The compelling case for vulnerability management

And why the LIR is a key factor

M. Steltman - RIPE79 – 16-10-2019

deVolkskrant

Voorpagina | Nieuws & Achtergrond | Columns & Opinie | Video | Wetenschap | Mensen | De Gids | Cultuur & Media | Foto | Economie | Sport

RECONSTRUCTIE PULSE SECURE

Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open

tweakers Nieuws Reviews Pricewatch

Zoek naar nieuws

'Netwerken KLM en Shell w door ongepatcht vpn-lek'

De interne netwerken van verscheidene grote bedrijven lij geweest voor kwaadwillenden door een lek in de vpn-soft beschikbaar die het lek verhelpt, maar die was niet geïnst

Dat meldt De Volkskrant zaterdag op basis van vertrouwelijke expert bij het Nationaal Cyber Security Center. Nog altijd zoud is niet duidelijk om welke bedrijven en organisaties het precies gaat. Wel is De Volkskrant erachter gekomen dat bedrijven zoals KLM, Shell en Luchtverkeersleiding Nederland kwetsbaar waren en kwaadwillenden via misbruik van de vpn binnen konden komen op de interne netwerken.

TEST AND MEASUREMENT

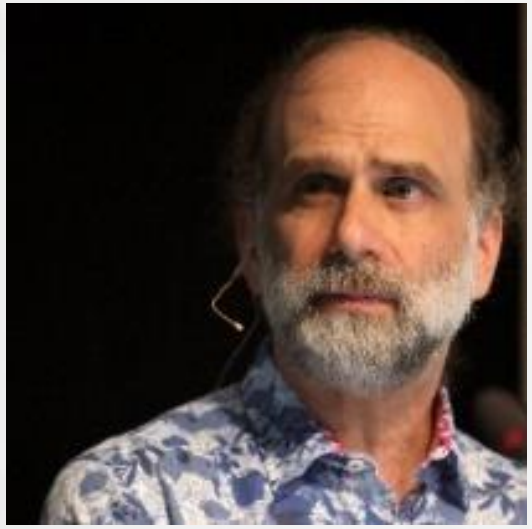
Study Finds Utility Industry Vulnerable to Cyber Attacks

A recent study assesses the utility industry's risk, readiness, and solutions to secure operational technology on the grid and recommends action to help utilities combat cyber threats.

DHS Alerts to Targeted Em

Last week, the Depart from Microsoft and U are targeting VPN vuln

Why are we vulnerable ?



“We are vulnerable, because hard- and software has vulnerabilities.
The bad guys find them and use them for themselves.
So we need good guys to find them too, and then fix those leaks. It’s all we have”

Bruce Schneier

So, why don’t we just patch?

5 Keep your devices and software up to date

No matter which phones, tablets, laptops or computers your organisation is using, it’s important they are kept up to date at all times. This is true for both Operating Systems and installed apps or software. Happily, doing so is quick, easy, and free.

Also known as ‘Patching’

UNITED STATES NEWS REVIEWS EVENTS AND AWARDS PROGRAMS NEWSLETTERS VIDEO RESOURCE LIBRARY

Home > Security > Data Security

ANALYSIS

Zero-days aren’t the problem -- patches are

Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

THE CONVERSATION

Academic rigour, journalistic flair

Arts + Culture Business + Economy Cities Education Environment + Energy Health + Medicine Politics + Society

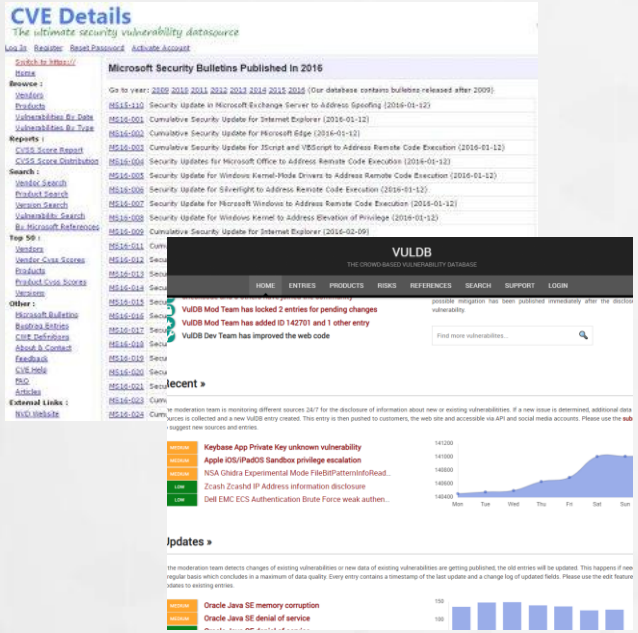
Why don’t big companies keep their computer systems up-to-date?

September 26, 2017 4.19pm BST

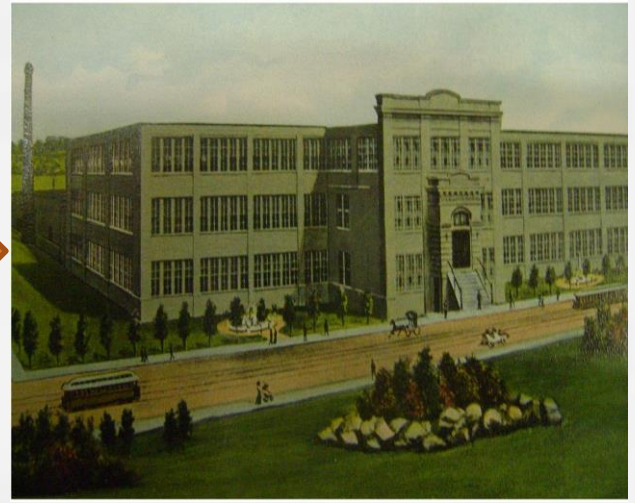
Security Center > How To > 5 reasons why general software updates and patches are important

5 reasons why general software updates and patches are important

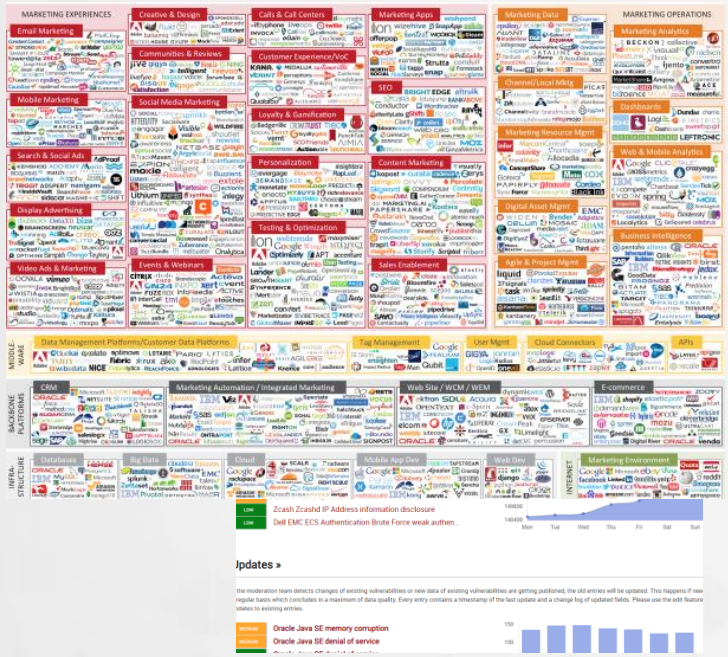
The patching process for companies explained



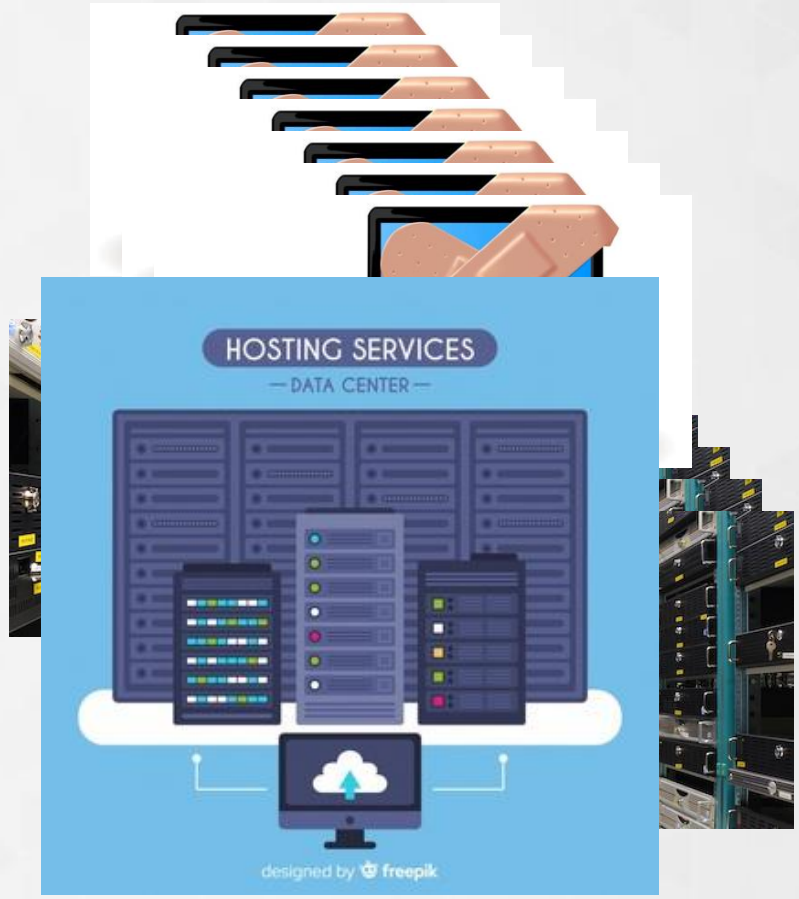
?



Sounds easy but hard to achieve 100%

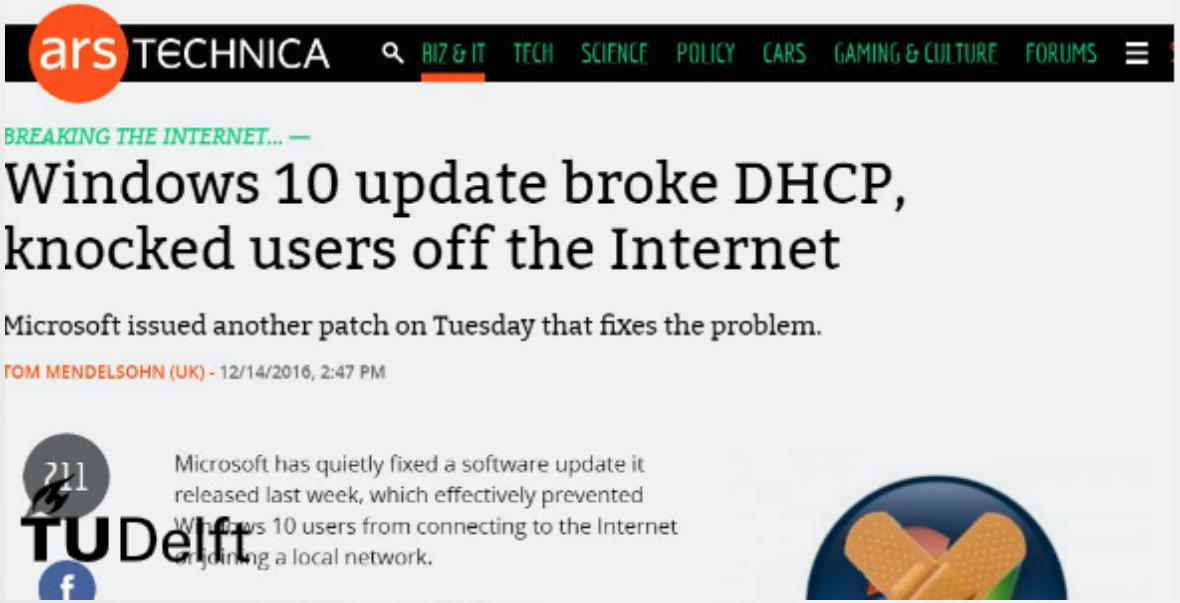


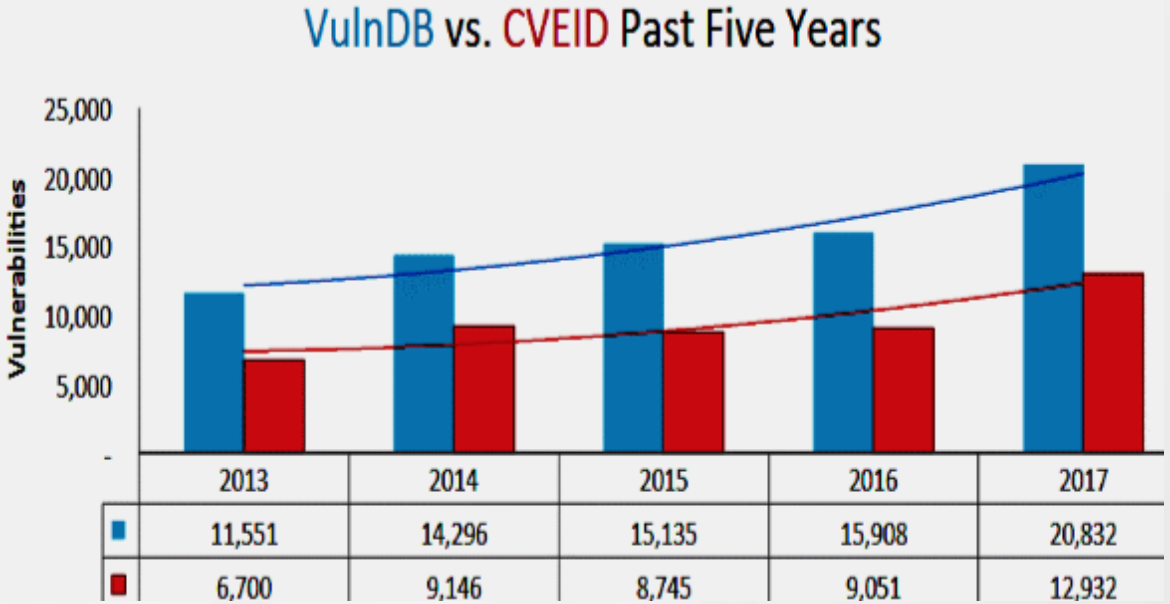
?



It's about economics, stupid

- Patching breaks things. Study at major network operator found that leading cause of outages was: patching.
- Over 20k vulnerabilities reported in 2017. Most are never exploited. CVSS critical score tells you nothing.





Plan B: Coordinated responsible disclosure / Bug bou

presence

Common approach: “Motivate”

Healthcare

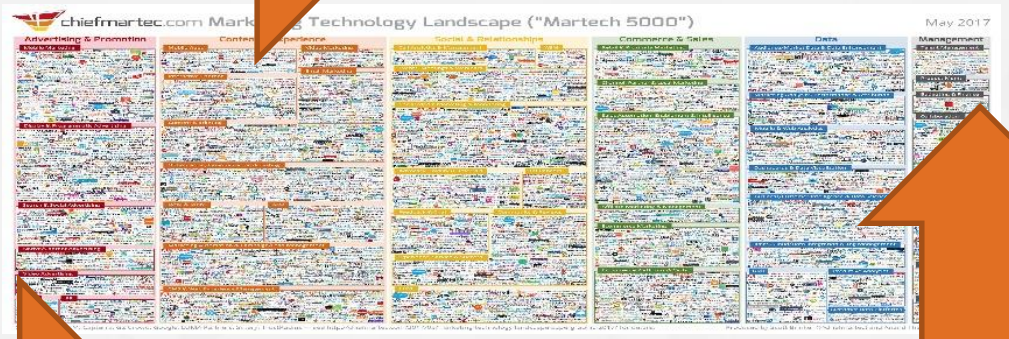
Financial services

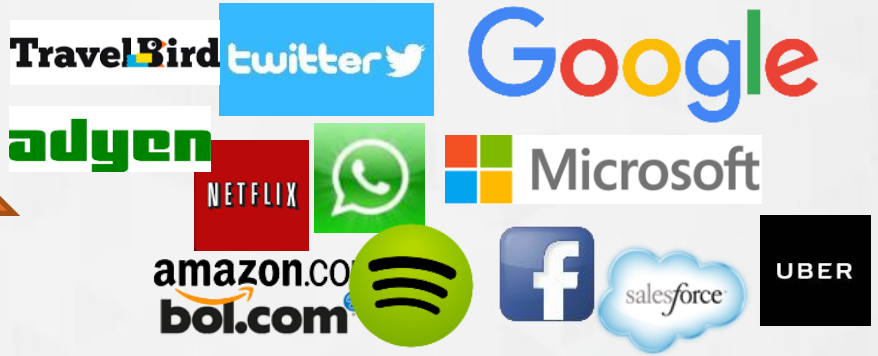
Retail

Government

Mobility

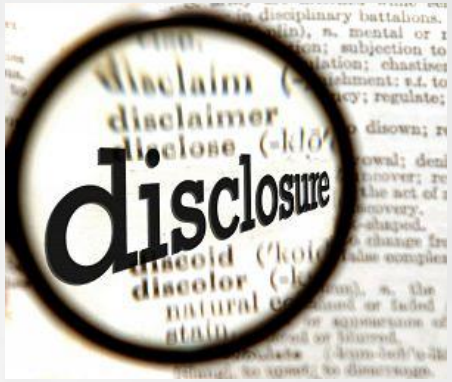
Digital Services

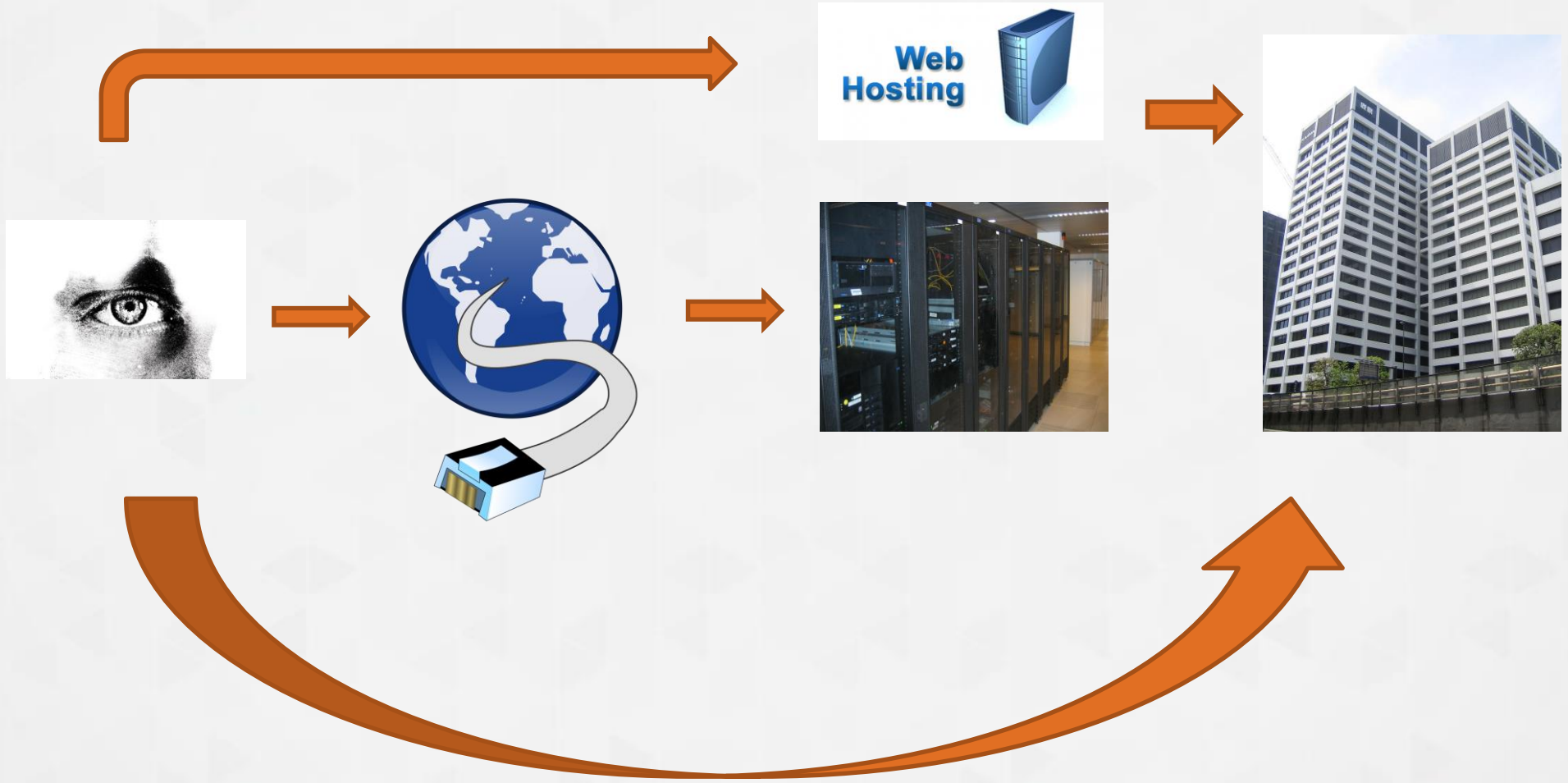




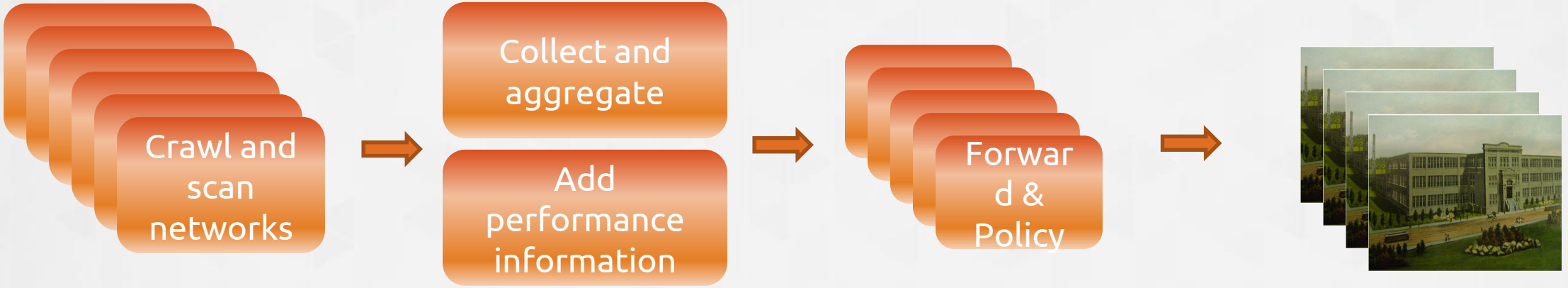
Add: Find and report

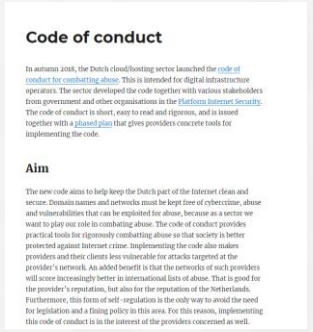
Coordinated responsible disclosure





=> towards: CRD on steroids





Code of conduct

In autumn 2018, the Dutch cloud/hosting sector launched the code of conduct for combatting abuse. This is intended for digital infrastructure operators. The sector developed the code together with various stakeholders from government and other organisations in the Platform Internet Security. The code of conduct is short, easy to read and rigorous, and is issued together with a phased plan that gives providers concrete tools for implementing the code.

Aim

The new code aims to help keep the Dutch part of the Internet clean and secure. Domain names and networks must be kept free of cybercrime, abuse and vulnerabilities that can be exploited for abuse, because as a sector we want to play our role in combating abuse. The code of conduct provides practical tools for rigorously combatting abuse so that society is better protected against Internet crime. Implementing the code also makes providers and their clients less vulnerable for attacks targeted at the provider's network. An added benefit is that the networks of such providers will score increasingly better in international lists of abuse. That is good for the provider's reputation, but also for the reputation of the Netherlands. Furthermore, this form of self-regulation is the only way to avoid the need for legislation and a fining policy in this area. For this reason, implementing this code of conduct is in the interest of the providers concerned as well.

What can and should LIRs do?

** Where does LIR responsibility start and stop **?

-> LIR is NOT responsible, but is (as other intermediaries) a key actor in getting this going

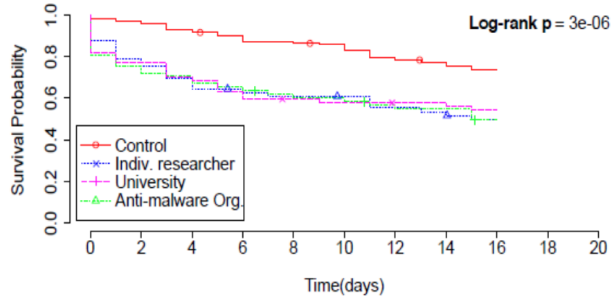
This goes way beyond ISP abuse mitigation!

-LIR (as ISP, hoster, CSP) is a key actor , the essential "middle man":

- **Monitor: Which badness is visible in my networks: vulnerabilities and abuse**
- **Receive: Subscribe to feeds, receive abuse- and vulnerability information**
- **Triage: Who has the actual problem, which user or cusromer?**
- **Forward: Who can and should fix this?**
- **Policy: "motivate" users / customers to act, or act yourself**

'Doing the right thing'

- Abuse reporting of malicious sites: voluntary clean up by providers



Questions for RIPE community / LIRs

- Do you agree that this “actual vulnerability”approach can be very effective?
- Do you agree that the LIR is a key middleman in this approach?

Concrete actions for such LIRs, what can you already do NOW:

- **Start with this mindset**
- **Update your policies, accept code of conduct NtD and Abuse**
- **Be reachable !**
- **Subscribe to offered aggregated feeds**
- **Forward info and act , to customers / users**
    - **Using standard OSS systems such as Abuse-IO**

- If this initiative will start, are YOU prepared to participate ?

The current approach : motivate companies to patch 100%, is insufficient

The solution: Find ACTUAL leaks, aggregate, add performance info

Then forward to those who can fix– or who can make someone fix

In NL:

All we need is already there! Just need to go on steroids

Gov: (NCSC): please take the lead, connect the dots

Providers / LIRS: Adopt the CoC , connect to NBIP and start making a difference

In your country: replicate the model

***** It is time to act, now! *****

Stichting
Digitale Infrastructuur
Nederland

www.dinl.nl