



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid



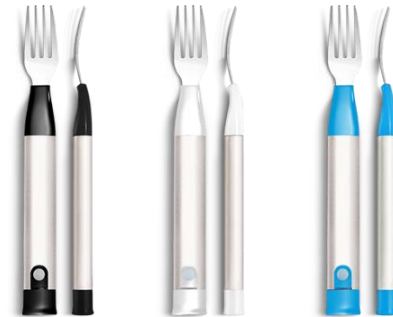
IOT: een nachtmerrie van slaapkamer tot staatsveiligheid?

20 november 2018

drs. J. (Jelte) Jansen
ir. R.H. (Rogier) van Wanroij MSIT



This is GeniCan.





These Flip Flops Are 'Smart' for the Dumbest Possible Reason



Christina Warren

3/28/17 5:58pm • Filed to: WHO NEEDS THIS? ▾

🔥 28.3K 💬 17 ⭐ 2

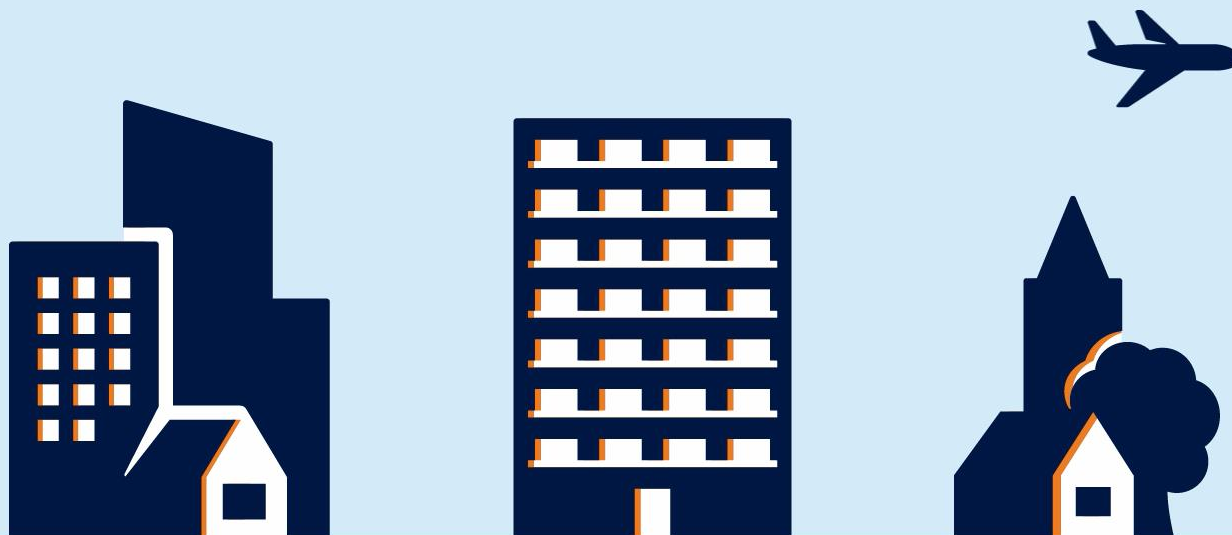


Image: Hari Mari



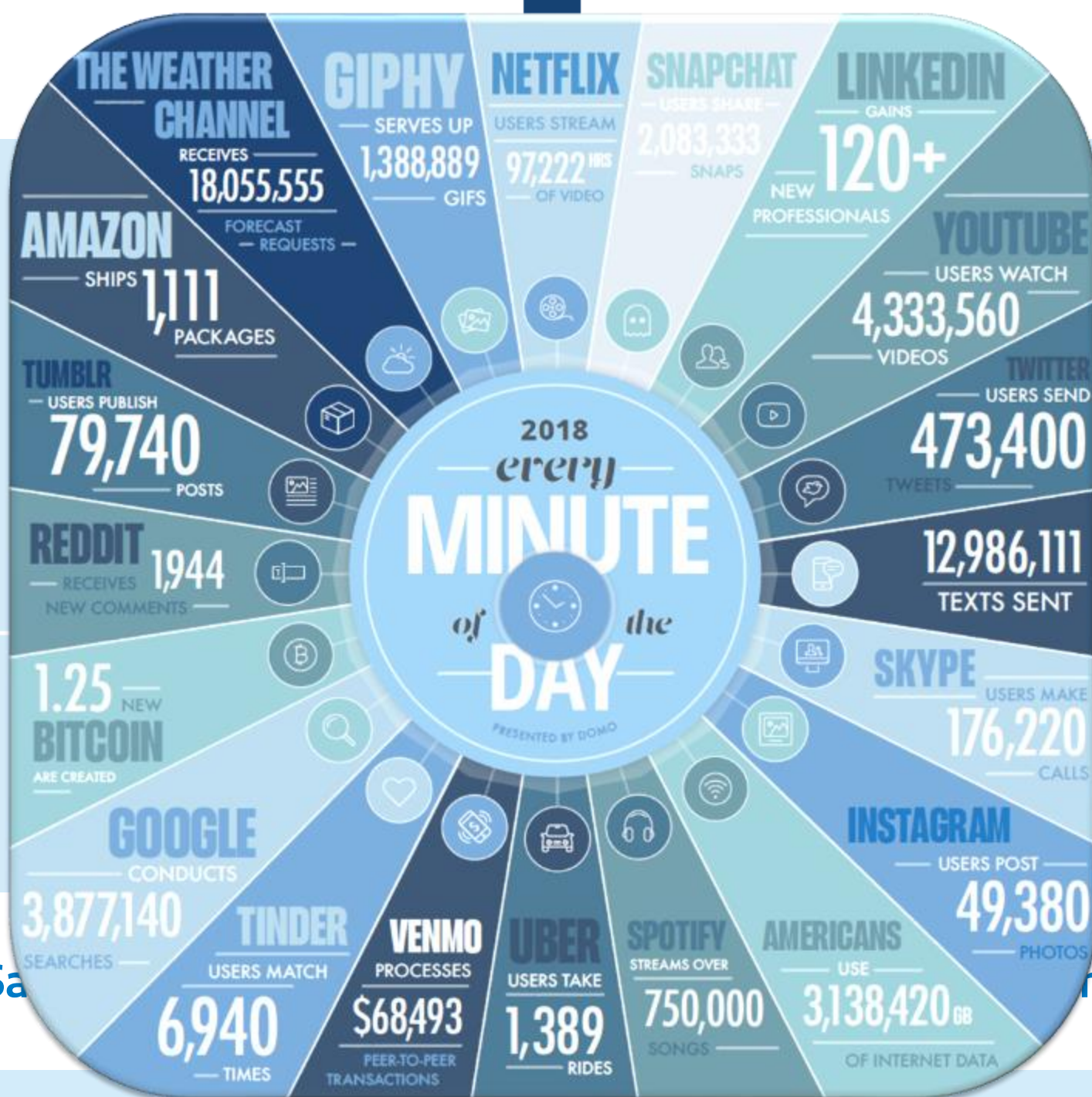






4 2 5 0 6 9 3 5 2 6 0 6 0 4 5 3 6 2 7 0 3 4 2 5 0 6 9 3
2 0 3 3 6 5 0 2 0 3 4 6 6 0 3 2 4 4 7 6 9 2 0 3 3 6 5 0
3 4 2 5 0 6 0 3 5 2 6 0 6 0 4 5 3 6 2 7 9 3 4 2 5 0 6 0
6 0 5 2 4 3 0 6 0 6 2 5 3 0 7 2 6 3 5 4 9 6 0 5 2 4 3 0
4 2 5 0 6 9 3 5 3 4 2 5 0 6 9 3

Samenleving volledig afhankelijk van digitaal fundament



San

nt

International Transportation Systems Crippled by "Notpetya" Ransomware

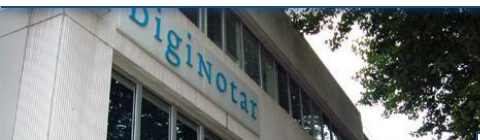
SMITH
LEATH

USA | July 25 2017

In the second major cyber attack in as many months, transportation giants A.P. Moller-Maersk Group ("Maersk") and TNT Express B.V. ("TNT") (now part of the

Nationale Politie ziet toename 'ceo-fraude'

Ruim 430 Nederlandse bedrijven zijn de afgelopen twee weken doelwit geweest van zogeheten ceo-fraude. Dat zegt de Nationale Politie [tegenover BNR](#).



Hack on Saudi Aramco hit 30,000 oil firm admits

First hacktivist-style assault to use malware?



OPM hack: 21 million people's information stolen, federal

- OPM background check applicants since 2000 'highly likely' to be affected
- Office of Personnel Management computer networks infiltrated in late 2015



Dyn

Aanval uitgevoerd door 'slimme apparaten'

MIVD verijdelde Russische cyberaanval op OPCW in Den Haag

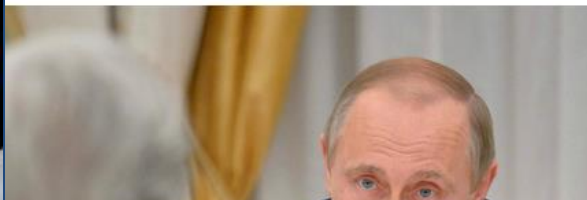
Vier agenten van de militaire inlichtingendienst GROe waren afgelopen april van plan binnen te dringen in het wifi-netwerk van de OPCW. Ze zijn het land uit gezet.

Liza van Lonkhuyzen & Vincent Sondermeijer | 4 oktober 2018



Alleged Russian involvement in DNC hack gives U.S. a taste of Kremlin meddling

DigiD



Warns That Ransomware is a Real Threat

in September 29, 2016 in **Device Security**

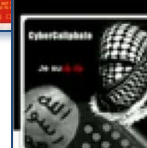
bedrijf

HLEY
ADISON®



CYBERCALIPHATE

Je suis IS



TV5MONDE
Réseau de Télévision

Journal À propos Photos TV5MONDE+ Plus +





CW Hacker hijacks wireless...

www.computerworld.com/article/2878741/hacker-hijacks-wireless-foscam-l

Search

DON'T MISS: Excel 2016 cheat sheet · Do IT certifications matter? · Microsoft pulls plug on Win 10's debut version · Newsletters

COMPUTERWORLD
FROM IDG

INSIDER Sign In | Register

Home > Security > Cybercrime & Hacking



SECURITY IS SEXY
By Darlene Storm, Computerworld | FEB 2, 2015 12:09 PM PT

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hacker hijacks wireless Foscam baby monitor, talks and freaks out nanny

This is the third time news has circulated about some jerk hijacking a wireless Foscam camera/baby monitor and made his virtual intrusion known by talking. Please change the default password!





MORE LIKE THIS

Hacker strikes again: Creep hijacks baby monitor to stream at infant and...

Populaire babyfoons en beveiligingscamera's lek, meekijken mogelijk

12 juli 2018 10:25

Aangepast: 12 juli 2018 11:14

Beeld © iStock



Een beveiligingscamera houdt een baby in de gaten (stockbeeld).

Babyfoons en beveiligingscamera's van het Chinese merk Foscam zijn

INFOSECURITY MAGAZINE

[HOME](#)[NIEUWS »](#)[BLOGS »](#)[VIDEO](#)[AGENDA](#)[VACATURES](#)[MAGAZINE »](#)[ABC](#)

Meekijken bij duizenden IP-beveiligingscamera's



4 november 2014



[Nieuws](#)



Wereldwijd worden duizenden IP-beveiligingscamera's gebruikt om woningen, bedrijfspanden en andere objecten te bewaken. De camera's zijn vaak niet of slecht beveiligd, waardoor de eigenaren door kwaadwillenden eenvoudig kunnen worden bespioneerd. Om dit probleem aan te tonen zijn op de website Insecam.com duizenden slecht of niet beveiligde IP-beveiligingscamera's verzameld, waarop iedereen kan meekijken.



Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ict te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.

**On December 23rd, 2015,
hackers caused a blackout
for roughly a quarter
million Ukrainians.**

**Sabotage en verstoring door staten
grootste dreiging voor de nationale veiligheid**



BBC

 Sign in

News

Sport

Weather

Shop

Earth

Travel

NEWS

Home

UK

World

Business

Politics

Tech

Science

Health

Family & Education

Health

NHS cyber-attack: GPs and hospitals hit by ransomware

🕒 13 May 2017



 Share





Aanvalsmiddelen eenvoudig toegankelijk



RAGE BOOTER

[HOME](#)[ABOUT US](#)[PLANS & PRICING](#)

FEATURES

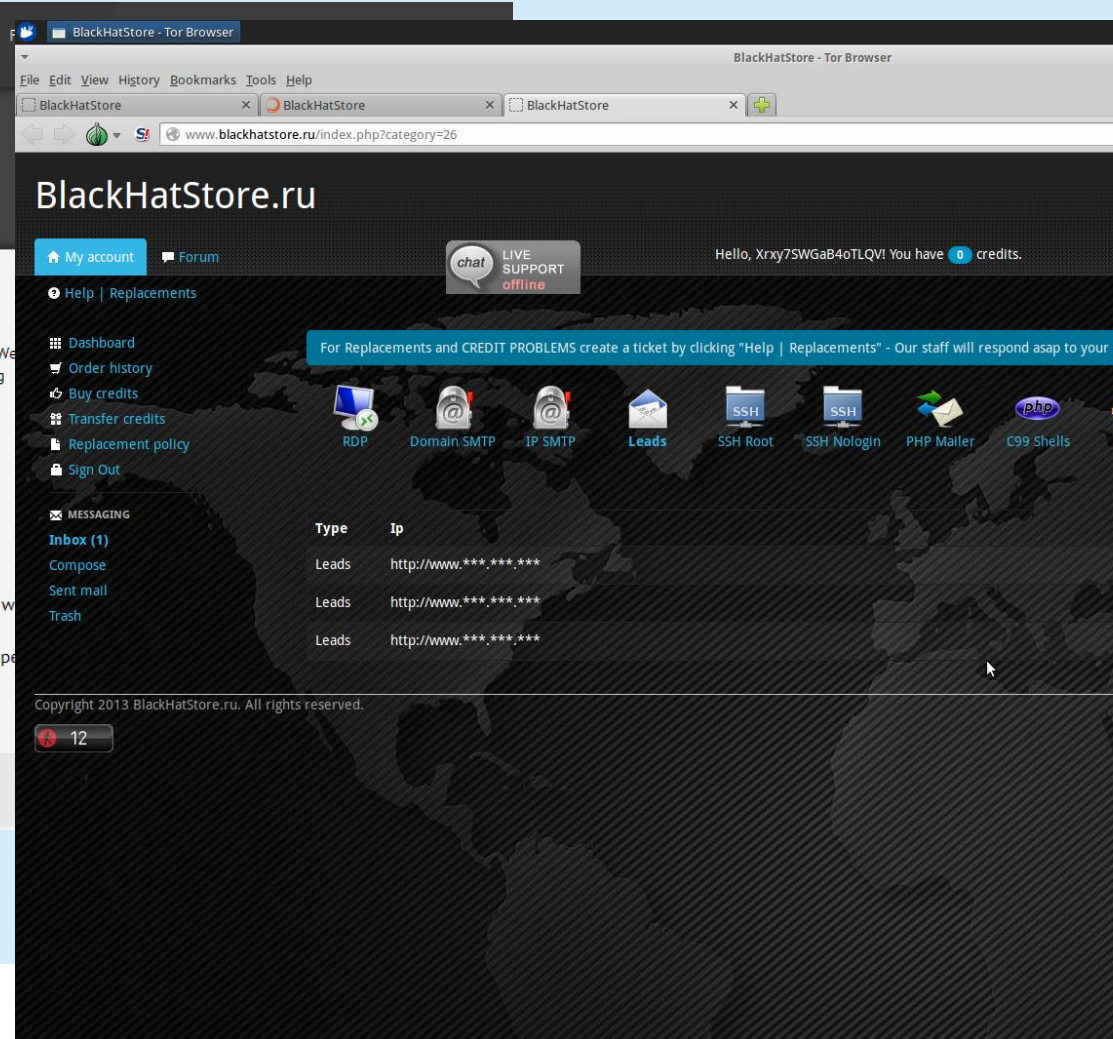
- Unlimited Testing
- Great User Experience
- 24/7 Live Support
- Easy Customizable
- Flexible Pricing
- VIP Support
- Affordable Plans
- Money Back Guarantee

Excellent Stress Testing Services!

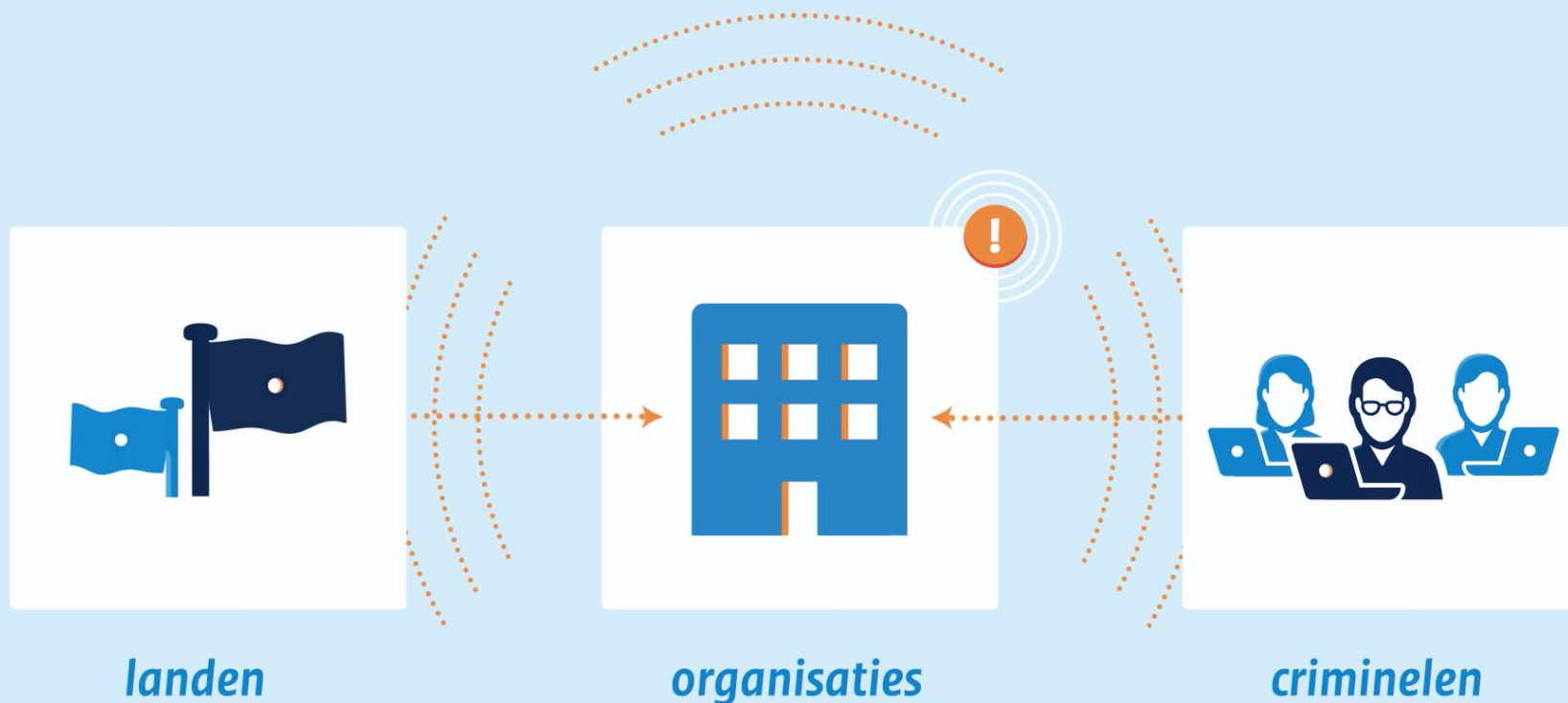
With Rage Booter, you never have to worry about power! We monitor our servers 24/7 to provide you a pure and strong attack to any target.

- ✓ Fast and Secure Stress Testing!
- ✓ Ticket & Live Support!
- ✓ A Variety of revolvers from Cloudflare to Skype, w
- ✓ We have been open since 2010 so you can feel pe

IF YOU HAVE ANY QUESTIONS?



Aanvalsmiddelen eenvoudig toegankelijk



Aanvallers blijven succesvol door ontbreken basismaatregelen

Hack kost Maersk honderden miljoenen

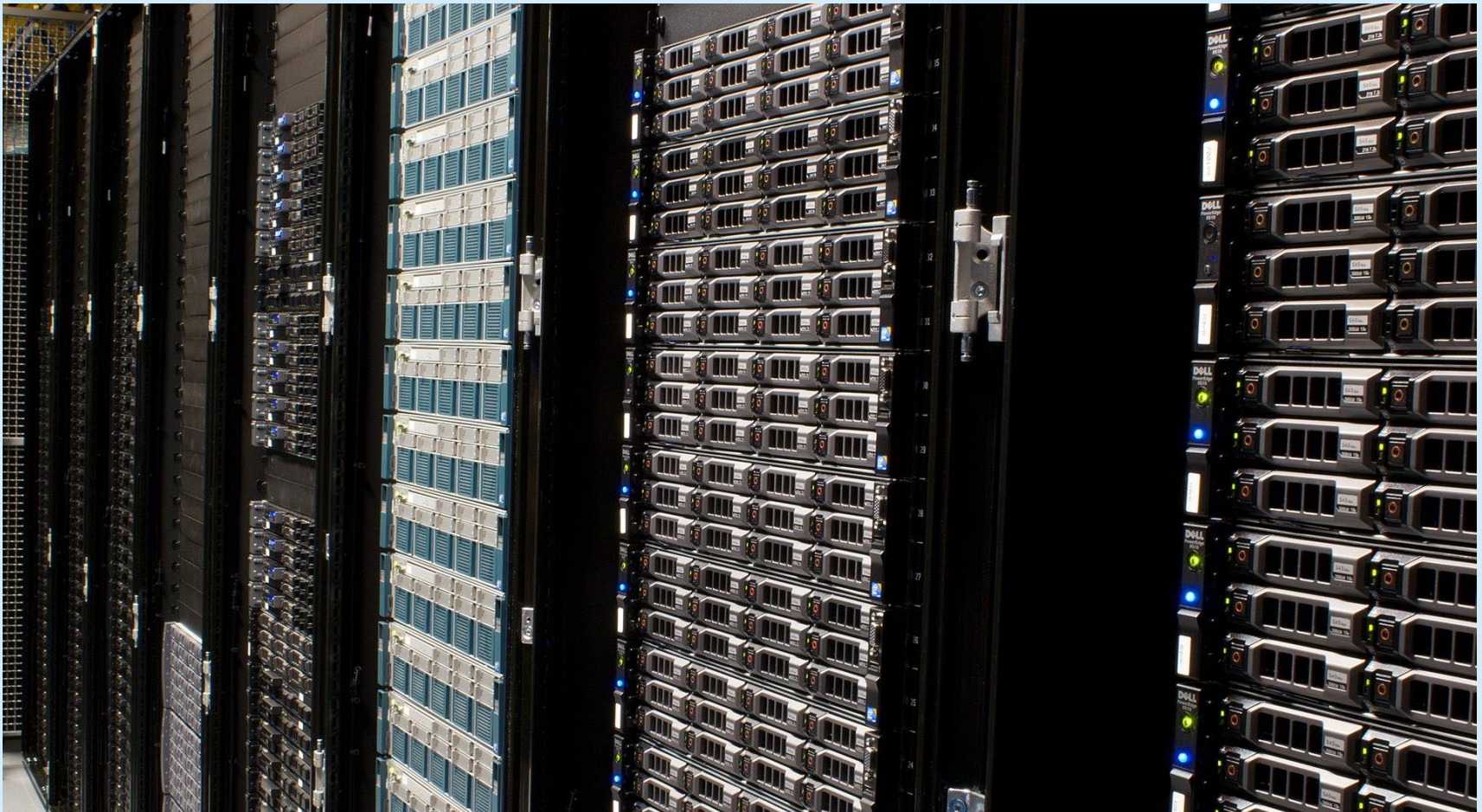
De cyberaanval van eind juni dit jaar kost de Deense rederij 200 tot 300 miljoen dollar, zei het woensdag bij de presentatie van de kwartaalcijfers.

Wouter van Noort 16 augustus 2017





Onveilige producten en diensten achilleshiel digitale veiligheid



Hoe veel systeembeheerders stel je aan voor een serverpark van een paar honderd servers?

Smart Buildings

A Back Door for Hackers?

Connected Building Systems Fly under the Cybersecurity Radar, Creating "Shadow IoT"

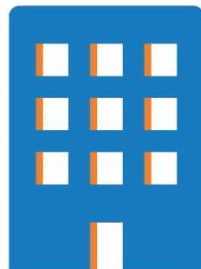


Smart Building Risks

Based on IBM Security analysis of real-world Smart Building automation systems



En hoe veel voor een paar honderd smart building nodes?



Tegengestelde belangen zorgen voor risico's op nationaal niveau

What should we do?

- Better practices for manufacturers?
- Free **secure** software stacks?
- International policy, regulation, certification?
- Clear up accountability issues?
- Generate market demand for secure products?
- Quarantine bad actors (e.g. at ISP)?
- Educate users?
- Empower users?

“Yes”

We need to do it all



Globale en lokale initiatieven

OTA IoT Trust Framework

The connected future is here - let's make a connected world that is secure.

The Internet of Things (IoT) offer consumers, businesses, and governments across the globe countless benefits. As is true with most emerging technology, however, there remain some significant challenges. The Online Trust Alliance (OTA), an Internet Society initiative, believes that through **leadership, innovation, and collaboration**, we can overcome these challenges and create a safer and more trustworthy connected world. This requires a shared responsibility including industry embracing security and privacy by design, and adopting responsible privacy practices.

IoT Trust Framework - Summary

IoT Trust by Design

The Internet Society's IoT Trust Framework identifies the core requirements manufacturers, service providers, distributors/purchasers and policymakers



Internal Market, Industry, Entrepreneurship and SMEs

Radio Equipment Directive (RED)

The Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market. It ensures a Single Market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software.

The RED aligned the previous Directive, the Radio and Telecommunication Terminal Equipment Directive (1999/5/EC (RATTE)), with the new regulatory framework for the marketing of products.

The revision also took account of the need for improved market surveillance. In particular, for the traceability obligations of manufacturers, importers and distributors. It has improved market surveillance instruments. One example is the possibility for required pre-registration of radio equipment in categories with low compliance levels.

The RED was published in the OJEU on 22 May 2014, entered into force on 11 June 2014 and is applicable as of 13 June 2016. It included a one-year transitional period, which ended on 12 June 2017 (Article 48). During the transitional phase, manufacturers were allowed to place on the market radio equipment compliant with either the RED or the EU legislation applicable before 13 June 2016 (e.g. RATTE).

For more details on the application of the RED, see the RED Guide under the Guidance section below.

Committee (TCAM)

Article 45 of the RED establishes the Telecommunication Conformity Assessment and Market Surveillance Committee (TCAM), a committee related to Regulation (EU) No 1024/2011. TCAM gives its opinion on proposed implementing acts under the RED, to discuss the application of the Directive when issues are raised either by its chair or by

Home - Blogs en Nieuws - Naar geautomatiseerde DDoS-bescherming met MUD

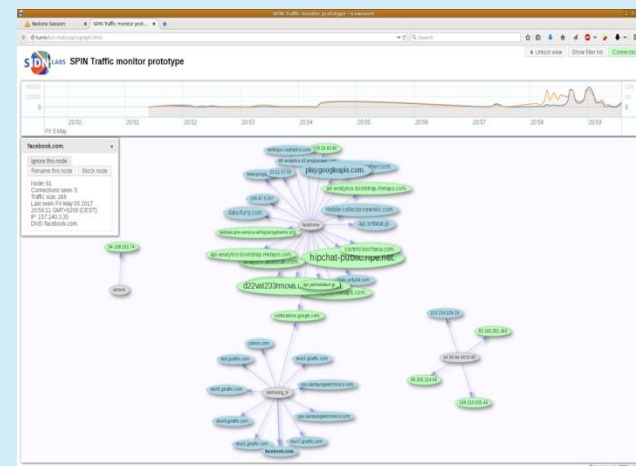
Naar geautomatiseerde DDoS-bescherming met MUD

Gepubliceerd op: maandag 29 oktober 2018

Onveilige Internet of Things apparaten (IoT-apparaten) worden gebruikt om Distributed Denial of Service (DDoS) aanvallen uit te voeren. Een bekend voorbeeld hiervan is de Mirai-botnet aanval op DNS-operator Dyn, die leidde tot grootschalige uitval van DNS-diensten. Om het schadelijke van onveilige IoT-apparaten te beperken, lanceerde SIDN Labs het SPIN-project. Hierbij evalueerden we de bruikbaarheid van de Manufacturer Usage Description (MUD) specificatie, die momenteel wordt ontwikkeld door de Operations and Management Area Working Group (OPSAWG) binnen de Internet Engineering Task Force (IETF).

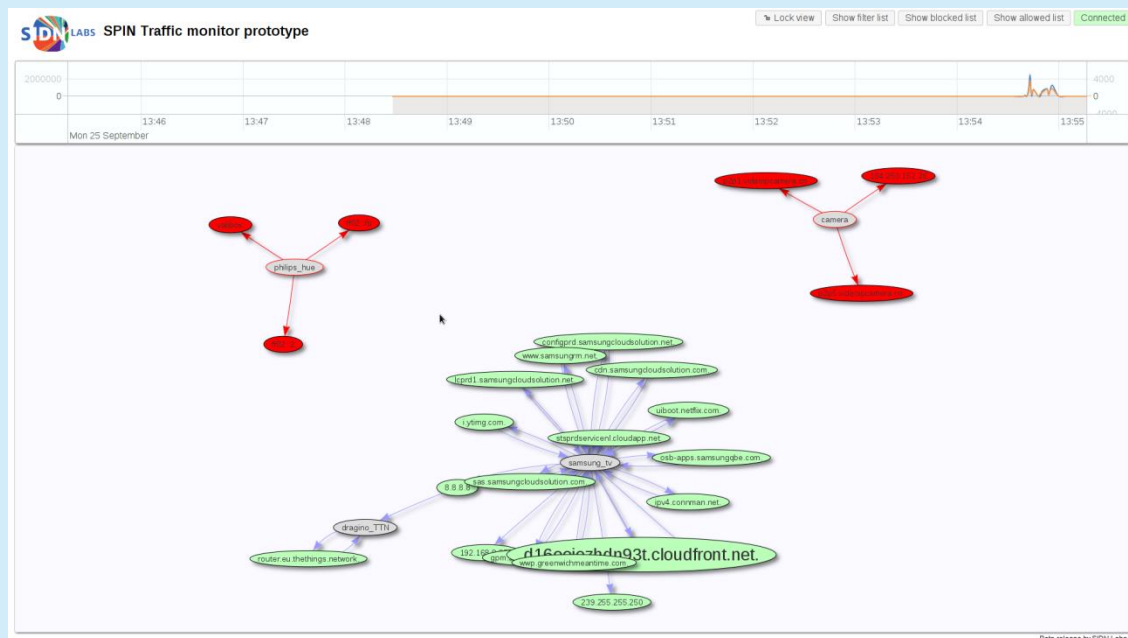
De achterliggende gedachte hierbij is dat wanneer een IoT-apparaat verbinding zoekt met een netwerk, het apparaat doorgeeft welke resources het nodig heeft om goed te kunnen functioneren. Deze informatie wordt vastgelegd in een *MUD-profiel*, dat het beoogde netwerkgedrag van het apparaat beschrijft op basis van een 'whitelist'. Deze whitelist zou compleet moeten zijn en dus kan de toegang tot andere netwerkresources worden geweigerd zonder dat dit de goede werking van het apparaat belemmert.

In dit onderzoek bestudeerden we de toepasbaarheid van MUD voor het beveiligen van IoT-apparaten tegen hackpogingen. Ook onderzochten we of de bruikbaarheid van IoT-apparaten voor DDoS-aanvallen afneemt door een profiel te handhaven. De MUD-specificatie is echter nog niet klaar voor gebruik en dus nog merendeels geïmplementeerd. Om MUD-profielen te



Het SPIN project bij SIDN Labs

- Security and Privacy for In-home Networks
- Onderzoek en prototype SPIN functies:
 - Dataverkeer visualiseren
 - Automatisch blokkeren
 - ‘Goed’ verkeer doorlaten
 - Deelplatform voor apparaatinfo







We leven in een glazen paleis...

...omgeven door apen en vijanden...

...met stenen en rotsen!



Maatschappelijke & econmische voordelen IoT...
...vooraf rekening houden met...
...privacy, digitale veiligheid en duurzaamheid