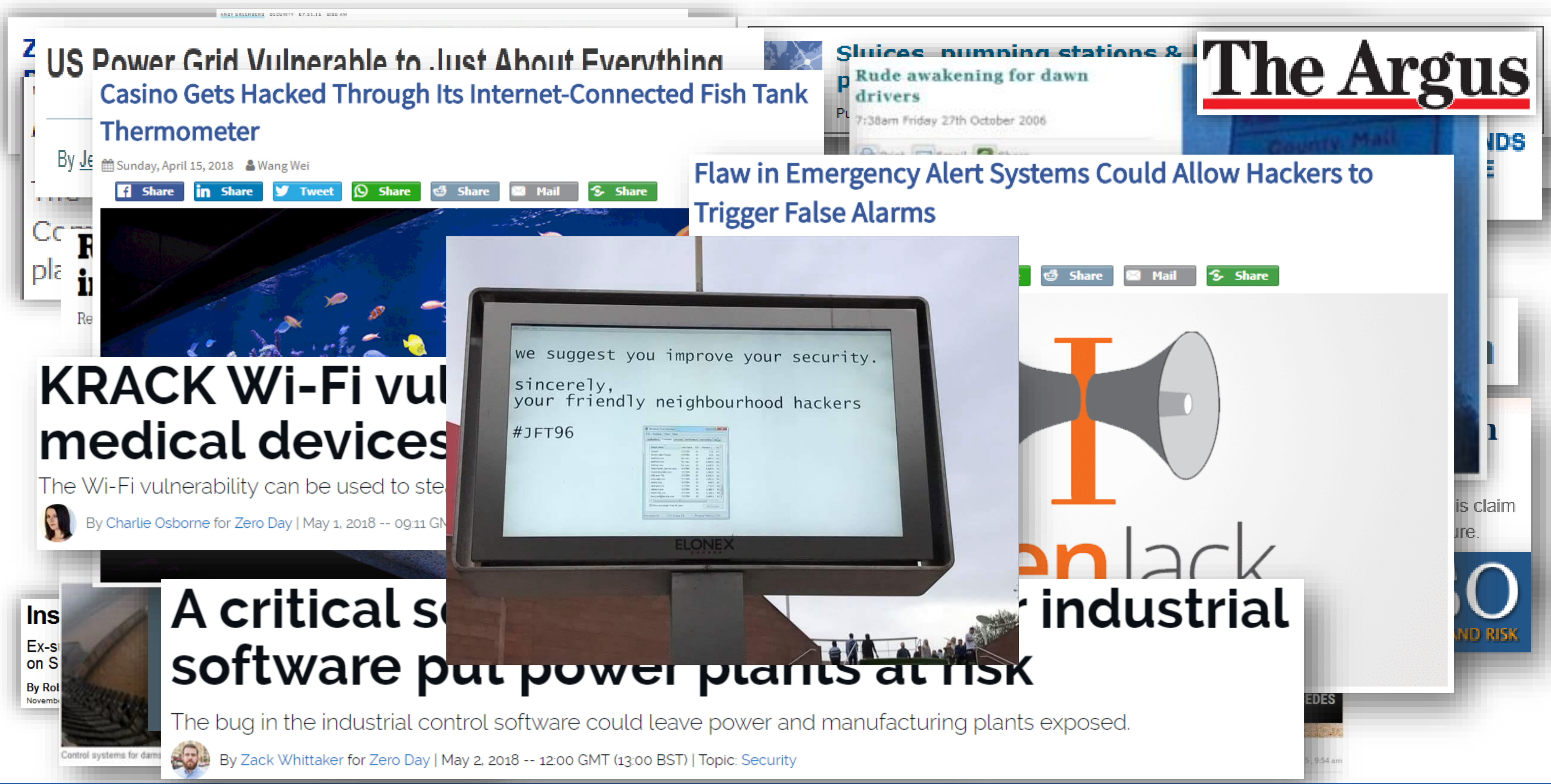
Still WTF…

About the insecurity of IoT



ANDY GREENBERG SECURITY 07.21.15 8:00 AM

US Power Grid Vulnerable to Just About Everything

Sluices, pumping stations &

Rude awakening for dawn drivers

7:38am Friday 27th October 2006

The Argus

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Flaw in Emergency Alert Systems Could Allow Hackers to Trigger False Alarms

KRACK Wi-Fi vul

medical devices

The Wi-Fi vulnerability can be used to ste

By Charlie Osborne for Zero Day | May 1, 2018 -- 09:11 GM

we suggest you improve your security.

sincerely,
your friendly neighbourhood hackers

#JFT96

A critical s industrial software put power plants at risk

The bug in the industrial control software could leave power and manufacturing plants exposed.

By Zack Whittaker for Zero Day | May 2, 2018 -- 12:00 GMT (13:00 BST) | Topic: Security

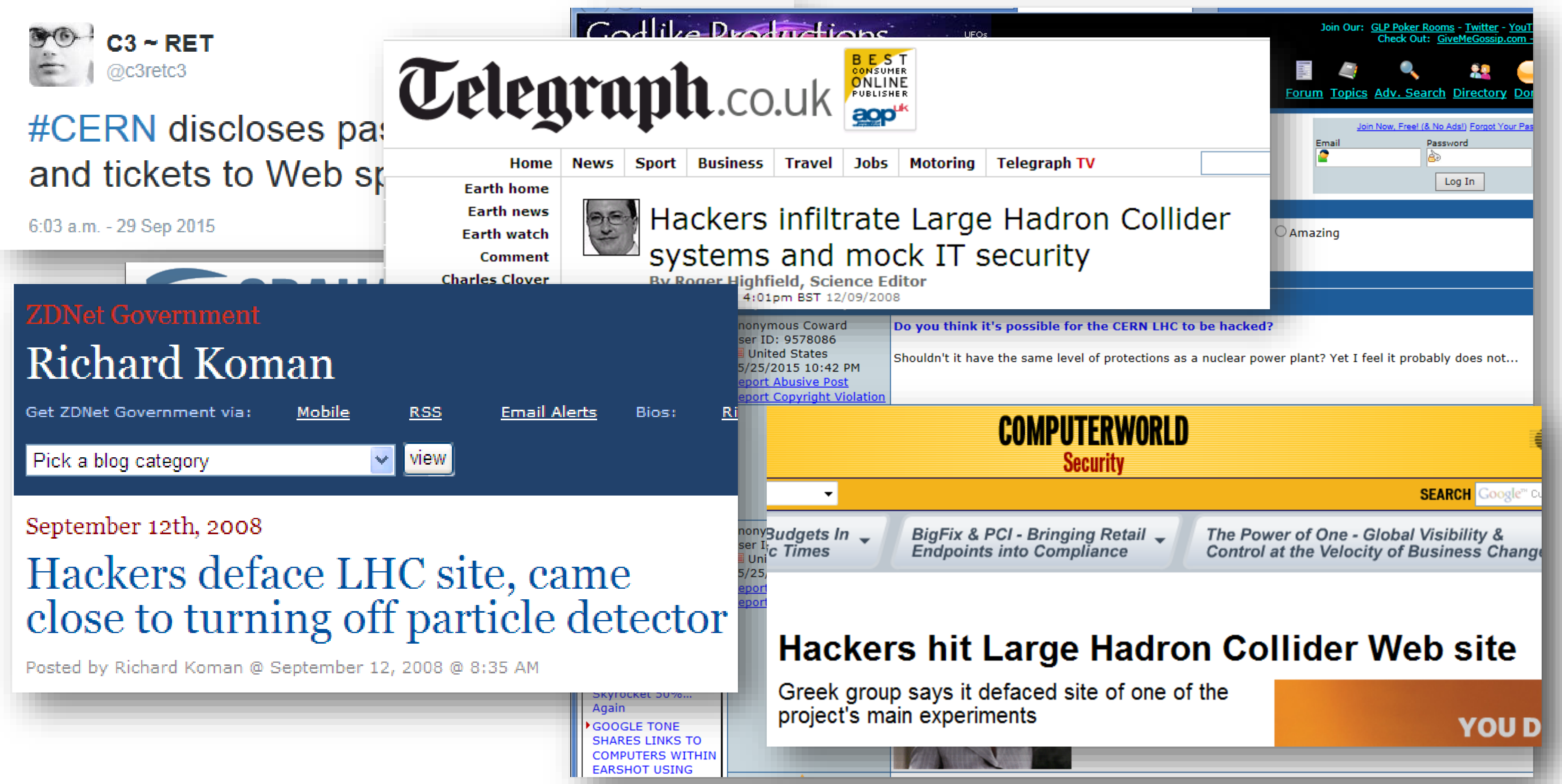
Control systems for dam

is claim

ure.

The Problem 2.0. 100% Fail. WTF.

CERN: Under attack like everyone else



C3 ~ RET
@c3retc3

#CERN discloses pa
and tickets to Web sp

6:03 a.m. - 29 Sep 2015

Telegraph.co.uk BEST CONSUMER ONLINE PUBLISHER aop uk

Home | News | Sport | Business | Travel | Jobs | Motoring | Telegraph TV

Earth home
Earth news
Earth watch
Comment
Charles Clover

Hackers infiltrate Large Hadron Collider systems and mock IT security

By Roger Highfield, Science Editor
4:01pm BST 12/09/2008

Godlike Productions UFOs

Join Our: GLP Poker Rooms - Twitter - YouT
Check Out: GiveMeGossip.com -

Forum Topics Adv. Search Directory Dor

Join Now, Free! (& No Ads!) Forgot Your Pas
Email
Password
Log In

○ Amazing

nonymous Coward
ser ID: 9578086
United States
5/25/2015 10:42 PM
eport Abusive Post
eport Copyright Violation

Do you think it's possible for the CERN LHC to be hacked?

Shouldn't it have the same level of protections as a nuclear power plant? Yet I feel it probably does not...

Skyrocket 50%...
Again
GOOGLE TONE SHARES LINKS TO COMPUTERS WITHIN EARSHOT USING

ZDNet Government

Richard Koman

Get ZDNet Government via: Mobile RSS Email Alerts Bios: Ri

Pick a blog category ⌄ view

September 12th, 2008

Hackers deface LHC site, came close to turning off particle detector

Posted by Richard Koman @ September 12, 2008 @ 8:35 AM

COMPUTERWORLD Security

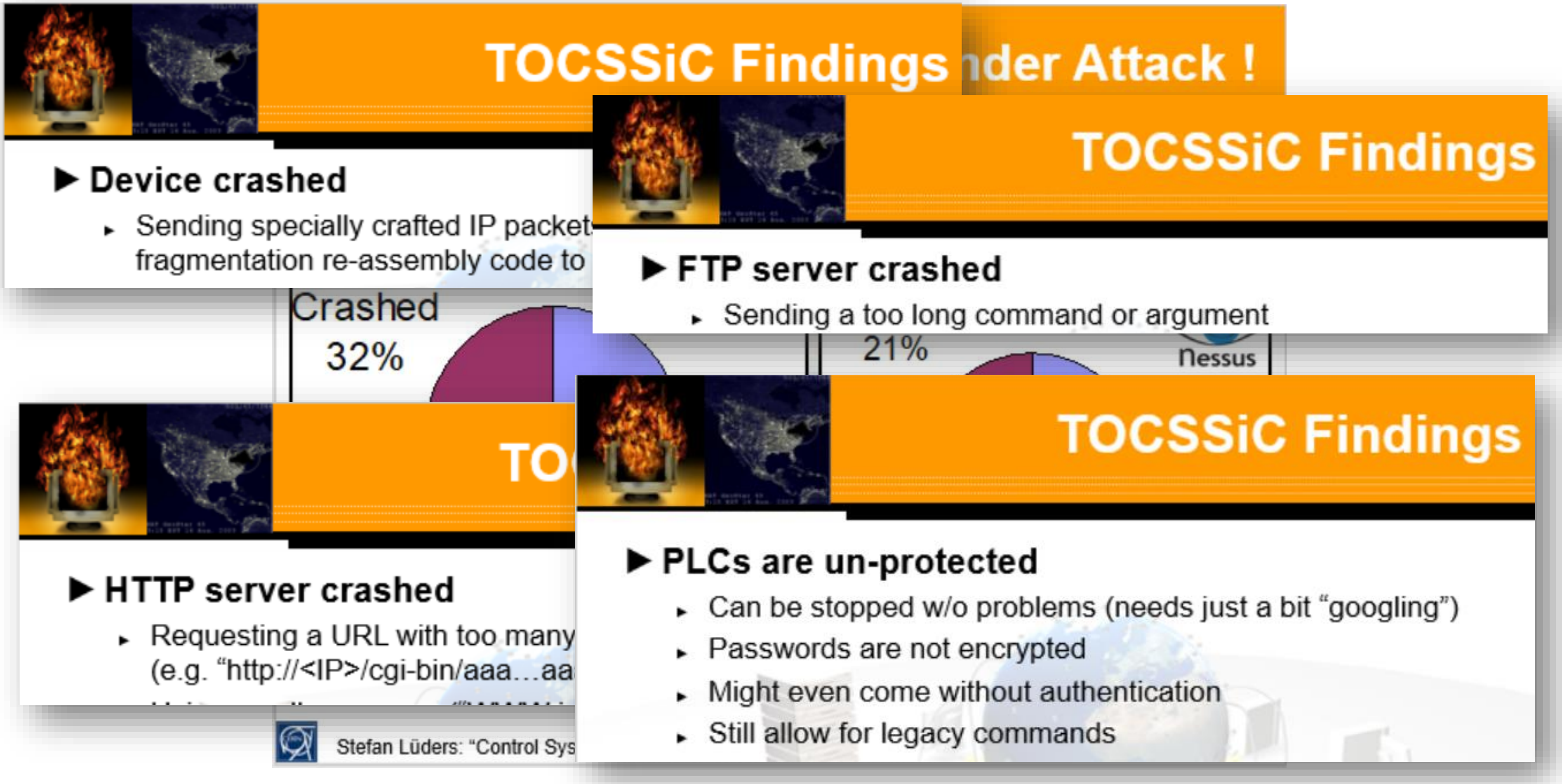
SEARCH Google

Budgets In c Times | BigFix & PCI - Bringing Retail Endpoints into Compliance | The Power of One - Global Visibility & Control at the Velocity of Business Chang

Hackers hit Large Hadron Collider Web site

Greek group says it defaced site of one of the project's main experiments

YOU D



TOCSSiC Findings

nder Attack !

- **Device crashed**
  - Sending specially crafted IP packet fragmentation re-assembly code to

Crashed
32%
21%
Nessus

TOCSSiC Findings

- **FTP server crashed**
  - Sending a too long command or argument

TO

- **HTTP server crashed**
  - Requesting a URL with too many (e.g. “http://<IP>/cgi-bin/aaa…aa

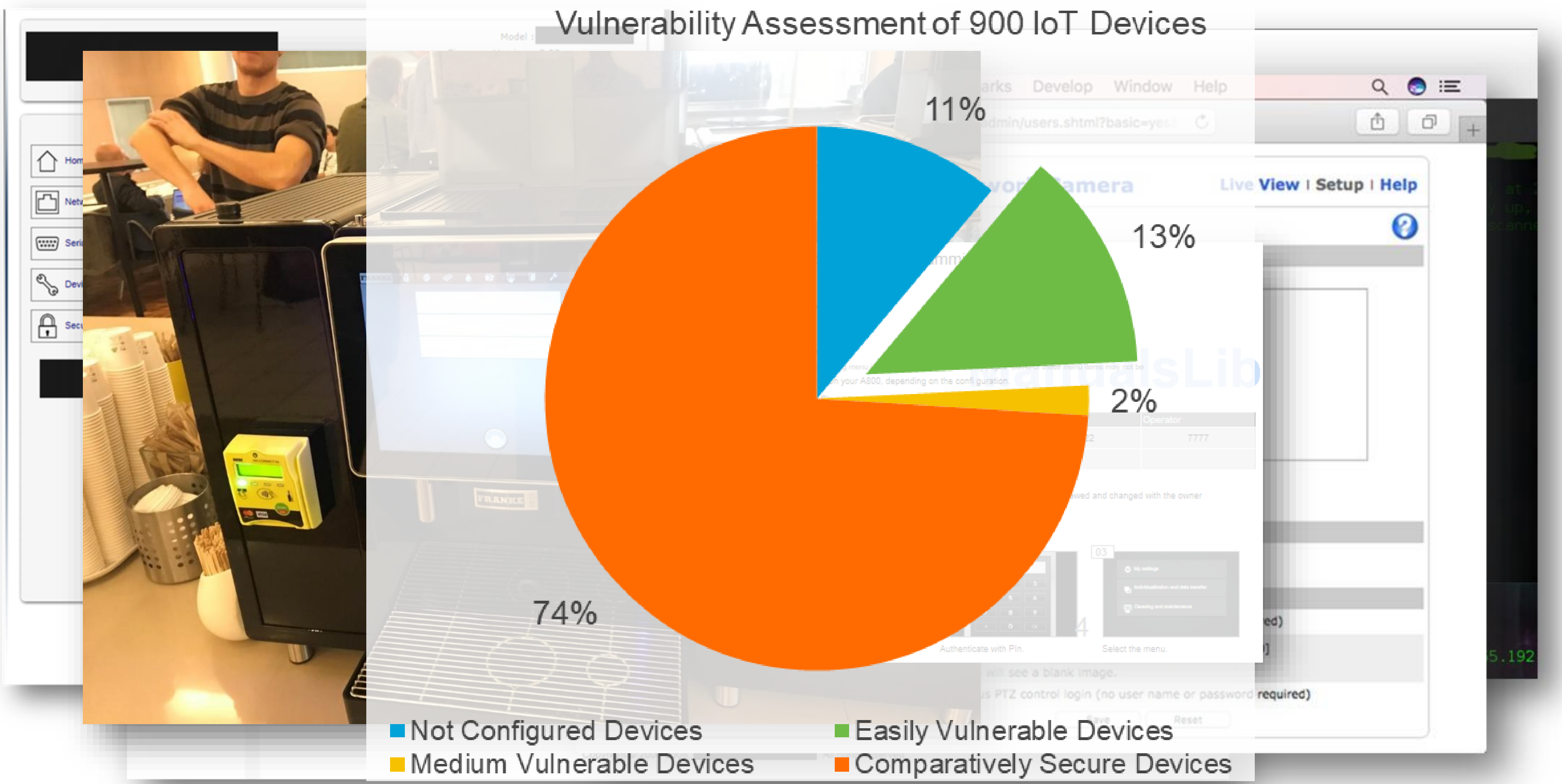
Stefan Lüders: “Control Sys

TOCSSiC Findings

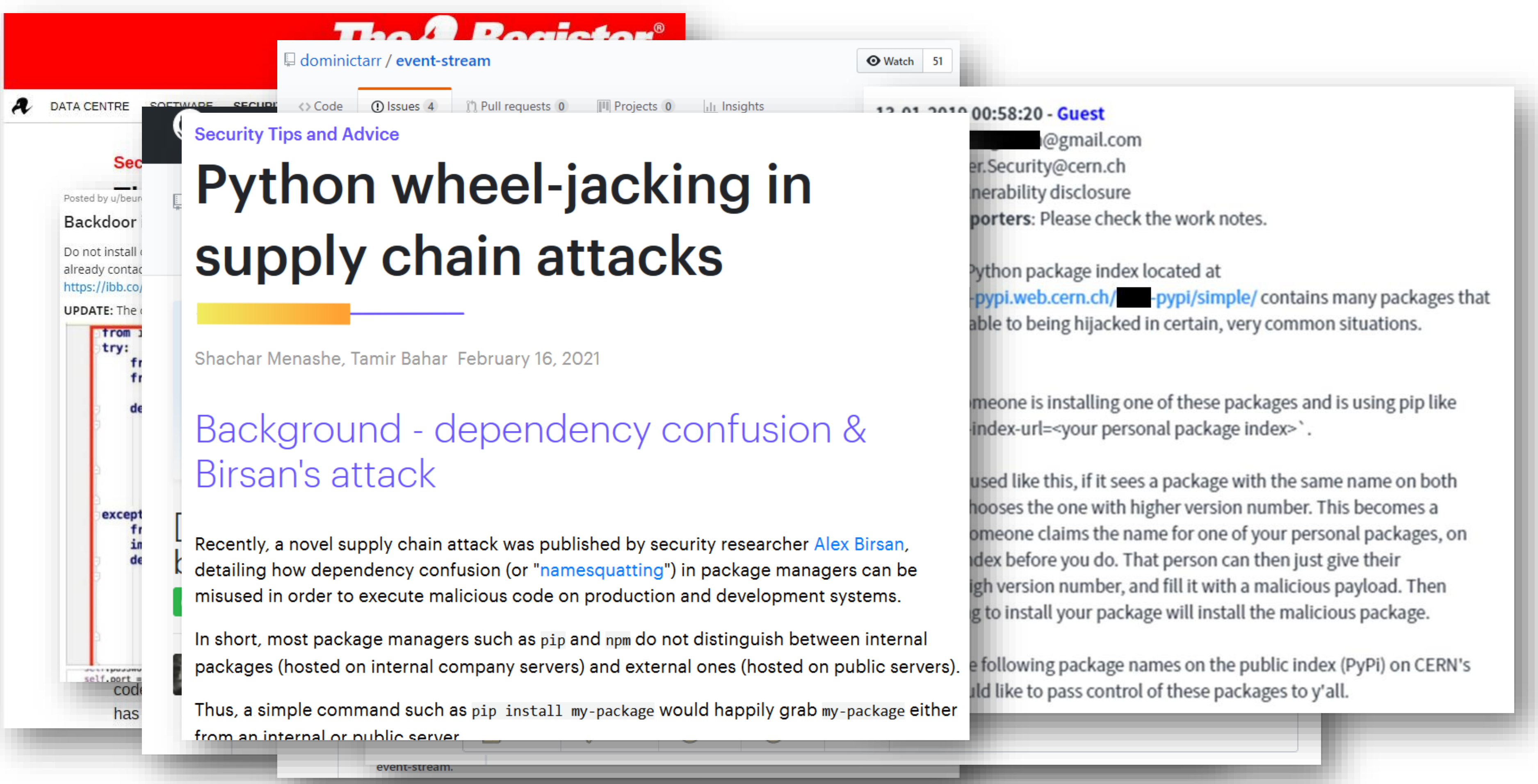
- **PLCs are un-protected**
  - Can be stopped w/o problems (needs just a bit “googling”)
  - Passwords are not encrypted
  - Might even come without authentication
  - Still allow for legacy commands

Emerging Threats? Not really

Vulnerability Assessment of 900 IoT Devices



(CERN's) Internet of Stupid Things



```
from i
try:
    fr
    fr

    de


except
    fr
    in
    de
```

Security Tips and Advice

Python wheel-jacking in supply chain attacks

Shachar Menashe, Tamir Bahar February 16, 2021

Background - dependency confusion & Birsan's attack

Recently, a novel supply chain attack was published by security researcher Alex Birsan, detailing how dependency confusion (or "namesquatting") in package managers can be misused in order to execute malicious code on production and development systems.

In short, most package managers such as `pip` and `npm` do not distinguish between internal packages (hosted on internal company servers) and external ones (hosted on public servers).

Thus, a simple command such as `pip install my-package` would happily grab `my-package` either from an internal or public server

13.01.2019 00:58:20 - Guest
[redacted]@gmail.com
er.Security@cern.ch
nerability disclosure
porters: Please check the work notes.

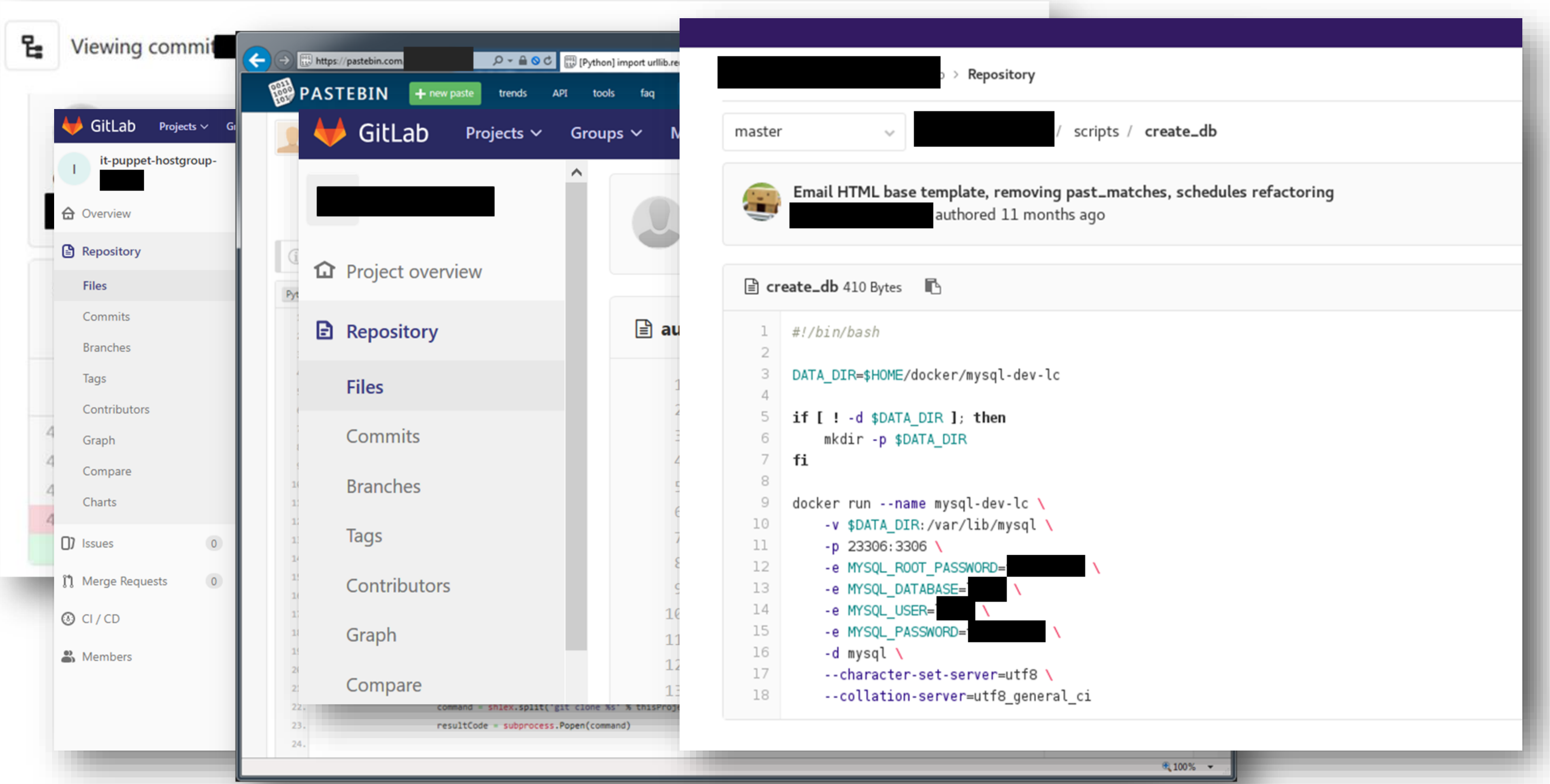
Python package index located at
-pypi.web.cern.ch/[redacted]-pypi/simple/ contains many packages that
able to being hijacked in certain, very common situations.

meone is installing one of these packages and is using pip like
index-url=<your personal package index>`.

used like this, if it sees a package with the same name on both
hooses the one with higher version number. This becomes a
omeone claims the name for one of your personal packages, on
dex before you do. That person can then just give their
igh version number, and fill it with a malicious payload. Then
g to install your package will install the malicious package.

e following package names on the public index (PyPi) on CERN's
ld like to pass control of these packages to y'all.

Internet of Stupid Dependencies



[redacted] > Repository

master [redacted] / scripts / create_db

Email HTML base template, removing past_matches, schedules refactoring

[redacted] authored 11 months ago

create_db 410 Bytes

```bash
#!/bin/bash

DATA_DIR=$HOME/docker/mysql-dev-lc

if [ ! -d $DATA_DIR ]; then
    mkdir -p $DATA_DIR
fi

docker run --name mysql-dev-lc \
    -v $DATA_DIR:/var/lib/mysql \
    -p 23306:3306 \
    -e MYSQL_ROOT_PASSWORD=[redacted] \
    -e MYSQL_DATABASE=[redacted] \
    -e MYSQL_USER=[redacted] \
    -e MYSQL_PASSWORD=[redacted] \
    -d mysql \
    --character-set-server=utf8 \
    --collation-server=utf8_general_ci
```

Internet of Stupid Developers

Exposure
Threats

Complexity
Vulnerabilities

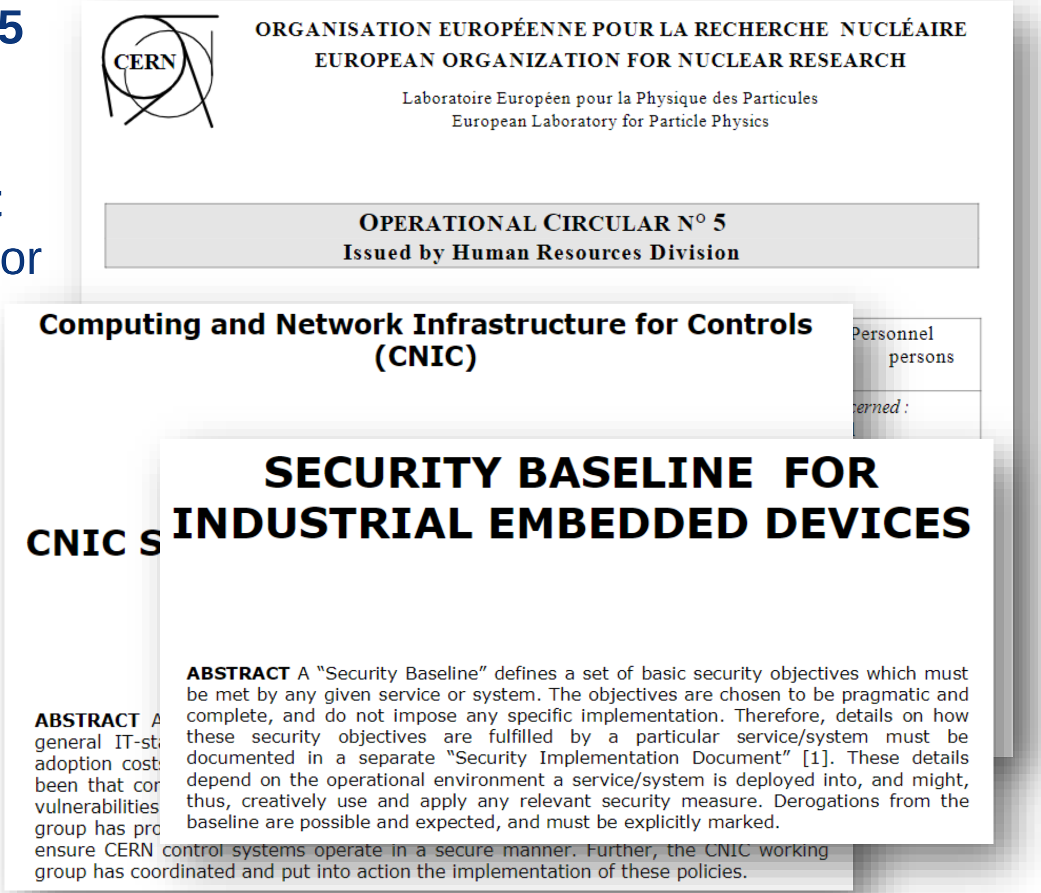
Dependencies
Consequences

This will not go away!

- “Computer Security” governed by **OC5**
- All CERN staff & users as well as **all users of CERN’s computing facilities are bound to it**
- In first instance, you are responsible for the cyber-security of your accounts, devices, systems, software, …
- Violation of OC5 might lead to sanctions

- **Control System Cyber-Security regulated** by the “CNIC”

- **All systems should follow their respective “Security Baseline”**



ORGANISATION EUROPÉENNE POUR LA RECHERCHE NUCLÉAIRE
EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH

Laboratoire Européen pour la Physique des Particules
European Laboratory for Particle Physics

OPERATIONAL CIRCULAR N° 5
Issued by Human Resources Division

Personnel
persons

cerned :

Computing and Network Infrastructure for Controls (CNIC)

CNIC S

ABSTRACT A
general IT-sta
adoption costs
been that cor
vulnerabilities
group has pro
ensure CERN control systems operate in a secure manner. Further, the CNIC working group has coordinated and put into action the implementation of these policies.

SECURITY BASELINE FOR INDUSTRIAL EMBEDDED DEVICES

ABSTRACT A “Security Baseline” defines a set of basic security objectives which must be met by any given service or system. The objectives are chosen to be pragmatic and complete, and do not impose any specific implementation. Therefore, details on how these security objectives are fulfilled by a particular service/system must be documented in a separate “Security Implementation Document” [1]. These details depend on the operational environment a service/system is deployed into, and might, thus, creatively use and apply any relevant security measure. Derogations from the baseline are possible and expected, and must be explicitly marked.

https://cern.ch/ComputingRules

The CERN Computing Rules

10 Points to Consider

1. **Stay mainstream:**
   Do not reinvent the wheel. With the crowd, you benefit from the below.
2. **Keep your system up-to-date:** Be able to patch in *reasonable time*.
3. **Kill all unnecessary services:** Disable Telnet, FTP …and *run a local firewall*.
4. **Control remote access:** Delete default accounts. *Change default passwords*.
5. **Filter inputs:** Every remotely provided input must be *validated and sanitized!*
6. **Develop software securely:** *Don't trust remotely imported libraries & packages*
7. **Use encryption:** …for confidential information (e.g. passwords).
8. **Understand dependencies:** DHCP? NTP? SSO/LDAP/AD?
9. **Have a plan:** For updating. For business continuity. For incident response.
10. **Get training & let us help you:**
    https://cern.ch/security & Computer.Security@cern.ch