



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

Journée informatique d'IN2P3, 2020/11/19

Scope:

CERN – Know your (security) footprint

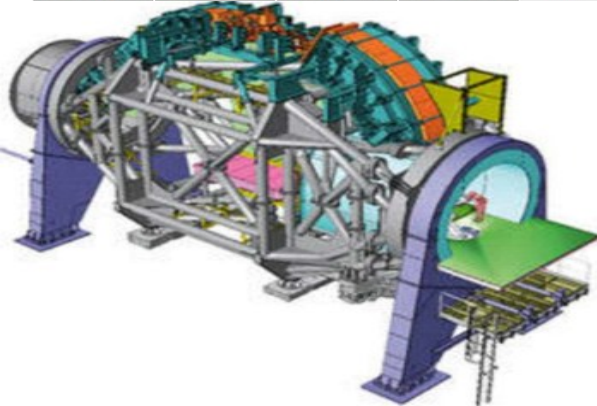
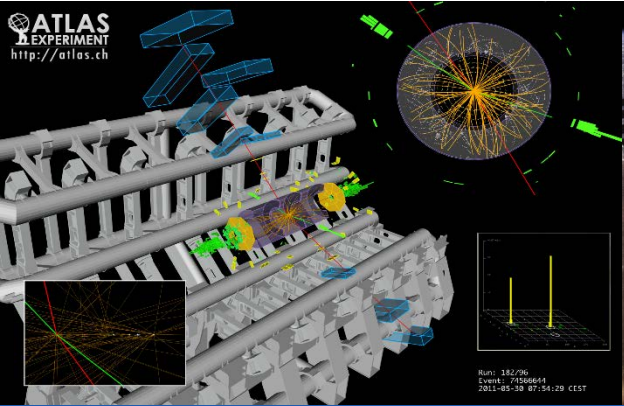
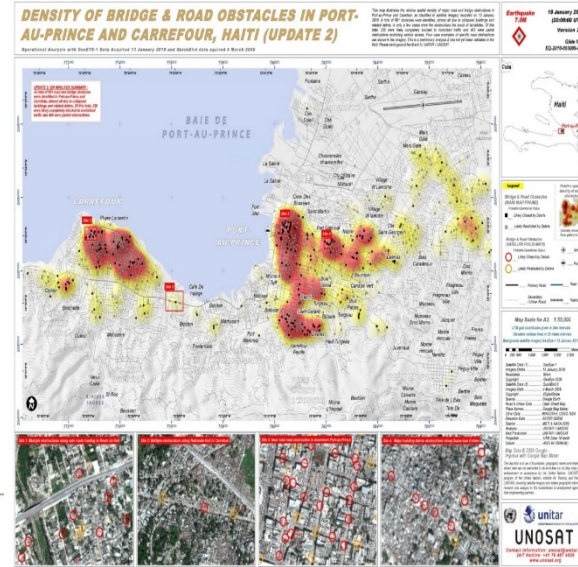
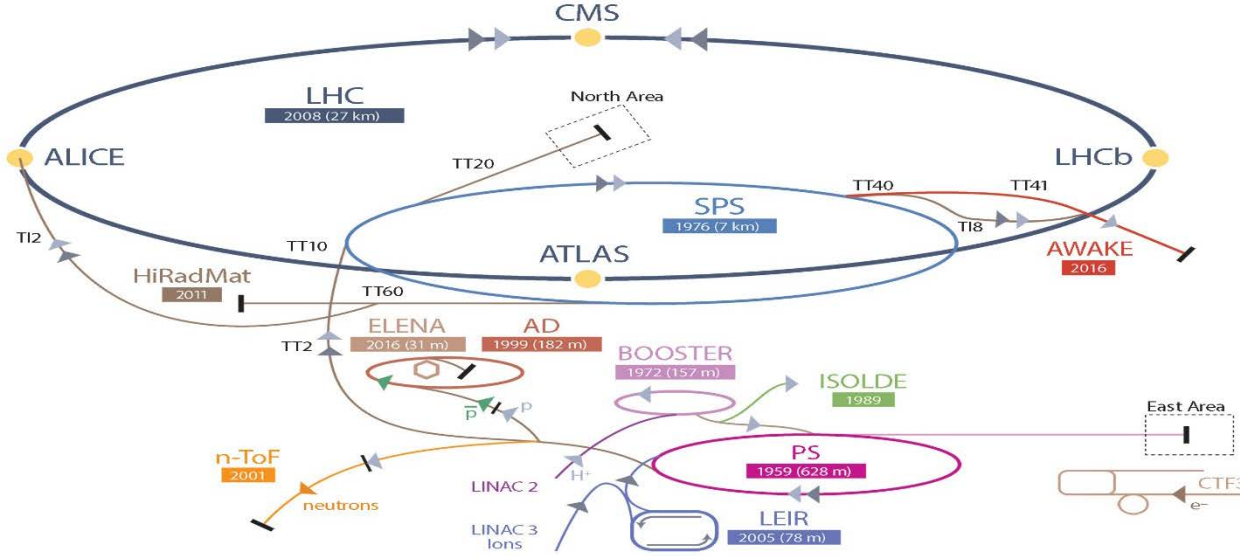
Risks:

Adversaries & Limitations

Controls:

Prevention/Protection, Detection & Response

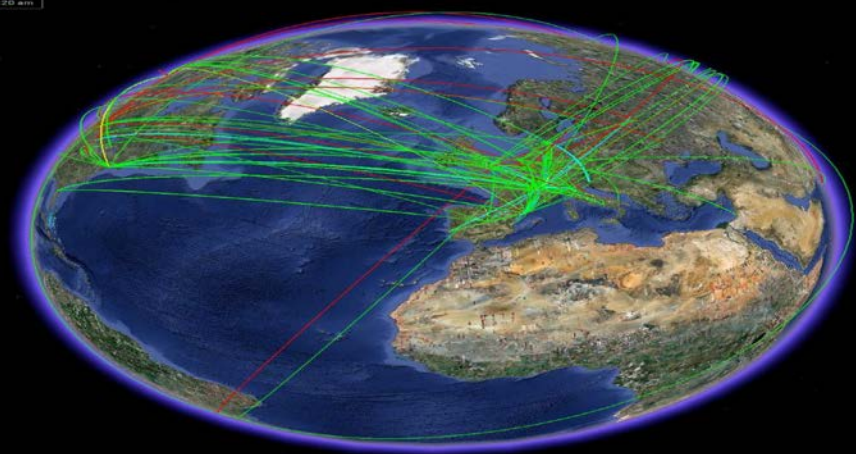






Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
Journée informatique, Nov. 19th 2020

A Worldwide Endeavour

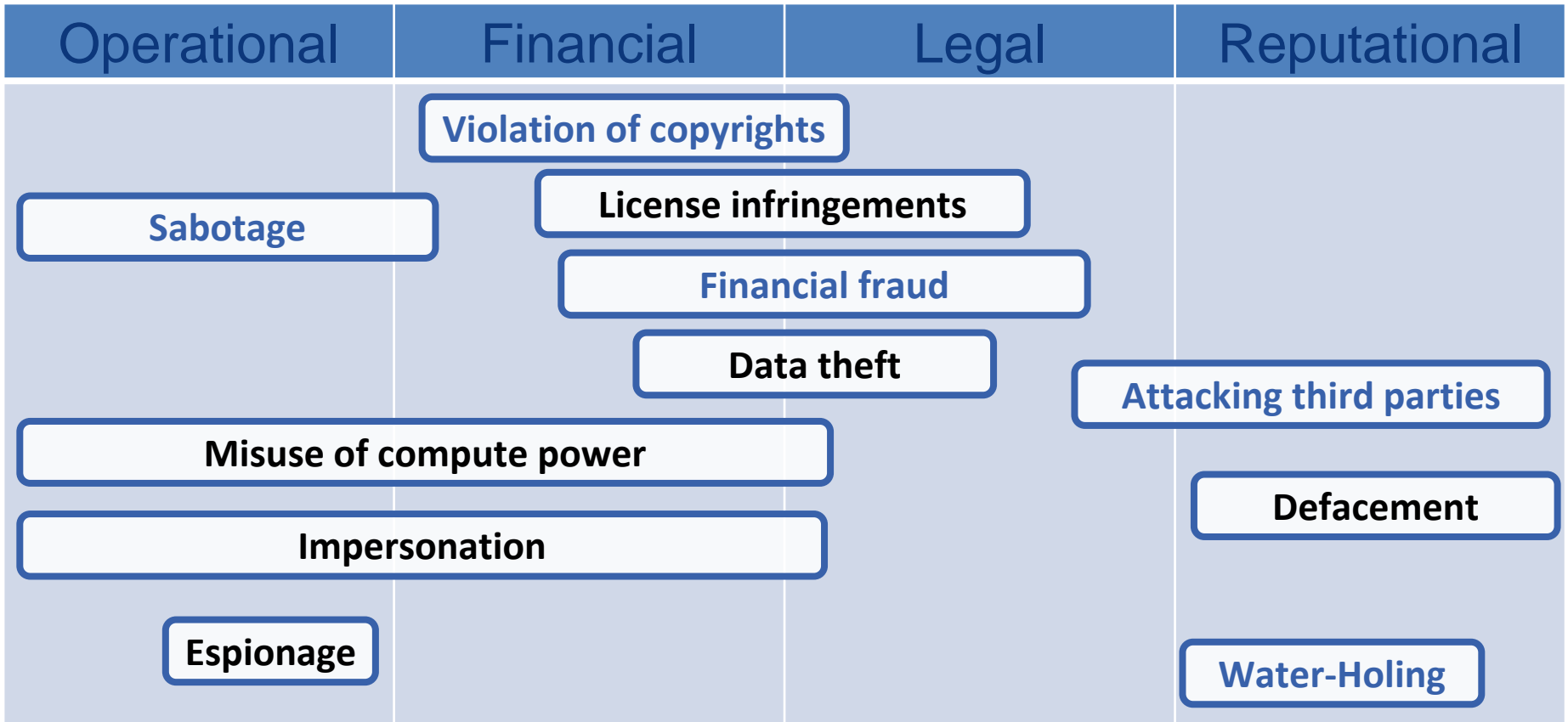


Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image © 2010 TerraMetrics
Image: Bing
© 2010 Chesapeake
38°12'16.64" N 11°55'14.00" W elev. 0 ft



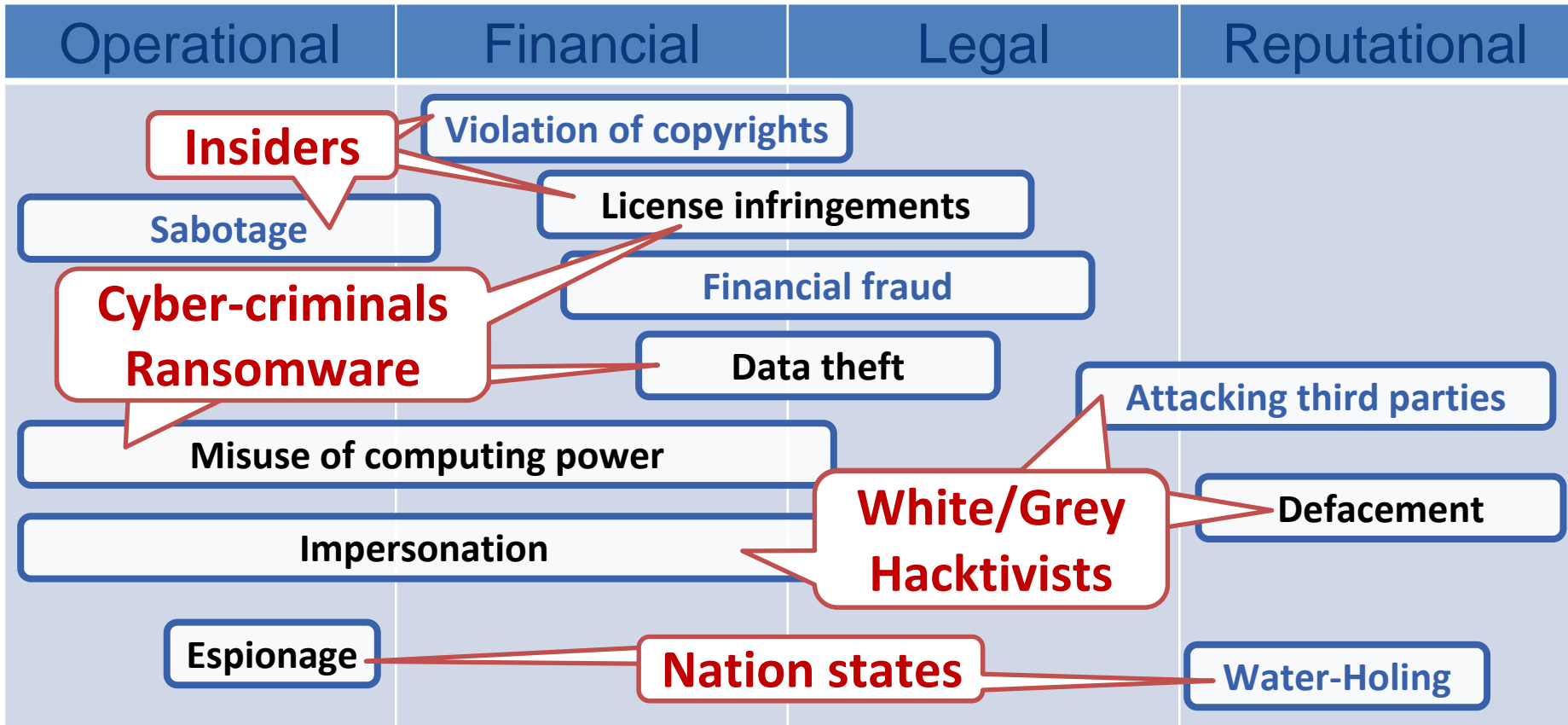
Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
Journée informatique, Nov. 19th 2020

Sectors of “Security” Operation



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





Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations

Controls:

Prevention/Protection

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.**



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.

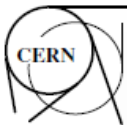
Information Access, Sharing and Disclosure

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.





Log in with your CERN account

Username

Password

This operation the Standing meeting of 7 Ju

In the interests masculine gender and women excep

3

Confirmation

DO NOT submit this request if the contact person does not know you or is not aware of your request!

An email will be sent to the contact person for your approval.

After the operation is completed, a confirmation message will be sent to your email address.

By submitting this form, you agree to comply with the [CERN computing rules](#).

I confirm that I have read and understood the [Computing Rules](#).

[Change password](#)

I have read and agreed to the [CERN Computing Rules](#) and taken into account the [website lifecycle policy](#).

[Create new website](#) (All fields are mandatory)

OC5

Please be aware that repeated, or a single sufficiently grave, infringement of CERN's Computing Rules (OC5) can result in the consequences defined in Section V 21, including the withdrawal of access to CERN computing facilities.

I confirm that I have read, understood and will abide by the [CERN Computing Rules \(OC5\)](#).

[Submit](#)

```
* *****
* Welcome to lxplus722.cern.ch, CentOS, 7.8.2003
* Archive of news is available in /etc/motd-archive
* Reminder: you have agreed to the CERN
* computing rules, in particular OC5. CERN implements
* the measures necessary to ensure compliance.
* https://cern.ch/ComputingRules
```



Accounts

Name, mail, login or ID

Search login only

Stefan Lueders (slued) Website review

Please review the sta

• Commitment

• LUI

Device

- Devi
- Loca
- Mani
- Mod
- Gen
- Desc
- Tag:
- Seria
- Oper
- CER
- Netw
- Resp

Website

Show

Website

apeg

aprilfo

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

Last changed: 14-07-2016 (10:32)

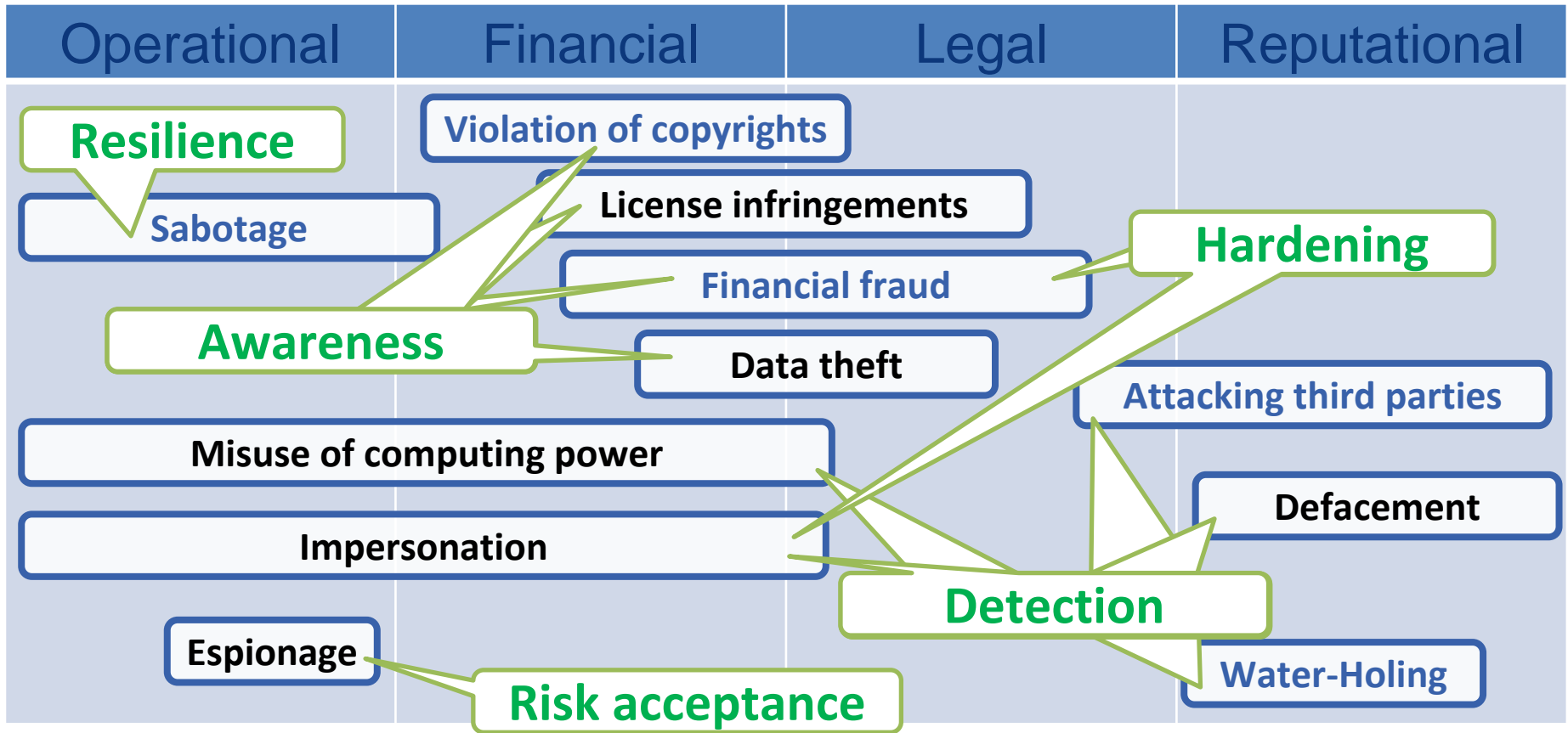
Firewall: Approval process with pentest & assessment



OpenVAS logo: A green dragon head inside a circle with dots around it.

skipfish logo: A stylized 'S' made of blue, red, and green shapes, with the text 'skipfish web application security scanner' below it.

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





SECURITY is not complete without U

“Home” Awareness

Quelques astuces pour protéger votre ordinateur et vos données

Posters, videos, ...you-name-it

Induction & On-Boarding Mandatory online courses Technical trainings

Consulting & audits Pre-Purchase analysis

SECURITY is not complete without U

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.

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.

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.

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.

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.

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.



Finding the Balance for Security
Dr. Stefan.Lueders@cern.ch
Journée informatique, Nov. 19th 2020

Six Recurrent Themes

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

**EXERCISE
ONLY**



BREAKING NEWS

CERN - EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH 'VICTIM OF CYBER ATTACK'
Personal details of around 1,000 CERN employees for sale on the dark web

SVN24

FOR EXERCISE PURPOSES ONLY - THIS CLIP CONTAINS FICTITIOUS INFORMATION - FOR E



Static Code Analysis Tools

Below you find recommendations for developers.

quickly, looking at non-secure code.

This is a suitable tool for Computer Security.

selection. And

The availability of Git for projects for

Securing Containers & Pods

Often people who are new to container and orchestration technologies are under the impression that these products are inherently secure and suitable for production use. While that might not be true, these solutions offer a lot of configuration options for strengthening the security of the containerized environment in order to get protections similar to that of a virtual machine. This way you can ensure that even if an attacker

How to keep secrets secret (Alternatives to Hardcoding Passwords)

"Hardcoding passwords" is a short name for putting non-encrypted (plain text) passwords and other secret data (like private keys etc.) into the source code. Typical examples could be:

```
...
private static String passwd = "mYv3rYSECr3tPWD";
...
db = MySQLdb.connect(host="db.server.com", user="admin",
passwd="NOBODYwilleVERguess", db="sales")
...
String url = "jdbc:mysql://" + serverName + "/access?user=webclient&
password=ILoveJuliet";
...
for i in 01 02 03 04; do ./remove_temp_files.sh --machine=appserv$i
--rootpassword="*d3H*sS-W"; done
...
```

Although software developers might not realize, in fact their source code is (or

Web Services

Manage your CERN websites

Home

My websites

Service Status

Current site is <http://cern.ch/apeg>

 Your access level is: **Site owner**


 [View details of apeg](#)


 [Manage this site](#)

 [Open website](#)


Toolbox for current site

 [Delete apeg](#)

 [Site Access & Permissions](#)

 [View quota usage](#)

 [View site statistics](#)

 [Download site logs](#)

 [Security scan](#)

 [Piwik web statistics](#)

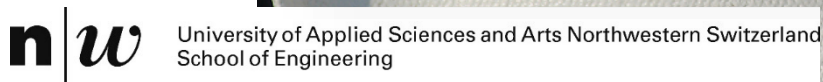
 [Archive site](#)



**Safety first
Availability next
Security third**

Impact & criticality analyses

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



HackCERN Penetration Test Report

Prepared for:

Dr. Stefan Lüders
CERN Computer Security Officer
European Organization for Nuclear Research (CERN)
Building 31, Room R-009, [PostBox G24010](#)
CH-1211 Geneva 23

Prepared on:

September 12th, 2017

Prepared By:

Allan Stojanovic
Team Lead [HackCERN](#) Project
Senior Security Architect and Analyst
University of Toronto
4 Bancroft Ave., Room 114
Toronto, Canada
M5S 1C1





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

Is the sender familiar to you?

Does the sender's name correspond with the shown e-mail-address?

Is the message addressed to you?

Hover your mouse pointer on top. Does the text correspond with the link?

Does the link look reasonable, is not too complex or unreadable?

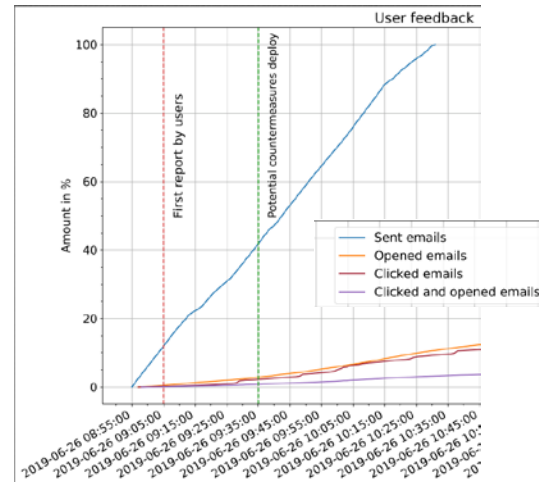
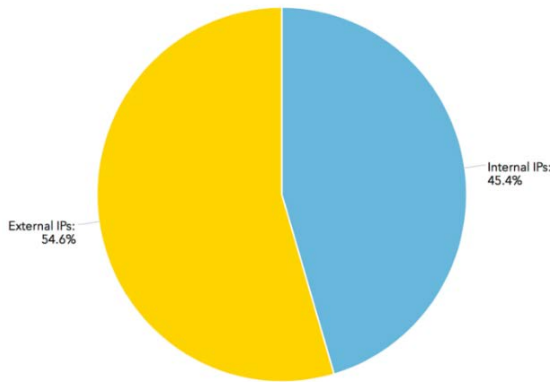
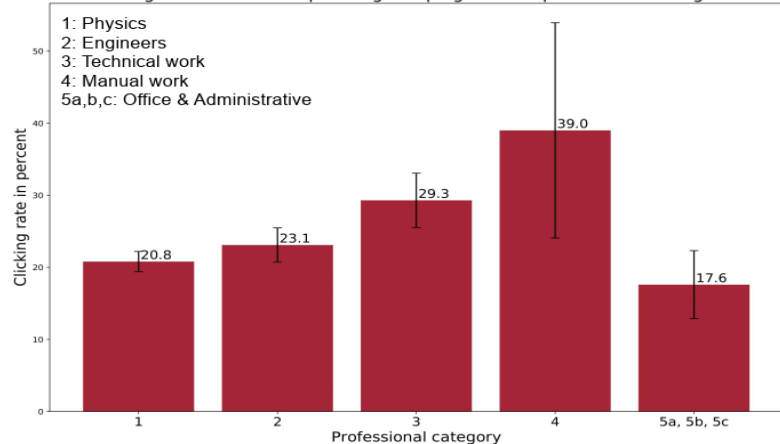
Does the message concern you? Is it one of your businesses?

Is the message signed ()?

Is the message correctly phrased, without blunt typos, in a language you are able to comprehend?

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.

Clicking rate of the 2019 phishing campaign across professional categories



Click rate (2016-2020): ~20.0%

DNS blocking catches only 50%...

...and you have to be quick!

To: cert-snow@cern.ch, service-desk@cern.ch
Subject: [security concern] FW: Testing of new boo

To: cert-snow@cern.ch
Subject: FW: Successful login attempts

Dear CERN's security experts,

Subject: FW: Testing of new booking system

Yesterday I received an email on my cern.ch account

This seems a very well done phishing email, using the name of "CERN Depart
Regards,

Hello,

- 1) The sender's email address ends with cern.com
- 2) The
- 3) The

I didn't click, but I forwarded it to a colleague and he clicked it to see the page...

I was
Please look into it and let me know if there is something to worry about.

Best Regards



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



CERN Computer Security

Computer security emergency contact
✉ Computer.Security@cern.ch ☎ 70500
Contact en cas d'incident de sécurité informatique

Home | Computing Rules | Recommendations | Training | Services | Reports & Presentations



Oops... We prefer you not going there...

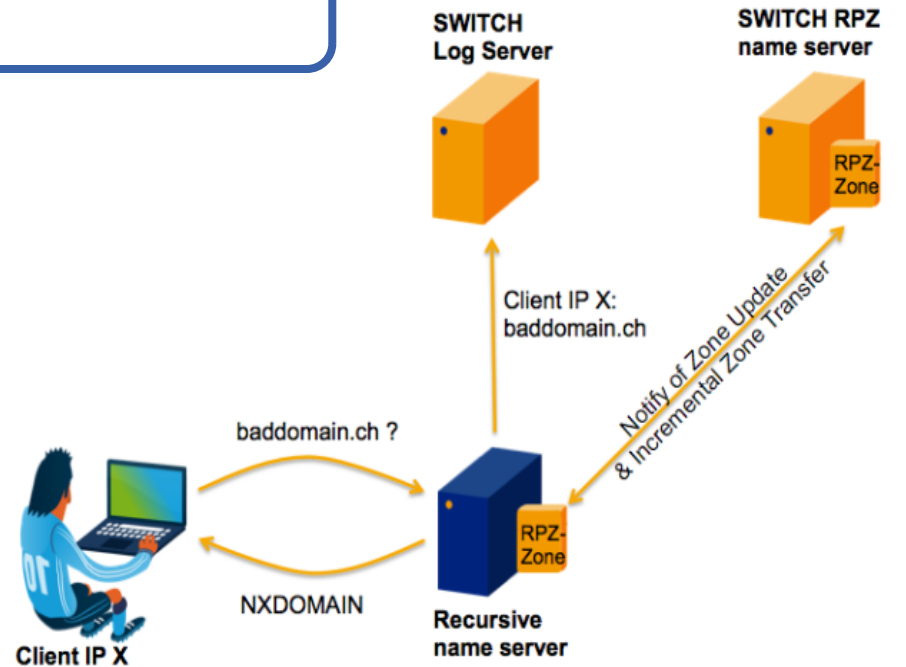
The page you were looking for has been blocked as it is likely hosting malicious contents.

"Malicious contents" is either malware, i.e. software aiming at infecting your PC, or a "Phishing" portal, where "Phishing" is a technique to trick you in disclosing your password. In the latter case, probably you just clicked on a link in a corresponding "Phishing" email sent to your CERN mail address? If so, just delete this email and ignore the web-site!

If you think that this web-site should be accessible from CERN, please contact us at Computer.Security@cern.ch.

Oops... C'est mieux si vous n'y allez pas...

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



Synchronizing with SWITCH's list of bad domains

JUNE 20TH, 2016

SECURITY BASELINE FOR HARDENED PCS AND LAPTOPS



PC Hardening & Alternative PDF Reader



Dedicated appliance to block sophisticated malicious emails & attachments

Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations

Controls:

Prevention/Protection, Detection



	11/17/2020, 6:36:57 AM	sviluppo_economico_20_245.xlsx	3 Malwares 15 Behaviors
	11/16/2020, 10:57:45 PM	EXCEL XLS FILE.htm.	Malware.Binar 8 Behaviors

Serving CERN, the WLCG and the HEP and academic community



Events - MSP

Home Event Actions Input Filters Global Actions Sync Actions Administration Audit Discussions

List Events
Add Event
Import From MISP Export

List Attributes
Search Attributes

View Proposals
Events with proposal

Export
Automation

<input type="checkbox"/>	2020-05-22	Network activity	domain	branter.tk	
<input type="checkbox"/>	2020-05-22	Artifacts dropped	regkey	{59031A47-3F72-44A7-80C5-5595FE6B30EE}	
<input type="checkbox"/>	2020-05-22	Artifacts dropped	regkey	(HKLM\HKCU)\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID	
<input type="checkbox"/>	2020-05-22	Artifacts dropped	regkey	HKLM\SOFTWARE\Microsoft\Software\Windows.WSqmCons	
<input type="checkbox"/>	2020-05-22	Artifacts dropped	filename	%TEMP%\iecache.bin	
<input type="checkbox"/>	2020-05-22	Artifacts dropped	filename	%TEMP%\FXSAPIDebugTrace.t	

Synchronized with CH law enforcement & CH CERTs

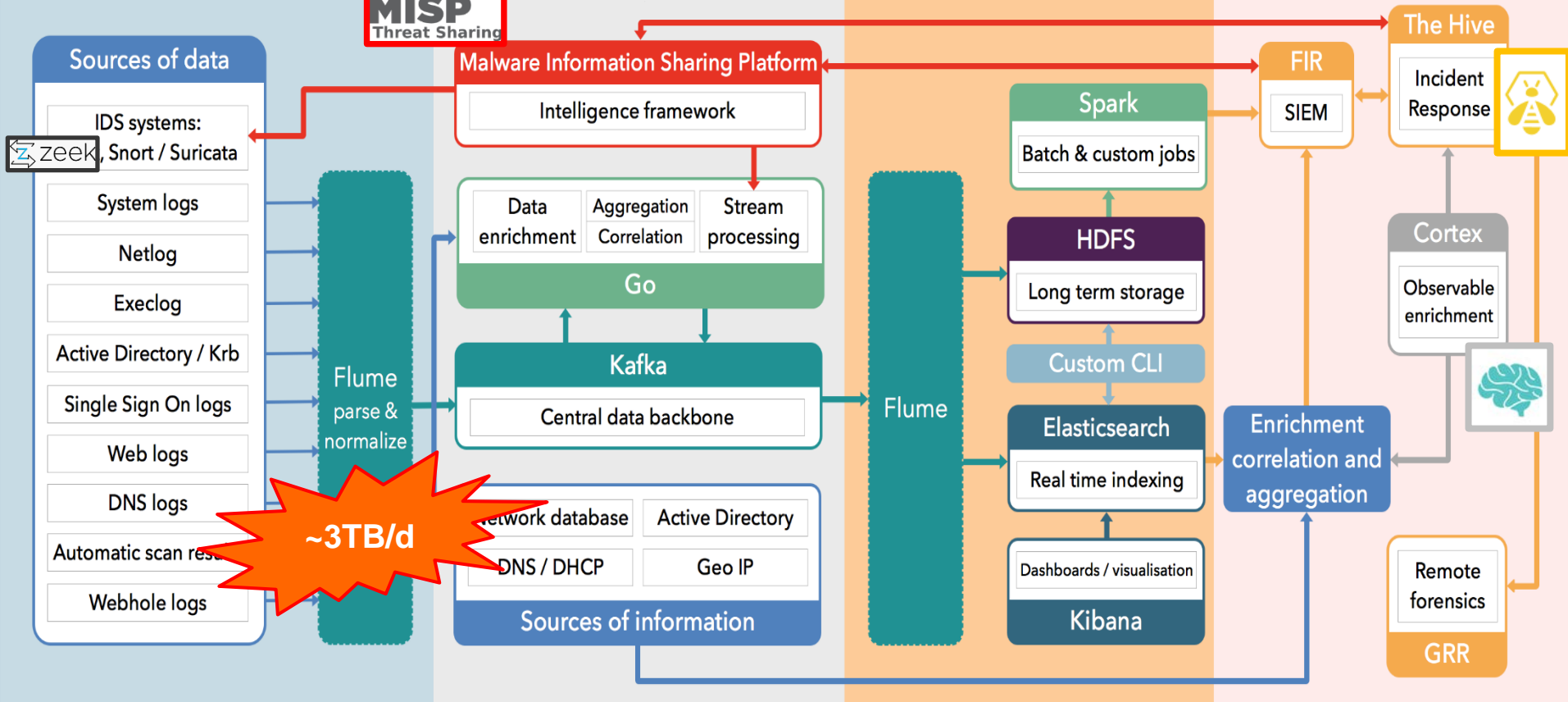
Also from external feeds:

Data ingestion

Data processing

Storage and visualisation

Incident response



Scope:

CERN – Know your (security) footprint

Risks:

Adversaries & Limitations

Controls:

Prevention/Protection, Detection & Response



Vulnerable device: [REDACTED]

Europe/Paris

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

Date	Category	Subject	Business Lines	Severity	Status
2020-05-25	★ Devices/SuspiciousActivity	Suspicious activity detected on device [REDACTED]	[REDACTED]	2	Open
2020-05-22	★ Devices/SuspiciousActivity	Suspicious activity detected on device [REDACTED]	[REDACTED]	2	Open
2020-05-22	★ Devices/SuspiciousActivity	Suspicious activity detected on device [REDACTED]	[REDACTED]	2	Open
2020-05-18	★ Devices/VulnerableWebserver	Your device [REDACTED] has not had a Puppet-run in 2020	[REDACTED]	2	Open
2020-05-18	★ Devices/VulnerableWebserver	Your device [REDACTED] has not had a Puppet-run in 2020	[REDACTED]	2	Open
2020-05-14	★ Webservices/VulnerableWebsite	Directory traversal vulnerability on the CERN [REDACTED] website	[REDACTED]	3	Open

I have setup stronger credentials for this device.
 I disabled the protocol which was detected as being insufficiently protected.
 I have updated the owner of this device, since I do not own it anymore.



CERN Computer Security

Computer security emergency contact
✉ Computer.Security@cern.ch ☎ 70500
Contact en cas d'incident de sécurité informatique

Home Computing Rules Recommendations Training Services Reports & Presentations

Privacy Statement

Computer Security Incident Response

Emergencies

Self-mitigation portal

Audits & Reviews

...on request

CERN WhiteHat Challenge

Host-Based Intrusion Detection

Central security logging

"SSH receipts"

Traffic Control & Monitoring

DNS analysis

Network-based intrusion detection

The CERN outer perimeter

What to do in an Emergency

If you have detected or encountered a security event, there are four basic steps to take:

- **Don't panic:** Security events develop and spread quickly. Panicking now and taking hectic actions is usually worsening the situation. If any damage has been done, it has been done already by now;
- If this concerns a device, **keep it connected and leave it "on"**: Do *not* disconnect the system/service/device from the CERN network by pulling out its Ethernet cable or by disabling the wireless adapter. Do *not* switch the power off !!!
- If this concerns an account, **Reset your password**: Do so via the [CERN account portal](#) . You might be asked to reset it again once that event has been understood;
- **Contact the Security Team**: Computer.Security@cern.ch or call 70500 (+41 22 767 0500) from inside (outside) CERN. Details as well as our PGP key can be found [here](#);
- **Don't touch anymore**: Wait for instructions before taking any further actions. Depending on the impact, we might have to understand the event in detail. Uncoordinated actions might destroy evidence.

- Triage
- Taking over service

- Coordinating comm's
- "Avalanching"
- Forensics



- Close out

CERN also provides incident response & forensics services to the WLCG, EGI as well as the HEP and academic community world-wide



CERN Computer Security

Computer security emergency contact



Home | Computing Rules | Recommendations | Tra

Security Reports

Monthly reports on CERN security

Monthly security reports from SWITCH CERT

Articles & Announcements

Articles in the CERN Bulletin, Computing Newsletter & others

Announcement archive

SWITCH Security Blog

Monthly reports on

If you are interested to receive reports, please contact us to the "cert-security-info@cern.ch"

2020

January - February - March

2019

January - February - March - April - May - June - July - August - September - October - November - December

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



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





www.cern.ch

Thank you for listening!

Questions?