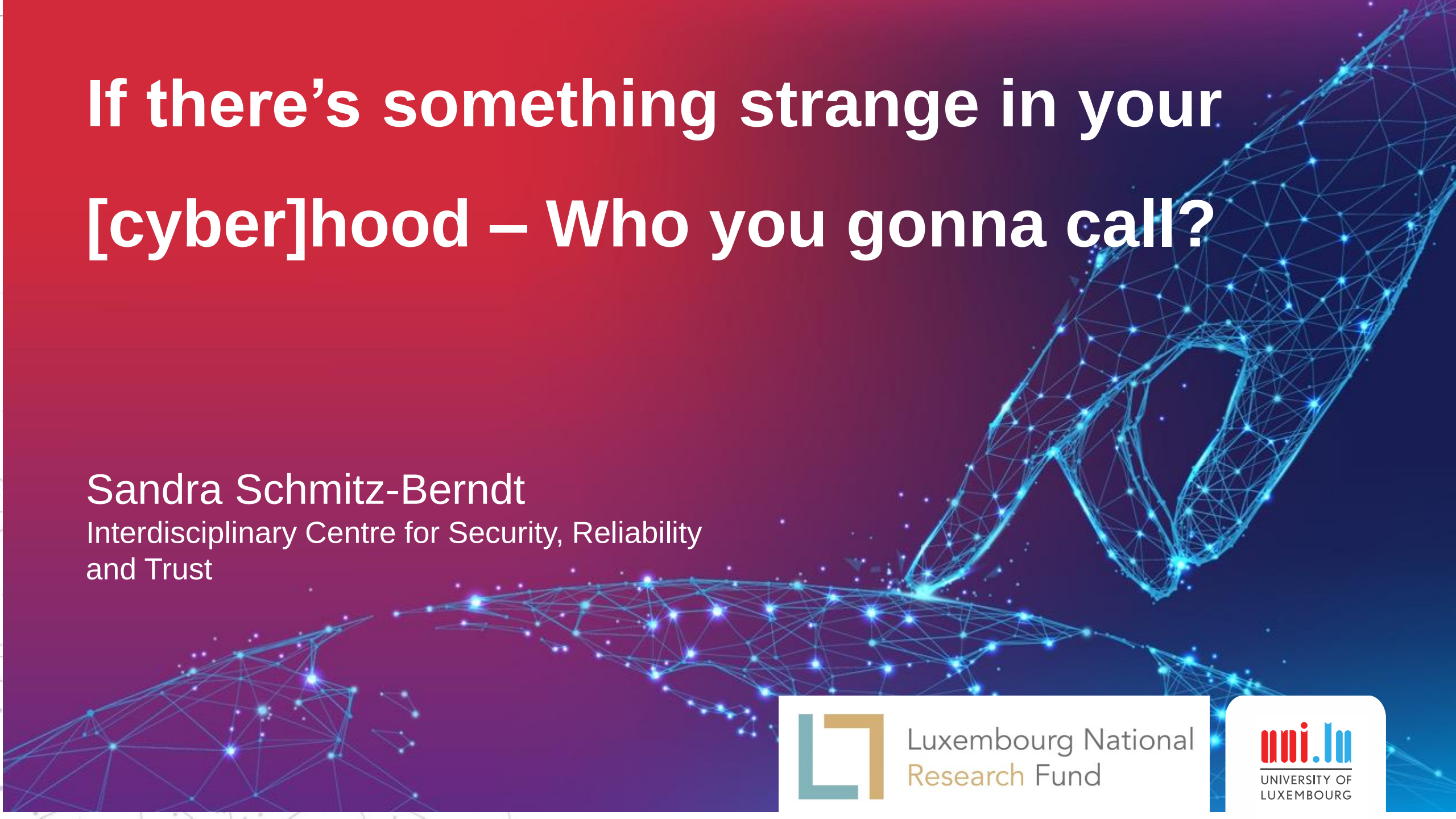
If there’s something strange in your [cyber]hood – Who you gonna call?

Sandra Schmitz-Berndt
Interdisciplinary Centre for Security, Reliability and Trust



Luxembourg National Research Fund

UNIVERSITY OF LUXEMBOURG

Agenda

1. If there's something strange in your neighborhood
2. If you're seeing things running through your [system]
3. If there's something weird and it don't look good, who you gonna call?
4. Don't get caught alone
3. I ain't afraid of no ghost

Threat awareness

Detect

Respond

Information sharing

Learn

1. Something strange in your neighborhood

TECH

Solarwinds hackers are targeting the global IT supply chain, Microsoft says

PUBLISHED MON, OCT 25 2021•7:46 AM EDT

Sam Shead
@SAM_L_SHEAD

UK warned to bolster defences against cyber attacks as Russia threatens Ukraine

By Gordon Corera
Security correspondent

28 January

February 24, 2022
5:50 PM GMT+1
Last Updated a month ago

Europe

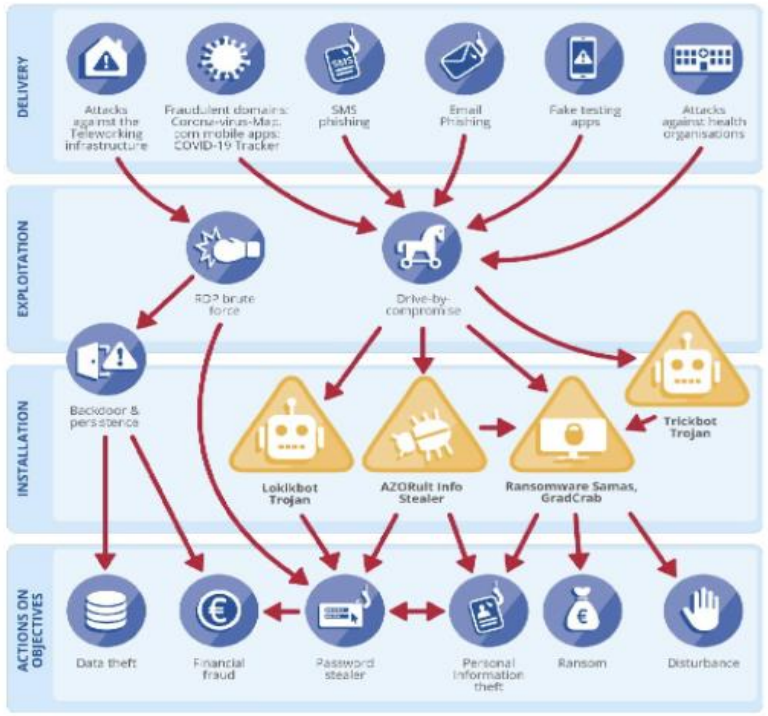
Ukraine computers hit by data-wiping software as Russia launched invasion

Reuters

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREAT LANDSCAPE MAPPING

Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

RANSOMWARE/DDOS

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung
Lösegeld-Erpressung
Schutzgeld-Erpressung

13 Tage lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.

144 MIO. neue Schadprogramm-Varianten
+22 % gegenüber 2020: 117,4 MIO.

DURCHSCHNITTLICH **394.000** neue Schadprogramm-Varianten pro Tag (2020: 322.000)
IM HÖCHSTWERT **553.000** (2020: 470.000)

DOPPELT SO VIELE BOT-INFEKTIONEN DEUTSCHER SYSTEME pro Tag im Tagesspitzenwert
20.000 > 40.000

98 % aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

ENISA: attacks on supply chains will have fourfold in 2021 compared to 2020

uni.lu | SnT

1. Something strange in your neighborhood

attacks

- Number
- Magnitude
- Sophistication
- Frequency
- Impact

+

risk surface

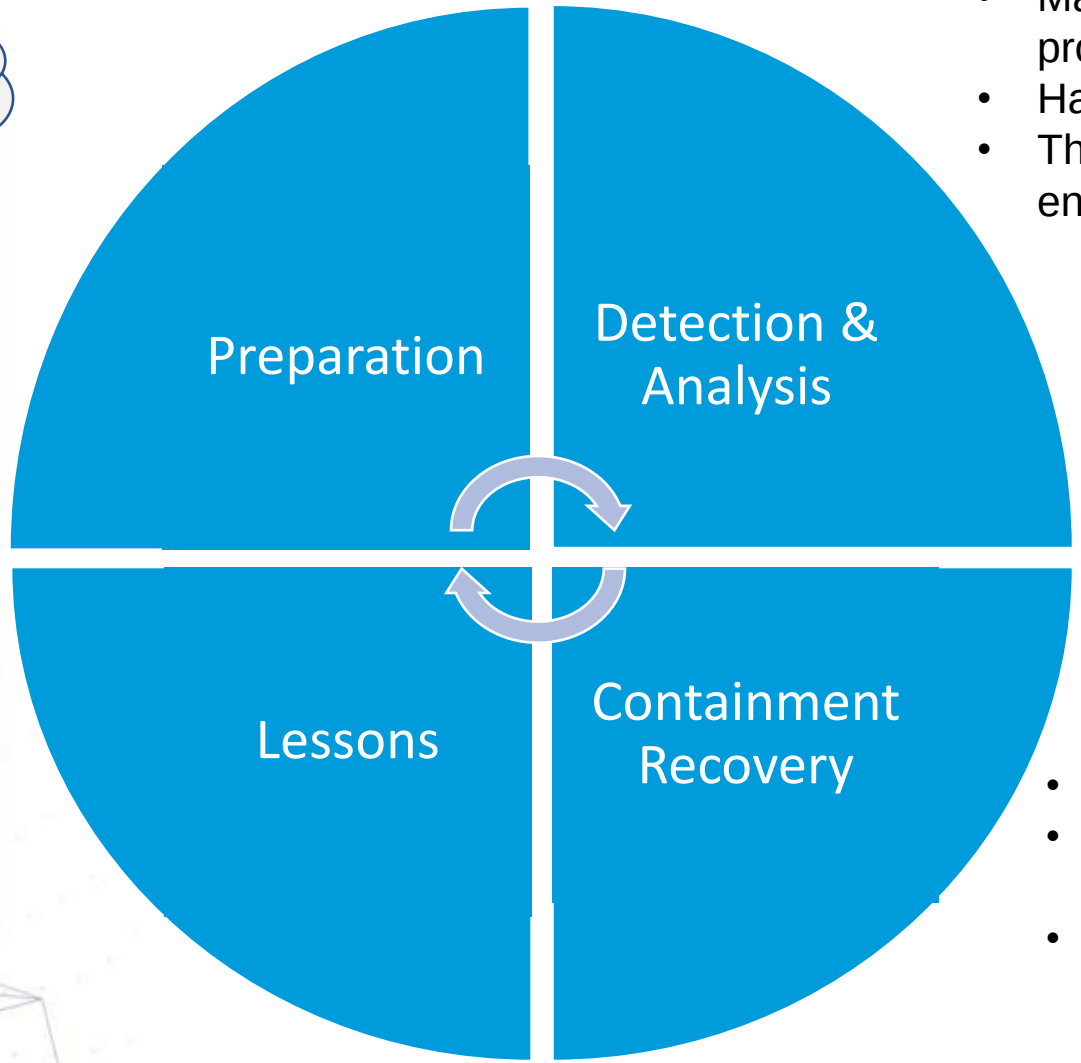
- Digital transformation
- Interconnectedness of society
- Connection of objects (IoT, etc.)
- Digitisation of internal market

Amplification during COVID19 crisis

=

Expanded cybersecurity threat landscape

2. *If you see things running through [your system]*



- Map IT system to functions, process and servicess
- Have an incident response plan
- Threat analysis = Know your enemy

- Monitor system
- Collect and analyse data to identify source of attack
- Track attacked system

3. If there's something weird and it don't look good, who you gonna call?

NIS Directive	MAJOR INCIDENT REPORTING for Operator Essential Services
GDPR	DATA BREACH NOTIFICATION
eIDAS Regulation	INCIDENT REPORTING for Trust Services Providers
PSD2	INCIDENT REPORTING for Payment Service Providers
ECB/SSM	INCIDENT REPORTING for Significant financial institutions
Target 2	INCIDENT REPORTING for Critical Participants
National Regulation	NATIONAL INCIDENT REPORTING (Systemically Important Processes)

EBF position on cyber incident reporting

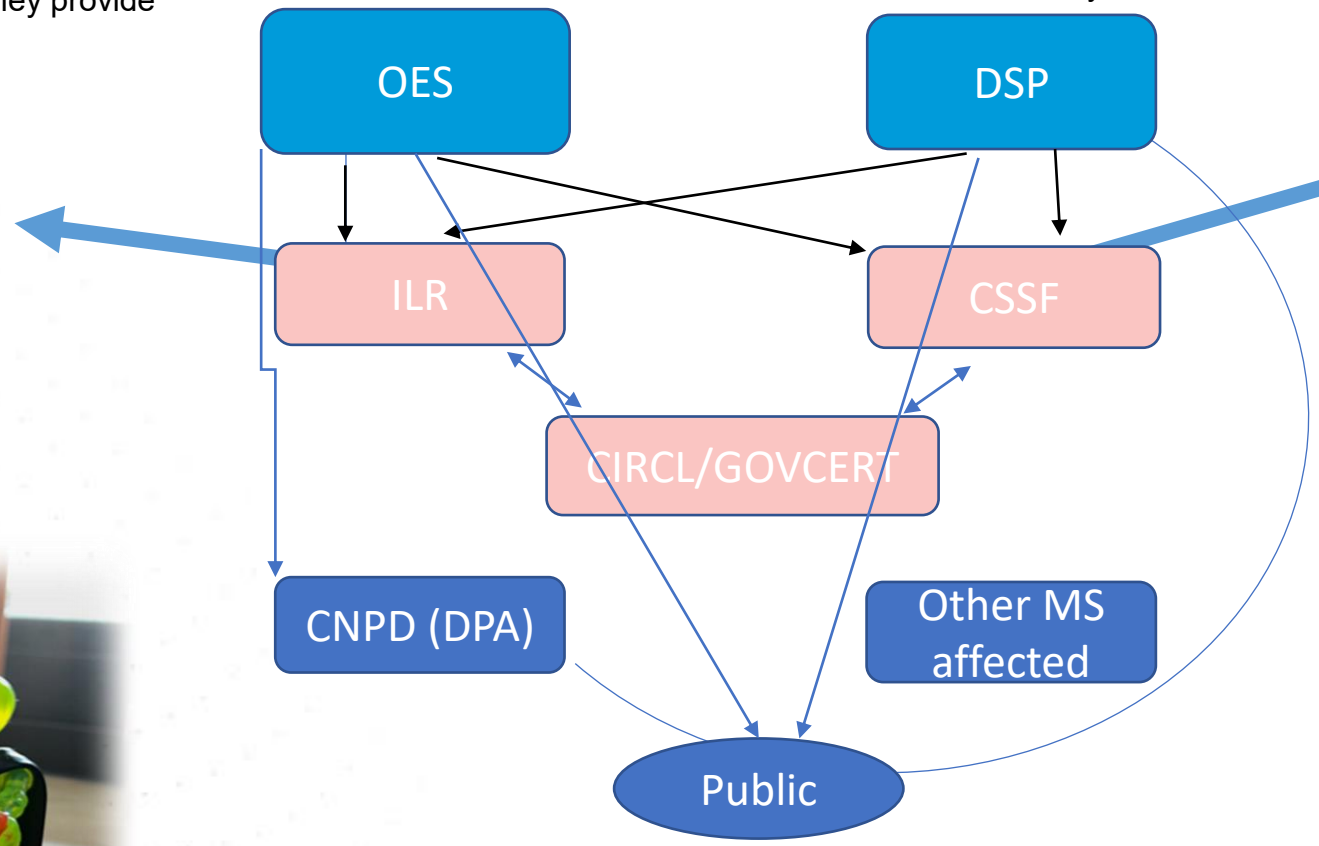
3. If there's something weird and it don't look good, who you gonna call?

and you provide services as a DSP or OES in Luxembourg…

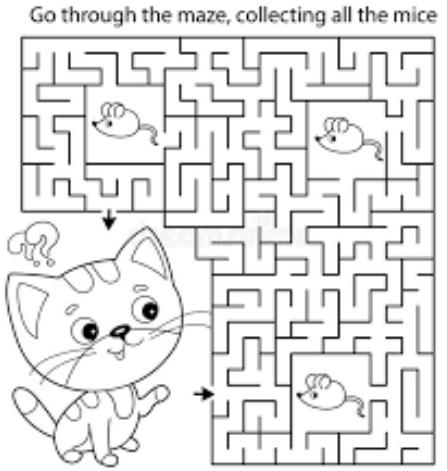
Art. 14(3): 'incidents having a **significant impact** on the continuity of the essential service they provide'

Art. 16(3): 'incidents having '**a substantial impact**' on the provision of a service 'that they offer within the Union' (Art. 16(3))

ILR (NISD 1148/2016):



CSSF (NISD 1148/2016):



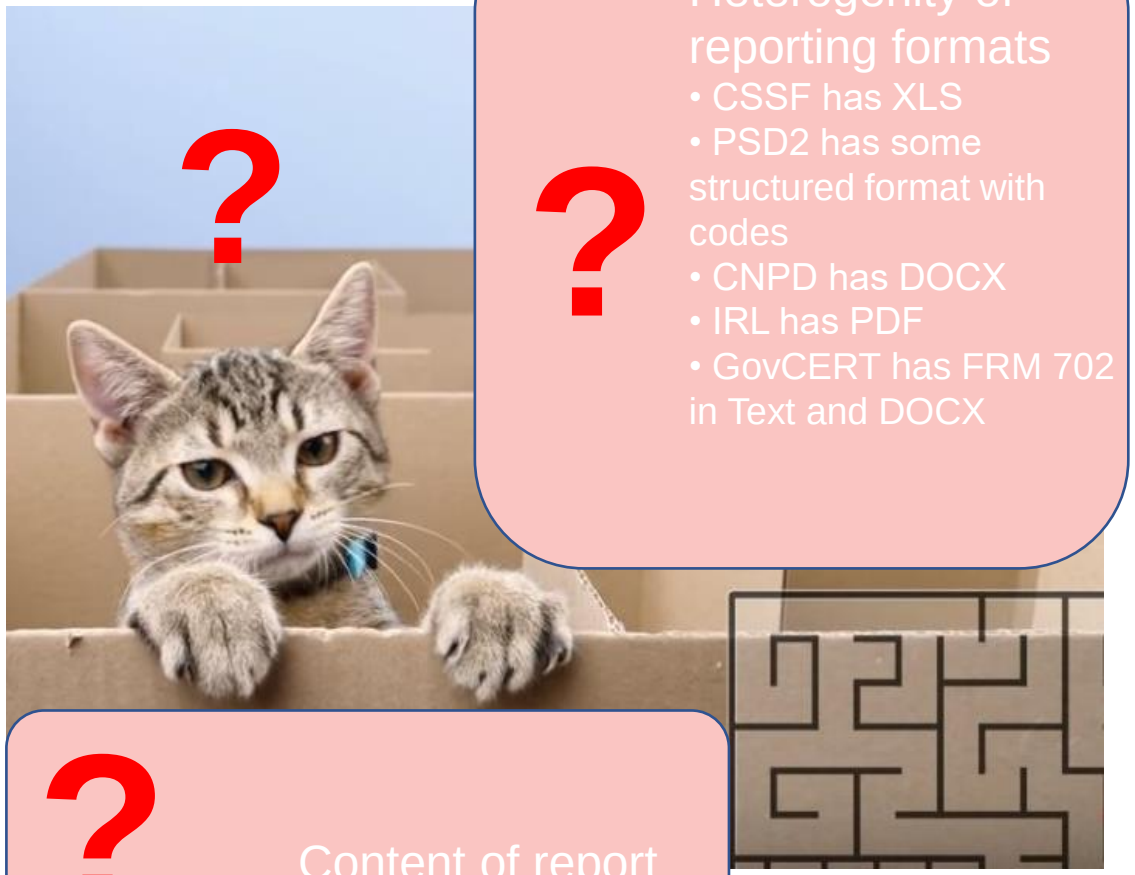
Incident = any event having an actual adverse effect on the security of NIS (Art. 4(7))

3. If there's something weird and it don't look good, who you gonna call?

MAIN INCIDENT REPORTING FRAMEWORKS IN EU

NIS Directive	MAJOR INCIDENT REPORTING for Operator Essential Services	NATIONAL NIS AUTHORITY	Without undue delay	Common EU cross-industry regulations (valid also for financial institutions)
GDPR	DATA BREACH NOTIFICATION	NATIONAL DATA PROTECTION AUTHORITY	Within 72 Hours	
eIDAS Regulation	INCIDENT REPORTING for Trust Services Providers	NATIONAL CERTIFICATION AUTHORITY	Within 24 Hours	
PSD2	INCIDENT REPORTING for Payment Service Providers	NCA / ECB / EBA	Within 4 Hours	Common EU stakeholders for financial institutions
ECB/SSM	INCIDENT REPORTING for Significant financial institutions	ECB / Joint Supervisory Team	Within 2 Hours*	
Target 2	INCIDENT REPORTING for Critical Participants	National Central Bank / TARGET 2	Within 48 hours	
National Regulation	NATIONAL INCIDENT REPORTING (Systemically Important Processes)	NATIONAL BC AUTHORTY (CODISE)	Without undue delay	Local opportunity of harmonization

EBF position on cyber incident reporting



4. Don’t get caught alone

	NIS 1.0	NIS 2.0 (Council Compromise)
Initial notification as an early warning	-	Yes, within 24 hours; where applicable indicating whether the incident is presumably caused by unlawful or malicious action
Feedback by Authority	-	Yes, without undue delay, including guidance on mitigation measures (in collaboration with national CSIRT)
Reporting	“without undue delay”	„without undue delay“ + Intermediate report upon request + Final report within one month following the initial notification incl. detailed description of the incident, its severiy and impact; type of threat or root cause; applied and ongoing mitigation measures encouragement of voluntary sharing
Single entry point	no	Encouraged for sector-specific EU legislation and personal data breaches (GDPR)

Alleviates burden to identify competent authority, but does not align notification timeframes or content of report

\+ ISACs (voluntary & private)

4. Don't get caught alone

and protect yourself

Art. 14(2): Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

These are real answers received from suppliers handling ICT infrastructure (not necessarily OES/DSP)

- ❑ switch-off multi-factor-authentication (MFA) as technical measure
- ❑ Do not apply patches as technical measure, because
  - ❑ Loss of compliace eg as regards medical devices
  - ❑ No time for testing the patches
  - ❑ No resources to make mandatory risk assessment, pentesting or tests

Source: CIRCL.LU

"security is always excessive until it's not enough"

4. Don’t get caught alone

And protect yourself

Real answers continued:

- ❑ Apply patches only 4 times a year as technical measure or due to contractual reasons
- ❑ Disable packet filtering as technical measure on industrial control systems (on-call operators or suppliers cannot connect remotely from their networks anymore)
- ❑ Disable logs/do not read logs since the less you detect, the less you have to report

Source: CIRCL.LU

“creative problem solving”

4. Don’t get caught alone

And protect yourself

Real answers continued:

- Logs are from the wrong day (no evidence of lateral movement)
- Only keep backups on online servers, because this is easier to manage
- CERT asks if forensics report was done and a report from an AV scan is sent by the supplier
- CERT informs about a compromised server due to a missing patch and supplier replies „now patched, all good“; CERT clarifies that a compromised patched server is still a compromised server and receives a report from an AV scan

“the best way to get management excited about a disaster plan is to burn down the building across the street”

5. I ain't afraid of no ghost

- Sharing is caring:
  - better sharing of information to combine metrics, investigation, impacts and technical reports;
  - Understand impact and use the experience to improve security
  - Feedback on incident reports

- Make things easier with a single entry hub
  - Should alleviate burden to identify competent authority
  - Should safeguard compliance with reporting format and content
  - However: does not provide for an alignment of reporting timeframes

Interdisciplinary Centre for Security, Reliability and Trust

Contact: sandra.schmitz@uni.lu

This research was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancingcybersecurity-across-vital-business-sectors-encavibs/.

Connect with us

@SnT_uni_lu

SnT, Interdisciplinary Centre for Security, Reliability and Trust