

HVAD MED SIKKERHEDEN NÅR DEN FYSISKE VERDEN BLIVER DIGITAL? (AKA SIKKERHED I IOT)

JACOB HERBST, CTO & CSO, DUBEX A/S

Dubex:

IDA Driving IT Aarhus, den 5. september 2019

DUBEX A/S

Highly specialized it-security experts



Quality
Service
Expertise



Managing risk – Enabling growth

First mover

Consulting and security services
locally and globally



A desired workplace
Highly motivated employees

Largest it security partner in Denmark



Self-financing and privately
owned since 1997

Dubex:



Own 7x24 onsite fully staffed
Security Analytic Center
Dubex Incident Response Team

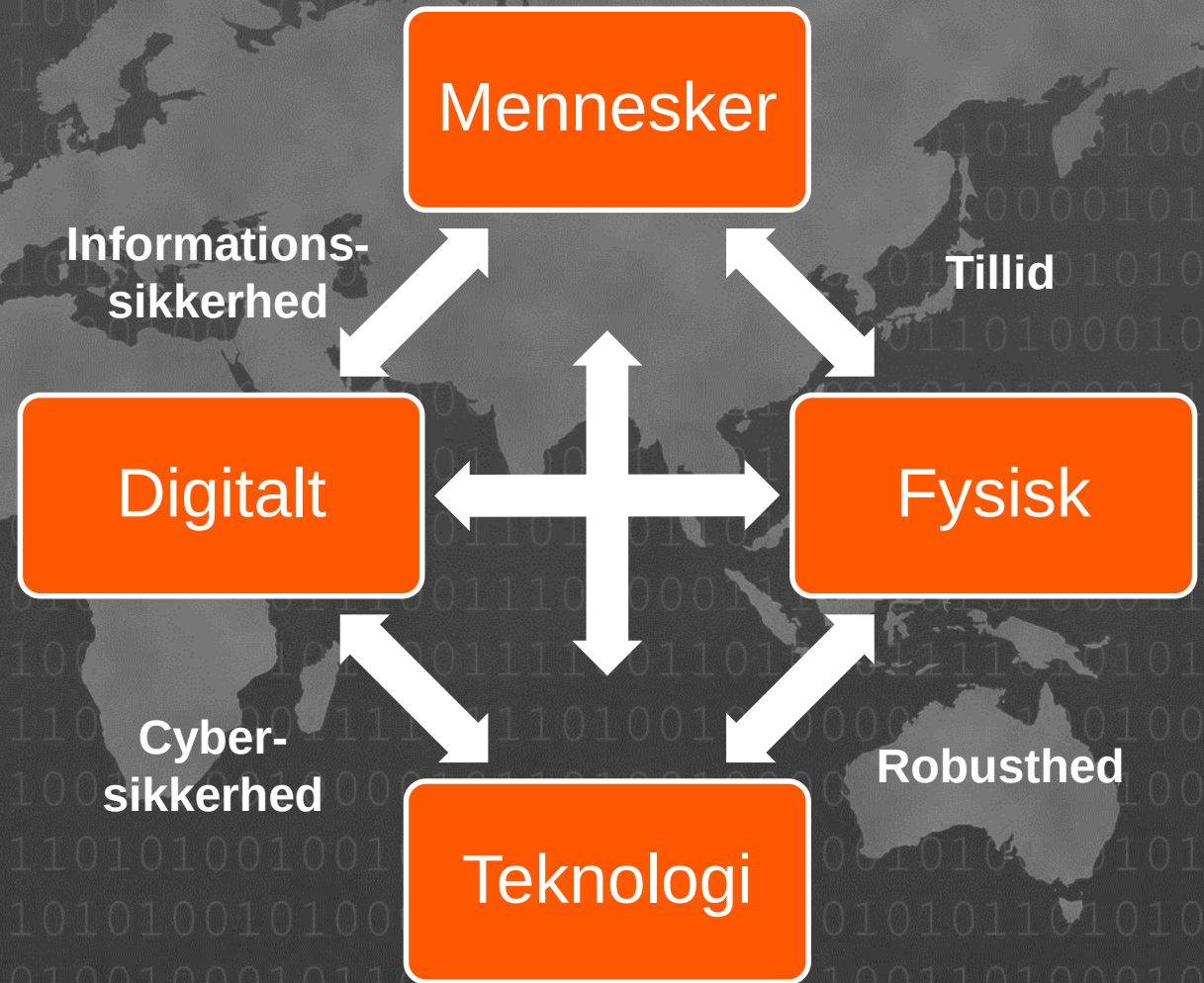
HVAD SKAL VI HAVE UD AF DETTE INDLÆG?

- Mål for dette indlæg er at give svar på:
 - Hvad er IoT?
 - Hvad er sikkerhedsudfordringerne ved IoT?
 - Hvad er eksempler på noget der går galt?

... så vi har fået øget opmærksomheden på sikkerhedsudfordringerne ved IoT.

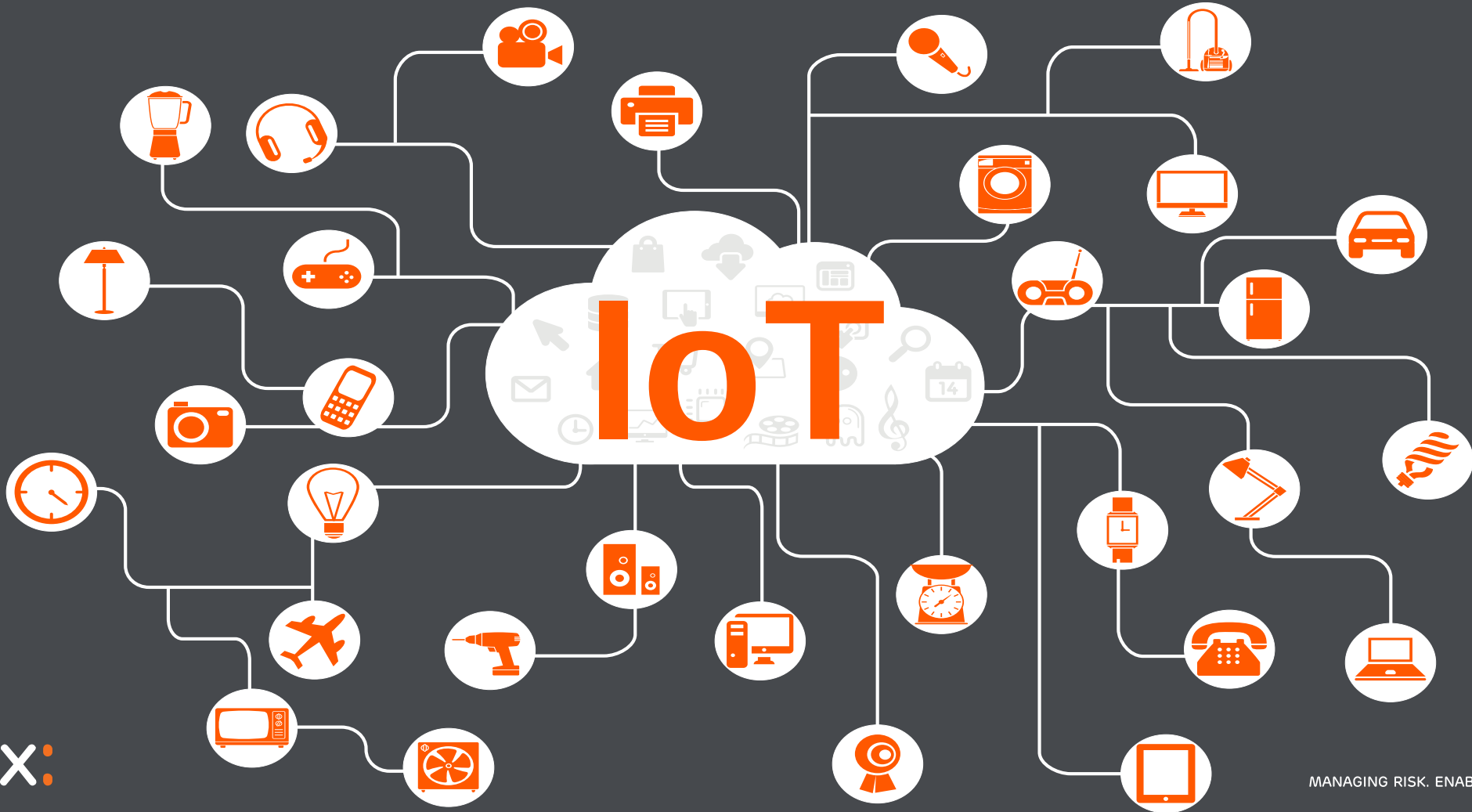
- Disclaimer: Sikkerhed, risikostyring og databeskyttelse i en IoT sammenhæng er et meget stort og komplekst emneområde som er i konstant forandring. I løbet af de 20 minutter når vi højst at skrabbe en lille smule i overfladen.

HVAD ER SIKKERHED?

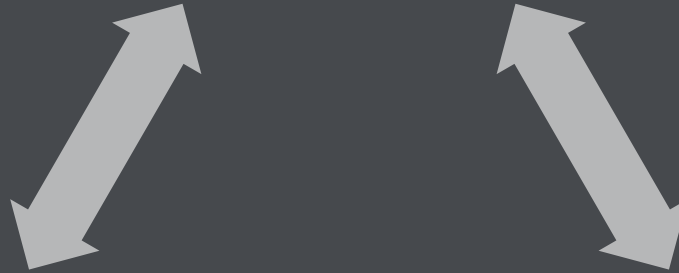


HVAD ER IOT?

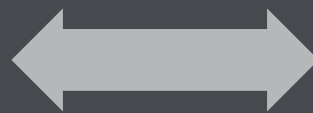
Internet of Things (IoT) refers to the ever-growing network of physical objects that somehow can be connected to the Internet



Ekspløsiv vækst
i IoT
anvendelsen



Ekspløsiv vækst
i
cyberkriminalitet



Manglende viden

HVAD ER ENABLERNE FOR IOT?

Billig hardware



ESP32-SOLO-1

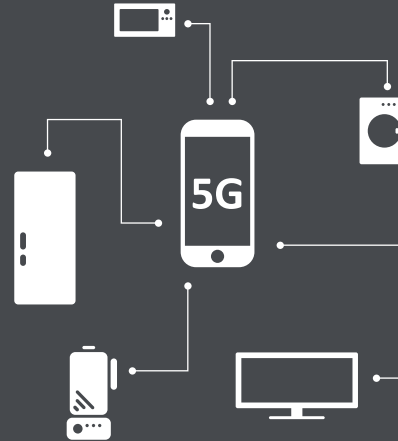
SoC: ESP32 single-core, low-power Xtensa 32-bit LX6 microprocessor
448 KB of ROM for booting and core functions
520 KB of on-chip SRAM for data and instructions
16 KB of SRAM in RTC
QSPI flash/SRAM up to 4 × 16 MB
Power supply: 2.3V to 3.6V
SPI, I2S, I2C, SDIO, UART, IR, PWM
Temperature sensor, touch sensor, ADC, DA
Connectivity: Bluetooth (Classic & Low-Energy) and Wi-Fi b/g/n dual mode

Pricing (EUR)

Qty.	Unit Price	Ext. Price
1	2,21 €	2,21 €

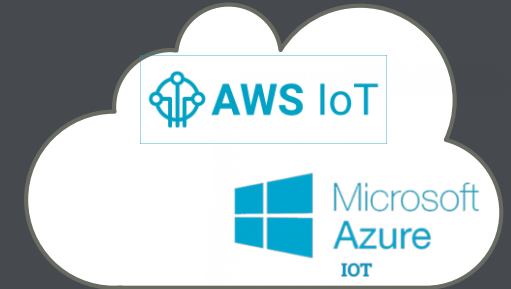
Dubex:

Billig forbindelse



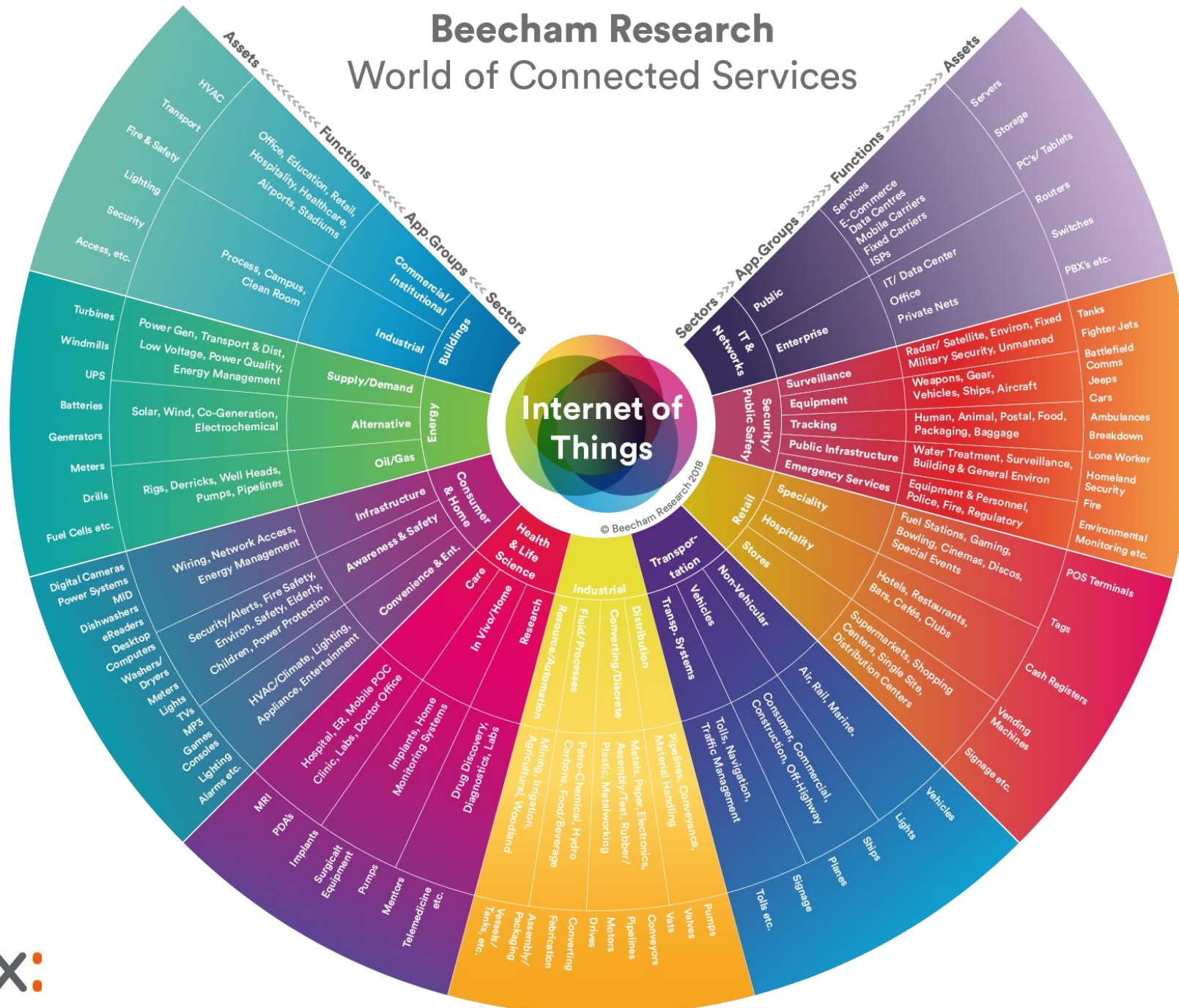
Global Machine-to-Machine Growth
Kilde: Cisco

Billig software



Beecham Research

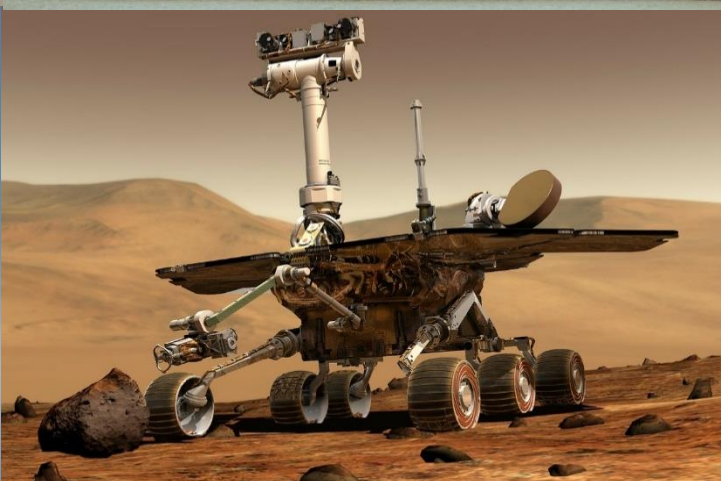
World of Connected Services



Shaping the IoT future

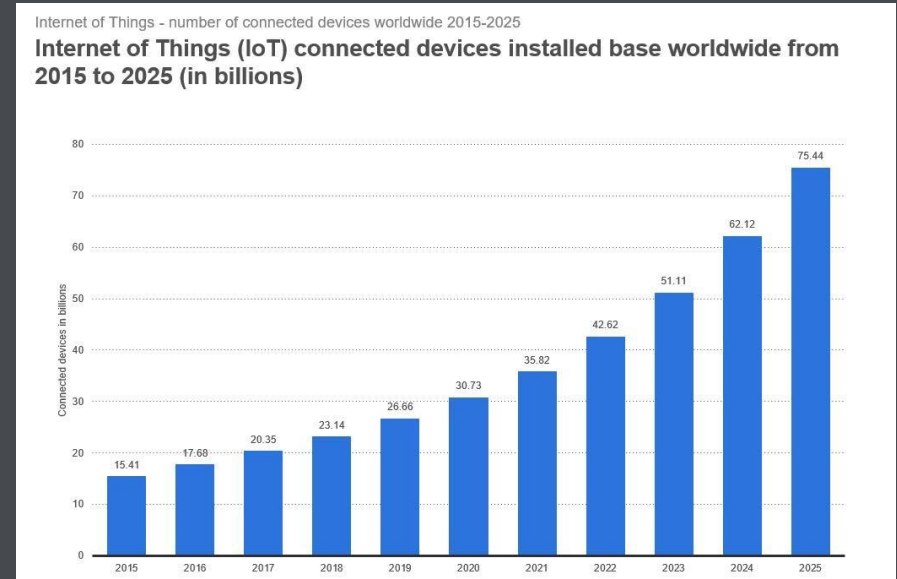
MANAGING RISK. ENABLING GROWTH.®

Dubex:

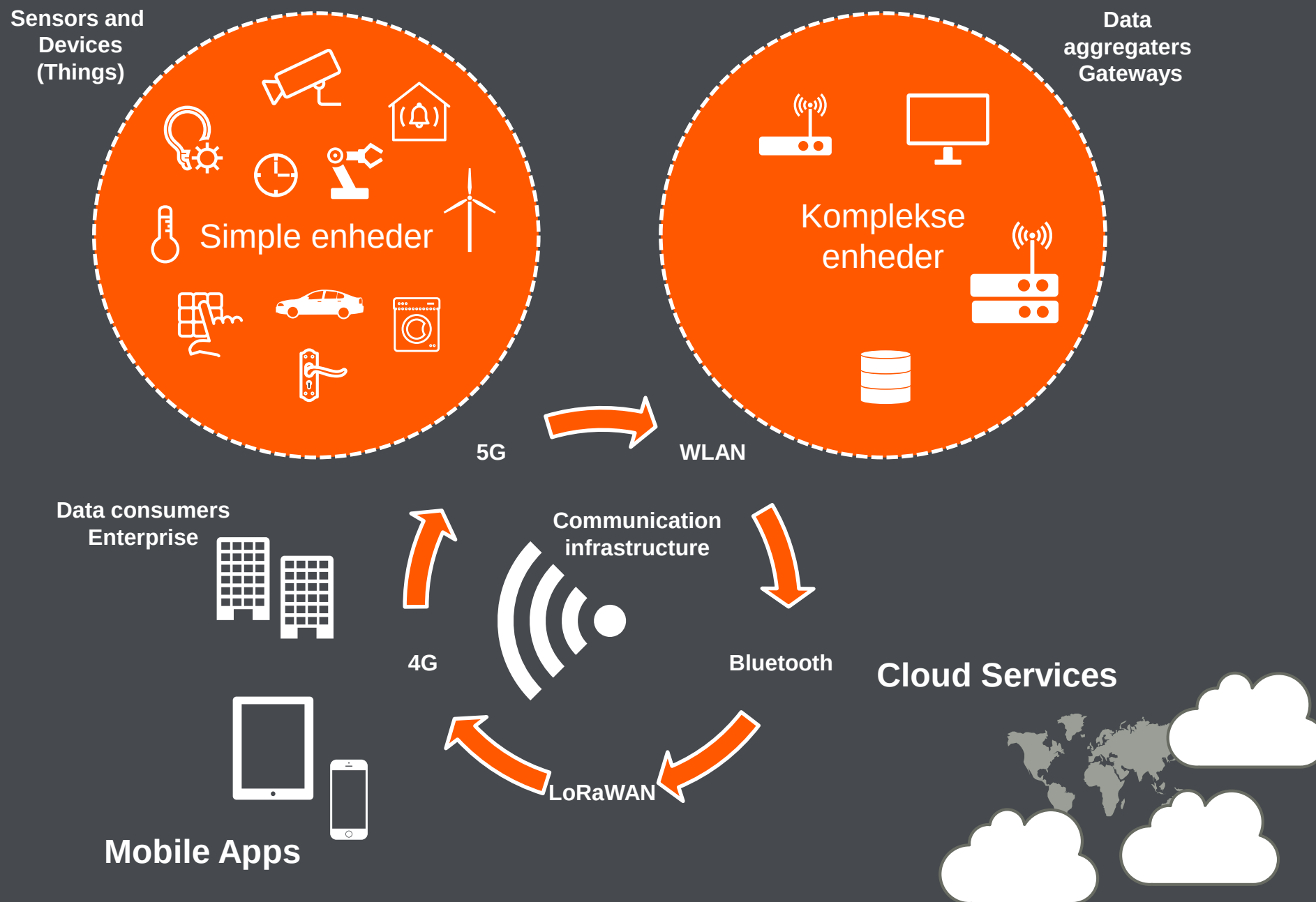


HVAD ER IOT UDVIKLINGEN?

- There are expected to be more than 64B IoT devices worldwide by 2025
- Consumer electronics will account for 63% of all installed IoT units in 2020.
- By 2022, 100% of the global population is expected to have LPWAN coverage
- IoT has the potential to generate \$4T to \$11T in economic value by 2025
- The main revenue driver for 54% of enterprise IoT projects is cost savings
- More than 80% of senior executives across industries, on average, say IoT is critical to some or all lines of their business in 2018
- 97% of organizations feel there are challenges to creating value from IoT-related data
- The IoT in Banking and Financial Services market size is expected to grow to \$2.03B by 2023



IOT



IOT - UDFORDRINGER



“Minimal Viable Products”

Poorly maintained operating systems

“Install and Forget” model

Commercial Off-the-shelf Technology (COTS)

Internet Communication protocols

Long lifespan of devices

Outdated code & no patching

Lack of security solutions

Constant Internet connection

SÅRBARHEDER – OWASP

Weak Guessable, or Hardcoded Passwords

Insecure Network Services

Insecure Ecosystem Interfaces

Lack of Secure Update Mechanism

Use of Insecure or Outdated Components

Insufficient Privacy Protection

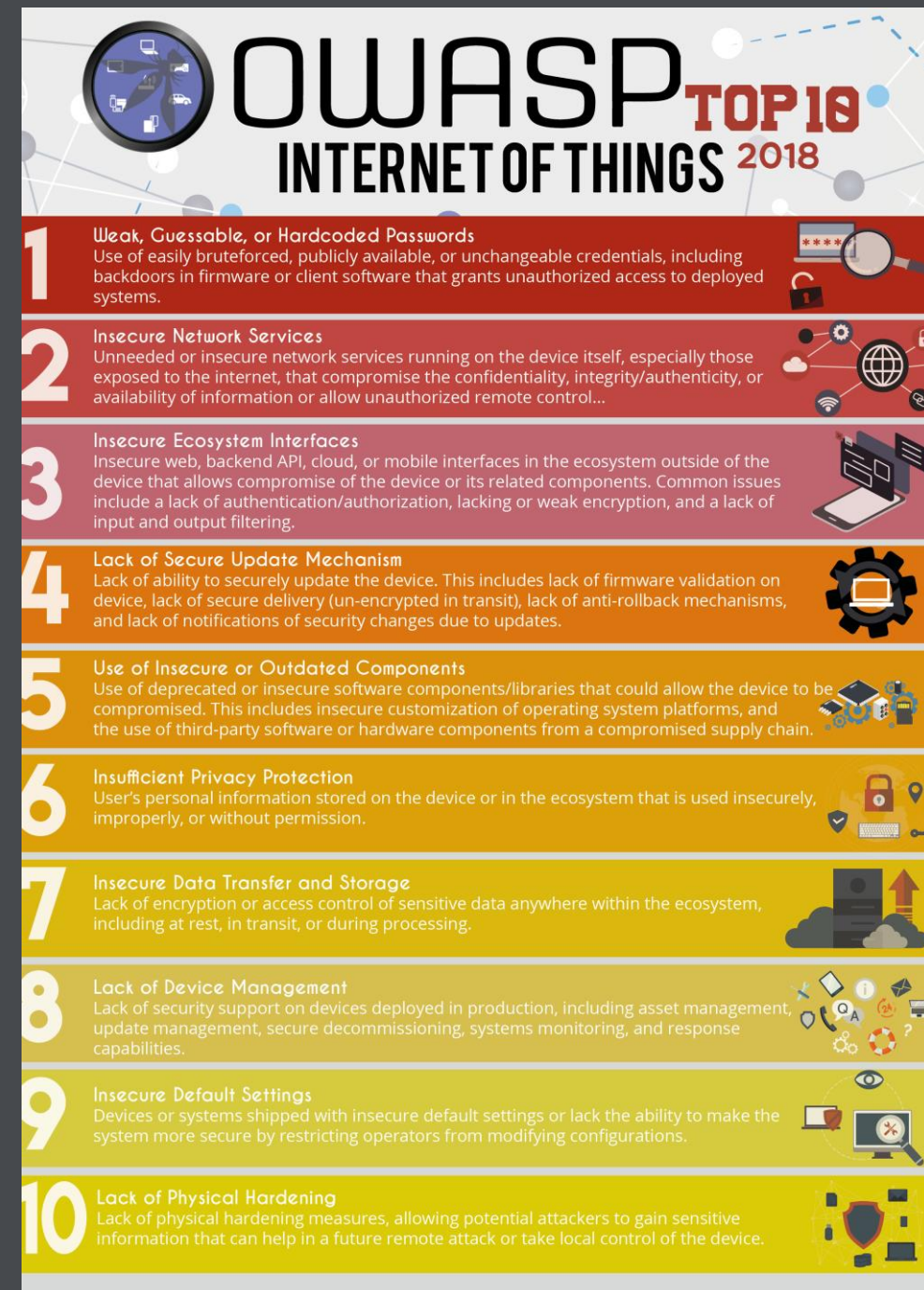
Insecure Data Transfer and Storage

Lack of Device Management

Insecure Default Settings

Lack of Physical Hardening

Dubex:



STUXNET

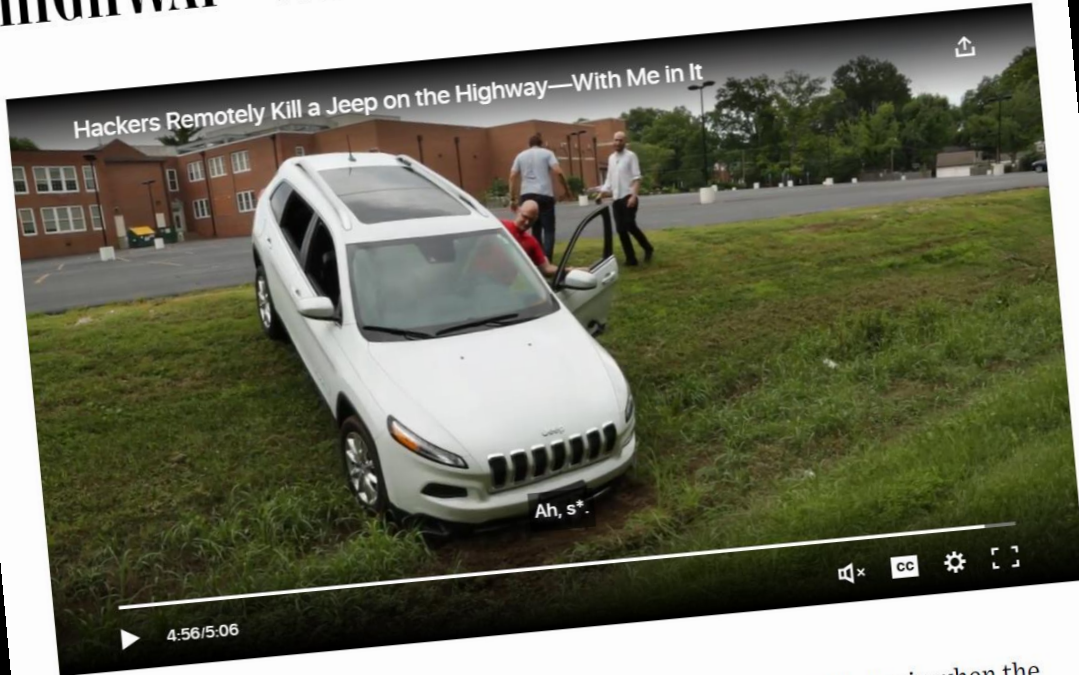
- Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities and has since mutated and spread to other industrial and energy-producing facilities.
- The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes. It generated a flurry of media attention after it was discovered in 2010 because it was the first known virus to be capable of crippling hardware and because it appeared to have been created by the U.S. National Security Agency, the CIA, and Israeli intelligence.
-



BLACK HAT USA 2015: JEEP HACKED

ANDY GREENBERG SECURITY 07.21.15 06:08 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



Share

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my forehead. Next the radio started playing a pre-recorded message. The car's climate control system. Next the radio started playing a pre-recorded message. The car's climate control system. Next the radio started playing a pre-recorded message. The car's climate control system.

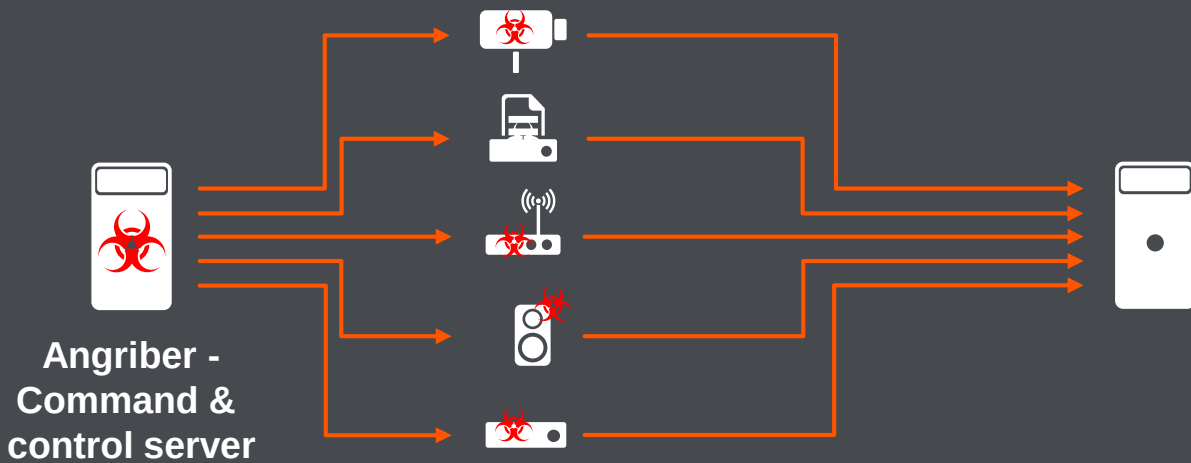


MANAGING RISK. ENABLING GROWTH.®

<https://www.wired.com/2015/07/hackers-remotely-kill-jEEP-highway/>

MIRAI BOTNET

IoT-enheder med offentligt eksponerede administrative porte kun beskyttet med standard password



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	
root/anko	ANKO Products DVR	https://ipvm.com/reports/ip-camera
root/pass	Axis IP Camera, et. al	http://www.cctvforum.com/viewtopic.php?p=1044
root/vizxv	Dahua Camera	http://www.cleancss.com/router-default-username-and-password
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=1044
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=1044
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=1044
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=1044
666666/666666	Dahua IP Camera	http://www.cam-it.org/index.php?topic=1044
root/dreambox	Dahua IP Camera	http://www.cam-it.org/index.php?topic=1044
root/zlhx	Dreambox TV receiver	http://www.cleancss.com/router-default-username-and-password
root/juantech	EV ZLX Two-way Speaker?	https://www.satellites.co.uk/forums/thread.php?p=1044
root/xc3511	Guangzhou Juan Optical	?
root/hj3518	H.264 - Chinese DVR	https://news.ycombinator.com/item?id=1044
root/klv123	HiSilicon IP Camera	http://www.cctvforum.com/viewtopic.php?p=1044
root/klv1234	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/08/
root/yvzdz	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd01044
root/admin	HiSilicon IP Camera	https://gist.github.com/gabonator/74cd01044
root/system	IPX-DDK Network Camera	https://gist.github.com/gabonator/74cd01044
admin/meinsm	IQinVision Cameras, et. al	http://www.ipxinc.com/products/cameras
root/54321	Mobotix Network Camera	https://ipvm.com/reports/ip-cameras-default-username-and-password
root/00000000	Packet8 VOIP Phone, et. al	http://www.forum.use-ip.co.uk/threads/mobotix-network-camera
root/realtek	Panasonic Printer	http://webcache.googleusercontent.com/search?q=panasonic+printer+default+username+password
	RealTek Routers	https://www.experts-exchange.com/questions/q.asp?qid=1044

Twitter og Spotify blev delvist slået ud af netangreb

Hundreder af netjenester var berørt af cyberdomænevirkksomhed. Angrebet ramte i det FREDAG D. 21. OKTOBER 2016 KL. 17:10



Washington. Flere store nettjeneste

BERLINGSKE

TECHNOLOGY

The New York Times
Hackers Used New Weapons to Disrupt Major Websites Across U.S.
OCT. 21, 2016

The New York Times

U.S.



Financial Times logo and masthead. The text "FINANCIAL TIMES" is prominently displayed in a large, bold, serif font. Below it, in a smaller font, are the words "WORK & CAREERS" and "LIFE & ARTS". The date "OCT 21, 2016" is visible in the upper right corner of the masthead area.

MARKETS OPINION WORK & CAREERS LIFE & ARTS

Cyber Security + Add to myFT

Connected devices create millions of cyber security weak spots

'Internet of Things' excitement masks attacks

...create millions of cyber
weak spots
'Internet of Things' excitement marred by vulnerability to hacking
attacks



NETFLIX



MANAGING RISK. ENABLING GROWTH.®

RANSOMWARE & IOT

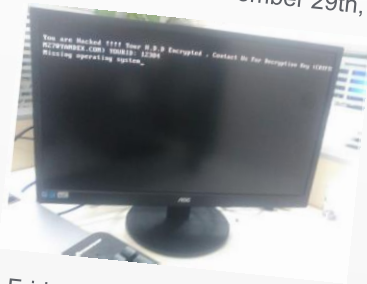
KrebsOnSecurity

In-depth security news and investigation



San Francisco Rail System Hacker Hacked

The San Francisco Municipal Transportation Agency (SFMTA) was hit with a ransomware attack on Friday, causing fare station terminals to carry the message, "You are Hacked. ALL Data Encrypted." Turns out, the miscreant behind this extortion attempt got hacked himself this past weekend, revealing details about other victims as well as tantalizing clues about his identity and location.



A copy of the ransom message left behind by the "Mamba" ransomware.

On Friday, The San Francisco Examiner reported that riders of SFMTA's Municipal Rail or "Muni" system were greeted with handmade "Out of Service" and "Metro Free" signs on station ticket machines. The computer terminals at all Muni locations carried the "hacked" message: "Contact for key (cryptom27@yandex.com)," the message read.

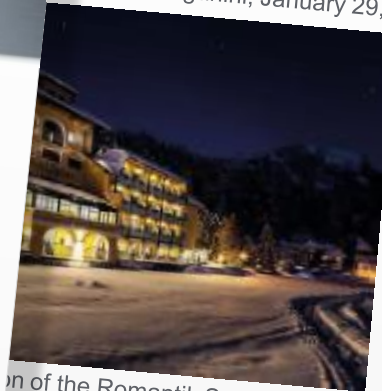
The hacker in control of that email account said he had compromised thousands of computers at the SFMTA, scrambling the files on those systems with strong encryption. The files encrypted by his ransomware, he said, could only be decrypted with a special digital key, and that key would cost 100 Bitcoins, or approximately USD \$73,000.

<https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/>

The Romantik Seehotel Jägerwirt 4-Star Superior Luxury Hotel was hit by a ransomware attack that locked guests in and out of the rooms

Another singular incident involved a ransomware, the victims are hundreds of guests of a luxurious hotel. The Romantik Seehotel Jägerwirt 4-Star Superior Hotel. The guests were locked in or out of the hotel as the malware infected the systems at the hotel and its administration opted to pay the ransom to resume a normal operation.

By Pierluigi Paganini, January 29, 2017 By Pierluigi Paganini



On Friday, the Romantik Seehotel Jägerwirt 4-Star Superior Hotel has admitted having been hit by a ransomware attack to restore the electronic key card system that was compromised by the ransomware. The luxury hotel uses the electronic key card system to manage key cards.

The hotel management said the cyber attack suffered by the luxury hotel, the hotel management had to pay the ransom multiple times, but this time crooks compromised the internal key management system. The news agency, cyber criminals gained control over the general computer system and any activity at the luxury hotel, including the reservation system and the hotel's website.

The top hotels has admitted they had to pay thousands in Bitcoin ransom to restore their electronic key system, locking hundreds of guests in or out of the hotel. The ransom was paid," reported The Local website.



<http://securityaffairs.co/wordpress/55790/cyber-crime/ransomware-luxury-hotel.html>

ICS SPECIFIC MALWARE

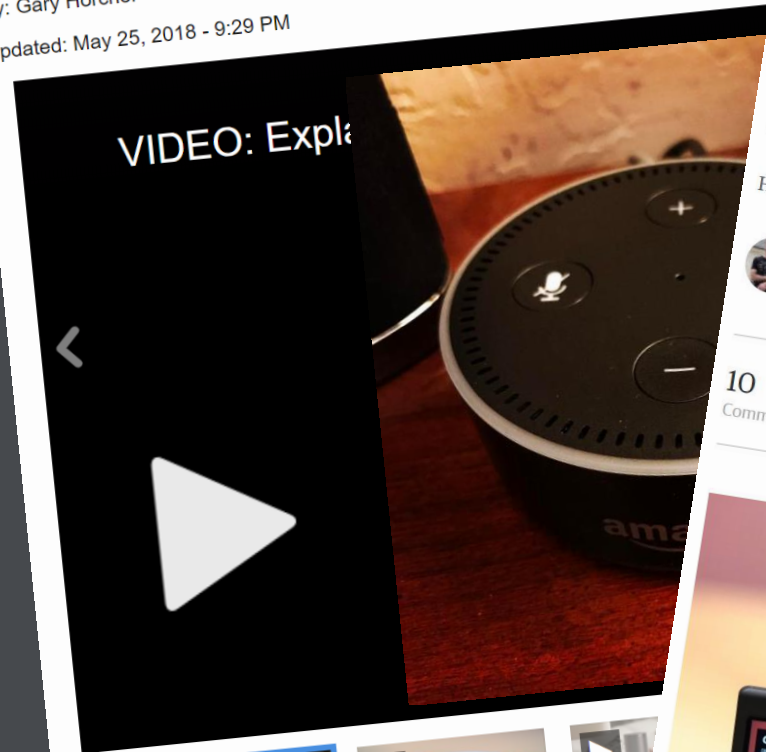
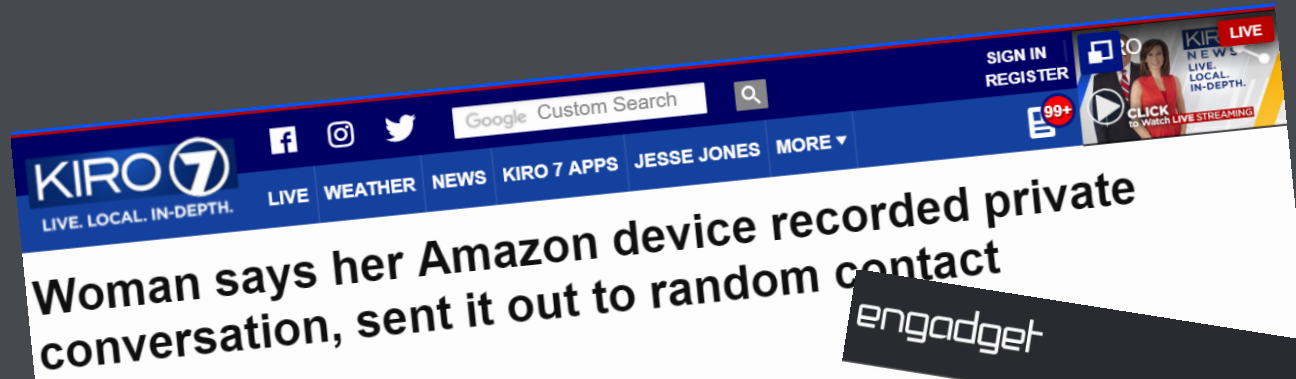
- CRASHOVERRIDE (A.K.A. INDUSTROYER)
- Malware to target different critical infrastructure environments attacking ICS protocols such as IEC 101 and 104, IEC 61850, and OPC. Protocols are mainly used in electric power
- Once on a system, CrashOverride looks for configuration files for remote terminal units (RTUs) and intelligent electronic devices (IEDs)
- CrashOverride had the ability to operate independently of the initial Command and Control (C2), bypassing most common behavioral checks.
- The malware has directly affected the civilian population, causing a blackout in Ukraine.



- TRITON
- This was the most recent malware tailored to attack an Operation Technology (OT) environment, and more specifically, safety instrumented system (SIS) controllers from Schneider Electric (Triconex 3008 processor modules).
- Until TRITON, there had been only four publicly known malwares specifically designed for OT environments: Stuxnet, Havex/Dragonfly, Blackenergy2 and Industroyer. The attackers reverse engineered the proprietary TriStation protocol and embedded specific functions necessary for the malware to disrupt the SIS controllers, such as halting the device or writing to memory.
- TRITON - Schneider Electric Analysis and Disclosure
 - <https://www.youtube.com/watch?v=f09E75bWvkk>



IOT & PRIVACY ...



VPNFILTER



WEDNESDAY, MAY 23, 2018

New VPNFilter malware targets at least 500K networking devices worldwide



VPNFilter malware infected 500K devices: SMB and home office routers are at risk

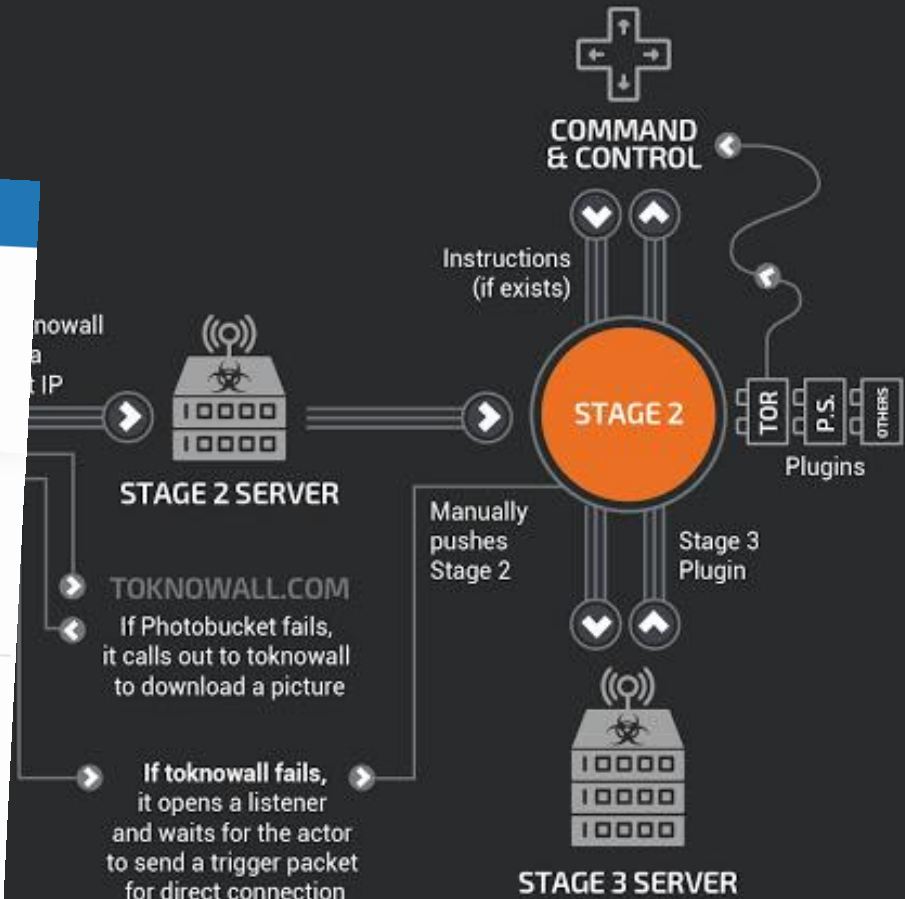
by James Sanders in Security on May 24, 2018, 5:40 AM PST

An advanced malware attack, believed to be developed by a nation-state actor, has been discovered by Cisco's Talos Intelligence research division. The attack, named "VPNFilter" in a Cisco blog post, has been found to infect routers manufactured by Linksys, MikroTik, Netgear, and TP-Link, as well as NAS devices by QNAP—all of which are products targeted toward the SMB and home office market.

More about cybersecurity

- Famous con man Frank Abagnale: Crime is 4,000 times easier today
- How to become a cybersecurity pro: A cheat sheet
- Dark Web: A cheat sheet for business professionals
- Why deepfakes are a real threat to elections and society

Talos notes that their research is incomplete, though they have disclosed their present findings due to the attack, and number of infected devices, rapidly accelerating over the last three weeks.



PACEMAKER SÅRBARHEDER



The FDA has reviewed information concerning potential **cybersecurity vulnerabilities** associated with St. Jude Medical's **RF-enabled** implantable cardiac pacemakers and has confirmed that these vulnerabilities, if exploited, could **allow an unauthorized user** (i.e. someone other than the patient's physician) to access a patient's device **using commercially available equipment**. This access could be used to **modify programming commands** to the implanted pacemaker, which could result in **patient harm** from rapid battery depletion or administration of inappropriate pacing.



IN THIS SECTION: Safety Communications

[← Medical Device Safety](#)

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

[Share](#) [Tweet](#) [LinkedIn](#) [Email](#) [Print](#)

Date Issued
August 29, 2017

Audience

- Patients with a radio frequency (RF)-enabled St. Jude Medical implantable pacemaker
- Caregivers of patients with an RF-enabled St. Jude Medical implantable cardiac pacemaker
- Cardiologists, electrophysiologists, cardiothoracic surgeons, and primary care physicians treating patients with heart failure or heart rhythm problems using an RF-enabled St. Jude Medical implantable cardiac pacemaker

Medical Specialties
Cardiac Electrophysiology, Cardiology, Cardiothoracic Surgery, Heart Failure

Devices

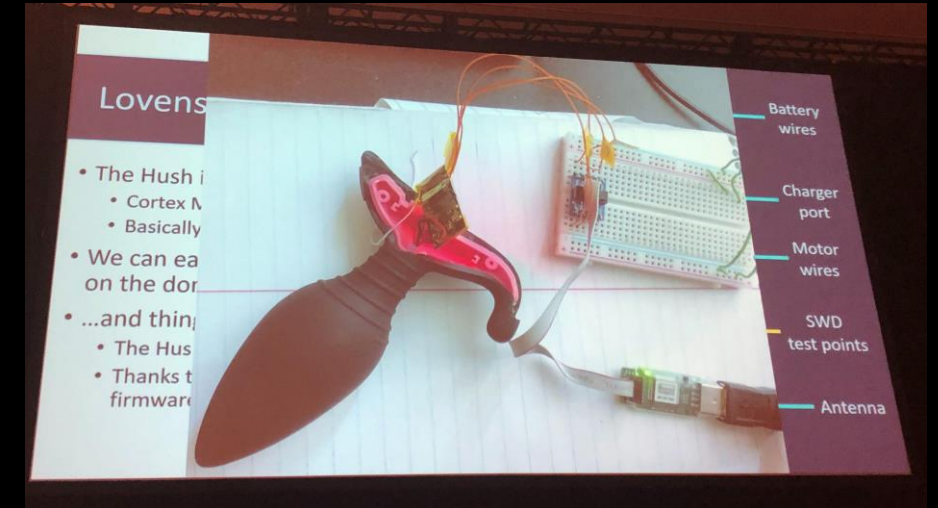
Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers, including cardiac resynchronization therapy pacemaker (CRT-P) devices, provide pacing for slow or irregular heart rhythms. These devices are implanted under the skin in the upper chest area and have connecting insulated wires called "leads" that go into the heart. A patient may need an implantable cardiac pacemaker if their heartbeat is too slow (bradycardia) or needs resynchronization to treat heart failure.

“If Your Vibrator Is Hacked, Is It a Sex Crime?”

BUTT PLUG HACKING!

REAL PENETRATION TESTING

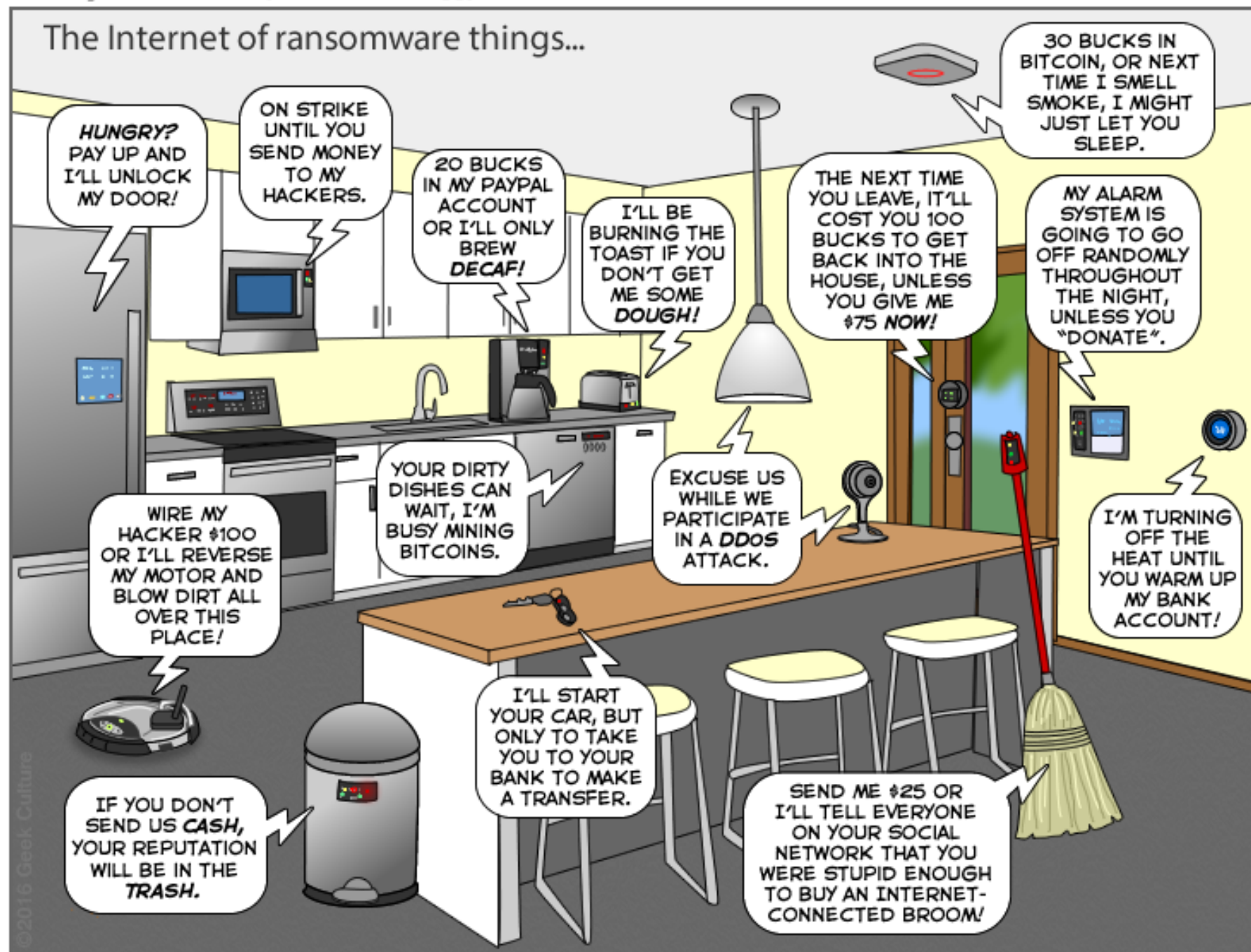
DEF CON 27

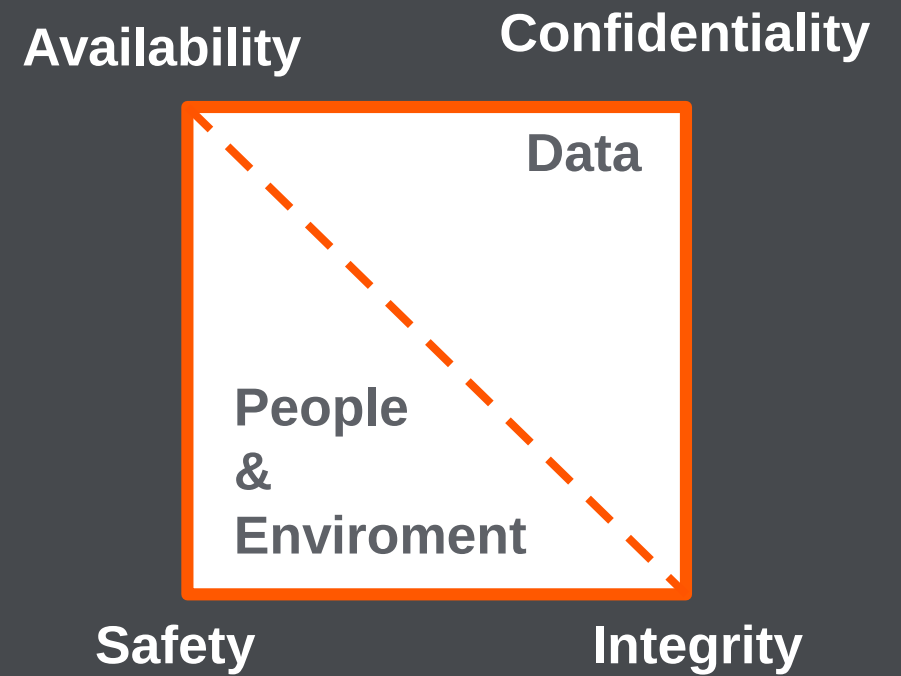
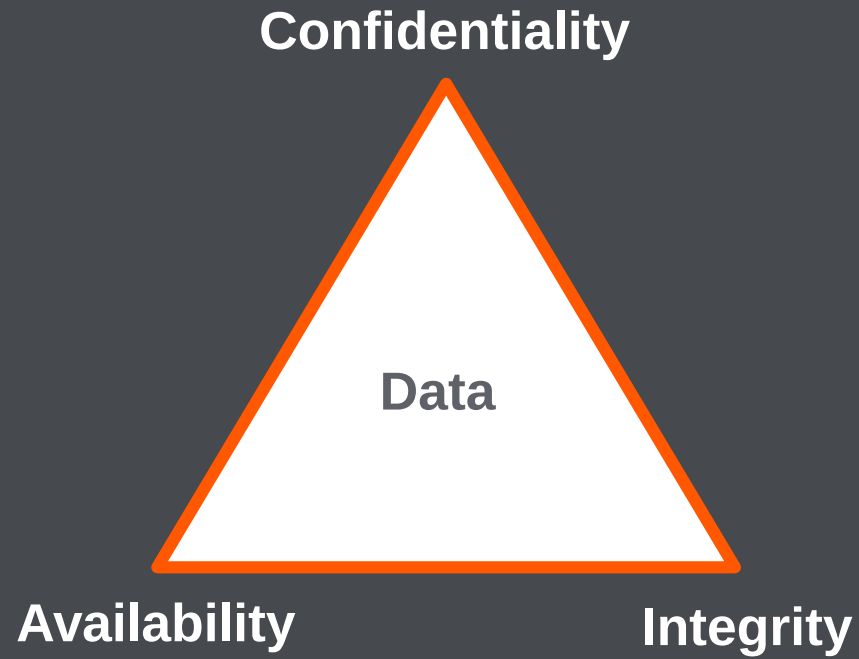


<https://gizmodo.com/if-your-vibrator-is-hacked-is-it-a-sex-crime-1820007951>

<https://www.youtube.com/watch?v=CsQ2VWEfdUM>

The Internet of ransomware things...





ANBEFALINGER

Producenter

- Struktureret proces omkring cybersikkerhed:
 - Security-by-design
 - Life Cycle-management
 - Udviklingsproces og sårbarhedstestning
 - Sårbarhedshåndtering
- Værktøjer til administration og håndtering fx
 - Fjernadministration
 - Adgangsstyring og passwords
 - Certifikathåndtering
 - Software-opdateringer
 - Overvågning

Leverandører

- Leverandøren skal forstå at lave en risikovurdering
 - Skabe et klart billede af slutbrugerens faktiske behov
- Sikre den nødvendige viden og modenhed
 - Undervisning af forbrugerne
- Procedurer og best-practice
 - Proces, hvor cybersikkerhed er tænkt ind, så installationen bliver etableret på en sikker måde
- Overdragelse til slutbrugerens
 - Instruktion i korrekt brug og anvendelse af løsningen

Forbrugere

- Forbrugere skal gøres bevidst om sikkerhed og cybersikkerhed bl.a.
 - Korrekt håndtering af IoT produkterne
 - Omtanke ved fysisk placering af udstyr
 - Forståelse for at IoT er it-systemer
 - Proces for opdatering af software – evt. serviceaftale

Awareness

IOT - LIFE SAFETY AND CYBERSECURITY

- Industrial and consumer products are being **connected to the internet**
- **Billions of IoT devices** gather data and exert direct control
- Risk of **catastrophic impacts** as our reliance and trust increase
- Many IoT devices have **publicly exposed administrative ports** protected only by **default passwords**
- The devices **lack security software** such as anti-virus
- Residential customers and small businesses that **lack security** sophistication are in charge of protecting the devices
- Device **firmware are not updated** from vendors and if updated are difficult to apply
- Typically IoT gear is connected to the internet **all the time**
- Attackers **don't have to deal with social engineering**, email poisoning or expensive zero day attacks
- Risks **first emerge for the transportation, healthcare, and industrial sectors**
- As IoT-devices **explode in number** and function, so will the potential misuse
- Remote devices, cameras, and drones become more concerning to safety and privacy. **Expect more regulations**

HOLD DIG OPDATERET



Besøg
www.dubex.dk

Abonnér på Dubex' nyhedsbrev

www.dubex.dk/aktuelt/nyhedsbrev



Følg Dubex på LinkedIn & Twitter



twitter.com/Dubex



www.linkedin.com/company/dubex-as



Deltag på Dubex' arrangementer



www.dubex.dk/aktuelt/events

Dubex:

MANAGING RISK. ENABLING GROWTH.®

KOMMENDE ARRANGEMENTER



Dubex Security & Risk Management Summit 2020

Sæt kryds i kalenderen allerede nu, og vær sikker på at få en plads på en af Danmarks største dedikerede it-sikkerhedskonferencer, når vi igen inviterer til Dubex Security & Risk Management Summit.

Tirsdag den 3. marts 2020 på Scandic Bygholm Park, Horsens
Torsdag den 5. marts 2020 i DGI-byen, København



InfoSecurity Denmark 2020

Onsdag den 29. april & torsdag den 30. april 2020



Webinars

On-demand

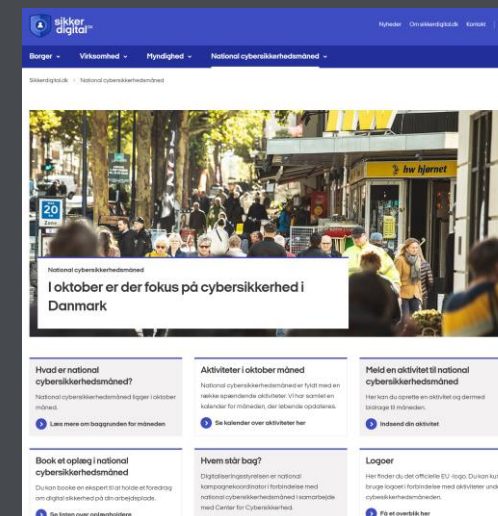
Se www.dubex.dk mere information

Dubex:

Læs mere www.dubex.dk



EUROPÆISK
CYBER
SIKKERHEDS
MÅNED



www.sikkerdigital.dk

MANAGING RISK. ENABLING GROWTH.®

TAK!

#SammenSikrerViDanmark

Dubex:

Jacob Herbst
jhe@dubex.dk

Dubex A/S
Gyngemose Parkvej 50
DK-2860 Søborg

Dubex A/S
Bredskifte Allé 11
DK-8210 Aarhus V

www.dubex.dk
+45 3283 0430
info@dubex.dk