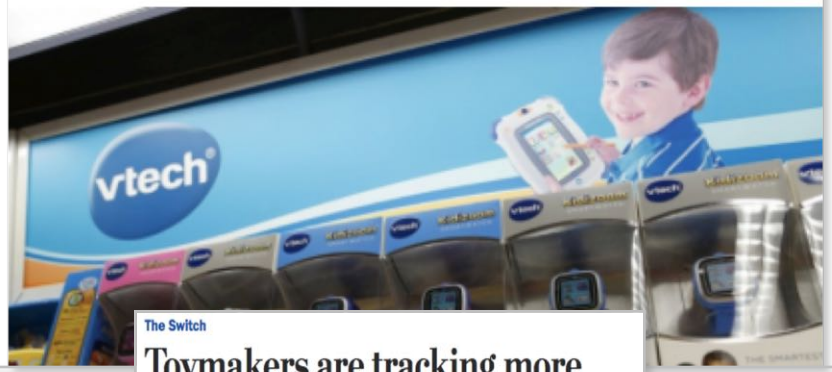
Consumer groups say the doll, which has a microphone and uses Bluetooth to transmit audio recordings via the Internet, poses both a security and a privacy threat.

By David Emery Feb 24th, 2017

The Switch

VTech says 6.4 million children profiles were caught up in its data breach

ayley Tsukayama December 1, 2015



The Switch

Toymakers are tracking more data about kids – leaving them exposed to hackers

By Andrea Peterson November 30, 2015

Boneca que pode espionar famílias teve a venda proibida na Alemanha

Cayla tem microfone e conexão bluetooth embutidos; o que é considerado ferramentas de espionagem

TECH JUL 18 2017, 3:10 PM ET

FBI Warns Parents of Privacy Risks With Internet-Connected Toys

by ALYSSA NEWCOMB

https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/
https://www.washingtonpost.com/news/the-switch/wp/2015/11/30/toymakers-are-tracking-more-data-about-kids-leaving-them-exposed-to-hackers/
http://www.snopes.com/2017/02/24/my-friend-cayla-doll-privacy-concerns/
http://www.em.com.br/app/noticia/internacional/2017/02/17/interna_internacional,848314/boneca-que-pode-espionar-familias-teve-a-venda-proibida-na-alemanha.shtml
https://www.nbcnews.com/tech/security/fbi-warns-parents-privacy-risks-internet-connected-toys-n784126

Ohio couple terrorized after hacker takes over baby-monitoring camera

Heather and Adam Schreck were terrified when they heard an unknown male voice in their Cincinnati home at midnight shouting 'Wake up, baby!' Adam rushed to baby Emma's room to make sure she was OK, but it was then that the family discovered their Foscam baby-monitoring camera had been hacked and was being controlled by a virtual intruder.

BY MELANIE GREENWOOD / NEW YORK DAILY NEWS / Monday, April 28, 2014, 9:52 AM

Share 1355 Tweet

SHARE THIS URL

nydn.us/1rwYG2C

Wake Up, baby

http://www.nydailynews.com/news/national/baby-monitoring-camera-hacked-taunts-family-article-1.1771399

The search engine for the Internet of Things

The most shocking of Shodan

SEE FULL GALLERY





"Internet of Things" security is hilariously broken and getting worse

Shodan search engine is only the latest reminder of why we need to fix IoT security.

J.M. PORUP (UK) - 1/23/2016, 1:30 PM

The cameras are vulnerable because they use the Real Time Streaming Protocol (RTSP, port 554) to share video but have no password authentication in place. The image feed is available to paid Shodan members at images.shodan.io. Free Shodan accounts can also search using the filter port:554 has_screenshot:true.

http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/
http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

Metadata From IoT Traffic Exposes In-Home User Activity

By Catalin Cimpanu August 29, 2017 07:15 AM 0

Metadata from web traffic generated by smart devices installed in a home can reveal quite a lot of information about the owner's habits and lifestyle.

According to research published this month by experts from Princeton University, a determined attacker with "capabilities similar to those of an ISP" can use passive network monitoring techniques to collect metadata exchanged by locally installed IoT devices and their remote management servers.

Even if encrypted or tunneled through a VPN, the traffic leaks enough metadata for an attacker to infer various details about the device's owner.

https://www.bleepingcomputer.com/news/technology/metadata-from-iot-traffic-exposes-in-home-user-activity/

Segurança

cert.br nic.br cgi.br

Falhas em IoT

- **Sendo exploradas por:**
  - criminosos
  - espionagem industrial
  - governos
  - vândalos
  - pessoas que querem diversão

- **Dificuldade de explicar e de entender o problema**
  - o que temos ouvido no dia-a-dia:
    - “Isto é apenas um(a) [_____]”
    - “Não, a gente não tem Internet aqui...”
    - “Esse dispositivo não é minha responsabilidade...”

Principais vulnerabilidades (1/2)

- **Projetos sem levar em conta segurança**
- **Políticas de atualização inexistentes**
  - *“deploy and forget”*
- **Defeitos de *software* / *firmware***
- **Falhas de configuração**
  - serviços desnecessários ativos por padrão

Principais vulnerabilidades (2/2)

- **Falta proteção de dados**
  - coleta excessiva
  - criptografia inexistente ou fraca
  - protocolos obsoletos
- **Autenticação falha ou inexistente:**
  - sem senhas, com senhas fracas ou padrão, contas ocultas (*backdoors*)

Mesmos velhos problemas: falhando no "básico"

2 CA-1990-02: Internet Intruder Warning

Original issue date: March 19, 1990
Last revised: September 17, 1997
Attached copyright statement

A comple

There hav
entitled "
ferred to a

At this po
not have h
tempts on systems using known security vulnerabilities. All of these vulnerabilities have been
previously reported. Some national news agencies have referred to a "virus" on the Internet; the
informati
an intrude

It is possi
tempts ha

2. Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites).

   Also uses finger to get account names and then tries simple passwords.

   Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

VMS SYSTEM ATTACKS:

13. The intruder exploits system default passwords that have not been changed since installation.

    Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

https://www.cert.org/historical/advisories/CA-1990-02.cfm

Riscos

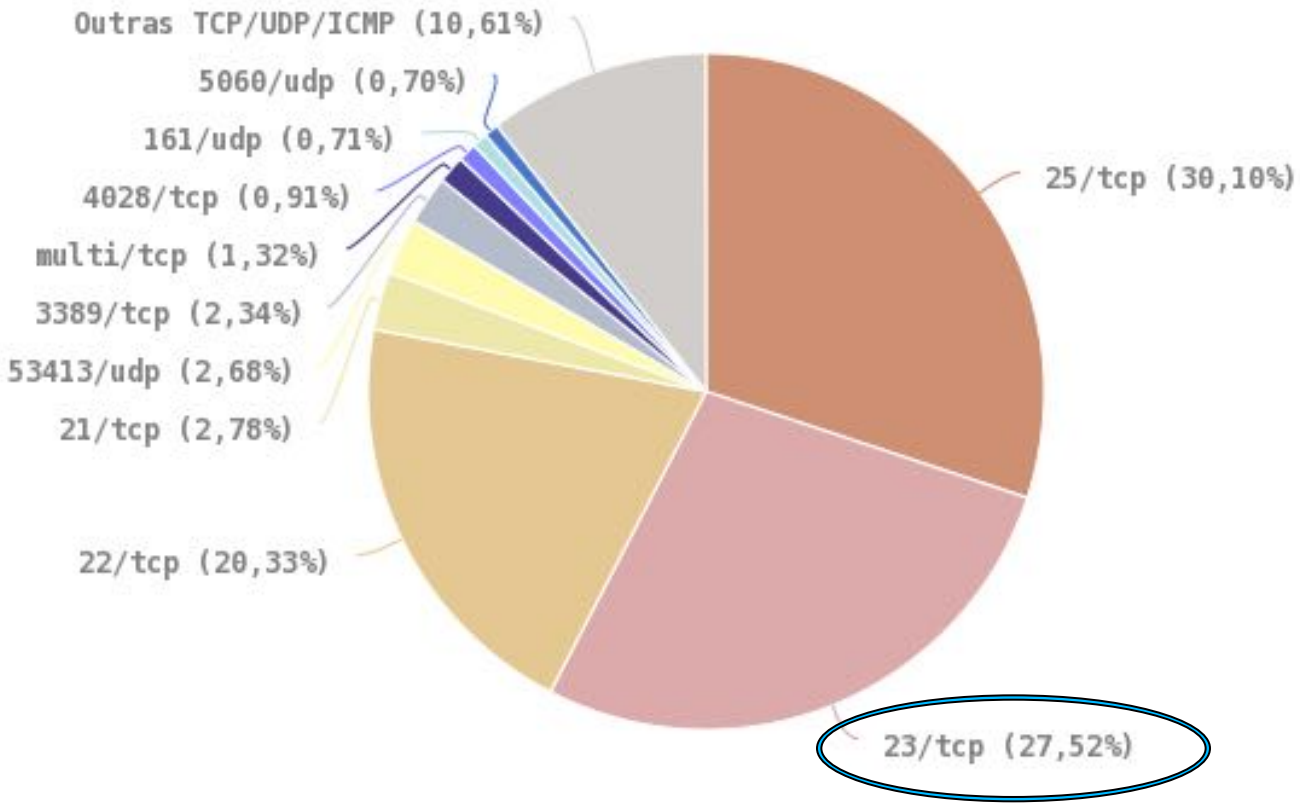
- **violação de privacidade**
- **furto de dados**
- **perdas financeiras**
- **danos à imagem**
- **perda de confiança na tecnologia**
- **indisponibilidade de serviços críticos**
- **participação em golpes**
- **propagação de códigos maliciosos**
- **envio de *spam***
- **risco de morte**

Problema:
telnet e senhas fracas

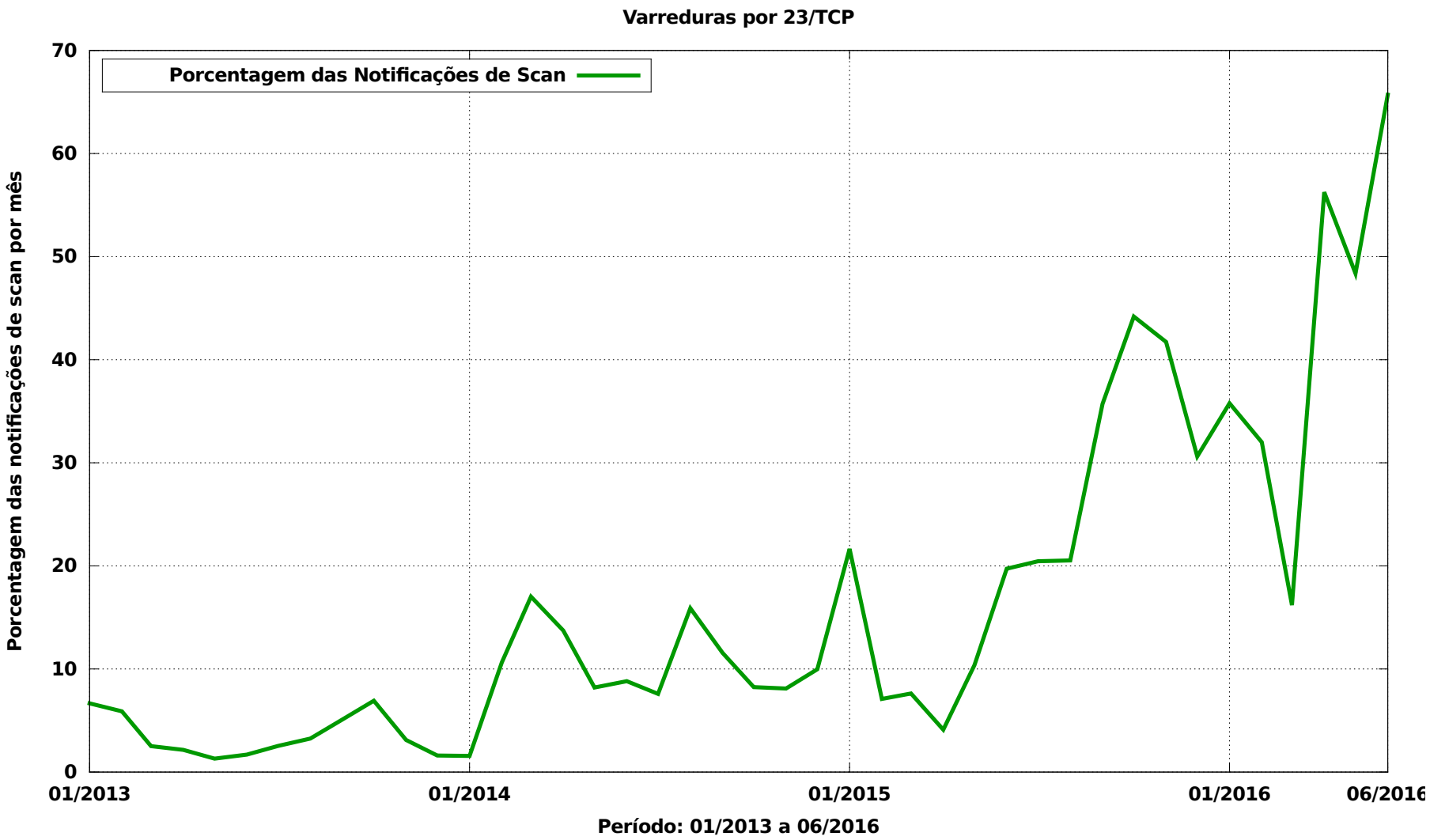
IoT *botnets*

- **CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc**
- ***Malware* se propaga geralmente via telnet**
- **Explora senhas fracas ou padrão**
  - muitas vezes são "*backdoors*" dos fabricantes

Notificações ao CERT.br: *Scans* por porta em 2016



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



Atividades nos *Honeypots* Distribuídos: Serviços mais Visados

Força bruta de senhas (usado por malwares de IoT e para invasão de servidores e roteadores):

- Telnet (23/TCP)
- SSH (22/TCP)
- Outras TCP (2323, 23231, 2222)

Protocolos explorados pela *botnet* Mirai, na variante para CPEs (roteadores de banda larga)

- TCP: 7547, 5555, 37777, 6789, 81, 37215, 52869

Busca por protocolos que permitam amplificação

- UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Projeto *Honeypots* Distribuídos
https://honeytarg.cert.br/honeypots/

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 functionality 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

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

Reader

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.

Contact Hospira

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

PLUM 360™ INFUSION SYSTEM

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

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities | ICS-CERT

https ics-cert.us-cert.gov/advisories/ICSA-15-161-01 Reader

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

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

STACK-BASED BUFFER OVERFLOW[b]

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 assigned; 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 pu
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

http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html

Innovations

How a fish tank helped hack a casino

By Alex Schiffer July 21

Hackers stole data from a casino by hacking into an Internet-connected fish tank, according to a new report. (iStock)

https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.5eac99bf1092

Hackers Breach Casino After Compromising a Smart Fish Tank

Start searching now... GO

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:

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

kb.cert.org

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

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

KIM ZETTER SECURITY 07.28.15 07:00

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/

Zeljka Zorz - Managing Editor
August 22, 2017

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

MOTHERBOARD Watch ▾ Sections ▾

Hackers Make the First-Ever Ransomware for Smart Thermostats

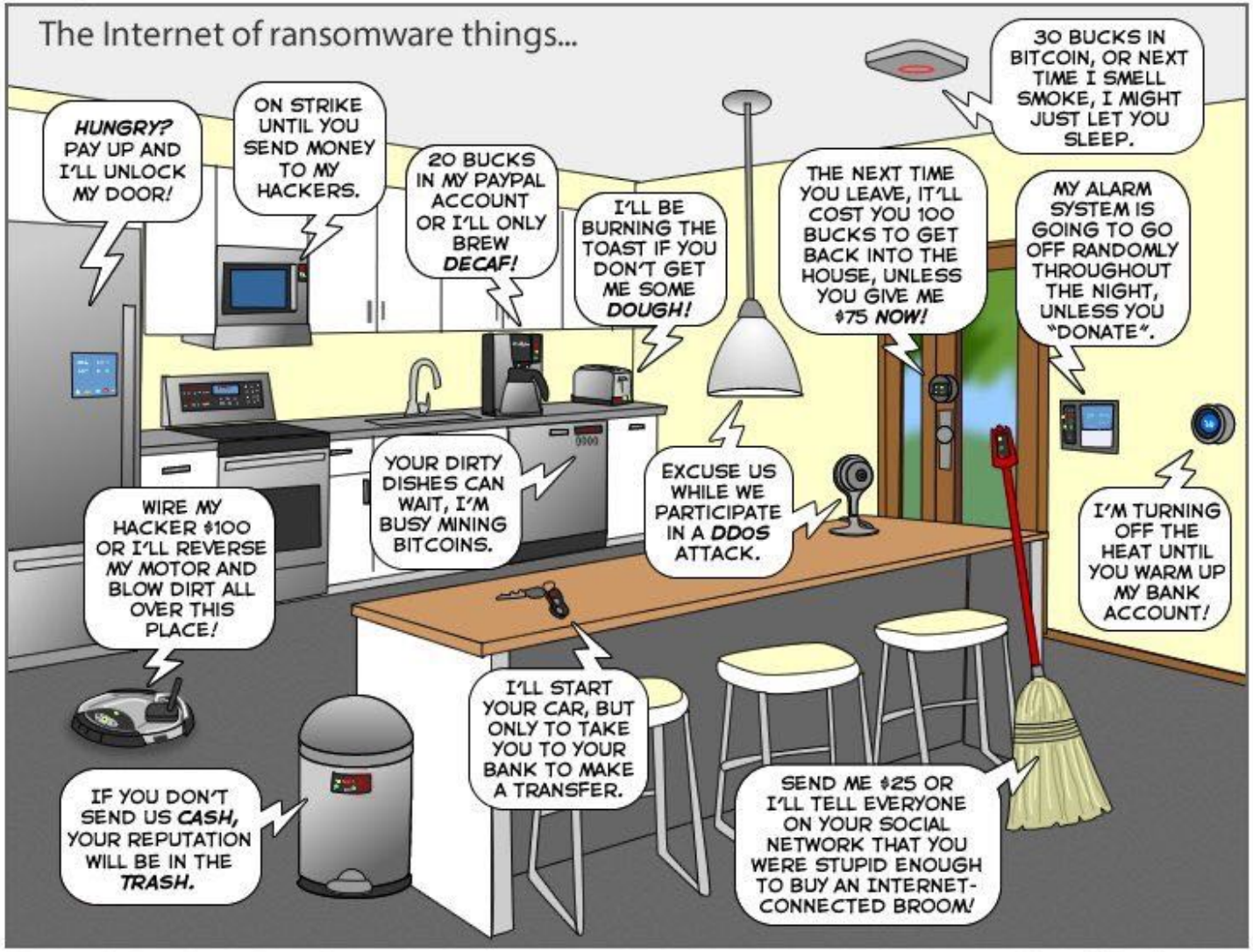
August 7, 2016 // 10:00 AM EST

One day, your thermostat will get hacked by som
away who will lock it with malware and demand
leaving you literally in the cold until you pay up a

This has been a scenario that security experts ha
dangers of the rise of the Internet of Things, inte
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

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

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.

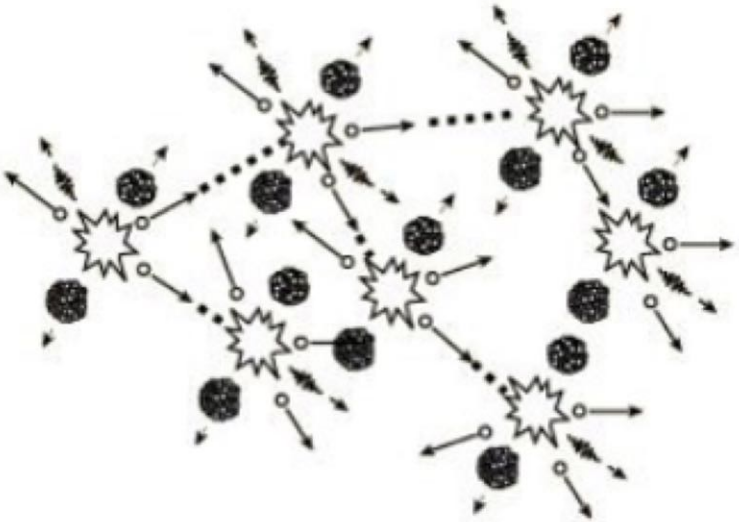
http://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html?_r=1

iotworm.eyalro.net

IoT Goes Nuclear - Creating a ZigBee Chain Reaction

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

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

RISK ASSESSMENT —

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

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

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.

Europol

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.

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/

NEWS

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

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

ibtimes.co.uk

Mirai botnet: Massive 'test' cyberattack temporarily knocks out Liberia's internet

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.

Como melhorar o cenário

Solução depende de diversas camadas

- **Usuários**
- **Desenvolvedores**
- **Administradores**
- **Fabricantes**
- **Pesquisadores**
- **Área acadêmica**
- **Governos / Legislação**

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*

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

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
  - investir em programação segura
- **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**
- **Ter grupo de resposta a incidentes preparado para lidar com os problemas (PSIRT)**

Área acadêmica, Governo e Legislação

- **Área acadêmica**
  - ensinar programação segura já nos primeiros anos
- **Governo e Legislação**
  - leis de proteção de dados
  - criar politicas públicas
  - Plano Nacional de IoT
    - estudo encomendado pelo MCTIC e BNDES
    - áreas prioritárias:
      - agronegócio, indústria, cidades e saúde

Obrigado

www.cert.br

marcus@cert.br @certbr

17 de maio de 2018

nic.br cgi.br

www.nic.br | www.cgi.br