Cyber Security and Society: a pre-war reality check

Bert Hubert / bert@hubertnet.nl

https://berthub.eu/prewar

First some important words from Donald T.

“I know it sounds devastating but we have to get used to the fact that **a new era has begun: the pre-war era.**”

“When **Donald Tusk** was Polish prime minister for the first time, from 2007 to 2014, he said few other European leaders beyond **Poland and the Baltic states** realised Russia was a potential threat.”

KIESRAAD

Toetsingscommissie
Inzet Bevoegdheden

POWERDNS

TU Delft

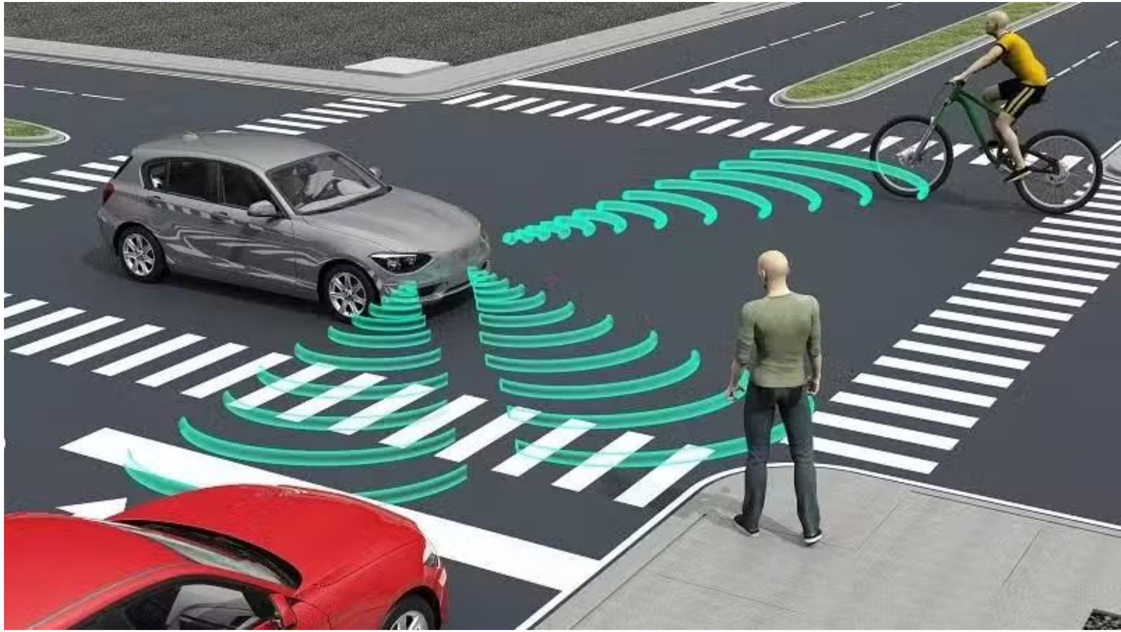
FOX-IT
FOR A MORE SECURE SOCIETY

POWERDNS

POWERDNS

TU Delft

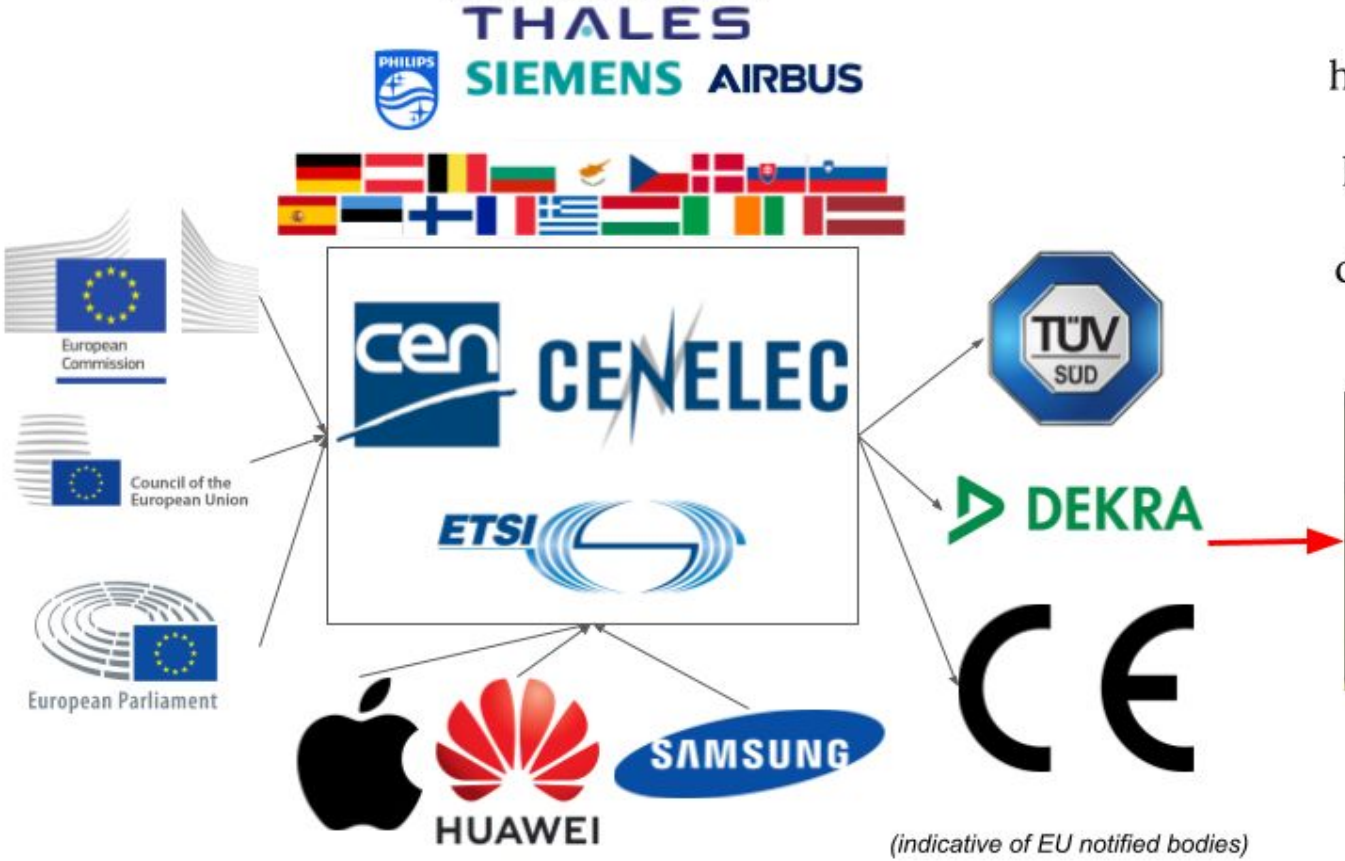
Toetsingscommissie
Inzet Bevoegdheden



https://www.drive.com.au/news/tesla-hit-and-run-driver-to-stand-trial-for-crash-blamed-on-autopilot/

- Cyber Security Act
- Cyber Resilience Act
- Cyber Solidarity Act
- Digital Operational Resilience Act (DORA)
- NIS2 Directive
- Product Liability Directive
- .. and they aren’t done yet

(some indicative companies)



(indicative of EU notified bodies)

(some indicative companies)

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

16
17
18
16
17
18
OK
www.President.ir

NEW UK AND US INTELLIGENCE:
RUSSIA BEHIND EUROPE-WIDE CYBER ATTACK

On 24 February, a cyber-attack against Viasat began approximately 1 hour before Russia launched its major invasion of Ukraine. Although the primary target is believed to have been the Ukrainian military, other customers were affected, including personal and commercial internet users. Wind farms in central Europe and internet users were also affected.

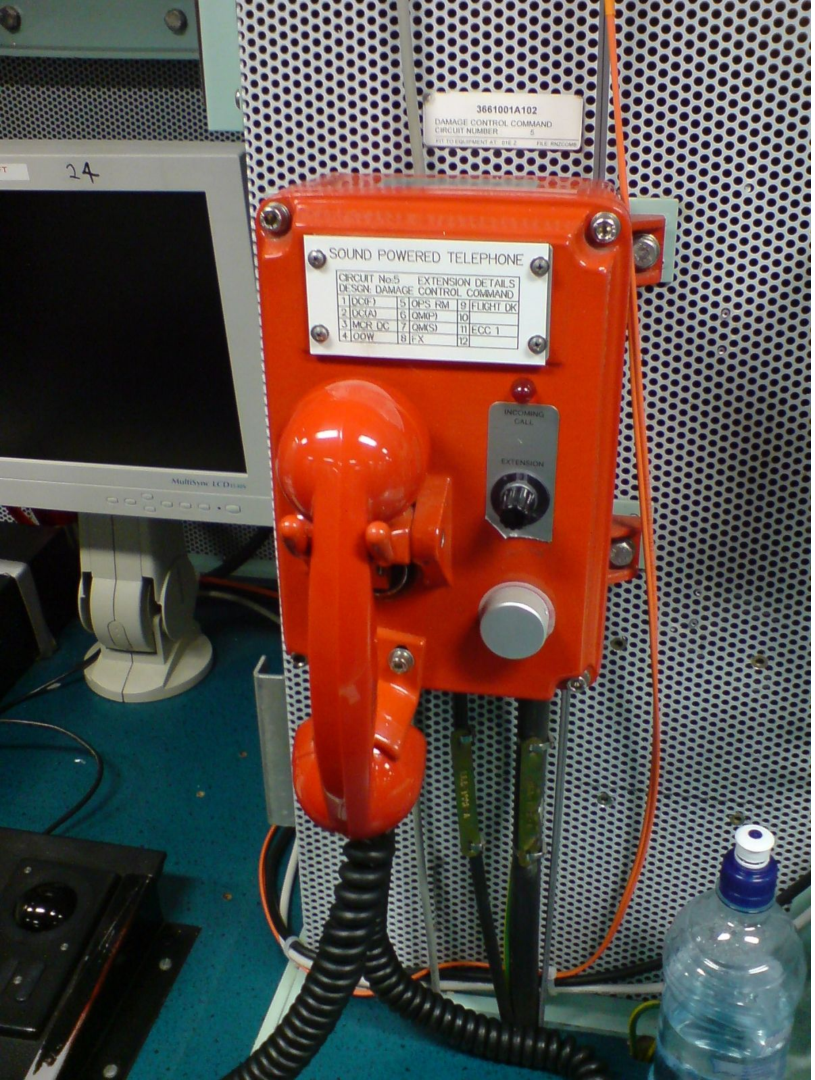
Viasat has said that “**tens of thousands of terminals have been damaged, made inoperable and cannot be repaired.**”

When times are bad, you are (much more) on your own!

- ROBUST: **Does not fall over by itself**

- LIMITED/KNOWN DEPENDENCIES: **Does not need too much unknown stuff too far away**

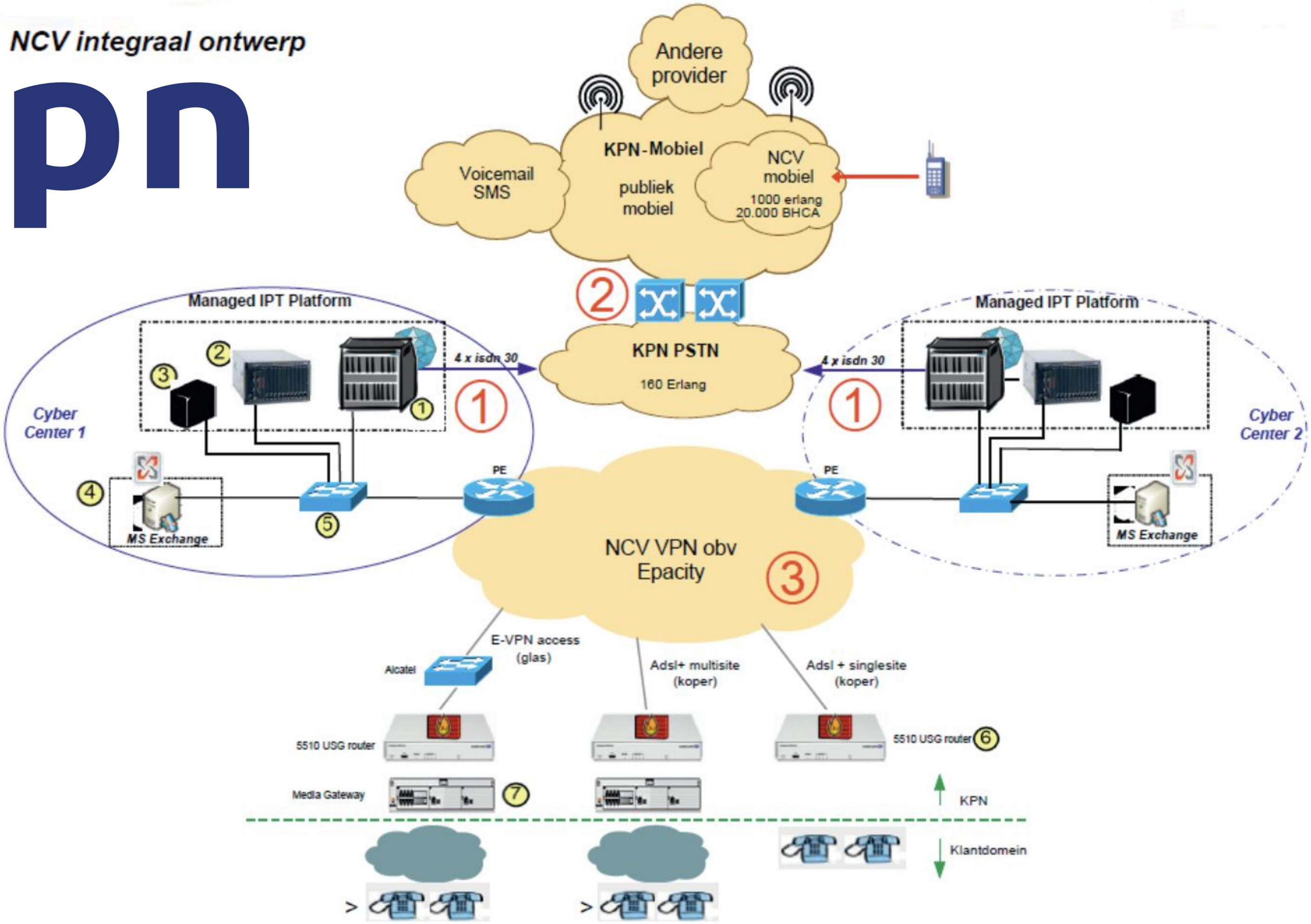
- OWNERSHIP/UNDERSTANDING: **If things break, you can improvise or fix things**



"Many different types of equipment have attempted, **but have largely failed**, to replace the incredibly simple sound-powered telephones on ships. Due to the rugged, reliable and **power-free** nature of this equipment, it remains in use on all US military vessels."

A
B
Niet voorbij
het afsluiten komen!

NCV integraal ontwerp



NCV Integraal Ontwerp.

Chat

9/22
That would be r

I'm pretty confident that this launch will be successful. The team has worked tirelessly to make it possible. This is going to be awesome.

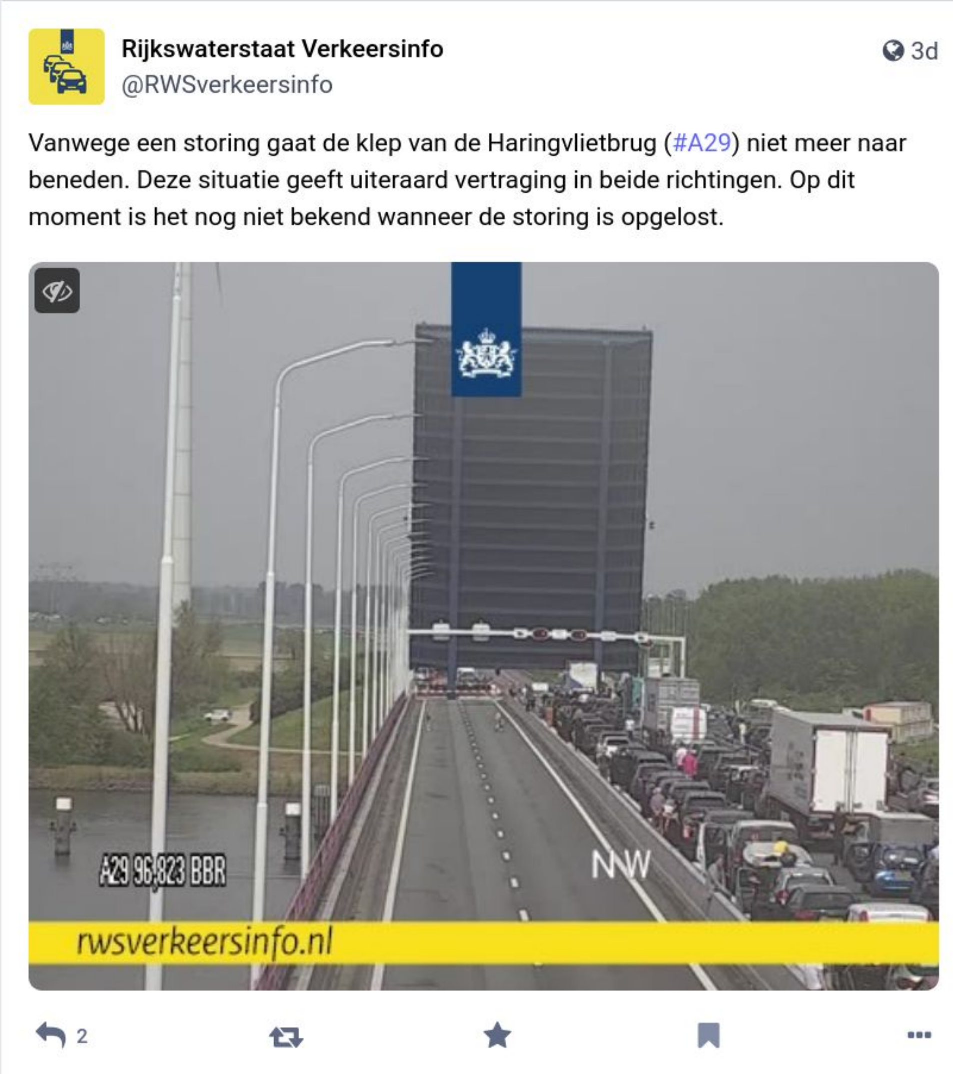
Kayo Miwa 9/22
Thank you for always being so positive!

I will push Krystal to give us a few more days. That shouldn't be a problem.

We haven't had a break in awhile.

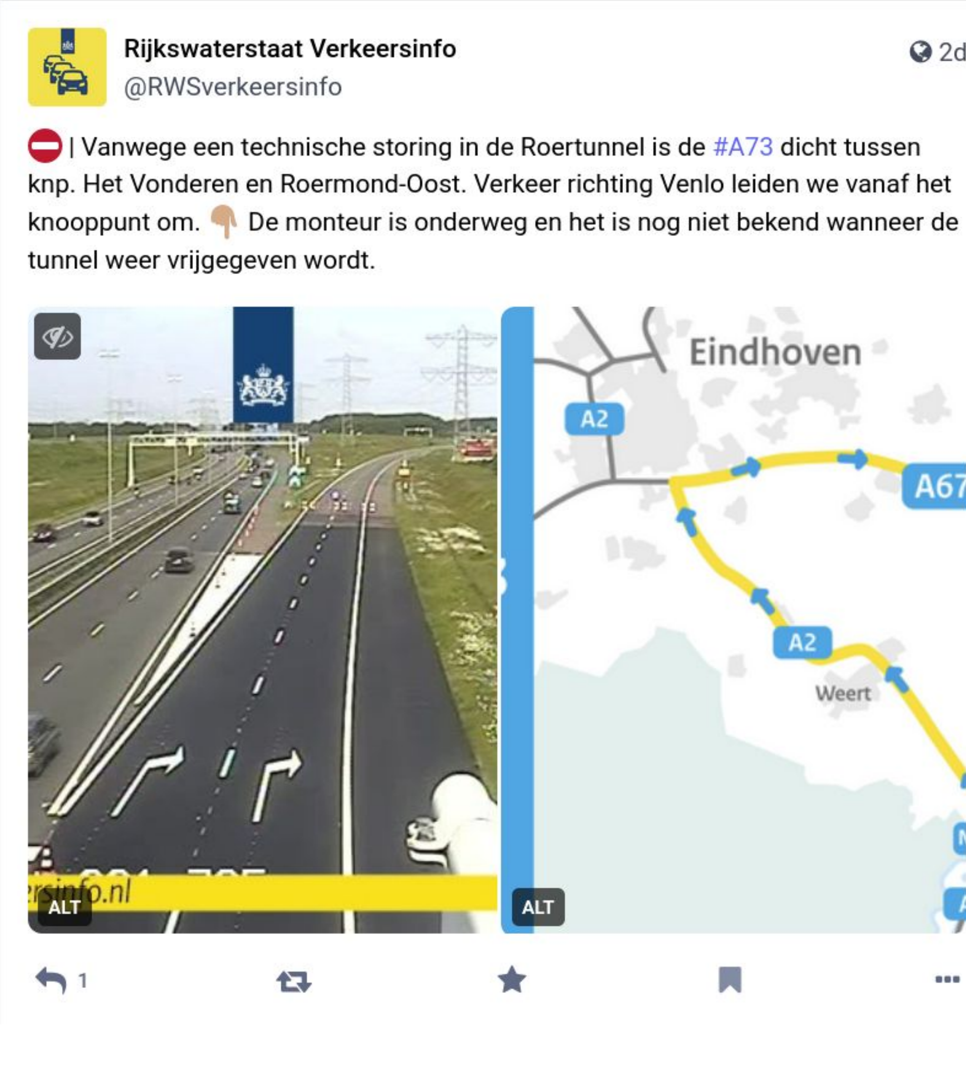
9/22
Let's do it!

WhatsApp



Rijkswaterstaat Verkeersinfo
@RWSverkeersinfo
3d

Vanwege een storing gaat de klep van de Haringvlietbrug (#A29) niet meer naar beneden. Deze situatie geeft uiteraard vertraging in beide richtingen. Op dit moment is het nog niet bekend wanneer de storing is opgelost.



Rijkswaterstaat Verkeersinfo
@RWSverkeersinfo
2d

⛔ | Vanwege een technische storing in de Roertunnel is de #A73 dicht tussen knp. Het Vonderen en Roermond-Oost. Verkeer richting Venlo leiden we vanaf het knooppunt om. 👇 De monteur is onderweg en het is nog niet bekend wanneer de tunnel weer vrijgegeven wordt.

AFP

NOS Nieuws • Vrijdag 14 april 2023, 15:57 • Aangepast vrijdag 14 april 2023, 17:01

Vodafone: storing lijkt opgelost, bellen met 112 weer mogelijk

De landelijke storing bij Vodafone lijkt opgelost. Klanten kunnen volgens de telecomprovider weer mobiel bellen en gebeld worden. Ook 112 is weer te bereiken.

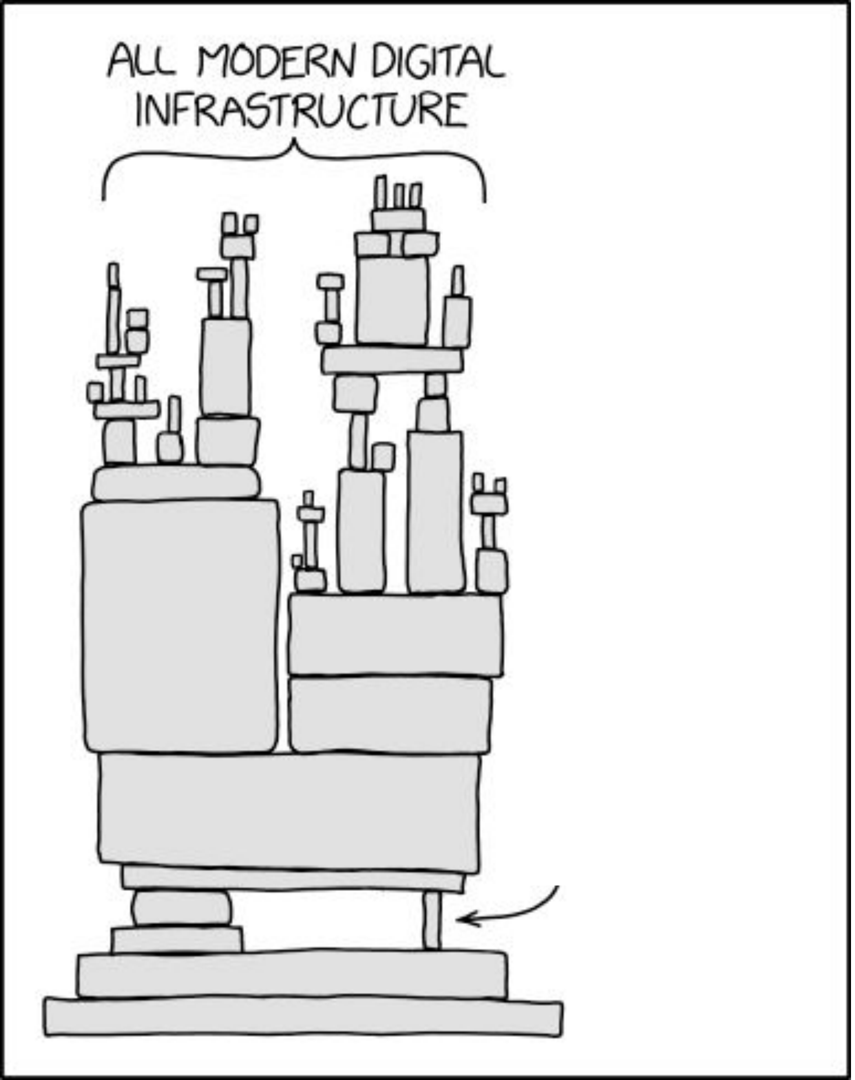
Software Apps

Microsoft 365 was down, stopping people from opening Office, Outlook, and OneDrive (Update)

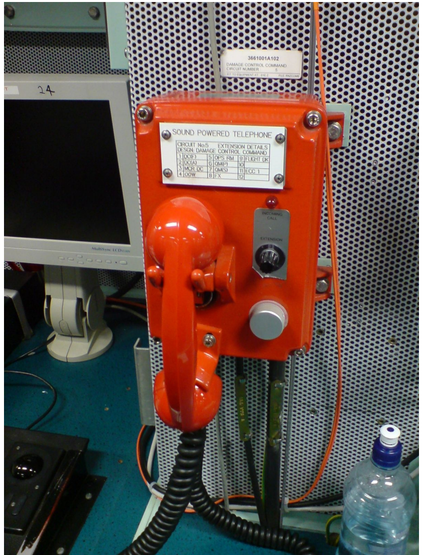
News By Sean Endicott published September 6, 2023

A Microsoft 365 outage could cause a stressful start to your workday.

Comments (0)



The stack is too high!



HEXTA

So where are we?

Also see: berthub.eu

5G: The outsourced elephant in the room

Jan 20 2020

> *This article is part of a series on (European) innovation and capabilities.*

In a break from the usual GPS/Galileo, DNA and C++ posts, here is a bit on 5G and national security. It turns out that through PowerDNS and its parent company Open-Xchange, we know a lot about how large scale European communication service providers work - most of whom are our customers in some way.

In addition, in a previous life I worked in national security and because of that I have relevant knowledge of how governments (your own and foreign ones) “interact” with telecommunication providers. So what follows is based on lived experience.

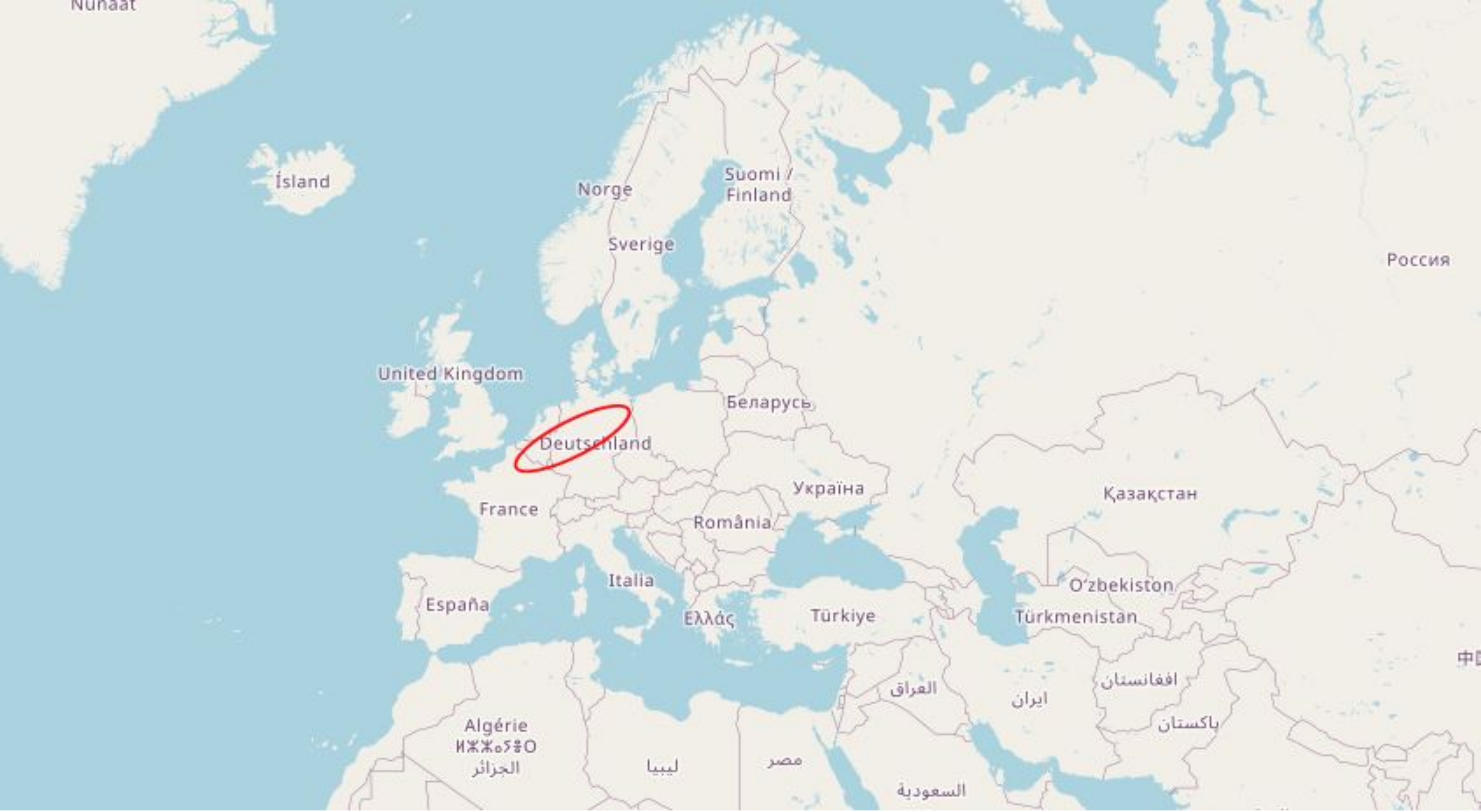
Note: this article is mostly about Europe. Considerations and conditions in the US and the rest of the world are very different.

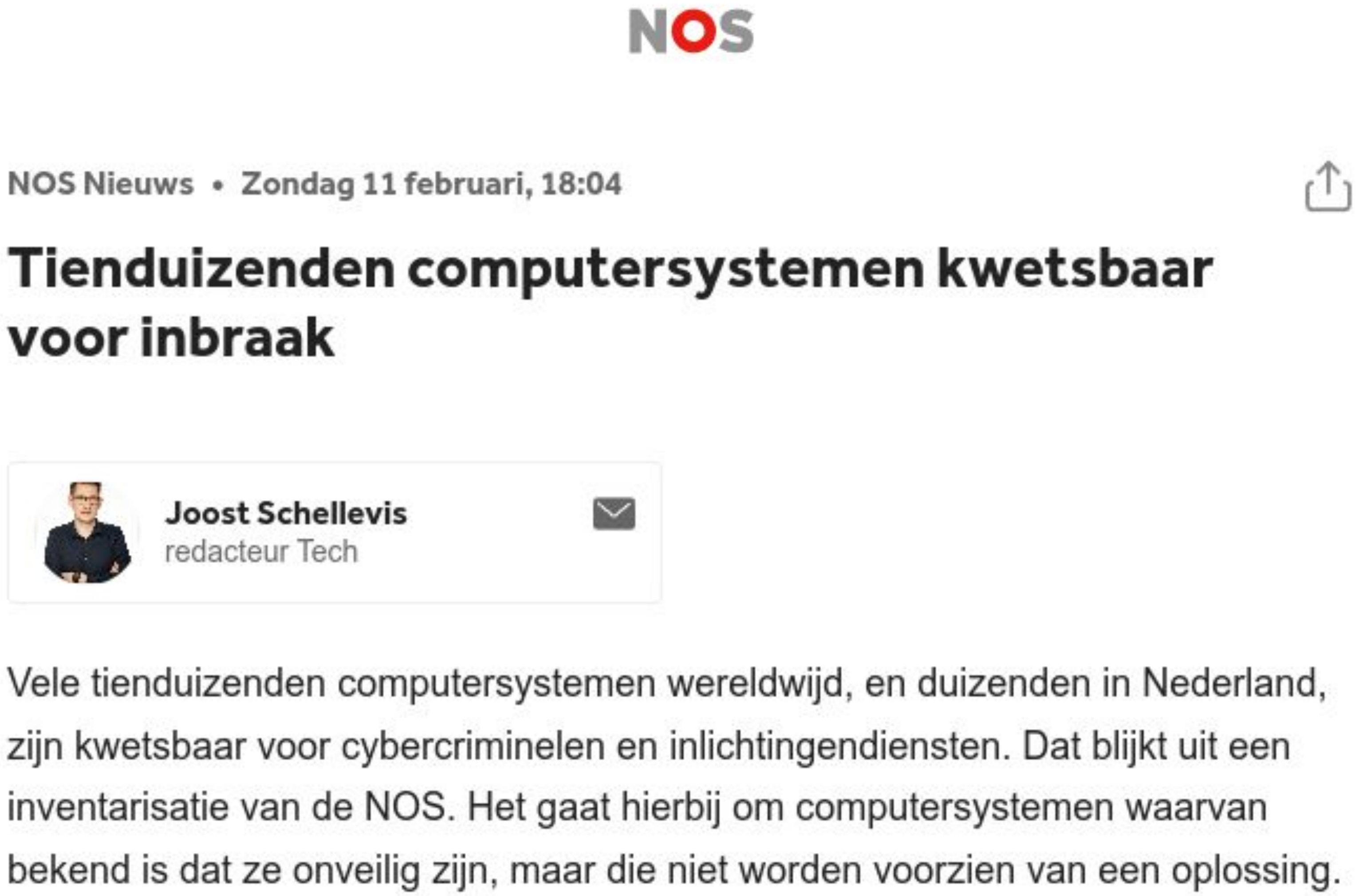
Telecommunication is what makes the world go round, and with everything moving to the cloud, any breakdown would severely disrupt our economy and safety. So it makes sense to think hard about this vital service to our society.

‘Any worries about “the Chinese” being able to disrupt our communications through backdoors ignore the fact that all they’d need to do to disrupt our communications.. **is to stop maintaining our networks for us!**’ (2020)

Google
aws

Google
aws
HUAWEI
Infosys
TECH mahindra
wipro
Kalaallit Nunaat
Canada
Ísland
Føroyar
Norge
Eesti
Danmark
Nederland
Беларусь
Luxembourg
France
Andorra
Malta
Κύπρος
Algérie
الجزائر
ليبيا
مصر
السعودية
ישראל
Россия
Қазақстан
Монгол
中华人民共和国
日本
台灣
Myanmar
Cambodia
Malaysia
Indonesia
Guam
Belau
Papua New Guinea
Marshall Islands
Nauru
Kiribati
Solomon Islands
Tokelau
Samoa
Vanuatu
Tonga
Australia
Norfolk Island
New Zealand
México
Cuba
Haiti
Guatemala
Aruba
Panama
Colombia
Ecuador
Perú
Brasil
Bolivia
Paraguay
Chile
Argentina
Pitcairn Islands
Falkland Islands (Malvinas)
South Georgia and South Sandwich Islands
Cabo Verde
موريتانيا
Niger
Ghana
Guinea Ecuatorial
السودان
South Sudan
Burundi
Saint Helena, Ascension and Tristan da Cunha
Angola
Malawi
Zimbabwe
Namibia
South Africa
Seychelles
Mauritius
الصومال
اليمن


Nunaat
Ísland
Norge
Suomi / Finland
Sverige
Россия
United Kingdom
Беларусь
Deutschland
Україна
France
România
Қазақстан
Italia
España
O'zbekiston
Ελλάς
Türkiye
Türkmenistan
中
العراق
افغانستان
ایران
پاکستان
Algérie
ⵍⵣⵣⴰⵢⴻⵔ
الجزائر
ليبيا
مصر
السعودية



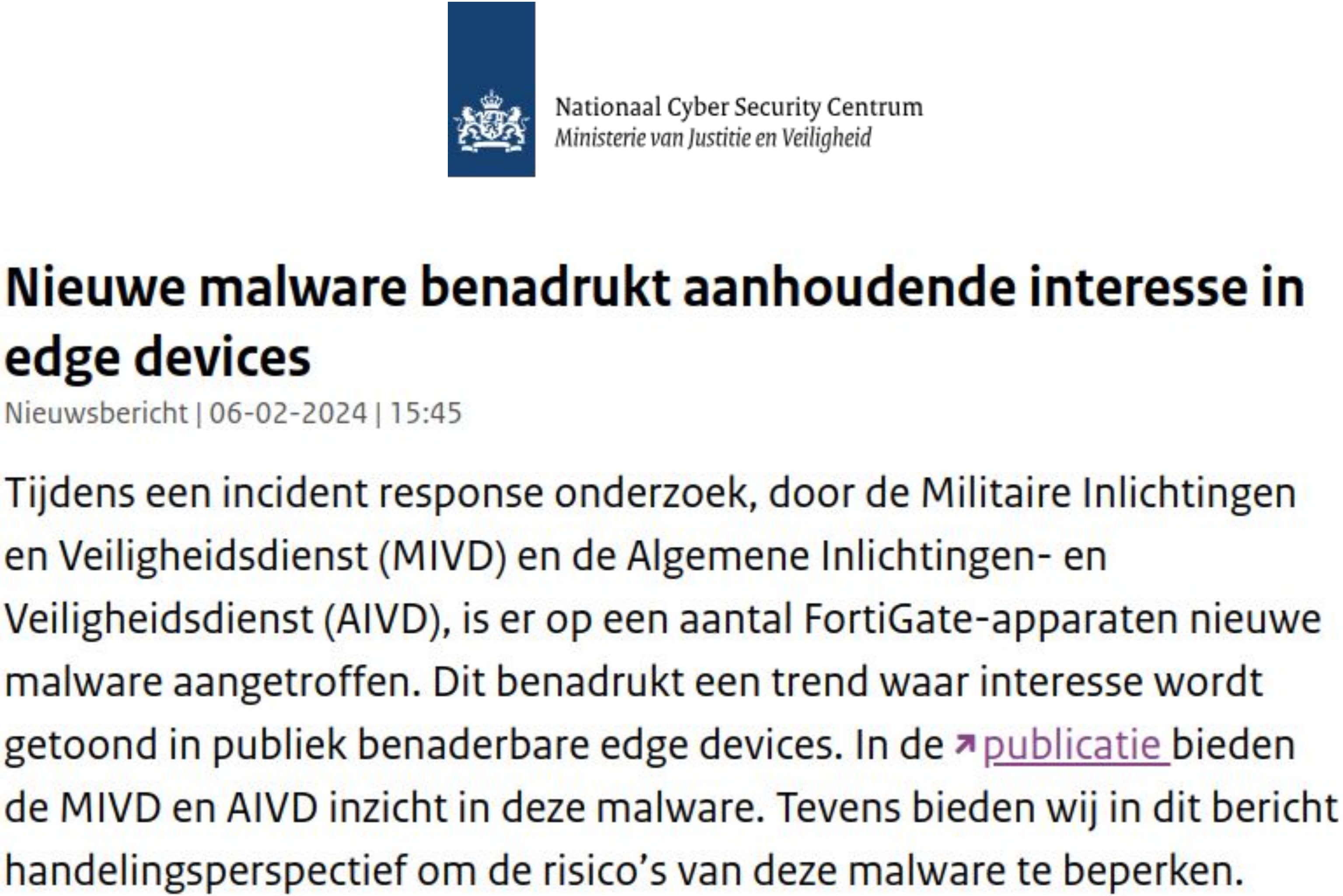
NOS

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.

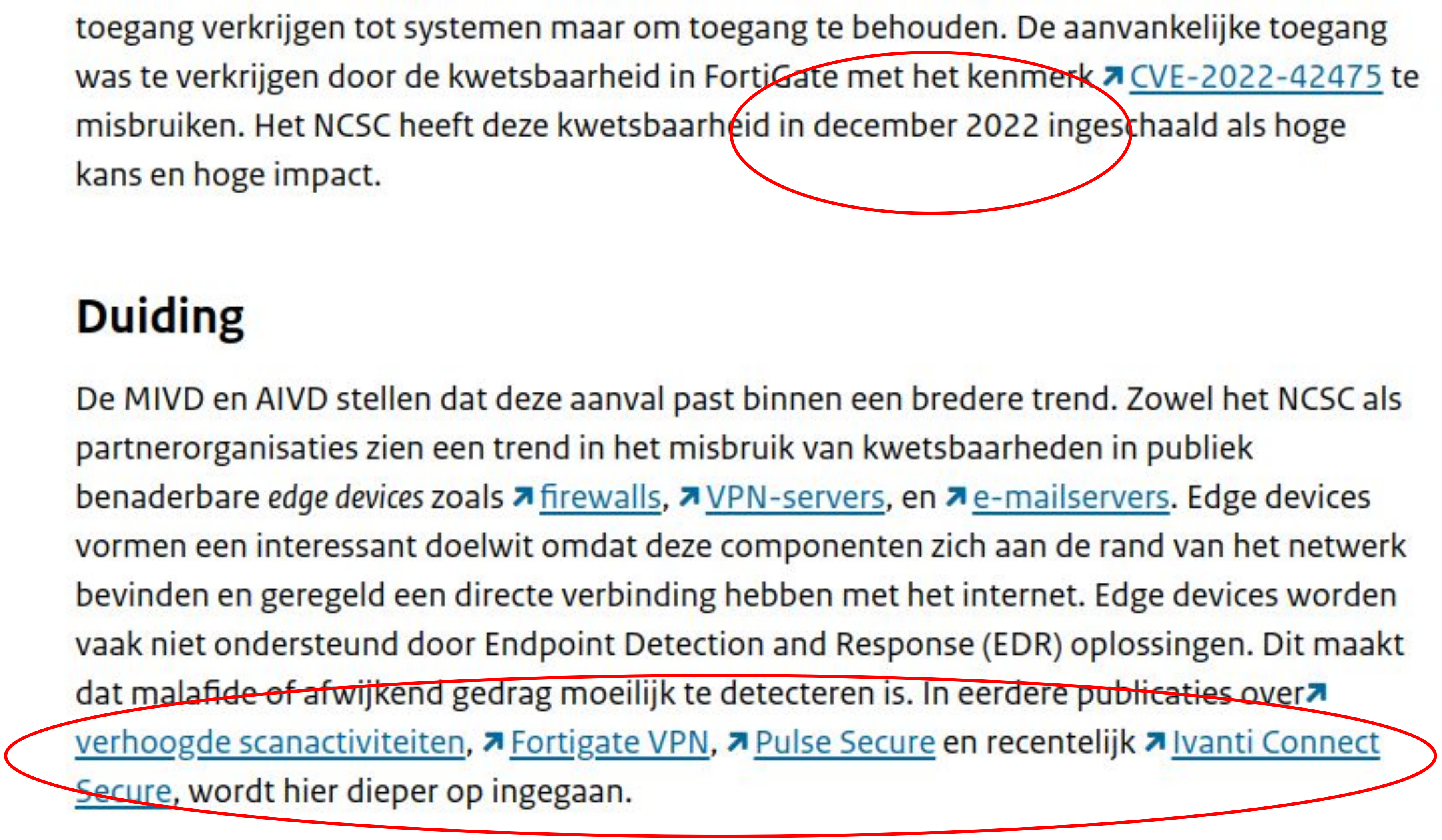


Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Nieuwe malware benadrukt aanhoudende interesse in edge devices

Nieuwsbericht | 06-02-2024 | 15:45

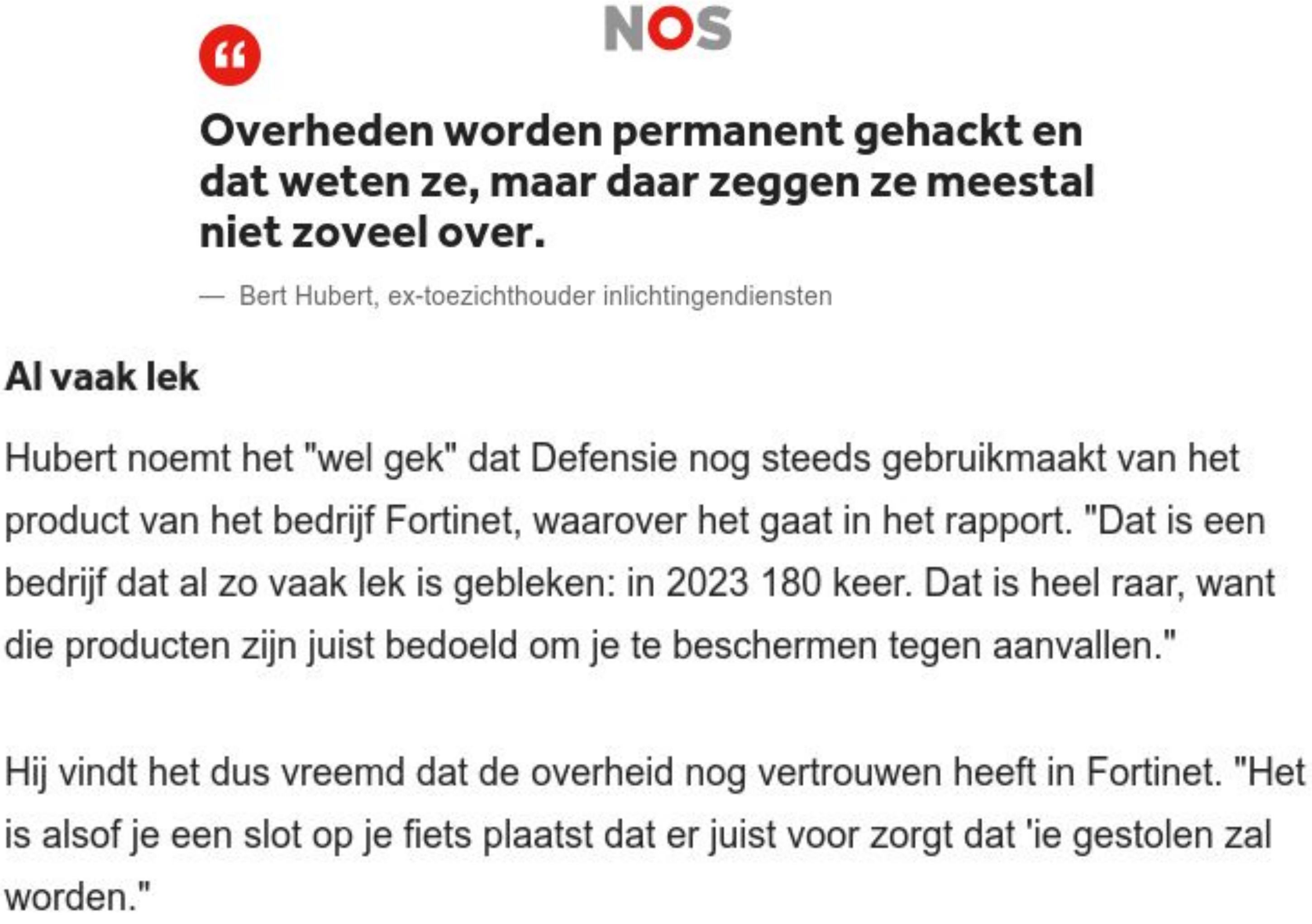
Tijdens een incident response onderzoek, door de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), is er op een aantal FortiGate-apparaten nieuwe malware aangetroffen. Dit benadrukt een trend waar interesse wordt getoond in publiek benaderbare 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.



toegang verkrijgen tot systemen maar om toegang te behouden. De aanvankelijke toegang was te verkrijgen door de kwetsbaarheid in FortiGate met het kenmerk ↗ CVE-2022-42475 te misbruiken. Het NCSC heeft deze kwetsbaarheid in december 2022 ingeschaald als hoge kans en hoge impact.

Duiding

De MIVD en AIVD stellen dat deze aanval past binnen een bredere trend. Zowel het NCSC als partnerorganisaties zien een trend in het misbruik van kwetsbaarheden in publiek benaderbare *edge devices* zoals ↗ firewalls, ↗ VPN-servers, en ↗ e-mailservers. Edge devices vormen een interessant doelwit omdat deze componenten zich aan de rand van het netwerk bevinden en geregeld een directe verbinding hebben met het internet. Edge devices worden vaak niet ondersteund door Endpoint Detection and Response (EDR) oplossingen. Dit maakt dat malafide of afwijkend gedrag moeilijk te detecteren is. In eerdere publicaties over ↗ verhoogde scanactiviteiten, ↗ Fortigate VPN, ↗ Pulse Secure en recentelijk ↗ Ivanti Connect Secure, wordt hier dieper op ingegaan.



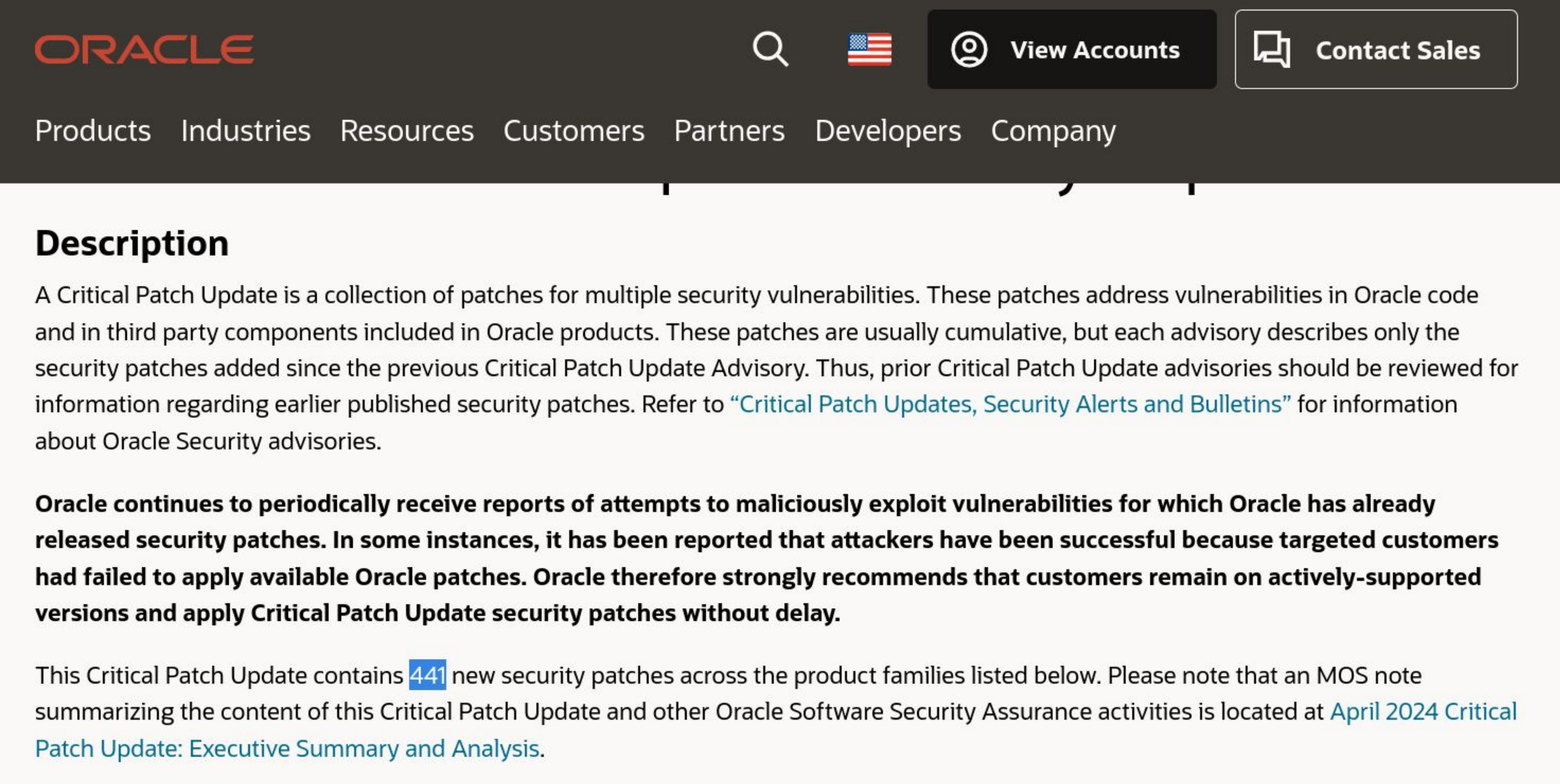
NOS

> **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."

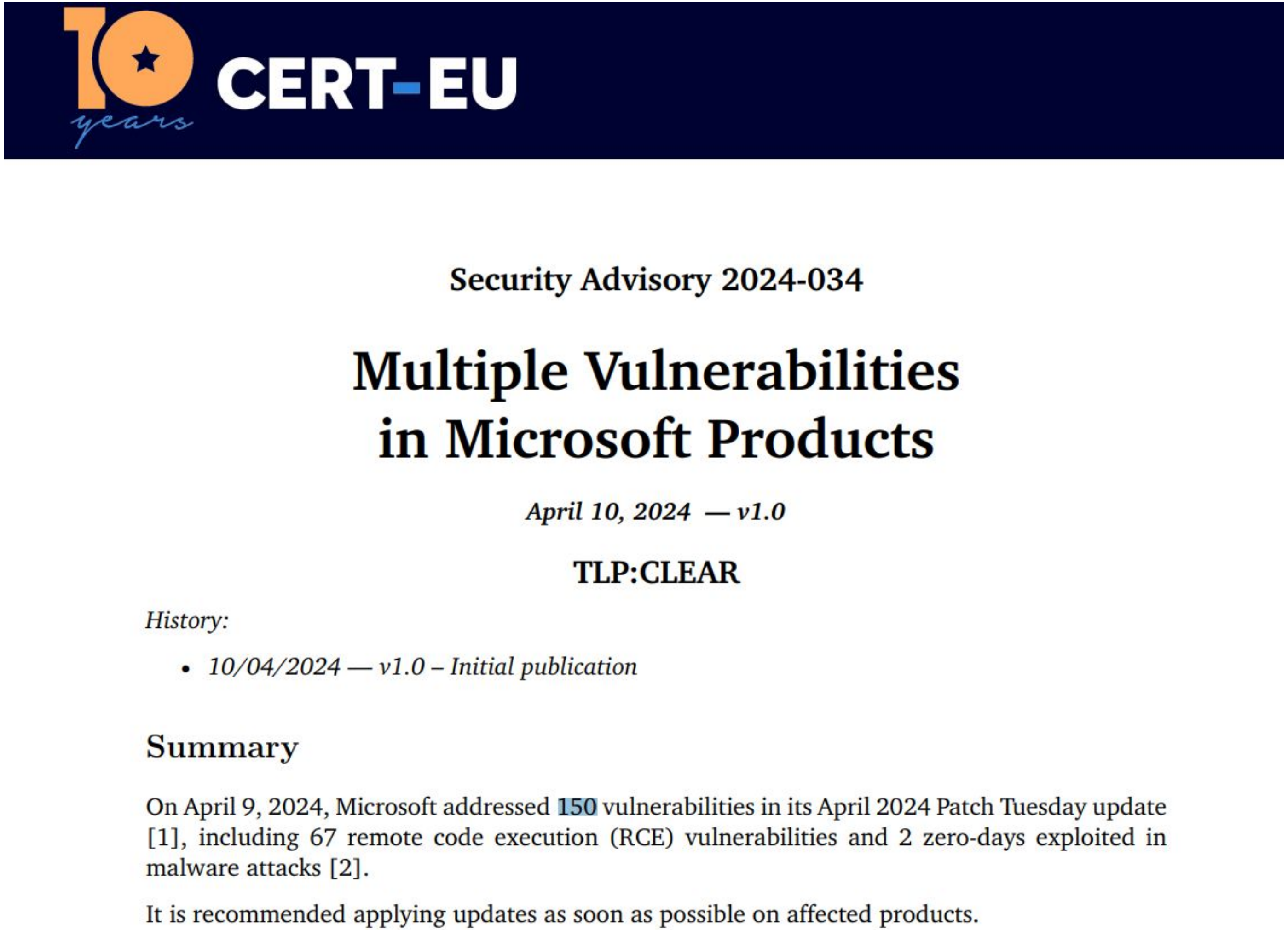


Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to “Critical Patch Updates, Security Alerts and Bulletins” for information about Oracle Security advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update security patches without delay.

This Critical Patch Update contains 441 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at April 2024 Critical Patch Update: Executive Summary and Analysis.



10 years CERT-EU

Security Advisory 2024-034

Multiple Vulnerabilities in Microsoft Products

April 10, 2024 — v1.0

TLP:CLEAR

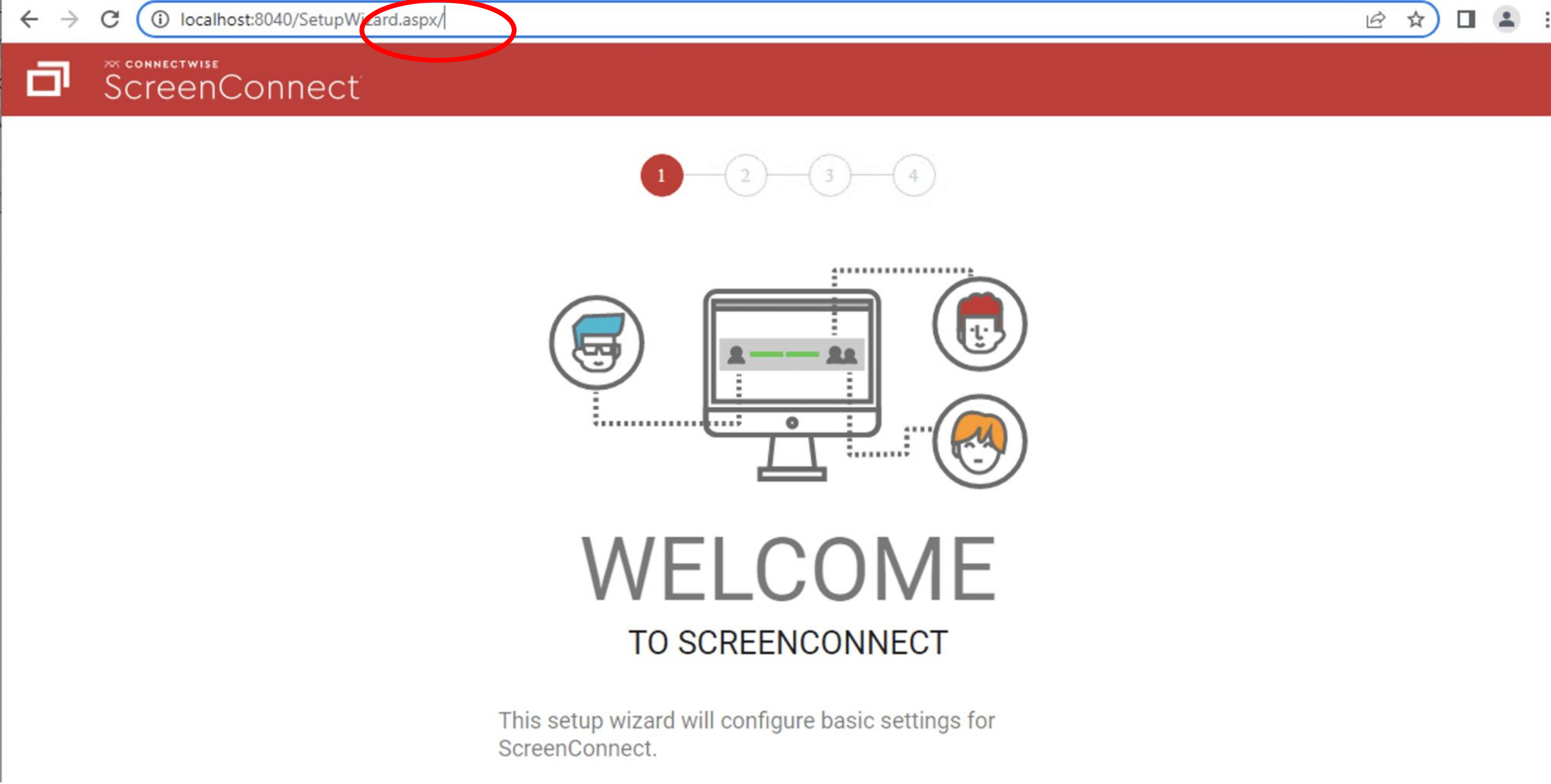
History:

- *10/04/2024 — v1.0 – Initial publication*

Summary

On April 9, 2024, Microsoft addressed 150 vulnerabilities in its April 2024 Patch Tuesday update [1], including 67 remote code execution (RCE) vulnerabilities and 2 zero-days exploited in malware attacks [2].

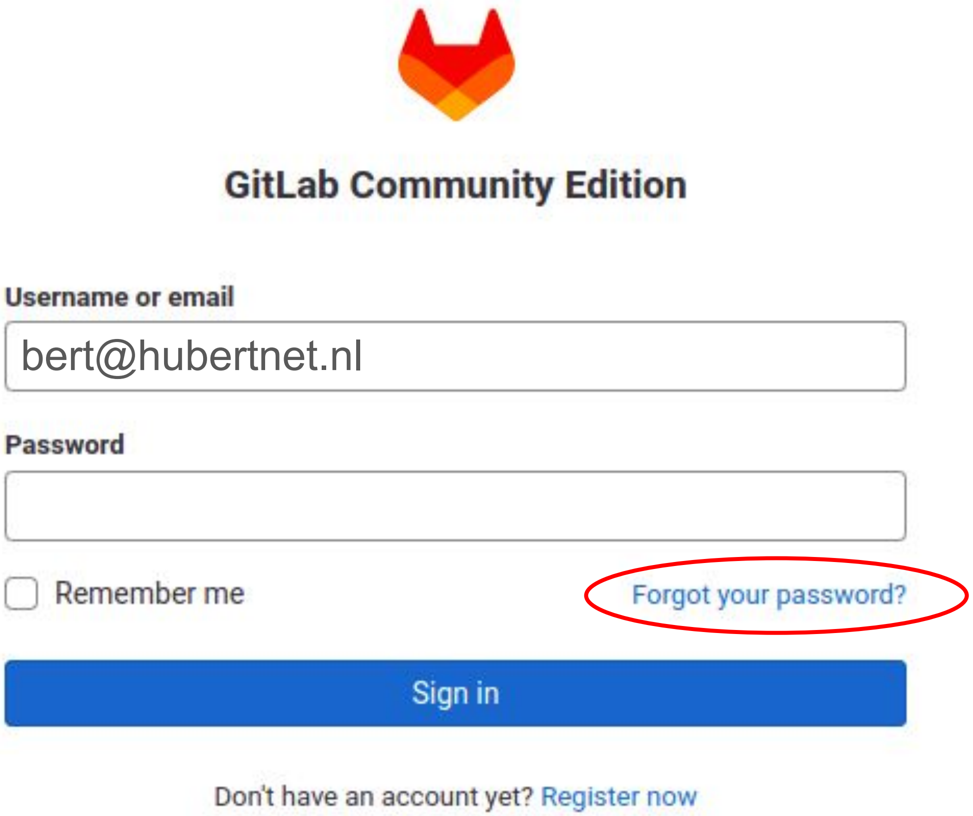
It is recommended applying updates as soon as possible on affected products.



WELCOME

TO SCREENCONNECT

This setup wizard will configure basic settings for ScreenConnect.



GitLab Community Edition

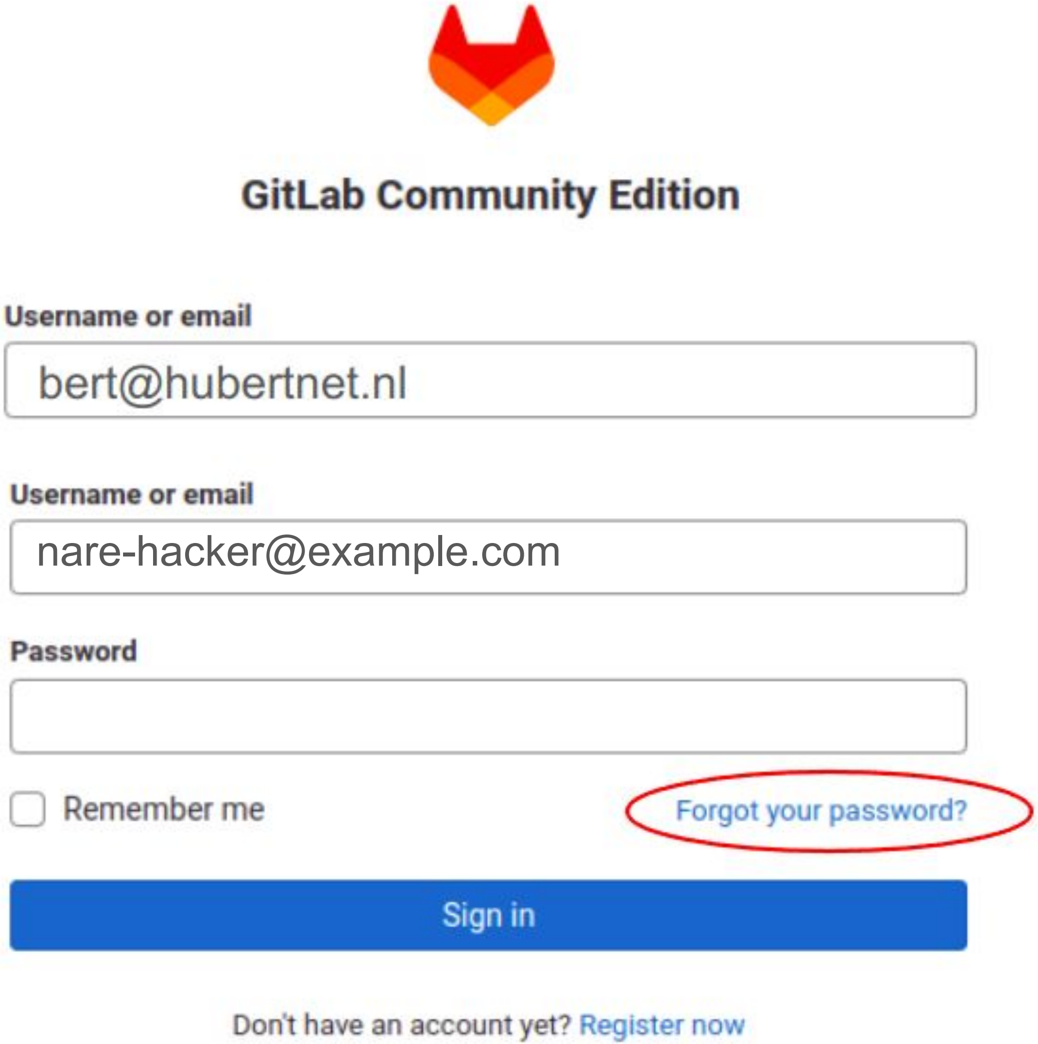
Username or email

bert@hubertnet.nl

Password

□ Remember me

Don't have an account yet? Register now



GitLab Community Edition

Username or email

bert@hubertnet.nl

Nog een keer!

Username or email

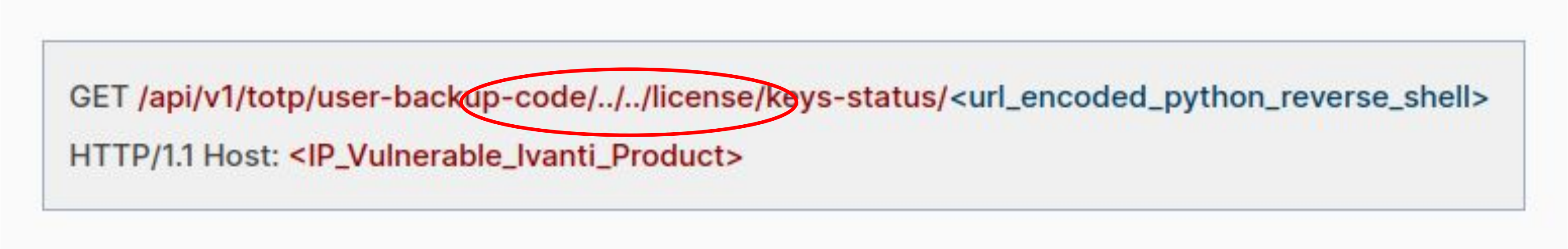
nare-hacker@example.com

Password

□ Remember me

KLIK!

Don't have an account yet? Register now



```
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

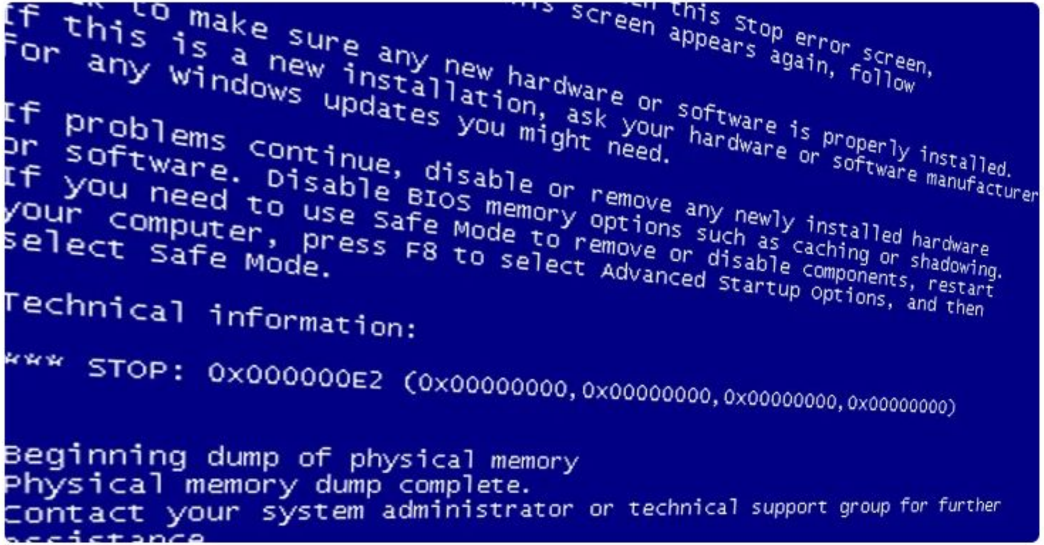
Composer (10.10.0.0)

Active Setup: Microsoft Edge... 1 (0%)

Perhaps move 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

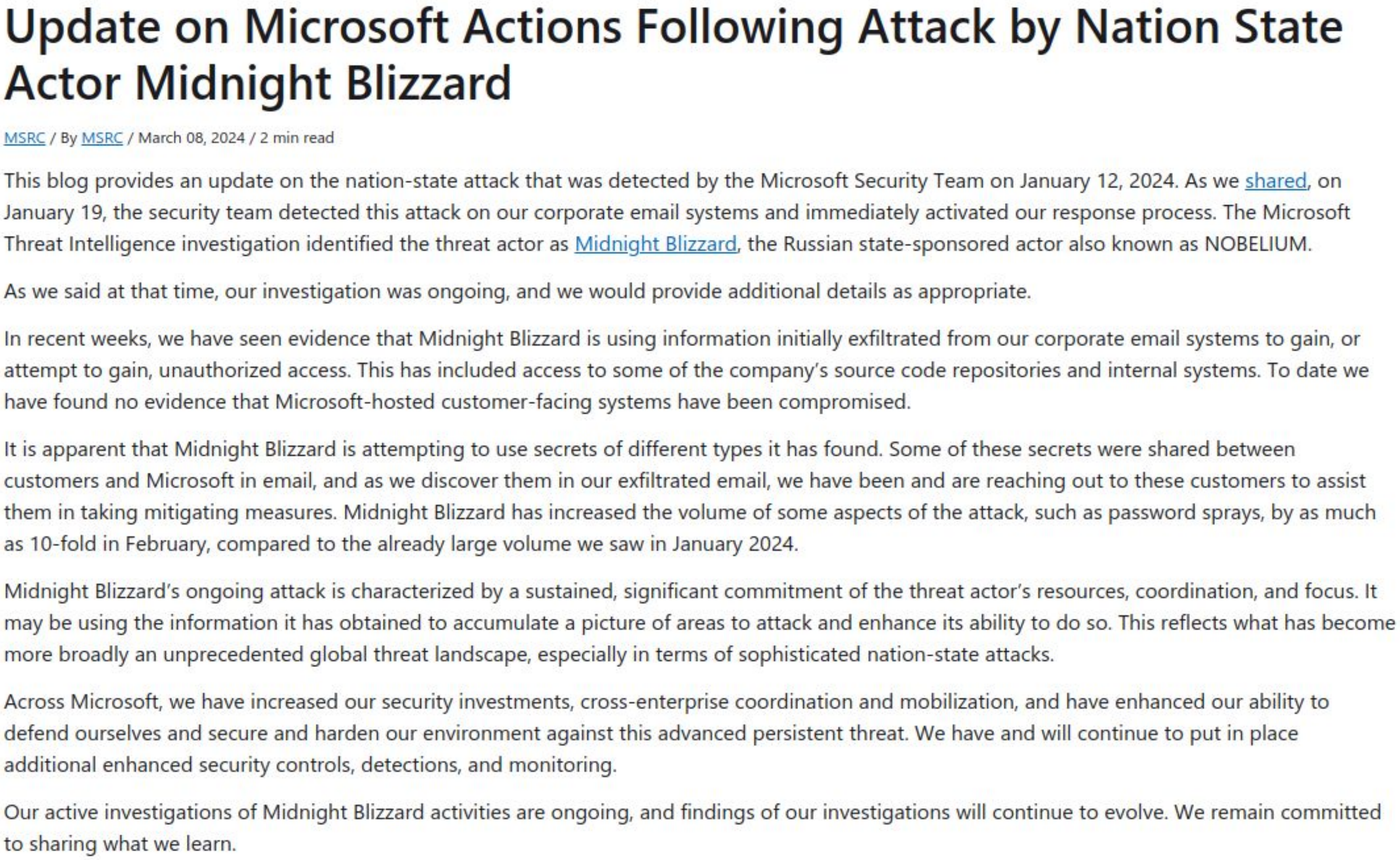


```
                                  this Stop error screen,
                           screen appears again, follow
  to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
For any Windows updates you might need.

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



Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

MSRC / By MSRC / March 08, 2024 / 2 min read

This blog provides an update on the nation-state attack that was detected by the Microsoft Security Team on January 12, 2024. As we shared, on January 19, the security team detected this attack on our corporate email systems and immediately activated our response process. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM.

As we said at that time, our investigation was ongoing, and we would provide additional details as appropriate.

In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access. This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised.

It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these secrets were shared between customers and Microsoft in email, and as we discover them in our exfiltrated email, we have been and are reaching out to these customers to assist them in taking mitigating measures. Midnight Blizzard has increased the volume of some aspects of the attack, such as password sprays, by as much as 10-fold in February, compared to the already large volume we saw in January 2024.

Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. It may be using the information it has obtained to accumulate a picture of areas to attack and enhance its ability to do so. This reflects what has become more broadly an unprecedented global threat landscape, especially in terms of sophisticated nation-state attacks.

Across Microsoft, we have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We have and will continue to put in place additional enhanced security controls, detections, and monitoring.

Our active investigations of Midnight Blizzard activities are ongoing, and findings of our investigations will continue to evolve. We remain committed to sharing what we learn.

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

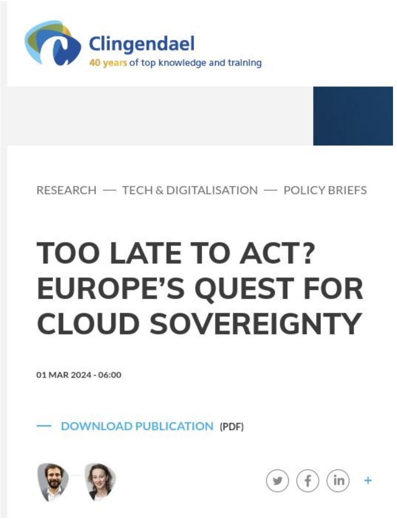
By Ellen Nakashima and Joseph Menn

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

Cloud Naïve: Europe and the 'Bijenkorf' Megascaler

Apr 28 2024

Lately there's been some confusion: places like SIDN (Dutch national operator of all internet names that end on .NL) claim that nobody in Europe can deliver their computer needs, and that they therefore must outsource their operations to American cloud providers.



Clingendael
40 years of top knowledge and training

RESEARCH — TECH & DIGITALISATION — POLICY BRIEFS

TOO LATE TO ACT? EUROPE'S QUEST FOR CLOUD SOVEREIGNTY

01 MAR 2024 - 06:00

— DOWNLOAD PUBLICATION (PDF)

Your tech or my tech: make up your mind quickly

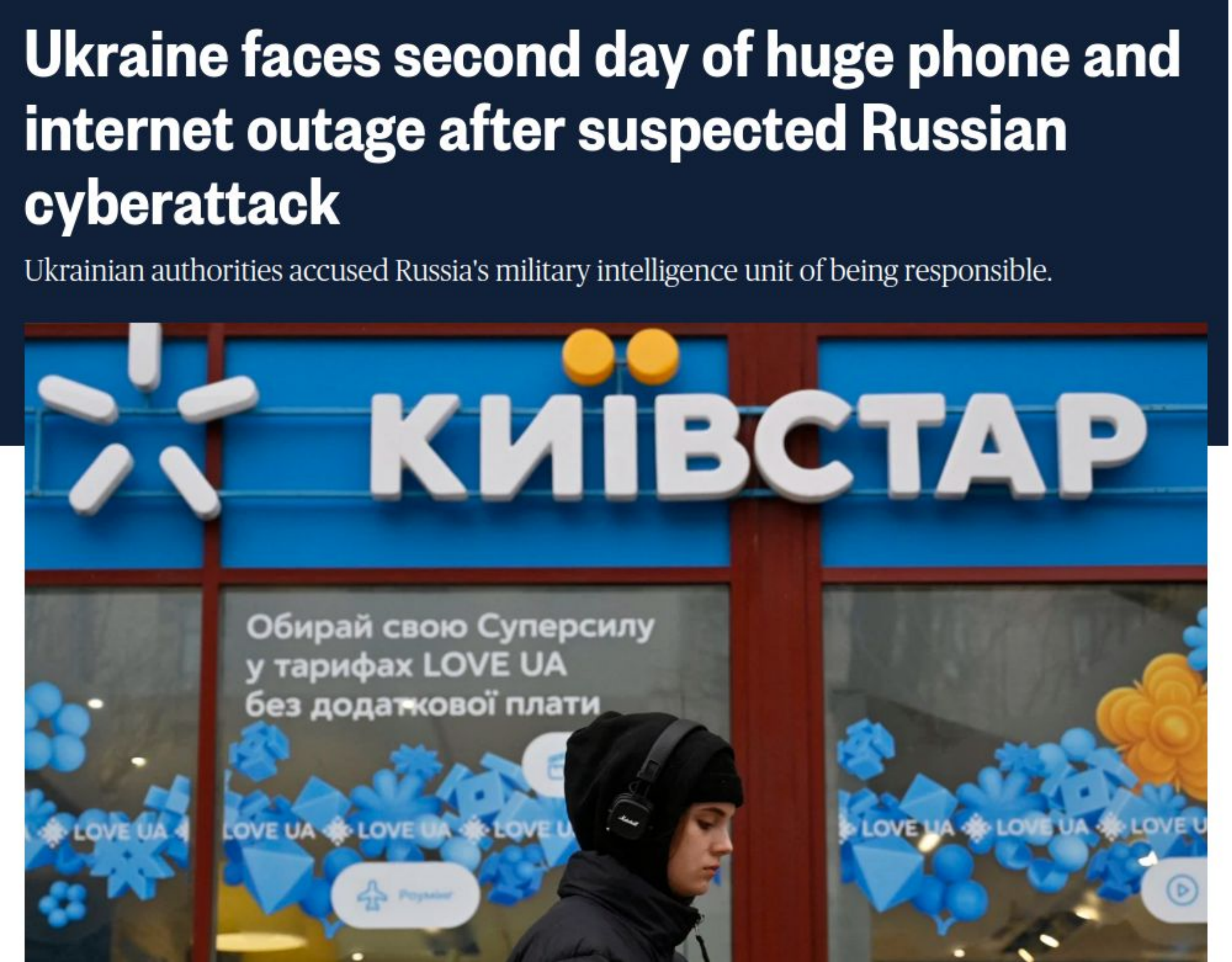
Mar 02 2024

There's no need to do everything yourself by the way. Source: Wikimedia

"You end up in a situation where everyone who loves IT has left, and as an employer you have also become very unattractive to people who have actual skills."

Why is this happening?

We can’t go on like this!



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

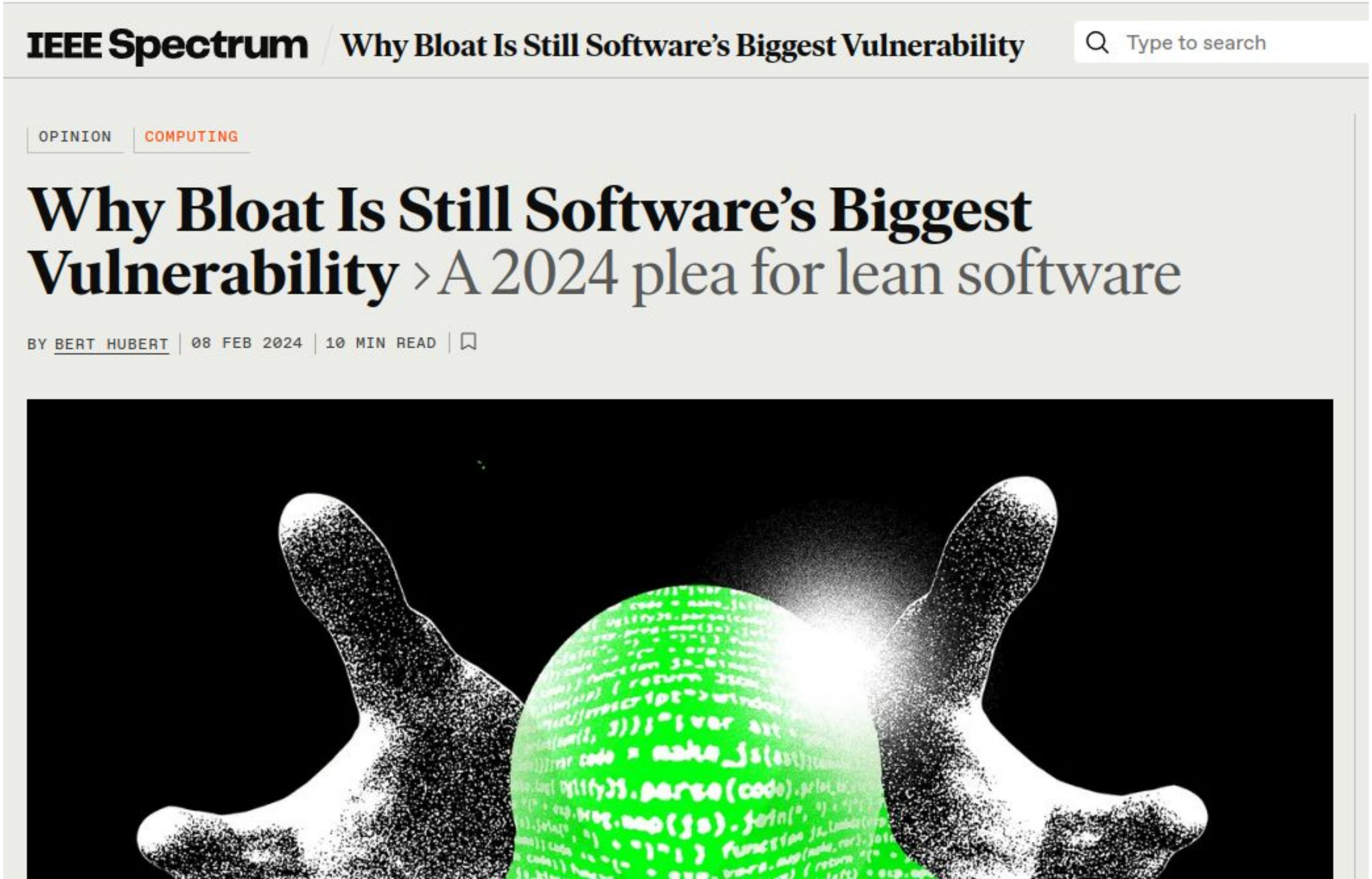
When times are bad, you are (much more) on your own!
(no one has time for you!)

- ROBUST: **Does not fall over by itself**

- LIMITED/KNOWN DEPENDENCIES: **Does not need too much unknown stuff too far away**

- OWNERSHIP/UNDERSTANDING: **If things break, you can improvise or fix things**

Is there a way back?



IEEE Spectrum | Why Bloat Is Still Software's Biggest Vulnerability

Type to search

OPINION | COMPUTING

Why Bloat Is Still Software's Biggest Vulnerability › A 2024 plea for lean software

BY BERT HUBERT | 08 FEB 2024 | 10 MIN READ

Summary

- The systems that support our daily lives are way way too complex & fragile
  - And getting more complex
- Maintenance is moving ever further away from us
  - As is understanding
- Our own skills are wilting, we are **no longer able to control our infrastructure**
- Now imagine a war where you need help from everyone else

- **We get this because non-technical people make economic choices**
- I don't know how we can fix this

Cyber Security and Society: a pre-war reality check

Bert Hubert / bert@hubertnet.nl

https://berthub.eu/prewar