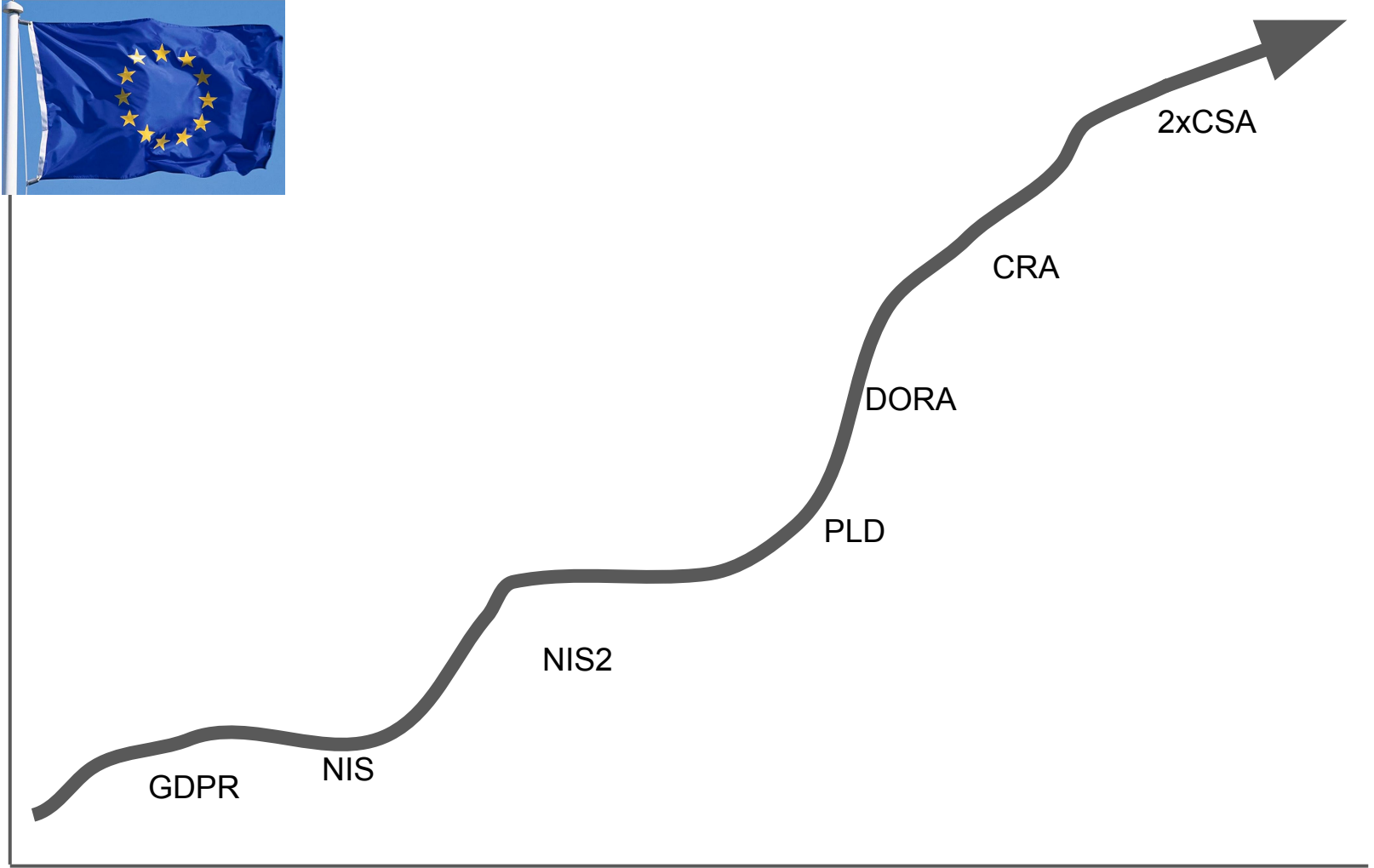


# EU and You: Upcoming regulation



[bert@hubertnet.nl](mailto:bert@hubertnet.nl) / <https://berthub.eu/>

Governments are  
coming to help us  
make more secure  
stuff!



GDPR

NIS

NIS2

PLD

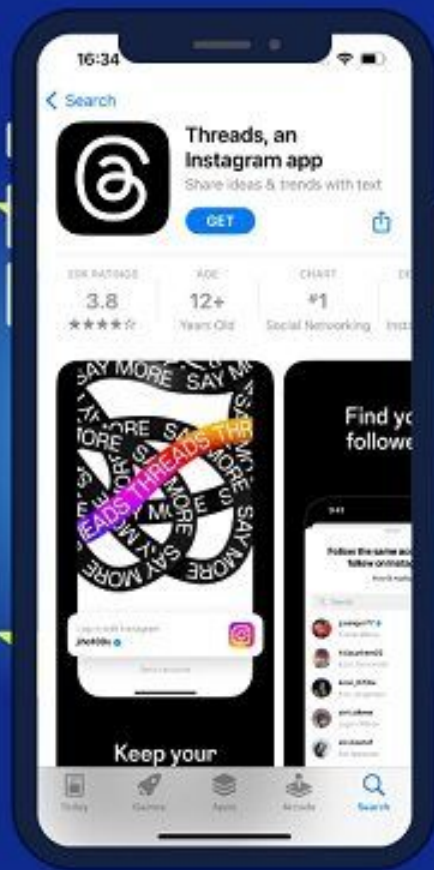
DORA

CRA

2xCSA



Not Available in the EU?







Thanks to BS EN 13772:2011, EN 1021:1994, EN 1021-1, EN 1021-2

**Awkward moment pro-Brexit protester fails to burn EU flag**





## Brits bedrijf mede wegens ransomware failliet, 730 medewerkers op straat

woensdag 27 september 2023, 09:46 door **Redactie**, 6 reacties

Het Britse logistieke bedrijf KNP heeft mede wegens een ransomware-aanval **faillissement aangevraagd**, waardoor 730 medewerkers hun baan verliezen. De aanval vond eerder dit jaar plaats en zorgde voor een grote verstoring van belangrijke systemen, processen en financiële informatie. "Hoewel KNP één van de grootste particuliere logistieke groepen is, werd het eerder dit jaar slachtoffer van een ransomware-aanval", **zegt** aangewezen bewindvoerder Rajnesh Mittal.

Volgens Mittal kan het bedrijf niet verder gaan vanwege de 'uitdagende marktomstandigheden' en het niet kunnen veiligstellen van voldoende investeringen als gevolg van de ransomware-aanval. "We zullen alle medewerkers in deze lastige tijd ondersteunen." KNP Logistics group was het moederbedrijf van de 158 jaar oude vervoerder Knights of Old. Het bedrijf had vorig jaar nog een omzet van omgerekend 115 miljoen euro.

- ▲ Minister: rechtszaak geen reden om uitvraag data ggz-patiënten te stoppen
- ▼ SP uit ongenoegen dat kabinet motie tegen client-side scanning niet uitvoert





## Building automation giant Johnson Controls hit by ransomware attack

5 days ago



## Exclusive: DHS investigating whether floor plans and other security information were exposed in ransomware attack on contractor

2 days ago



## News about ransomware, Pinal County

---

azfamily

## 14 Pinal County school districts hit with ransomware attack to payroll system

3 days ago



# A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.



TECHNOLOGY

# Pegasus spyware used to hack U.S. diplomats working abroad

Confirmation of the attacks comes one month after the U.S. blacklisted NSO Group

By [Craig Timberg](#), [Drew Harwell](#) and [Ellen Nakashima](#)

Updated December 3, 2021 at 5:24 p.m. EST | Published December 3, 2021 at 12:48 p.m. EST

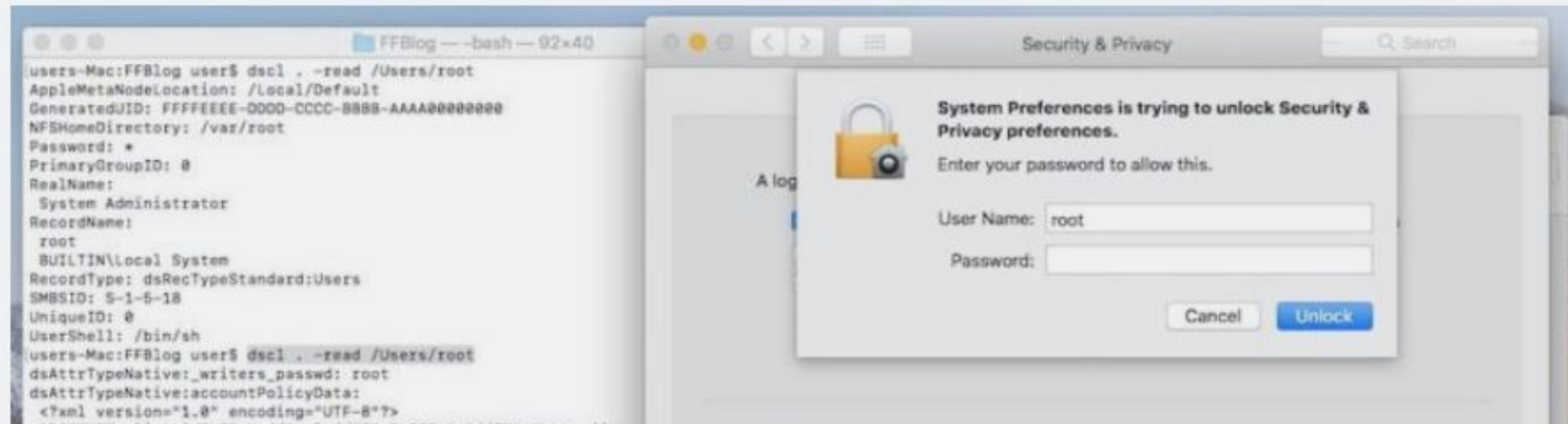


MOTHER OF ALL BUGS —

# macOS bug lets you log in as admin with no password required

Here's how to protect yourself until Apple patches bafflingly bad bug.

DAN GOODIN - 11/29/2017, 12:05 AM



Politician's view: it is  
like there is a huge  
arson problem,  
houses keep burning  
down





**Slashdot**   
@slashdot



## Apple Patches Dozens of Security Flaws With iOS 15.5, Over 50 Fixes For macOS 12.4



[apple.slashdot.org](https://apple.slashdot.org)

Apple Patches Dozens of Security Flaws With iOS 15.5, Ov...

Apple has released iOS 15.5, macOS 12.4, and more today with updates like new features for Apple Cash, the Podcast...

12:00 AM · May 17, 2022 · slashdotbot

**200** Retweets   **20** Quote Tweets   **1,447** Likes



Security Advisory 2022-034

# Multiple Critical Vulnerabilities in Microsoft Products

May 17, 2022 — v1.1

TLP:WHITE

## History:

- 11/05/2022 — v1.0 – Initial publication
- 17/05/2022 — v1.0 – Updated with information about issues with Domain Controllers

## Summary

On May 11th, Microsoft issued May 2022 Patch Tuesday including fixes for three zero-day vulnerabilities and 75 flaws. Among the zero-days, the vulnerability tracked as CVE-2022-

We can't credibly claim things are going well. "Cyber" must become more secure.

"Everything is on fire and we admittedly ship **highly flammable** products"

Governments are coming for us.

C

E



RoHS



# Regulation!

Known: Vertical regulation of cars, planes, healthcare, spaceflight etc

**Current status is that being hacked or shipping incredibly badly protected stuff is somehow allowed & you won't get blamed**

New: horizontal regulation of everything 'cyber' or 'with digital elements'

Three kinds + 1:

- EU Radio Equipment Directive, EU Cyber Resilience Act: Sorta product legislation, put requirements on hardware **and software**
- EU NIS2, EU Cyber Solidarity Act, DORA: Rules on services, continuity, preparedness
- GDPR: Rules on data
- *Renewed Product Liability Directive: pay up for broken software*

# Upcoming regulation

- NIS2: All about services, **including those provided by governments**
  - Implementation of legislation ongoing, consultations ongoing, active end 2024 (?!)
  - **All about having plans.**
  - DORA: Digital Operational Resilience Act, for financials
- Cyber Resilience Act: rules for **products, including lots of audits**
  - Still political. Would be active in 2025/2027 timeframe
- Cybersecurity Act: an EU-wide cybersecurity certification framework for ICT products, services and processes
- Cyber Solidarity Act: Mandatory disaster recovery/incident preparation for some sectors
- New Product Liability Directive: Pay up for broken software too

# NIS 2: THE RETURN OF BRUSSELS

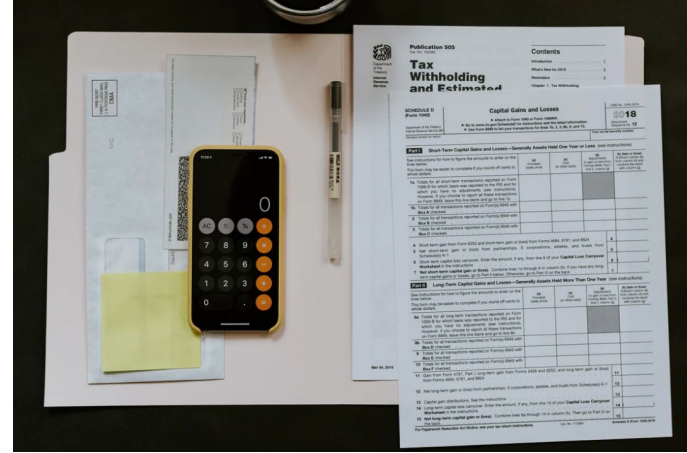
- Big changes:
  - “Brussels” determines rules that say who NIS 2 will apply to:
  - Simpler criteria:
    - If you provide Important Services, you will be an Important Entity
    - If you provide Essential Services, you will be an Essential Entity
  - Some explicit listings:
    - Internet Exchanges
    - ccTLD operators
    - Large scale authoritative servers
    - Large scale DNS resolvers
    - Data center service providers
    - Content Delivery Networks
    - **Government services**
- **In short: this will apply to many of you**
  - **Even if you are not in the EU!**



**NOT YET SURE WHAT THE REQUIREMENTS ARE!**

# What does it mean?

- Must report incidents Pretty Damn Quickly
- Implement the following measures:
  - Risk analysis, security policies
  - Incident handling
  - Business continuity & crisis management plan
  - Know dependencies on your service suppliers, **be sure they also have a plan**
  - Plan for vulnerability handling & disclosure
  - Testing & audits of effectiveness of cybersecurity measures
  - Use cryptography and encryption
- If you don't, there can be: Warnings, Orders to fix, Fines, **Criminal Procedures, Orders to cease doing business, Bans on persons from management (!!)**
  - There can also be on-site inspections, even unannounced, in case of problems
- If you are **essential** you need to have these plans ready for inspection. If you are **important** you'd better have had these plans ready if you had an incident.



## Interaction!

- Existing **vertical** regulations get you presumption of conformity in EU CRA
  - Medical, cars, planes etc
- Complying with NIS2 continuity requirements means **having** to use EU CRA certified equipment/software
- EU CRA attempts to “bake in” GDPR into your hardware software: can only log and process data required for **actual operation**
- For product liability, you would be in a **bad place** if your products/services did not adhere to NIS2/CRA etc



# What the EU Cyber Resilience Act covers

- Any connected piece of hardware, almost every piece of software sold for **money OR DATA**.
- Either the producer is compliant, or the importer/distributor/seller has to validate compliance
- Producer is 100% on the hook for its own code
- Must perform due-diligence on sourced components
  - Intensity of due-diligence is variable but not precisely known
- Critical products (definition is not very useful) most undergo third party audits by “notified bodies” (think TÜV etc)
- *Does NOT cover services themselves directly*
- **Industry must write a standard for compliance, until that time ALL products must undergo third party audits**
  - (in flux)

(some indicative companies)

**THALES**  
**SIEMENS AIRBUS**



(some indicative companies)

(indicative of EU notified bodies)

“And this is how you have to code, according to the EU and its harmonised standards organizations, to be checked by EU notified bodies.”



You will not be able to **buy**  
non-compliant products.

People will not **sell** you non-compliant  
products.

For NIS2, you **must** buy compliant  
products

- (a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;
- (b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;
- (c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;
- (d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;
- (e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');
- (f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

← GDPR

- (g) minimise their own negative impact on the availability of services provided by other devices or networks;
- (h) be designed, developed and produced to limit attack surfaces, including external interfaces;
- (i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
- (j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;
- (k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.





- (1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;
- (2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;
- (3) apply effective and regular tests and reviews of the security of the product with digital elements;
- (4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;
- (5) put in place and enforce a policy on coordinated vulnerability disclosure;

- (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;
- (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;
- (8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.



# Further things

- 3? 5? Longer? Years of security support
  - Maybe 10 years for some products
  - **Would be nice!**
- Reporting vulnerabilities to governments
  - Not all of them friendly
  - **Not all of them known reliable at keeping secrets**
  - Worrying
- Reporting ongoing exploitation to governments
  - Again - issues where you might HAVE to report to government X which is not allowed by government Y.

# The Open Source Problem

## CRA DOES NOT APPLY TO YOUR HOBBY OR ACADEMIC OPEN SOURCE PROJECT

Who does the due diligence for OpenSSL? **Linux**? SQLite?

Electron? Android? JQuery? Angular?

Grub?

Will it help? Is the lack  
of rules the problem?

# Chrome Flags Third Zero-Day This Month That's Tied to Spying Exploits

So far this year, Google has disclosed six vulnerabilities that attackers were actively exploiting before the company had a patch for them.



**Jai Vijayan**

Contributing Writer, Dark Reading

September 28, 2023



[Printer-Friendly View](#)



## CVE-ID

**CVE-2023-41064**

[Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

## Description

A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 16.6.1 and iPadOS 16.6.1, macOS Monterey 12.6.9, macOS Ventura 13.5.2, iOS 15.7.9 and iPadOS 15.7.9, macOS Big Sur 11.7.10. Processing a maliciously crafted image may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

# Microsoft leak exposed 60,000 government emails



## Recent in Security

- ▶ Hundreds of thousands of mail servers vulnerable due to Exim bug
- ▶ Cisco routers vulnerable due to replacing firmware with backdoor version
- ▶ Hertzbleed: how GPUs can leak data to hackers
- ▶ LockBit 3.0 most active ransomware gang in August
- ▶ New Windows 11 22H2 update puts stronger focus on passkeys

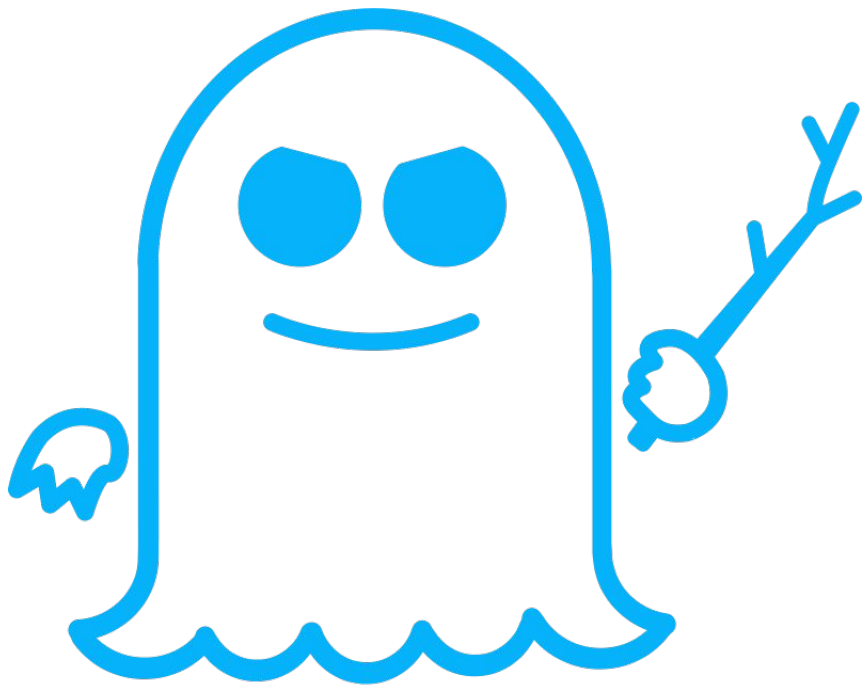


CLOUD SECURITY

## 6 'nightmare' cloud security flaws were found in Azure in the last year. Does Microsoft have work to do?

Many security researchers agree that **cross-tenant vulnerabilities** are a new type of risk for customers to be aware of, one that wasn't supposed to happen in the cloud.





**SPECTRE**



**MELTDOWN**



**F**  **RTINET**®

Problem is not lack of  
rules but **lack of care.**



New regulations will:

- Make your life more difficult
- Give you greater leverage on your management
- **Make it possible for management to be prosecuted / fired if they ignore security (!!)**
- Allow you to kick vendors where it hurts

It will be painful:

- **Too much regulation at the same time**
  - Not enough auditing capacity, not enough learning/tuning
- Quality of implementation is worrying or at least a challenge

**But: I think you can use this to effectively improve security**

More EU regulation:

Tomorrow 11:45,

“We need better regulatory tools for cyber  
resilience”

Yangtze track

Angeline van Dijk, Ludo Baauw, Michiel  
Steltman, Jacco Jacobs

# EU and You: Upcoming regulation



[bert@hubertnet.nl](mailto:bert@hubertnet.nl) / <https://berthub.eu/>