European Organization for Particle Physics

Exploring the frontiers of knowledge

Finding the Balance between Academic Freedom, Operations & Security

Dr. Stefan Lüders
CERN Computer Security Officer

CERN/CNAF Seminar, 2020/5/27

“Security”: The state of being free from danger or threat.

Security is like contraception...

https://www.lexico.com/en/definition/security

- Will never be 100% effective.
- Does not contribute to performance.
- Never sure you actually need it all the time.
- Don’t know whether it has worked until after (even long after..) the event

- The measure of effectiveness is in terms of failures.
- A combination of methods gives the greatest reduction in risk.
- Should never rely on someone else’s precautions - *take care yourself*.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
INFORMATICS

FIRST Conference -Sevilla – June 2007 Slide: 65

SEVILLE JUNE 20 SPAIN 19th Annual FIRST Conference

Scope:

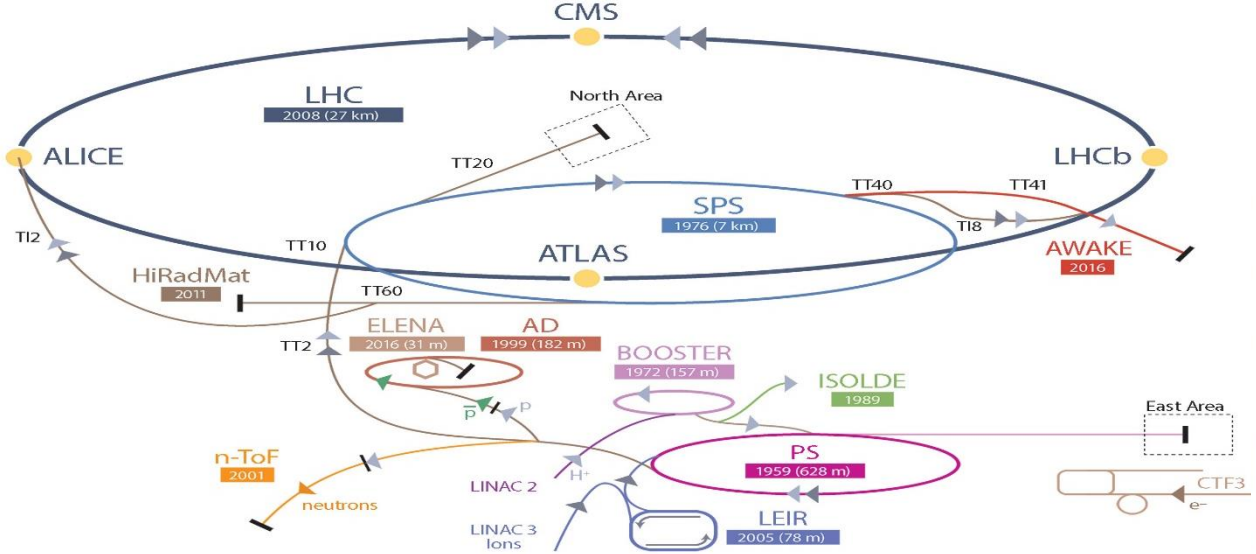
CERN – Know your (security) footprint

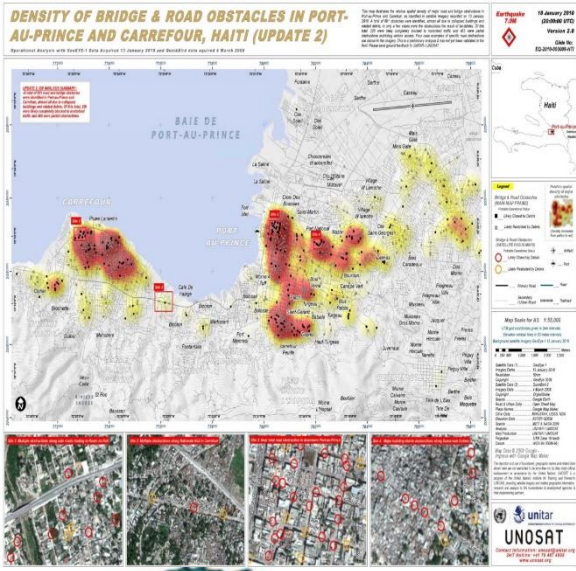
Risks:

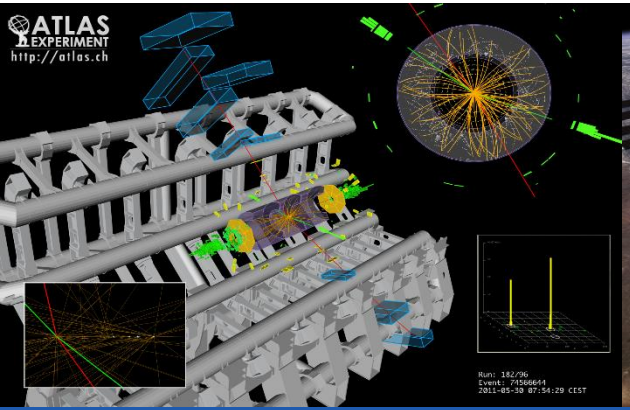
Adversaries & Limitations

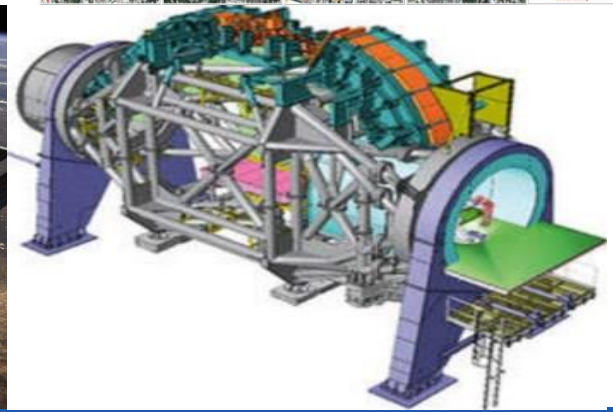
Controls:

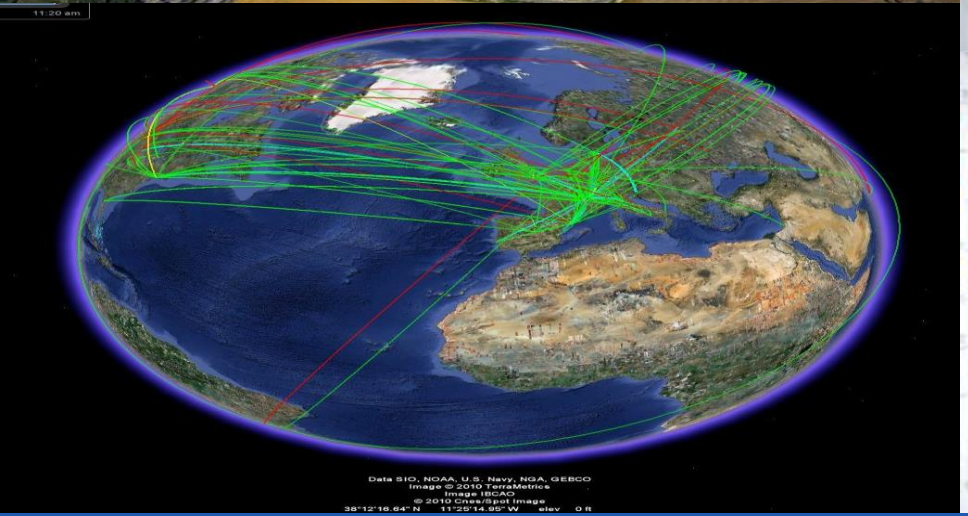
Protection, Detection & Response


CMS
LHC
2008 (27 km)
North Area
ALICE
LHCb
TT20
TT40
TT41
SPS
1976 (7 km)
TI2
TT10
TI8
ATLAS
AWAKE
2016
HiRadMat
2011
TT60
TT2
ELENA
2016 (31 m)
AD
1999 (182 m)
BOOSTER
1972 (157 m)
ISOLDE
1989
East Area
p
p
n-ToF
2001
PS
1959 (628 m)
CTF3
e⁻
H⁺
neutrons
LINAC 2
LINAC 3
Ions
LEIR
2005 (78 m)


DENSITY OF BRIDGE & ROAD OBSTACLES IN PORT-AU-PRINCE AND CARREFOUR, HAITI (UPDATE 2)
BAIE DE PORT-AU-PRINCE
CARREFOUR
unitar
UNOSAT


ATLAS EXPERIMENT
http://atlas.ch





Sectors of “Security” Operation

One flat office, wireless & data centre network
plus an external visitor network

5 Class-B IPv4 & 4 IPv6 networks
(+many non-routable networks)

200Gb/s to Internet, >20 Gb/s flat throughput,
>5000 switches, 100s routers,
6k firewall openings

~40k heterogeneous devices:
any hardware, any operating system, any (legal) application

~37k user account & mailboxes, 2M emails/d, 70% SPAM

Office Computing Security

6 data centres serving
users, infrastructure, compute &
storage, accelerators & experiments

17k servers, 300k cores, 35k virtual machines,
625PB storage (133k hard disks + 30k tapes)

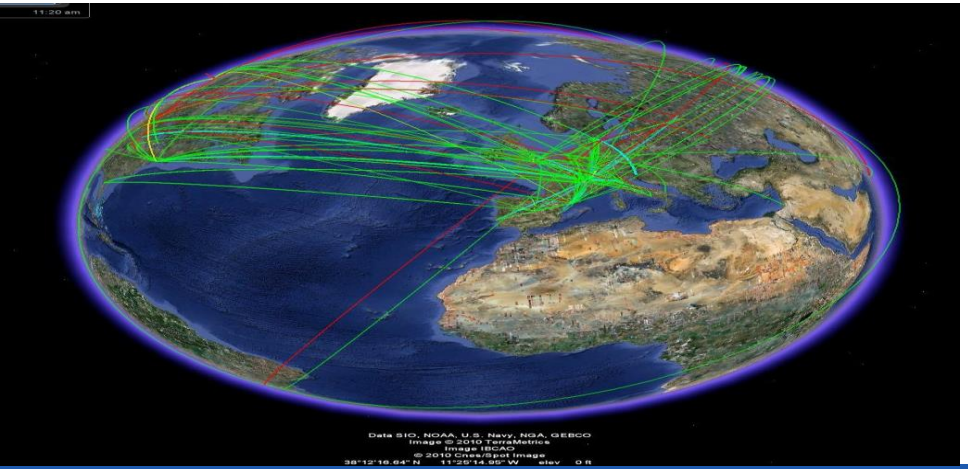
Provisioning of operating systems, anti-virus software,
printing, office/engineering/HR/finance apps,
databases, versioning/build systems,
virtualisation & container services,
collaboration tools, video/audio conferencing, …

50 central + 500 non-central webservers,
>10k websites, >1.5M webpages, webcast

Worldwide LHC Computing Grid (WLCG):

- Tier-0 (CERN: ~7k nodes)
- 13 Tier-1s, >150 Tier-2s and 3s

Permanently running >300k analysis jobs on >650k CPU cores at >20Gb/s through-put



Adeli	
BIT (Swiss Confederation)	Media-Lite SA
CERN	Opentransit (France Telecom Network Services Switzerland)
COLT	Orange Business Services - GIBN
CTI	RIPE-RIS
euNetworks (was Fibrelac)	Sunrise (TDC Switzerland AG)
Init7	Swisscom / IP-Plus
K-Net / K-Sys	T-Systems Schweiz AG (Deutsche Telekom)
K-root (RIPE)	UPC Cablecom
KPN Eurorings BV	VTX Services SA

CERN Internet Exchange Point (CIXP): Peering of 20 ISPs & TelCos

Experiments:
ALICE, ATLAS, CMS, LHCb, LHCf and TOTEM

AD, AMS, Cast, Cloud, Collaps, Compass, Dirac, Gamma Irradiation Facility, ISOLDE/ISOLTRAP, MICE R&D, Miniball, Mistral, NA48/3, NA49, NA60, NA62, nTOF, Witch, …

GCS, MCS, MSS, and Cryogenics System

Accelerators:
AB/OP, AD, CNGS, CCC, CLIC, ELENA, ISOLDE, ISOLDE offline, LEIR, LHC, Linac 2/3/4, PS, PS Booster, REX, SM18, and SPS

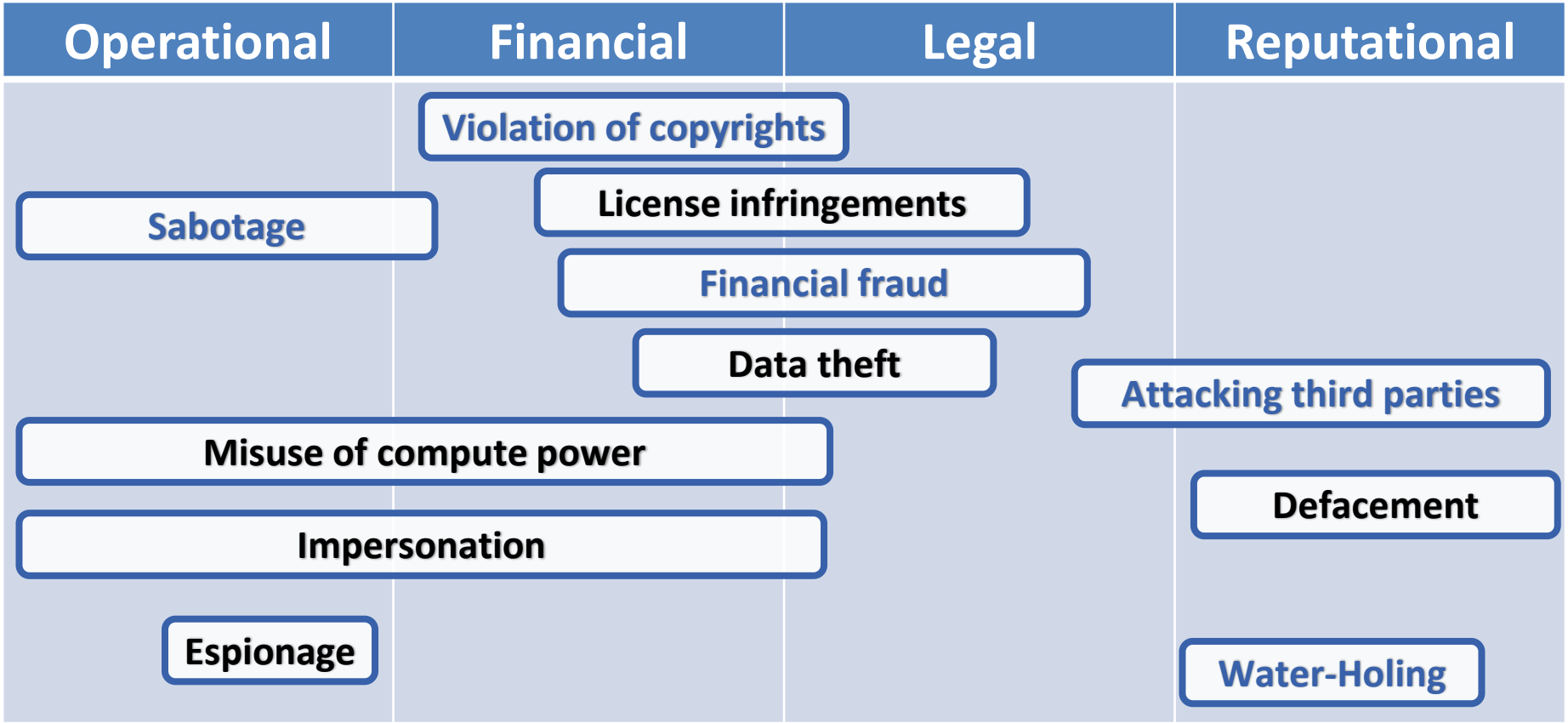
Accelerator Infrastructure:
ADT, ACS, BQE, BPAWT, BDI, BIC, BLM, BOF, BPM, BOB, BSRT, BTV, BRA, CWAT, Cryo (Frigo, SM18 & Tunnel), BCTDC, BCTF, FGC, LEIR Low Level RF, LHC Beam Control System, LBDS, HC, LHC Logging Service, LTI, MKQA, APWL, BPL, OASIS, PIC, QDS/QPS, BQS, SPS BT, BQK, Vacuum System, WIC, and BWS

Safety:
ACIS, AC PS1, AC PS2, AC SPS1, AC SPS2, Alarm Repeater, ARCON, ADS, CCTV, CSA, SGGAZ, SFDIN, CSAM, CESAR, DSS, LACS, LASS, LASER, Radmon, RAMSES, MSAT, Radio Protection Service, Sniffer System, SUSI, TIM

Infrastructure:
CV, ENS, FM, DBR, Gamma Spectroscopy, TS/CSE, and YAMS

Examples of Control Systems / IoT

And the Human Factor...



The "Security" Risk Matrix

Scope:
CERN – Know your (security) footprint

Risks:
Adversaries & Limitations

Like any other company, organization or university, CERN is under permanent attack.

Search Twitter Have an account? Log i

C3 ~ RET
@c3retc3
Follow

#CERN discloses passwords, source code and tickets to Web spiders

6:03 a.m. - 29 Sep 2015

C3 ~ RET @c3retc3 · 2h
@c3retc3 There are 150 Oracle DB hosts at least!

Kate Kahle @katekahle · 2h
@c3retc3 Thanks for the heads-up! What about sharing details with us via Computer.Security[at]cern.ch?

C3 ~ RET @c3retc3 · 51m
@katekahle Surely I will write you. You have really surprised me with the reaction - glad to see this approach to security of the org.

1

© 2015 Twitter About Help Terms Privacy Cookies Ads info

@reversemode
Rubén Santamarta

Writing a post involving CERN, LHC, SCADA, passwords... one of the most curious cases I've found.

9 Aug via TweetDeck

Dan Tentler
@Viss
Follow

someone asked earlier if I was gonna find CERN - here's one (I got their CERT guys email. I'll notify) pic.twitter.com/zu180KzyBo

Reply Retweet Favourite More

```
Welcome to CERN Virtual Machine, version 2.6.0
vm2209280-01 login:  --- a new cmtuser directory has been created in your HOME directory
================================================================================
=                        ---- LHCb Login v7r10p4 ----                          =
=       Building with gcc46 on slc5 x86_64 system (x86_64-slc5-gcc46-opt)       =
================================================================================
--- User_release_area is set to /opt/dirac/cmtuser
--- LHCBPROJECTPATH is set to:
   /cvmfs/lhcb.cern.ch/lib/lhcb
   /cvmfs/lhcb.cern.ch/lib/lcg/releases
   /cvmfs/lhcb.cern.ch/lib/lcg/app/releases
   /cvmfs/lhcb.cern.ch/lib/lcg/external
--------------------------------------------------------------------------------
```

GRAHAM CLULEY
award-winning computer security news, advice and opinion

38.9k

News | Forum | GCHQ Newsletter | Speaking | Sponsor | About | Contact | Games | Log

This week's sponsor: The 2015 Industrial Control Systems (ICS) Cyber Security Conferenc

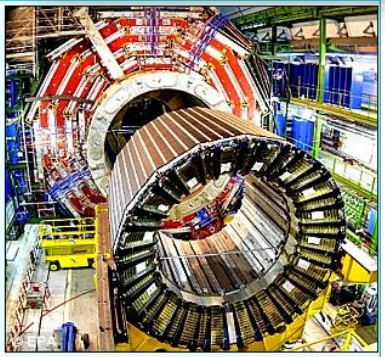
If you look after the Large Hadron Collider you should read this...

Mail Online

THREE CLICKS AND WE WERE IN CERN'S PRIVATE WEBSITE

The Shodan search engine is so powerful, it could even put the world's most expensive science experiment at risk.

By searching the site's 'most popular' searches, reporters at The Mail on Sunday were able to find out the internet location of the home of the Large Hadron Collider, the world's largest particle accelerator.



Hacking risk: CERN's Large Hadron Collider in Switzerland

Anonymous Coward
User ID: 69274093
United States
05/25/2015 11:18 PM
Report Abusive Post
Report Copyright Violation

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

Scary thought. Hollywood hit..
Really cern has been hacked, it is ran by mad scientists, hell bent on crazy.
These are the type of people that jump from rocks with wing suits with life mentality.
They want crazy. Cern is a weapon, the biggest and most psychotic ever created.

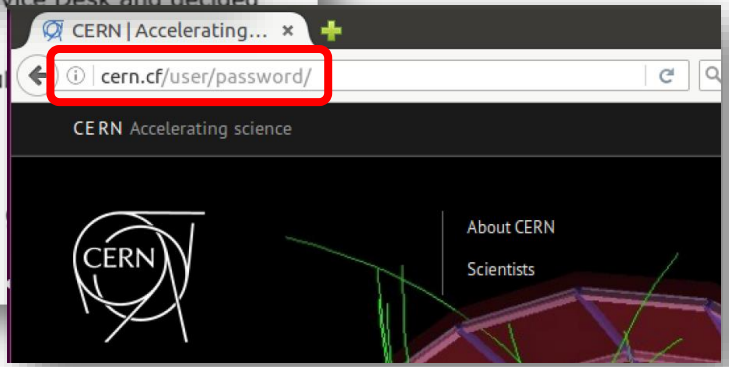
By the
the log
three passwords. So I thought it was a joke from someone that noticed I am not really CERN Service Desk and decided to troll me a little. I totally forgot about other login methods.

So I made NICE login of my own with Windows/Kerberos authentication included. This is the resu[redacted]

http://its.cern.cf/jira/browse/FWINS-1224

Thanks for giving me this chance without legal trouble. I had fun and learned a lot thanks to you

Looking forward to hearing from you. It would be really a priviledge for me to work at CERN.



<sc0rp> nice

<MLT> using the exploit on CERN would be win, hac

<s

Lab Mouse Security @InfoSecMouse · Jul 7

Hacking CERN - Exploiting pytho
Particles and Profit

From: [redacted] Sent: Fri 2012/03/23 15:02
To: Press Office
Cc:
Subject: URGENT

Hello,
I'm contacting you because I've an important thing to let you know.
I've found some vulnerabilities on cern.ch system and I've hacked it.

I didn't get acess of databases but hacked the website with a XSS attack. Would like know if you're the right person to talk about this and try make a deal to give you all details, all strings I used, the links and all stuff that I did.
If you aren't the right person to talk just give me a email to contact to let him know the details please.
I'm waiting your reply ASAP,

http://www.yout... black01white Greek Hackin...

YouTube

black01white Greek Hacking Documentary trailer ripped

mpampisg Subscribe 38 videos

CERN CONTROL CENTRE HACKED

1:07 / 1:35

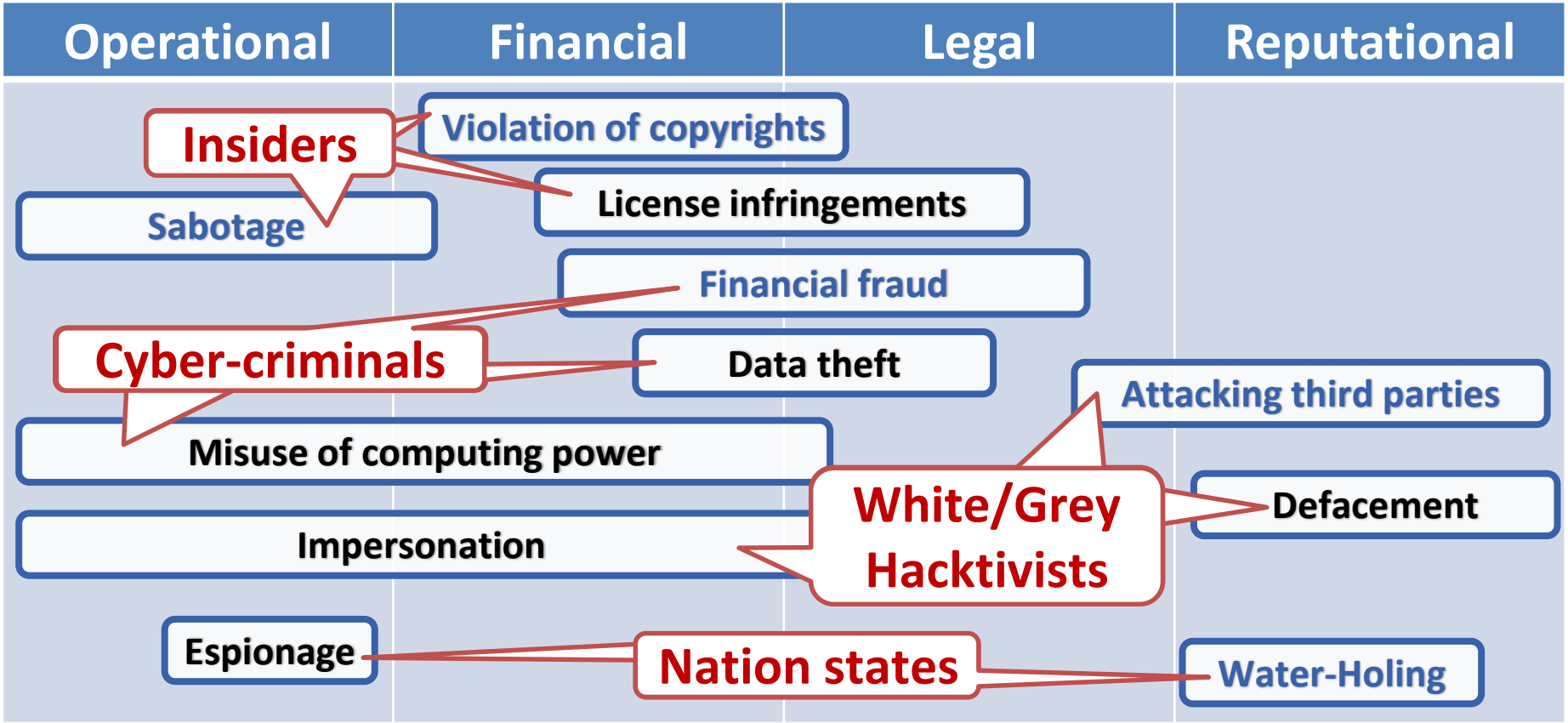
Like Add to Share 5,788

PART 1: HACKING THE LARGE HADRON COLLIDER (XSS VULNERABILITY)

Published by cammilla c. | Filed under General, News, Spreadin'

PART 2: HACKING THE LARGE HADRON COLLIDER (AUTHORIZATION BYPASS)

Published by cammilla c. | Filed under General, News



Adversaries & Motivation

Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations

Controls:

Protection, Detection & Response

Mandate:

Protect the operations and reputation of CERN against cyber-threats

Find an appropriate balance between
academic freedom, operations & security.

“Academic Freedom” implies “Responsibility”!

CERN Cyber-Security is everyone’s responsibility
and not that of the Computer Security Officer alone!

Responsibility can be (partially) delegated to CERN’s IT department.

The Computer Security Team acts as facilitator & enabler.

We help people to do their job securely. We secure CERN.
We take over responsibility when handling security incidents.

Governance: Basic Paradigms

“Security” is the responsibility of every individual at CERN

Everyone is bound to CERN’s Staff Rules & Regulations (SRR), CERN’s Code of Conduct (CoC) and administrative & operational circulars (e.g. “OC5”)

In particular, ideally, CERN IT experts directly manage the security of their services (e.g. email, DBs, O/S, storage, web)

"These functions, allowing access to personal data or other confidential and/or sensitive information, imply strict conformance to the rules laid down in OC11 and OC5, in particular those governing confidentiality.."

IT professionals at CERN usually also come with some “security” expertise. Depending on the department/group this is tested during their job interview.

11. Which of the following values/fields coming from HTTP client can be easily forged by malicious attacker on the client side, and set to any arbitrary value:
    a. GET arguments
    b. GET and POST arguments, cookies, hidden form fields
    c. GET and POST arguments, cookies, hidden form fields, user-agent, referrer
    d. GET and POST arguments, cookies, hidden form fields, user-agent, referrer, remote (client) IP address

12. Which of the following HTTPS protocol does *not* offer:
    a. Client authentication
    b. Protection against eavesdropping
    c. Prevention against man in the middle attack
    d. Prevention against cross site request forgery attack

13. Security-wise, which of the following PHP settings would you consider the best:
    a. "register globals" disabled, "display errors" disabled
    b. "register globals" disabled, "display errors" enabled
    c. "register globals" enabled, "display errors" disabled
    d. "register globals" enabled, "display errors" enabled

14. Which of the following file permissions can be represented as 0536?
    a. -r-x-wxrw-
    b. -rw-r-xr--
    c. --wxr--rw-
    d. -r-xrw--wx

HEP community, in particular with the WLCG/EGI, and multiple ties with academia in general (e.g. REN-ISAC, SWITCH WG, IHEP/CAS)

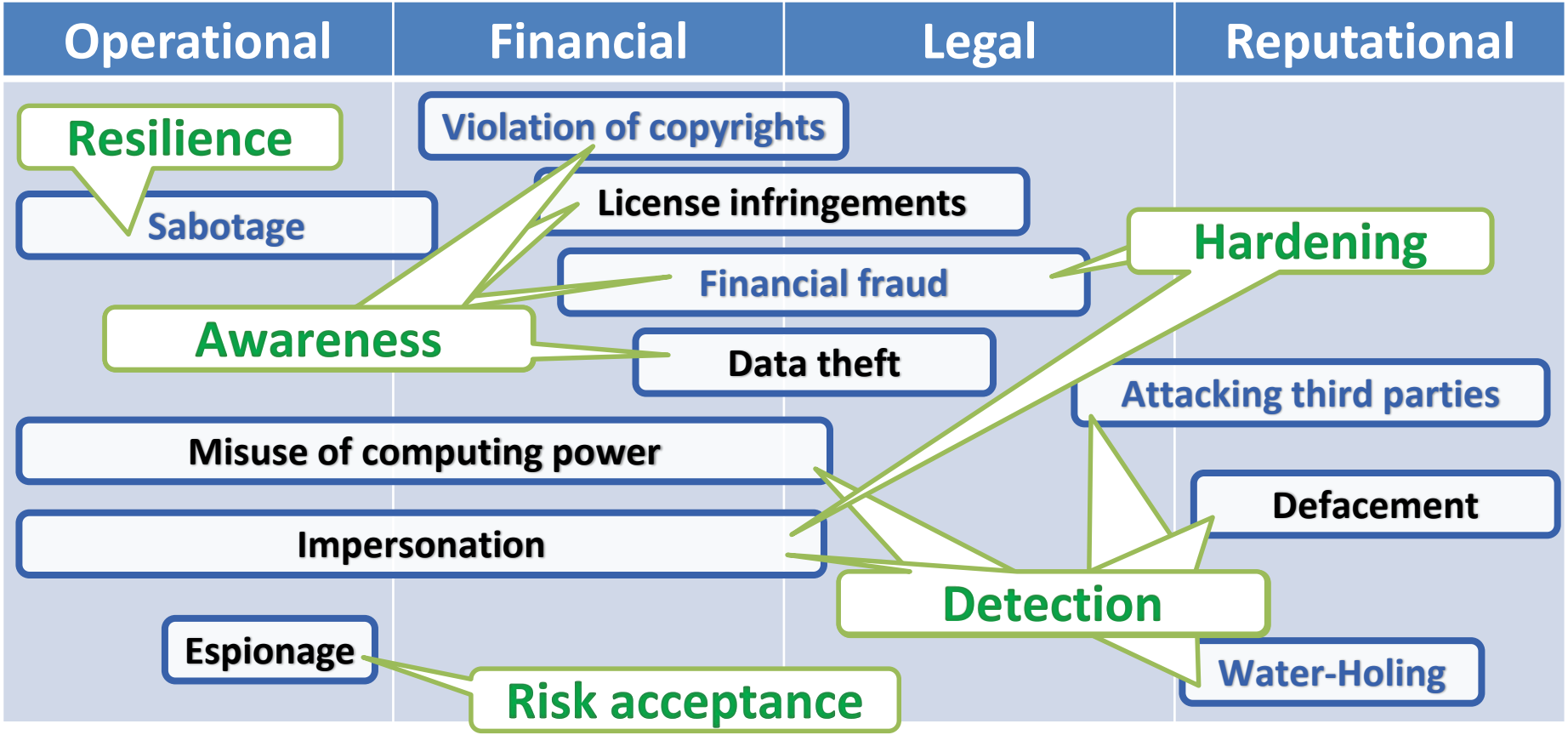
Geneva-based int'l organizations (The Global Fund, ICRC, IFRC, ILO, ITU, OHCRH, UN, UNHCR, WHO, WIPO, WTO)

Governments (e.g. CH, D, EU, F, N, NL, S, UK) and int'l & local law enforcement (e.g. Europol, FBI, Geneva police, Interpol)

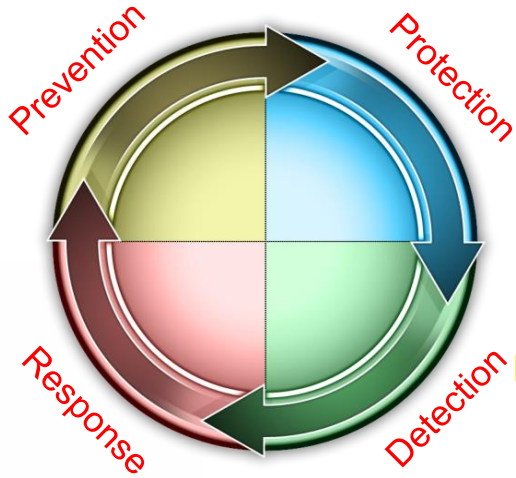
Security & software companies, and industry in general (e.g. CERT-CH forum, ENISA ICS-SG)

Member of vetted closed security forums

Governance: Worldwide Collaboration


Operational
Financial
Legal
Reputational
Resilience
Violation of copyrights
Sabotage
License infringements
Hardening
Financial fraud
Awareness
Data theft
Attacking third parties
Misuse of computing power
Defacement
Impersonation
Detection
Espionage
Water-Holing
Risk acceptance

resource inventories Defense-in-Depth training
pen testing change of culture
central/agile patching network segregation
security intelligence awareness networking
keeping informed audits firewalling static code analyzers
SSO/2FA baselining reviews
central anti-virus resource life-cycles
ID federations consulting security policies



WhiteHat Challenges
vulnerability scanning
statistical traffic analysis
netflow
integrity checkers
DNS verification
credential hunts SSHgrep
URLgrep IDS
monitor-the-monitoring
remote login receipts
syslog/netlog analysis/Snoopy
web application checking

triage
CSIRT/CERT
costing
forensics
WLCG Grid Security Officer
Security Event Self-Mitigation Portal

"Security" Portfolio

https://cern.ch/resources

Accounts

Name, mail, login or ID

Search login only

Stefan Lueders (slue

Website review

Please review the st

Websit

Sh

Websi

apeg

aprilfo

Devic

- Devi
- Loca
- Manu
- Mod
- Gene
- Desc
- Tag:
- Seria
- Oper
- CER
- Netw
- Resp
- Main
- HCP
- IPv6
- Last changed: 14-07-2016 (10:32)

New Firewall Opening Request

You are requesting an opening in the main CERN Firewall to allow Internet access to your machine. Please be aware that machines directly exposed to the Internet will be continually attacked and create a risk for the rest of the site. To avoid this you should access your machine from off-site using an intermediate gateway system, as described here. In general, you should reach your system via LXPLUS which has additional intrusion checks.

1. Request Information

Interface Name

Interface Name

Service

Dual Web server (HTTP and HTTPS) on ports 80/tcp and 443/tcp

Port number

80, 443

Protocol

TCP

Application

Give the name of the application listening on this port.

HTTP/HTTPS

Expiration Date

This firewall opening, if authorised, will be automatically deleted on this date. The maximum time span at any given time is two years. You will be notified before expiration in order to reconfirm and prolong this firewall opening.

25-05-2021

Firewall: Approval process with pentest & assessment

OpenVAS

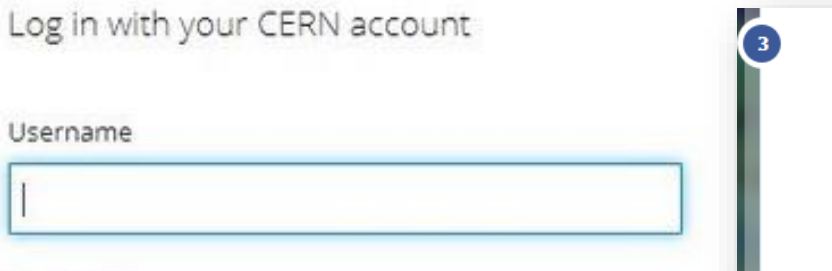
skipfish

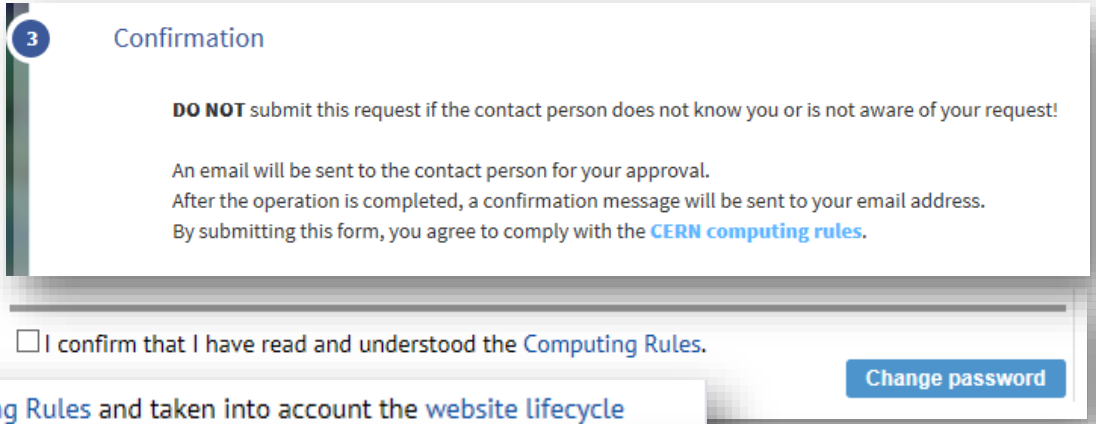
web application security scanner

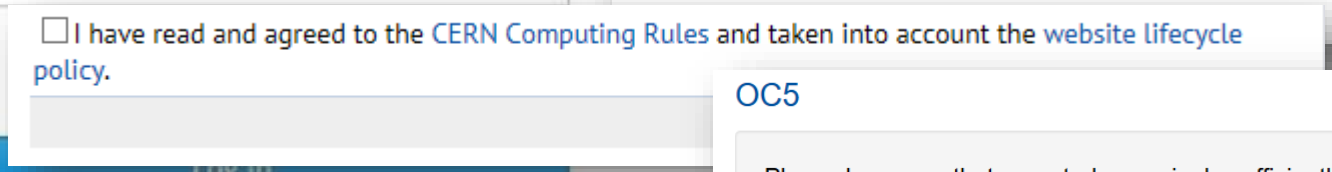
Regular verification:
Opened service still listening?
Network traffic to that opening?

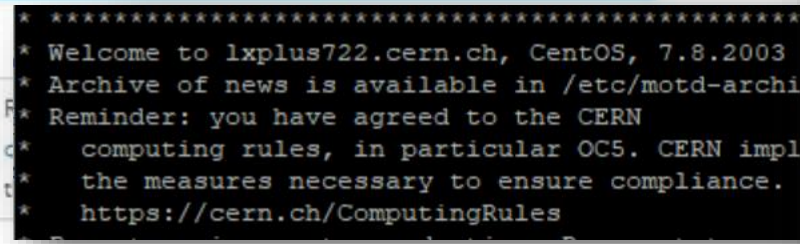
Prevention: Inventories & Lifecycle

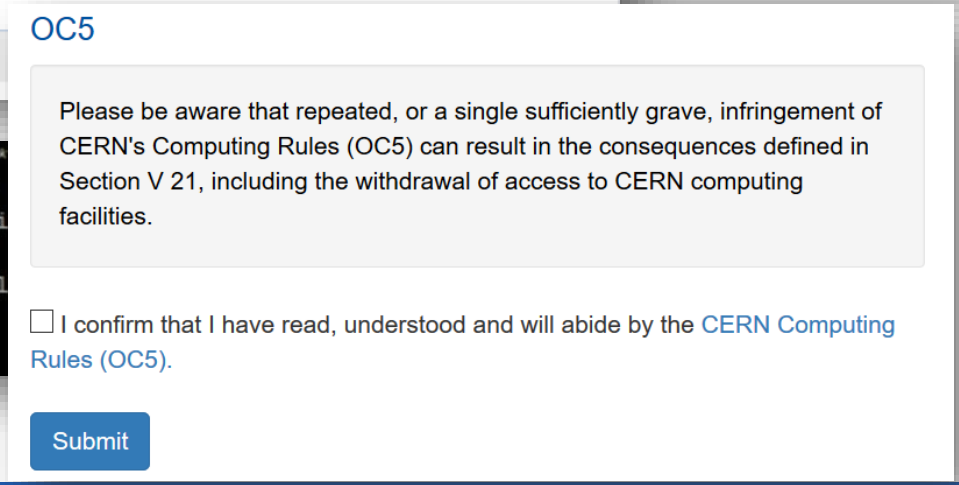
https://cern.ch/ComputingRules











Prevention: Reminders of the Rules

Protect your computers

Any unprotected computer connected to the Internet is likely to be infected within minutes!

- Keep your system up to date.
- Use anti-virus software.
- Do not install untrusted software.
- Lock your screen with a password.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

Be careful with e-mail & Web

Cybercriminals are trying to trick you!

- Do not open unexpected or suspicious e-mails or attachments.
- Stop-think-click.
- Protect your passwords.
- Do not install untrusted software or plug-ins.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

Protect your passwords

A cybercriminal, who knows your password, will abuse your computing account.

- Never share your passwords with anybody.
- Choose good passwords.
- Do not reuse old passwords.
- Change your passwords regularly.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

Protect your files & data

Cybercriminals are trying to find confidential or sensitive information, also here at CERN.

- Restrict access to your documents and folders.
- Follow the principle of least privilege.
- Do not run file sharing applications.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

Follow the computing rules

Help us to protect CERN's mission and reputation.

- Follow the CERN Computing Rules.
- Take responsibility.
- Do not run restricted applications.
- Respect confidentiality and copyrights.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

Respect copyright

Don't break the law!

- Do not distribute copyrighted material.
- Refrain from file sharing applications or file hosting services.
- Violating copyright is not a trivial offense.
- Protect the Organization.

Let us help you: visit http://cern.ch/Computer.Security or contact Computer.Security@cern.ch

https://cern.ch/security/training/en/posters.shtml

- "Home" Awareness
- Posters, videos, …you-name-it
- Induction & On-Boarding
- Mandatory online courses
- Technical trainings
- Consulting & audits

Prevention: Six Recurrent Themes

https://cern.ch/security/recommendations/en/code_tools.shtml

Static Code Analysis Tools

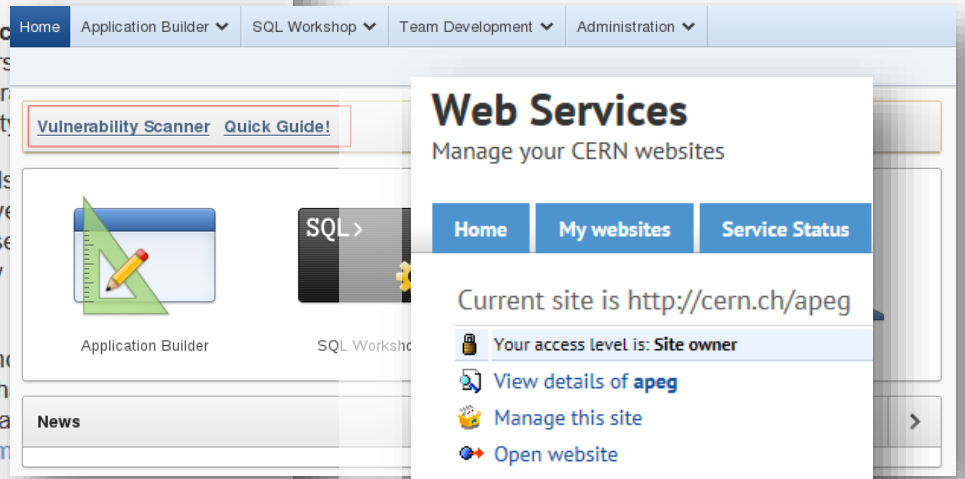
Below you find a list of **static source code analysis tools rec**
developers. These tools are supposed to allow developers
quickly, looking for some common potential bugs and vulner
and non-security-related), thus increasing reliability and securit

This is a summary of an evaluation of code analysis tools
Computer Security Team. It is by no means a comprehensive
tools, nor is it a list of the most complete tools. The tools prese
selected for their ease of use, simplicity and by their efficiency
Another list can be found here.

The tools and the documentation provided are for Linux, but m
available on Windows as well (links are provided). If you h
Gitlab-CI (Continuous Integration) service, note that all sta
provided through a dedicated Docker image. See these exam
for details.

C / C++

CppLint	Free	stand-alone script	CppLint is a script that checks for compatibility of code with Google's style guide for the C++ language. It can find some dangerous constructions and report general bad practices, syntax errors and style inconsistencies.
Flawfinder	Free	stand-alone script	Flawfinder checks for calls to known potentially vulnerable library function calls.

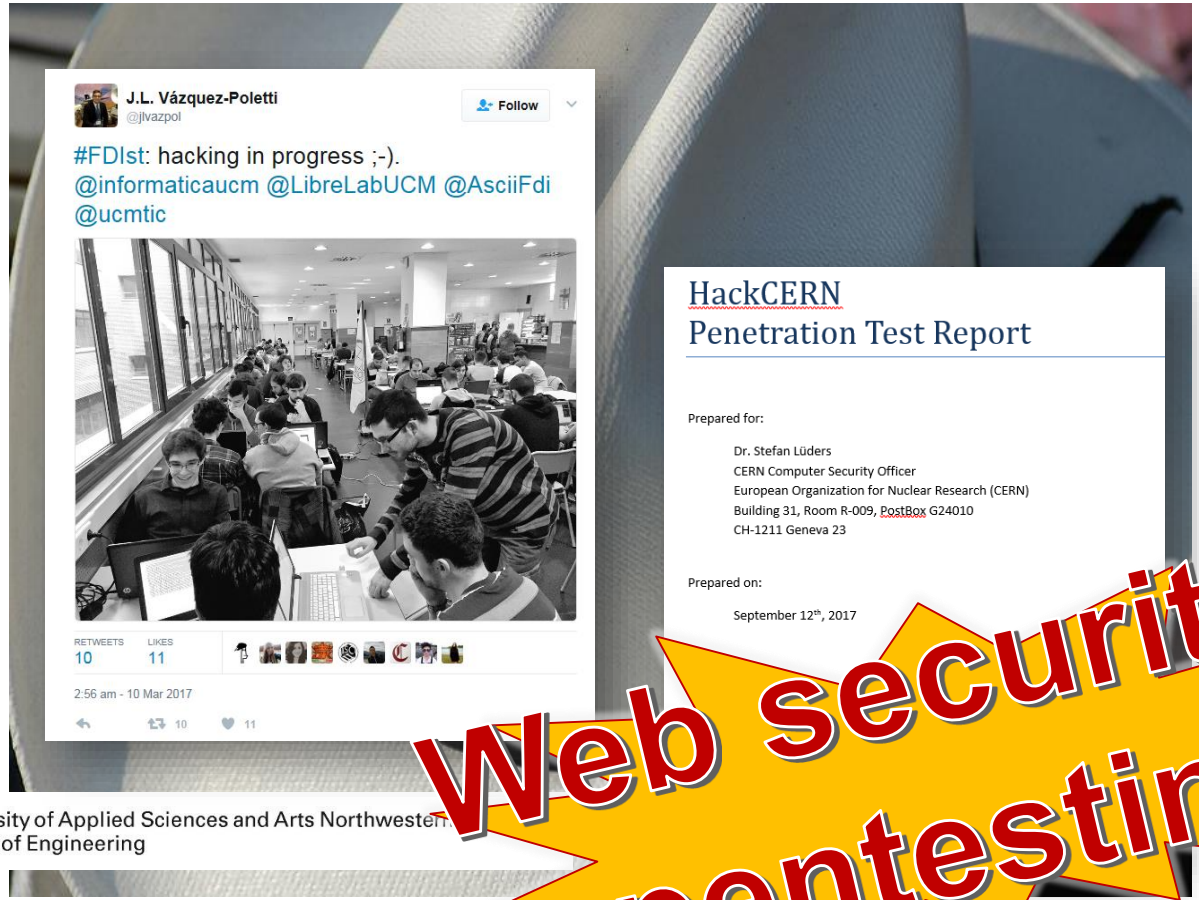


https://cern.ch/web

https://cern.ch/security/recommendations/en/apex_applications.shtml

Prevention: Tools for Developers

https://cern.ch/security/services/en/whitehats.shtml



Web security & pentesting

University of Applied Sciences and Arts Northwestern Switzerland
School of Engineering

Prevention: Crisis Management

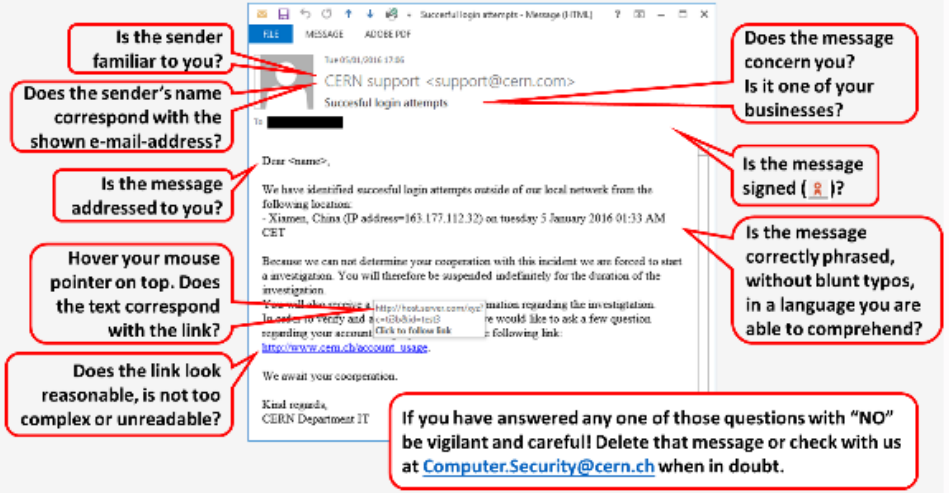
https://cern.ch/security/malicious_email.shtml

Oops... The link you've just clicked is evil!

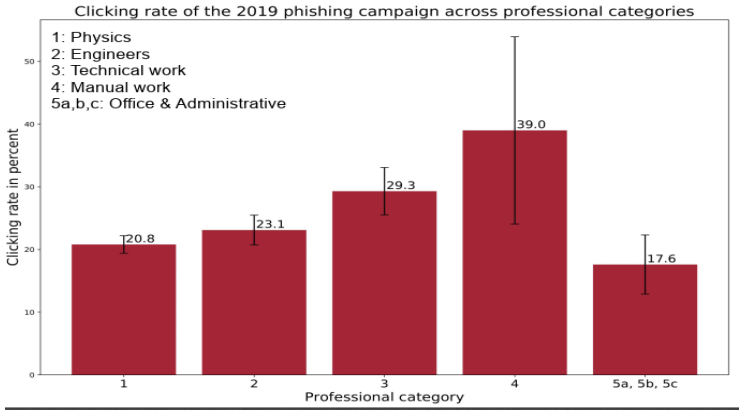
(Version française ici/en-dessous)

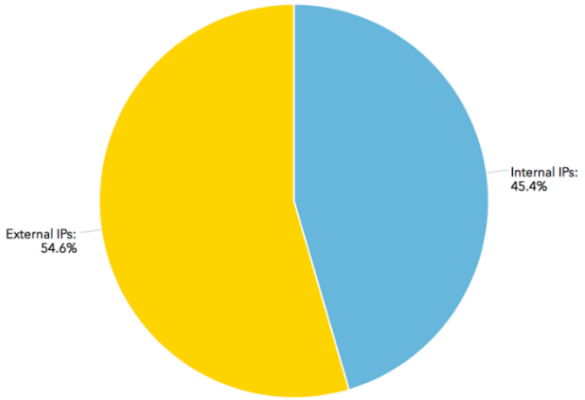
You just fell for a scam. The e-mail whose link you just have clicked is fake. Your "click" could have had severe operational and financial consequences for CERN... Let us explain to you how you can better identify such emails and which consequences clicking on such a malicious link might have for you and your digital assets...

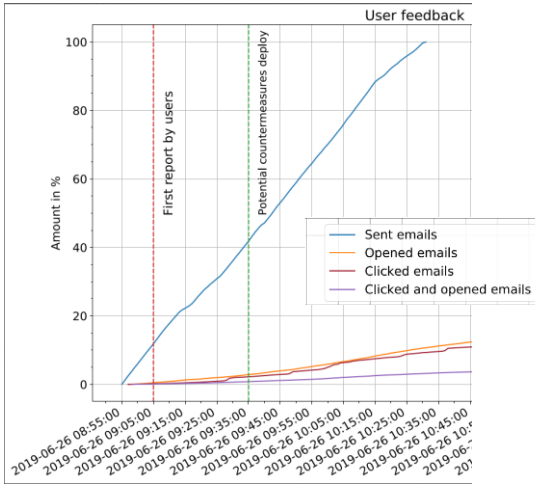
How to identify malicious e-mails



If you have answered any one of those questions with "NO" be vigilant and careful! Delete that message or check with us at Computer.Security@cern.ch when in doubt.







Click rate: ~20.0%
(2018: 15.3%; 2017: 18.7%; 2016: 19.8%; HEPix BNL 2015: 29%)

DNS blocking catches only 50%...

...and you have to be [illegible]ick!

Subject: FW: Testing of new booking system

Hello,

I received the email below from the mail address @cern.COM and unfortunately I clicked on the link.
What should I do?

To: cert-snow@cern.ch

I didn't click, but I forwarded it to

Regards,

Human aspects of email security

Dedicated appliance to block sophisticated malicious emails & attachments

CERN
CH-1211 Geneva 23
Switzerland

Document
Security Baseline for Hardened PC
CERN Div./Group or Supplier/Contractor Document No.
Computer Security Officer
EDMS Document No.
1593100

JUNE 20TH, 2016

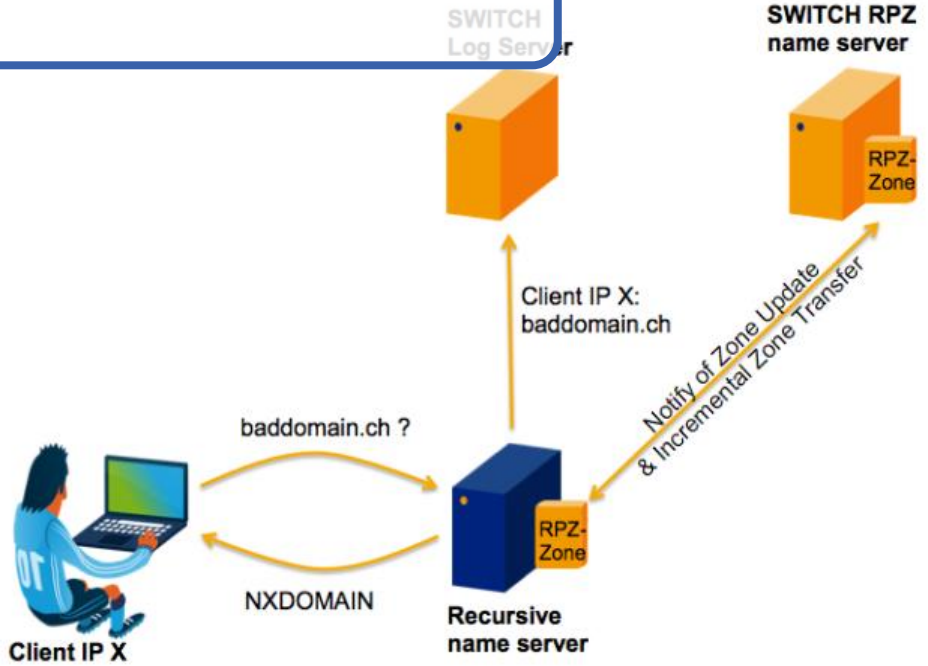
SECURITY BASELINE FOR
HARDENED PCS AND LAPTOPS

PDF

PC Hardening & Alternative PDF Reader

Blocking certain malicious & typo-squatting domains in the Domain Name Servers (DNS)

https://cern.ch/security/blocked.shtml



Synchronizing with SWITCH's list of bad domains

Safety first
Availability next
Security third

Impact & criticality analyses

Rigorous safety systems prevent (malicious) damage, but reduce availabilities

- Insecure embedded devices
- Wireless to the plant floor
- (No) Network segregation
- One Data Center to serve them all
- Remote development and testing

Why (Control System) Cyber-Security sucks…

Control System Cyber-Security

Headache #1 still to be Overcome

Transparency is paramount for successfully running an ethical and trustworthy Computer Security Team.

https://cern.ch/security/home/en/privacy_statement.shtml

Digital Privacy Statement of CERN's Computer Security Team

2016/11/15 by CSO

Introduction

The CERN Computer Security Team ("the Team") takes great care to protect the personal data collected or accessed by us. This Privacy Statement describes how and when the Team gathers, accesses, uses and shares information about you or your usage of CERN's computing facilities and how the Team protects this information.

Scope

This Privacy Statement applies to all persons accessing or using CERN computing facilities, including websites hosted at CERN. It complements the CERN's Computing Rules, i.e. the Operational Circular No. 5 on the Use of CERN Computing Facilities, in particular its subsidiary rules, and Administrative Circular No. 10 on Personal Data Protection.

Information Collection and Use

The CERN Computer Security Team automatically records information ("Log Data") created by your use of CERN's computing facilities in order to detect and understand any abuse of CERN's computing facilities as well as any other violation of the CERN Computing Rules in real time and/or in retrospect.

Log Data contains information on your digital access to CERN's computing facilities including access to the wired and wireless networks, unencrypted network traffic of your device(s) with external services on the Internet, as well as all your activities linked to CERN's interactive computing clusters and its web services. Log Data is always registered with an accurate time stamp. In detail, Log Data includes:

- Usage information when connecting your device(s) to CERN's wired or wireless networks (i.e. ARP and DHCP meta data);

Information Security and Retention

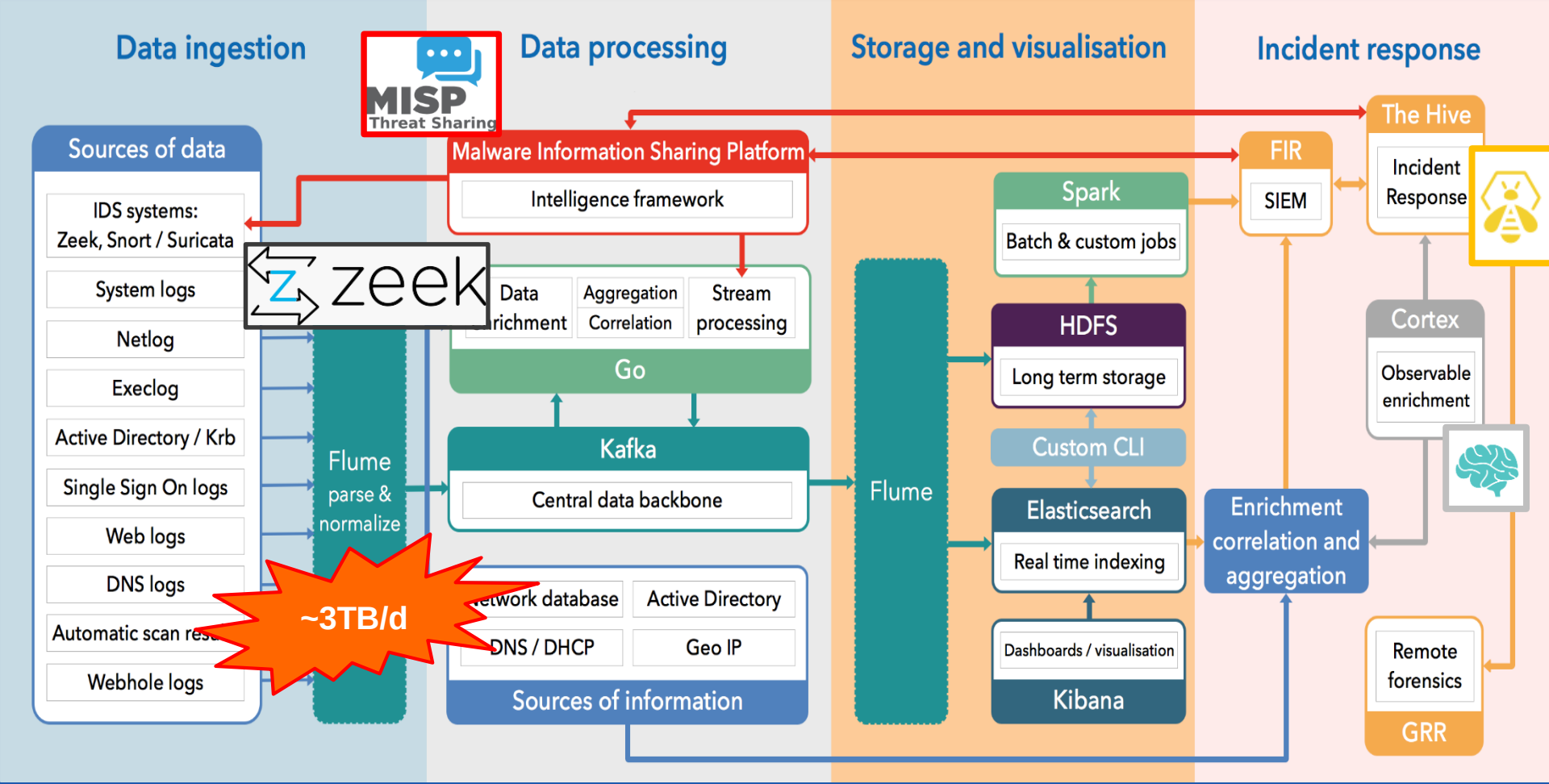
Log Data is stored using the computing facilities provided by CERN's IT department. CERN makes best efforts to protect this Log Data from unauthorized access, or alteration, disclosure or destruction (also see CERN's Digital Privacy Statement). Past experience has shown that a retention period of one year is sufficient to perform the analysis of security related events in retrospect, but this is subject to periodical reviews. Log Data linked with any abuse of CERN's computing facilities as well as any other violation of the CERN Computing Rules is kept indefinitely.

Information Access, Sharing and Disclosure

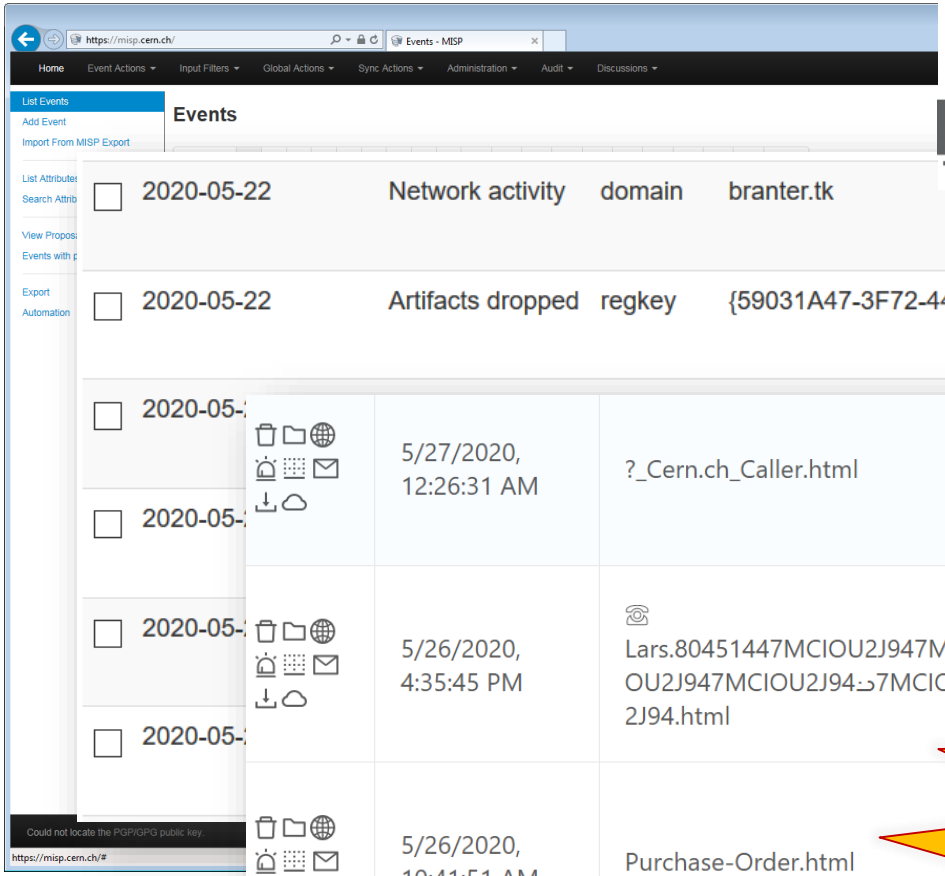
As stipulated in the CERN Computing Rules, access to Log Data is limited to members of the CERN Computer Security Team, i.e. a limited number of individuals appointed ad-personam by CERN's Computer Security Officer, and only authorized when suspicious activity or activity potentially violating CERN's Computing Rules related with your activity, account(s) or device(s) has been detected by or reported to the Team. In those cases, the Team may preserve or disclose your information only if deemed by CERN to be necessary for legal purposes; to protect the safety of any person; to address fraud, security or technical issues; or to protect CERN's rights or property. In particular, the Team reserves the right to disclose (parts of) your data promptly to third parties in order to avert any further harm to you, your account(s), your device(s) or your data.

Revisions

This Privacy Statement may be periodically revised. Prior versions of the Privacy Statement will be archived and kept available.



Detection: The SOC Infrastructure



MISP Threat Sharing

Serving CERN, the WLCG and the HEP and academic community

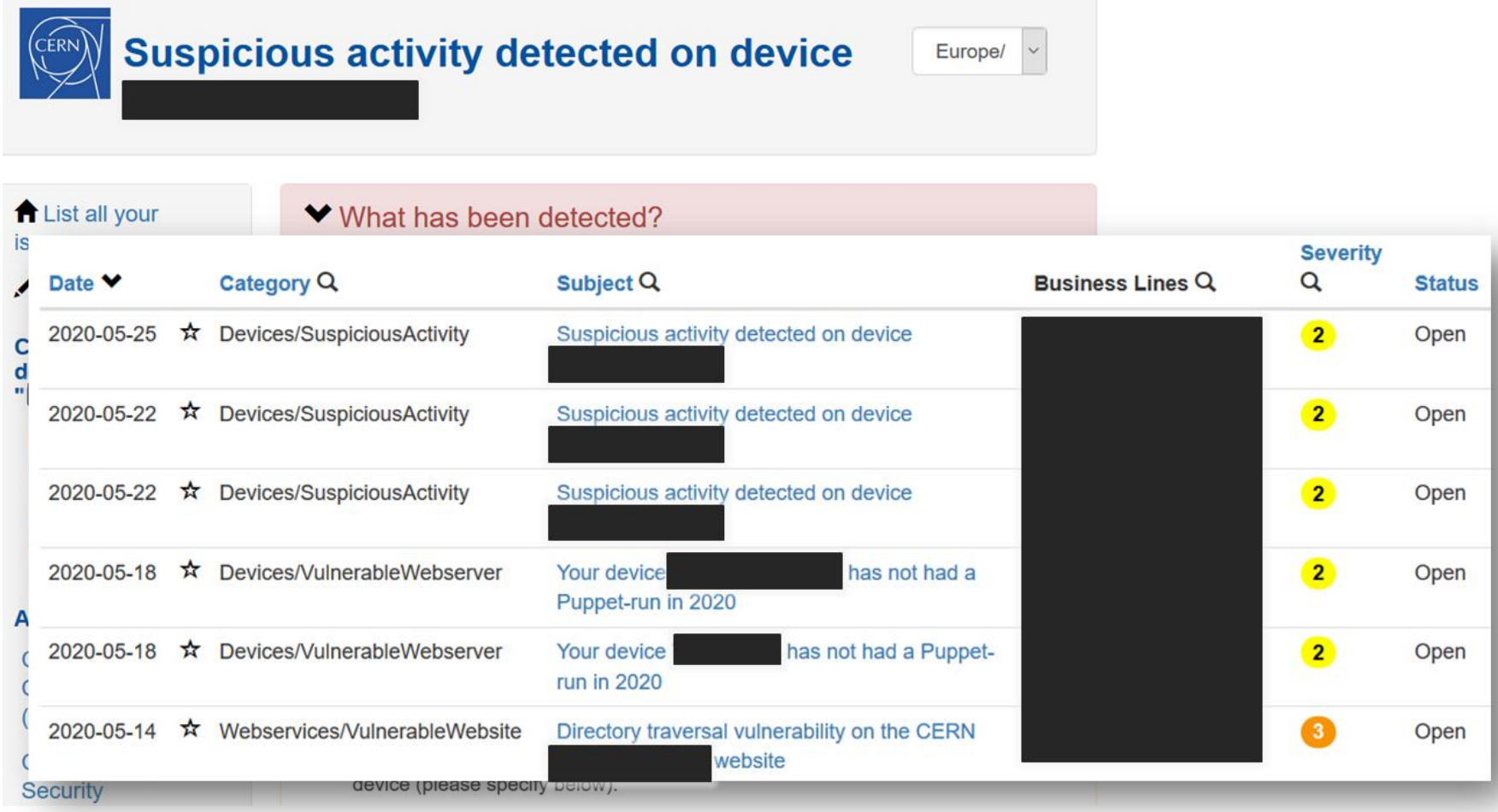
Synchronized with CH law enforcement & CH CERTs

Also from external feeds:

SOC/MISP/Bro/Zeek

Detection: Intelligence

https://cern.ch/security/services/en/sems.shtml



Response: “Auto-Notify”

https://cern.ch/security/services/en/emergency.shtml

- Triage
- Taking over service
- Coordinating comm's
- "Avalanching"
- Forensics

JoeSandbox

- Close out

CERN also provides incident respo & foren

Forensics

Response: CERT & Forensics

A Unit of Information Technology Services

UCLA Information Security Office

SERVICES

Security

New Li

UPDATED

A recently

believed

VENOM a

communi

You can r

THE UNIVERSITY OF BRITISH COLUMBIA

UBC IT Bulletins

Home / Security Advisory: BusyWinman Linux Intrusion – July 21, 2017 15:40 PT

Security Advisory: BusyW
July 21, 2017 15:40 PT

Operation Windigo – the vivisection of a large Linux server-side credential-stealing malware campaign

welivesecurity
Security news, views and insight from the ESET experts

BY PIERRE-MARC BUREAU POSTED 18 MAR 2014 - 01:3

During the course of our analysis, we have had the opportunity to collaborate with various international organizations, including CERT -Bund, the Swedish National Infrastructure for Computing, the European Organization for Nuclear Research (CERN) and others forming an international Working Group. With the help of the working group, thousands of victims have been notified that their servers

Response: Advisories

https://cern.ch/security/reports/en/monthly_reports.shtml

Computer Security Report for April 2020

Corona Warning Please be extremely skeptical when receiving emails around the subject "Corona"/"COVID-19", in particular if those emails containing links or attachments. STOP --- THINK --- DON'T CLICK! ...and don't open any attachment. If you are in doubt, cross-check with us at Computer.Security@cern.ch.

Blackmailed with your password? If you received recently an email with a password similar to one of yours, claiming that they "know every think about you", and asking you to transfer Bitcoins to them, don't worry and don't answer. This is a scam. The password, eventually a real one, has been exposed in a data breach, likely already a while ago, and was made public in so-called "password dumps" containing of millions of other passwords. The scammers here just took advantage of those dumps to blackmail you. If you recall that password and still use it somewhere, time to change it now. In parallel, we continue to inform owners of exposed passwords if we get hold of similar password dumps... More details can be found in those two Bulletin articles.

iOS/iPhone/iPad Exploit A zero-day vulnerability, i.e. a vulnerability which has not patches ready yet, of the native mail client in the iOS operating system has been reported being actively exploited. Unfortunately, there is no fix out yet. Only option for the moment is avoiding having your emails pushed to your iPhone/iPad ("Settings" -> "Passwords & Accounts" -> have "Fetch New Data: Off" by disabling "Push" and

Response: Monthly Reports

CERN values its open environment

⇨ "Security" delegated to everyone

Like others, permanently under attack

- Training the minds of people
- Keeping inventories & life-cycles
- Being prepared + trying to detect early

More “security” seminars coming every other week from now on:

https://indico.cern.ch/category/82/

Hacking

Human aspects of email security

Web security & pentesting

Forensics

OpenBSD security

The Deep & Dark Web

Control system cyber-security

SOC/MISP/ Bro/Zeek

www.cern.ch

Thank you for listening!

Questions?