Digitale autonomie & Cybersecurity

Bert Hubert / bert@hubertnet.nl
https://berthub.eu/security-congres

Eerst wat belangrijke woorden van 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.”

Smart guy

https://edition.cnn.com/2024/03/29/europe/poland-tusk-europe-pre-war-russia-ukraine-intl/index.html

EUROPE

'We are already in conflict with Russia' — Merz says Putin destabilizing Germany

August 30, 2025 2:43 pm • 2 min read

by Kollen Post

German Chancellor Friedrich Merz talking to journalists at the NATO summit in The Hague, Netherlands, on June 25, 2025. (Nick Allard/The Kyiv Independent)

Map 0.1: **Methods of Russian hybrid-warfare activity across Europe, January 2018–June 2025**

https://kyivindependent.com/we-are-already-in-conflict-with-russia-german-chancellor/
https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

BBC

Government to guarantee £1.5bn JLR loan after cyber shutdown

28 September 2025

Share Save

Ruth Comerford and Rachel Clun business reporter, BBC News

BBC

EU cyber agency says airport software held to ransom by criminals

22 September 2025

Share Save

Joe Tidy Cyber correspondent and Tabby Wilson

NOS

Weer meer digitale systemen van Openbaar Ministerie in werking na hack

Het Openbaar Ministerie (OM) is zo goed als helemaal weer aangesloten op de digitale systemen. Afgelopen juli koppelde het OM de systemen los van het internet na een hack.

"Maar gewoon even rondkijken op een site is er nog niet bij", aldus een woordvoerder. "Het gaat echt om de primaire systemen die het OM draaiende houden." Ook kunnen medewerkers nog niet thuiswerken.

NOS Nieuws • Maandag 11 augustus, 17:37 •
Aangepast maandag 11 augustus, 19:17

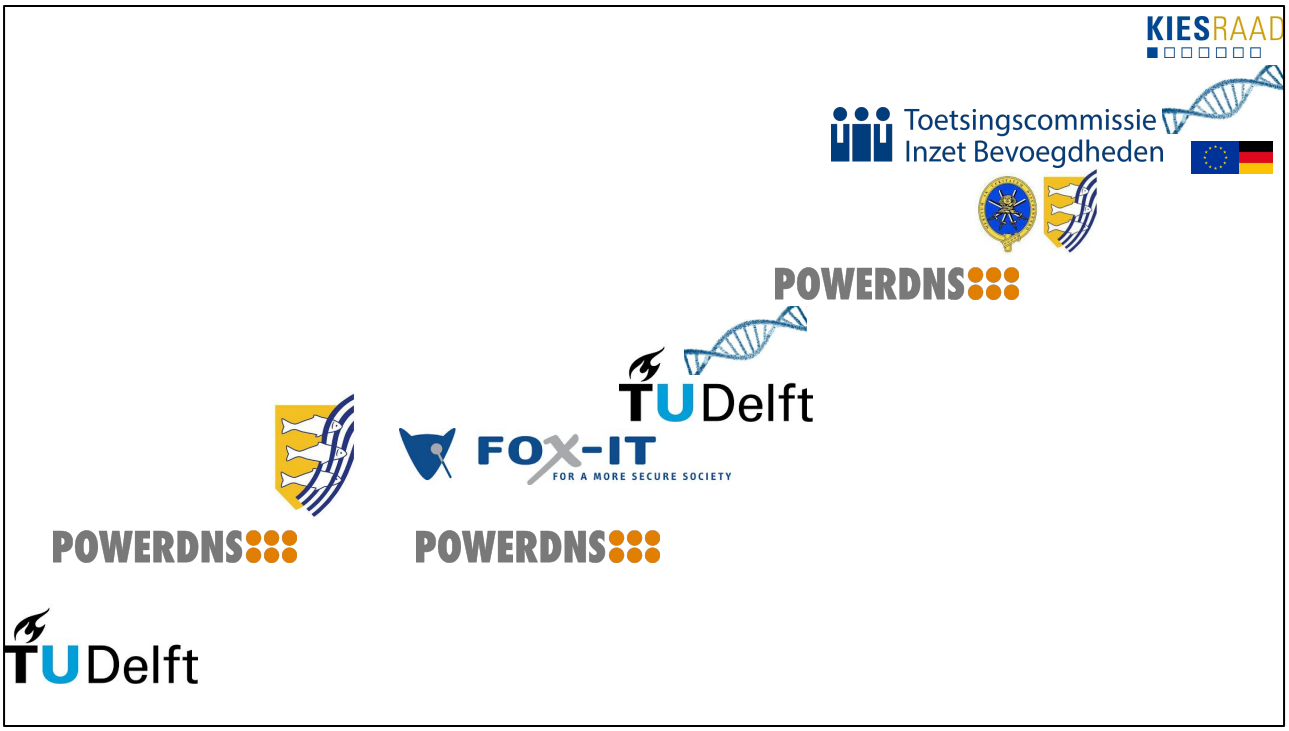
Datahack bij laboratorium veel groter, deel gegevens op dark web

Bij de hack van een laboratorium dat onder meer het bevolkingsonderzoek naar baarmoederhalskanker uitvoert zijn veel meer gegevens buitgemaakt dan eerder werd gemeld. Dat schrijft RTL Nieuws.

De gestolen data van laboratorium Clinical Diagnostics in Rijswijk zijn ook afkomstig van huid-, urine-, penis-, anus- en wondvochtonderzoek. Volgens het laboratorium betreft het vooral gegevens uit de periode van 2022 tot en met dit jaar.

Informatiebeveiliging is ineens een stuk meer dan een theoretisch iets.

En u bent onderdeel van onze verdediging!



Things I have done - only interesting to put my (strong) claims on later pages in context. I failed in my studies of physics, launched an unsuccessful startup (PowerDNS), and when that did not go well joined Dutch intelligence & security agency AIVD. From there I went on to develop software for police and intelligence agencies, while PowerDNS went on. After Fox-IT I did DNA research in Delft again, and then focused on PowerDNS again. After that, I became a regulator of Dutch intelligence services for 2 years. During this time I managed to get my DNA paper published in Nat. Scientific Data.
https://www.nature.com/articles/s41597-022-01179-8

POWERDNS

opentk.nl

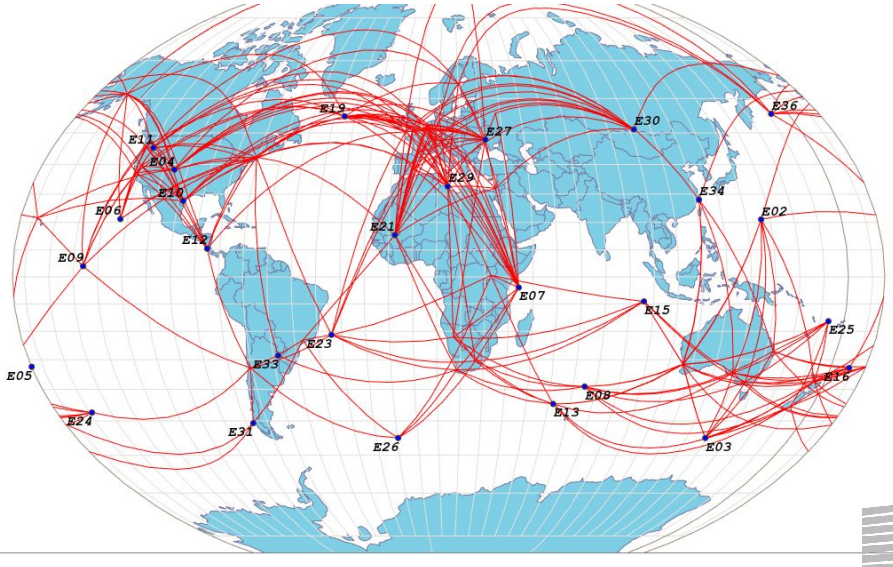
[overzicht] [activiteiten] [ongeplande activiteiten] [besluiten] [commissies] [geschenken] [kamerleden] [kamerstukdossiers] [mijn] [open vragen]
[toezeggingen] [stemmingen] [verslagen] [uitgebreid zoeken] [**wat is dit?**]

Zoek in alle kamerstukken, of voer document-, zaak- of activiteitnummer in

Meest recente documenten (live updates)

Alleen regeringsdocumenten

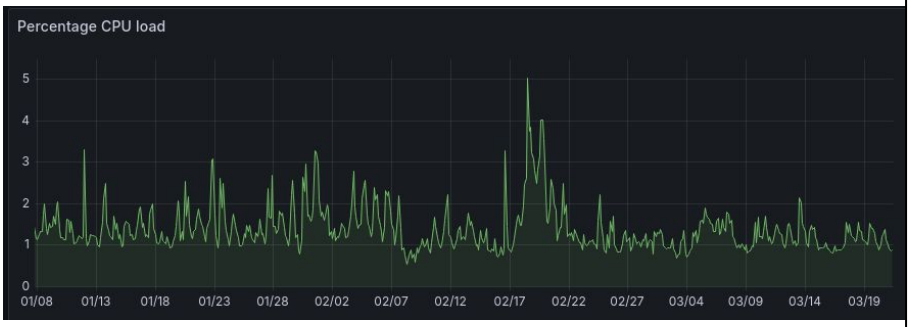
Datum	Bijgewerkt	Comm.	Onderwerp	Titel/Soort
2025-10-06	2025-10-06 17:21	K&GG	Geannoteerde Agenda Energieraad (formeel) 20 oktober 2025 (2025D43662)	Brief regering
2025-10-06	2025-10-06 17:20	I&W	Reactie op verzoek commissie over de correspondentie tussen het ministerie en de Europese Commissie inzake het LVB Schiphol openbaar aan de Kamer te doen toekomen (2025D43623)	Evaluatie Schipholbeleid
2025-10-06	2025-10-06 17:18	I&W	Startbeslissing Nedersaksenlijn (2025D43614)	Vaststelling van de begrotingsstaat van het Mobiliteitsfonds voor het jaar 2026
2025-10-06	2025-10-06 17:15	FIN	Inspectiebelastingen, toeslagen en douane (IBTD)-rapportage "Rechtsbescherming geschillen douaneheffingen' (2025D43655)	Brief regering
2025-10-06	2025-10-06 17:13	DEF	Geannoteerde Agenda Raad Buitenlandse Zaken Defensie d.d. 15 oktober 2025 (2025D43645)	Brief regering



European Commission

https://galmon.eu/

- Bare metal, 64 GB RAM, 1TB SSD
- Intel(R) Core(TM) i5-10500T CPU 6 cores
- “500 euro/year”
- <35W
- **ALSO RUNS GALMON.EU, BERTHUB.EU**



Behold, the server that powers _all_ of this

In de **operationele** wereld hebben we niet zoveel op met jullie compliance en jullie DPIA's en DTIA's en ISO's en BIO's…

Maar, I ❤️ Asset Registers

Had me drie hacks bespaard..

1: Digitale autonomie
&
2: Daadwerkelijke cybersecurity

Confidentiality
Integrity
Availability

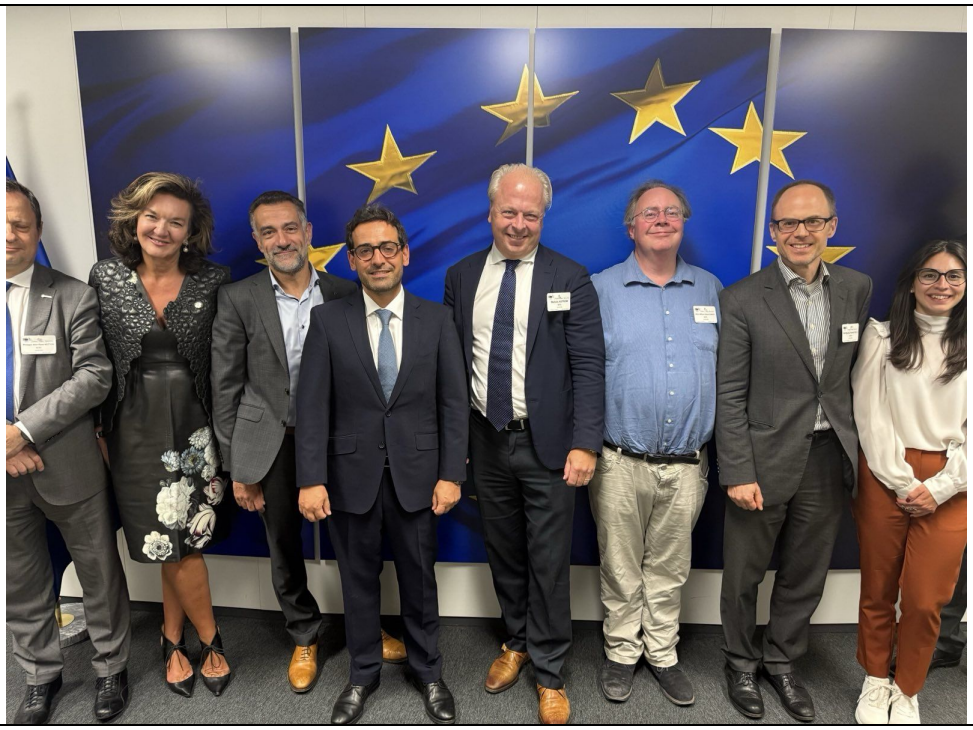
Wendbaarheid, **Weerbaarheid**

Ja dit is niet best, alle clouds komen dus van buiten Europa. Tot nu toe hebben mensen wel door dat je je overheid of andere belangrijke processen niet op de Alibaba Cloud moet draaien, maar dat komt vermoedelijk niet omdat mensen nadenken over de ‘soevereiniteit’. Het lijkt erop dat Europa z’n overheden nog op Noord Koreaanse servers zou draaien als de gebruikersinterface een beetje aantrekkelijk was.

De Europese en Amerikaanse cloudproviders. Niet echt op schaal, maar het schetst een beeld. Kijk goed onder de ‘e’ van Google. OCI is Oracle

Een beetje willekeurige selectie van Europese providers van beperkte clouddiensten. Met een focus op voor Nederland relevante partijen. Maar de schaal is wel even iets anders.


0:22 / 3:00




King

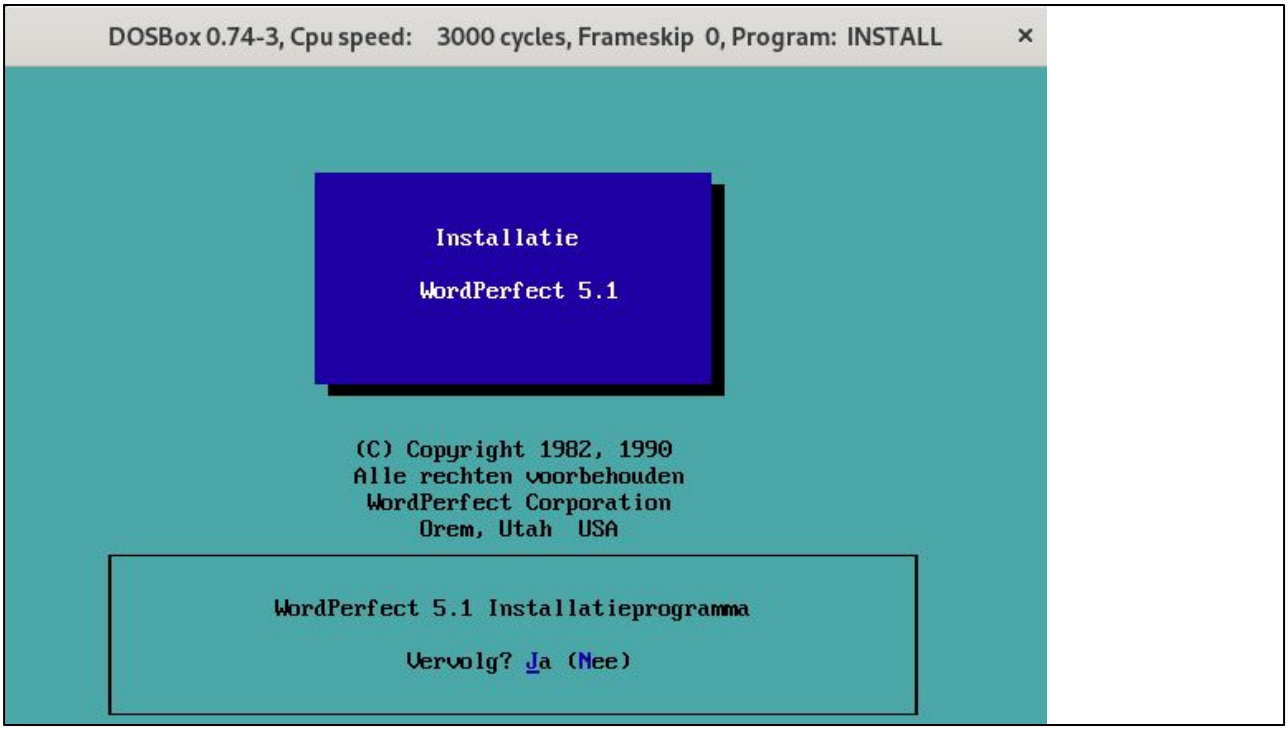
Ber Huber de Tech Exper

WordPerfect CORPORATION

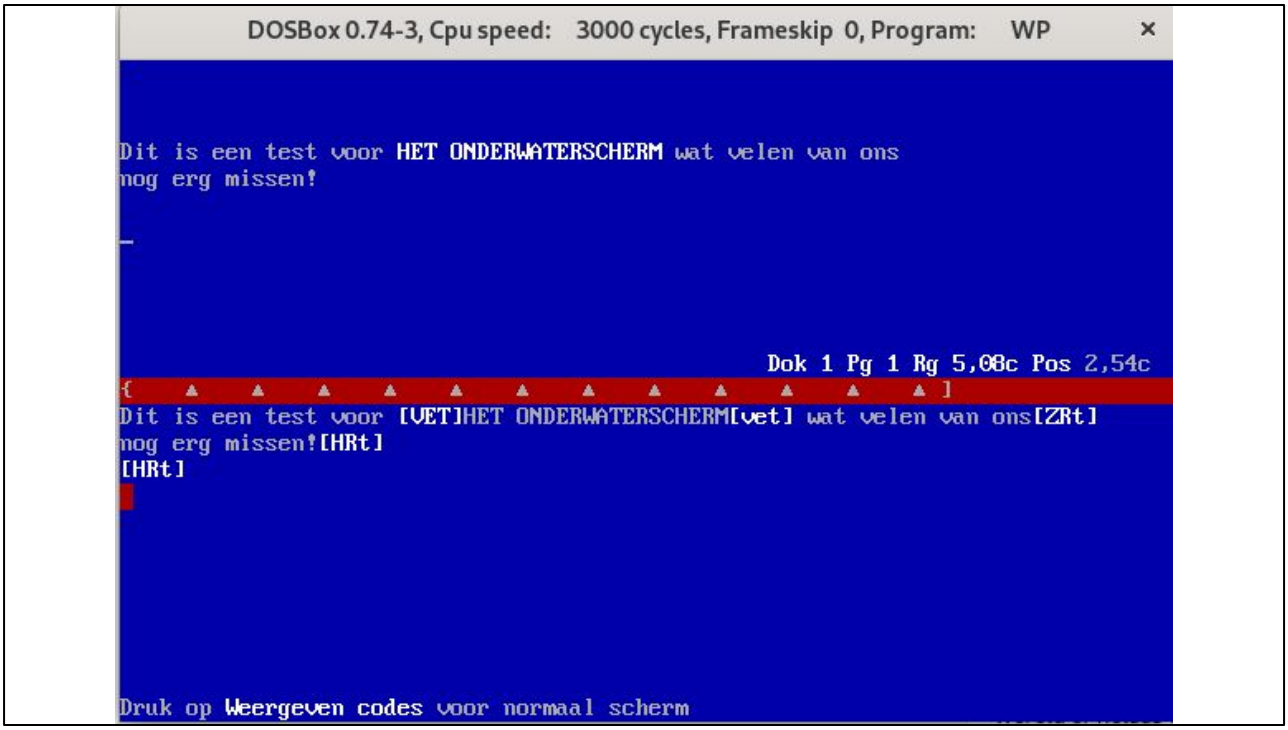
"Air-gapped sovereign computing solution"

WordPerfect™ for IBM® Personal Computers	Shell	Spell	Screen	Move	Ctrl	Text In/Out	Tab Align	Footnote	Font	Ctrl	Merge/Sort	Macro Define		
Column Left/Right Home, ←/→	Thesaurus	Replace	Reveal Codes	Block	Alt	Mark Text	Flush Right	Columns/Table	Style	Alt	Graphics	Macro		
Compose 2	Setup	♦Search	Switch	♦Indent♦	Shift	Date/Outline	Centre	Print	Format	Shift	Merge Codes	Retrieve		
Delete to End of Ln/Pg End/PgDn	Cancel	♦Search	Help	♦Indent		List	Bold	Exit	Underline		End Field	Save	Reveal Codes	Block
Delete Word Backspace	F1	F2	F3	F4		F5	F6	F7	F8		F9	F10	F11	F12
Hard Page Enter														
♦Margin Release Tab														
Pull-Down Menus =														
Screen Up/Down –/+ (num)														
Word Left/Right +/–														
74210–74210–74210														
© WordPerfect Corp. 1990 TM/UK/WP51KID—3/90														

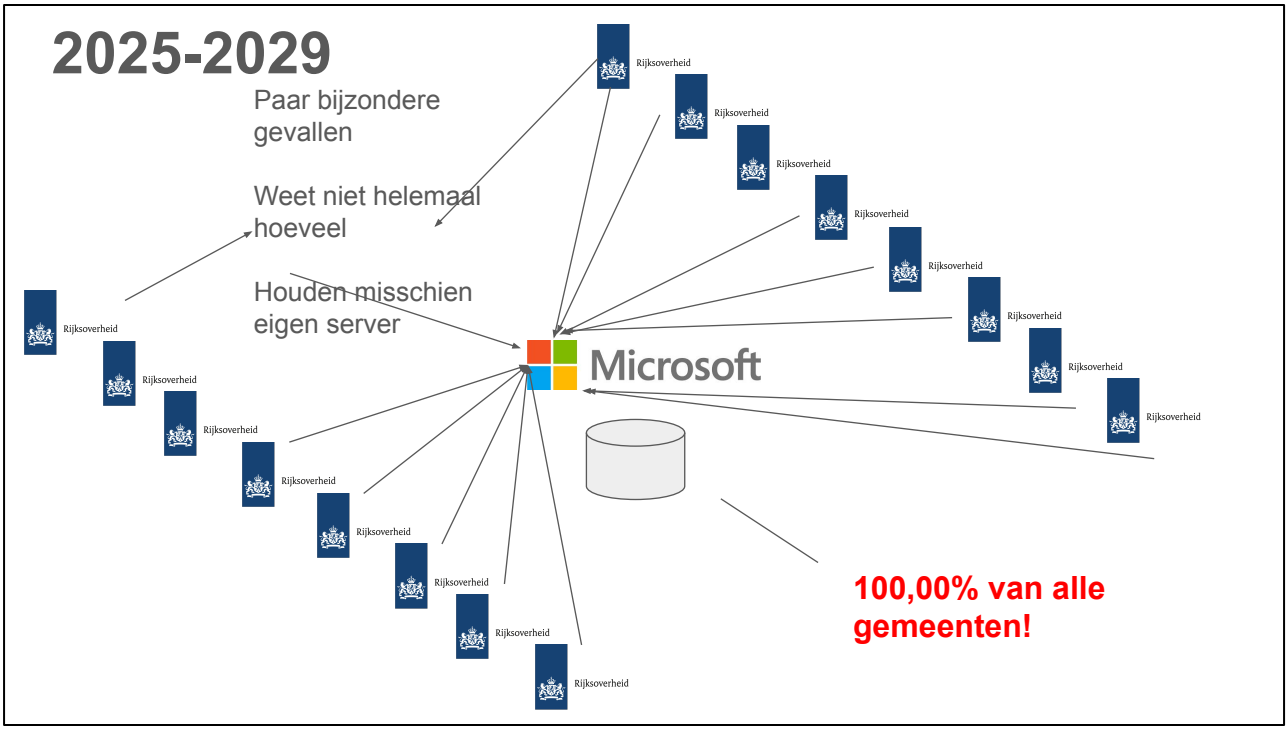
https://nl.wikipedia.org/wiki/IBM_PC_XT - hoe computers ooit waren. Software die je gekocht had die draaide op jouw computer. En ook toen maakten we ons al wat zorgen over de dominantie van WordPerfect, trouwens. Maar je data was wel je data. Alleen met diskettes (rechtsboven) ging je data ergens heen.



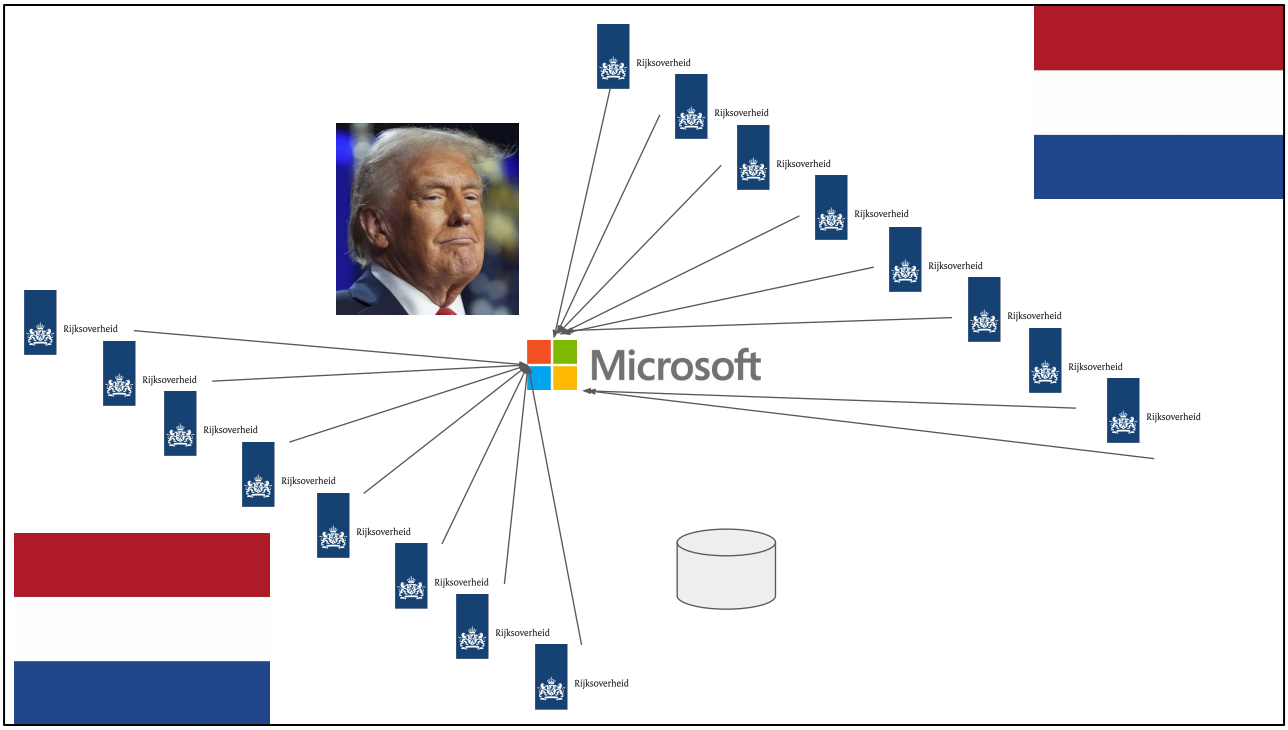
Nostalgisch intermezzo. Relevant is wel dat deze 34 jaar oude software het gewoon nog doet op moderne computers, en zelfs nog nuttig bruikbaar is. Kom daar nog maar eens om.



Nostalgisch intermezzo. Maar toch ook een serieus punt. WordPerfect liet je zien wat er onderwater gebeurde allemaal, en daar kon je dingen ook weer rechtzetten. Met moderne computers zoek je het maar uit. Je krijgt het niet te zien.



Dit is waar we in razend tempo op afstevenen: de hele overheid communiceert met elkaar via de Microsoftcomputers. Dit gaat dus niet om het bestaande *gebruik* van Microsoft software. Het gaat er dan om dat werkelijk iedere communicatie eerst naar een server van Microsoft gaat. Daar wordt de email bewaard, tot iemand op een ander ministerie de mail wil lezen. Alle email blijft permanent op Microsoft servers staan. Er zijn geen eigen mailservers meer. Als Microsoft een storing heeft, of ruzie met ons, dan werkt er niets meer, en kunnen we ook niets meer repareren.



En feitelijk krijgen we dan dit

Your Word documents will be saved to the cloud automatically on Windows going forward

MARTIN BRINKMANN Aug 27, 2025

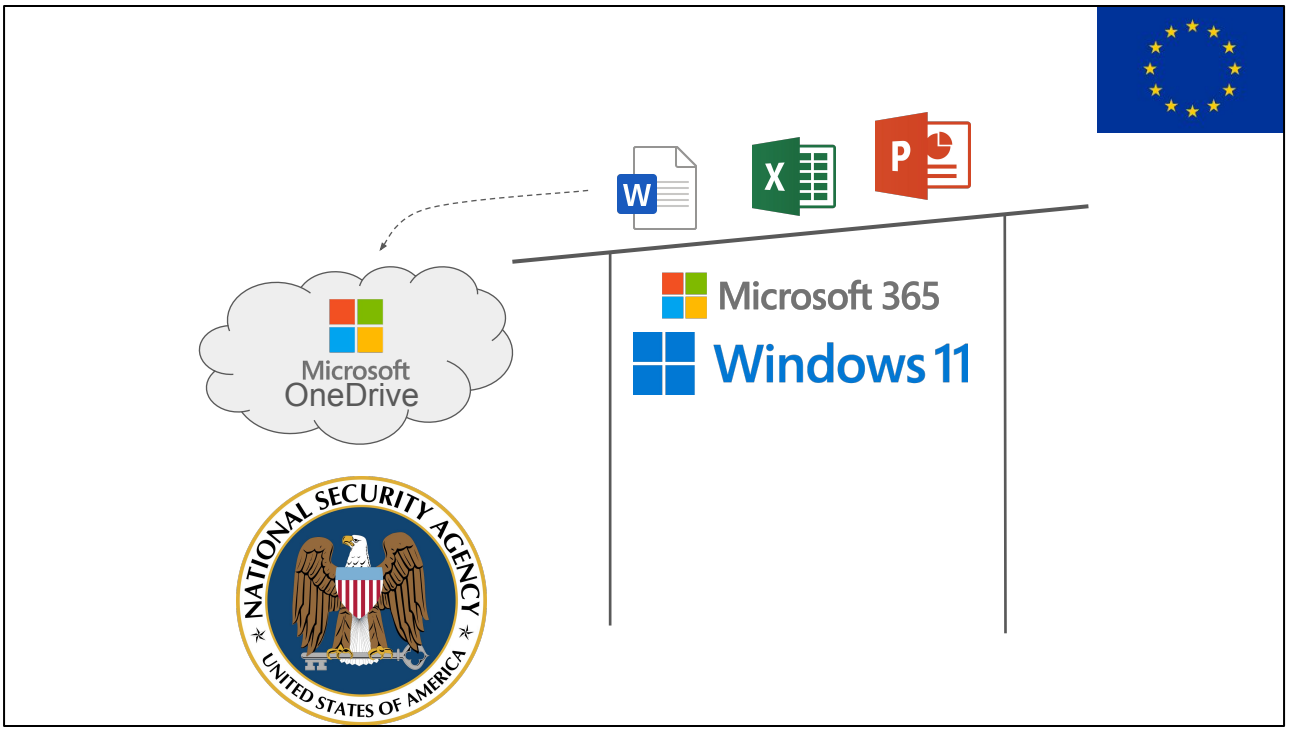
Windows 10, Windows 11
News

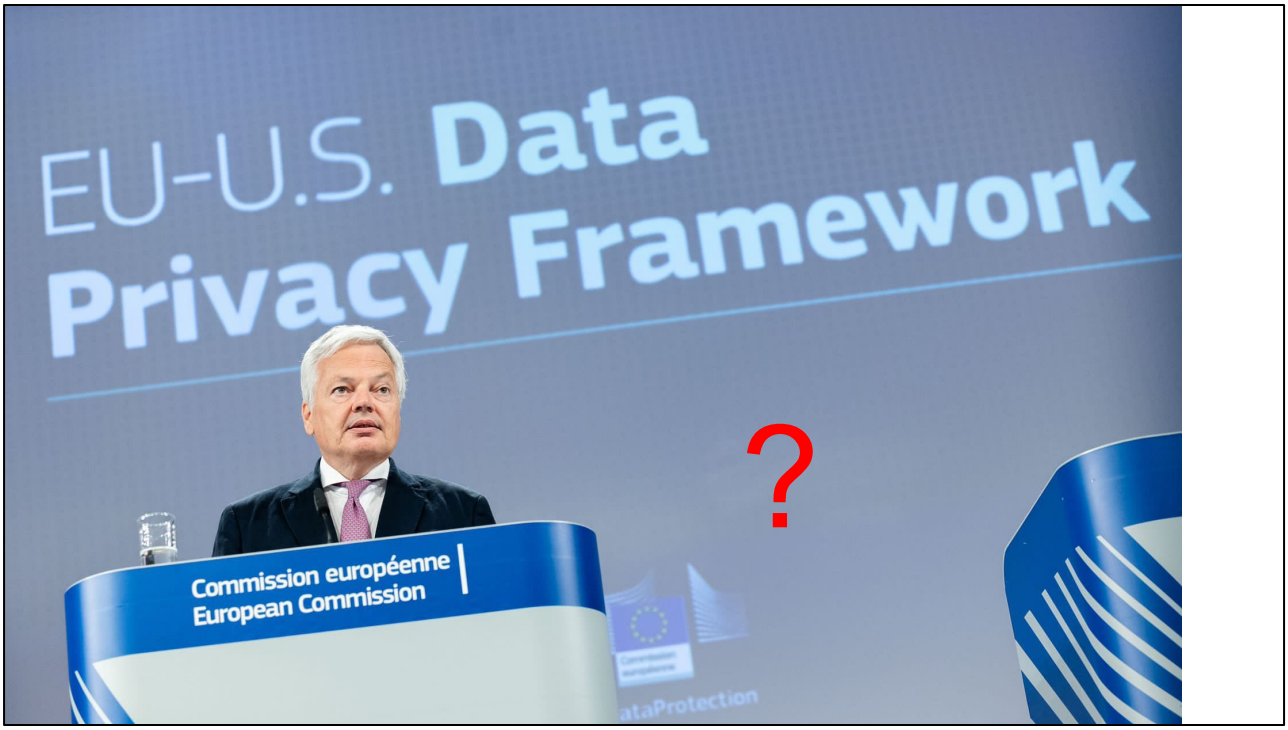
This really is a VERY strange situation that we have somehow gotten used to.

Law firms suing Microsoft.. Using Microsoft servers.

Governments planning US policy.. On US servers

A whole CONTINENT that can not control its data.


Microsoft
OneDrive
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Microsoft 365
Windows 11


EU-U.S. Data
Privacy Framework
?
Commission européenne
European Commission

IT DOES NOT MATTER WHERE THE SERVERS ARE

IF AMERICANS ARE INVOLVED

NO MATTER HOW INDIRECTLY

THE US CLOUD ACT & SECTION 702 APPLY

And they will have LEGAL ACCESS TO OUR DATA!

"This amount has been on a gradually rising trend with budget requests in 2020 and 2022 of US$62.7 billion and **US$65.7 billion** respectively"

GT GreenbergTraurig

Memorandum

TO:	Dutch Ministry of Justice and Security –NCSC
FROM:	Greenberg Traurig LLP | Gretchen Ramos, Andrea Maciejewski and Herald Jongen
DATE:	July 26, 2022
RE:	Application of the CLOUD Act to EU Entities

https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/augustus/16/cloud-act-memo/Cloud+Act+Memo+Final.pdf - en dat is gek. De Amerikaanse overheid heeft rechtmatig (volgens hun wet) toegang tot alle data op Microsoft servers. En ze geven ook 65 miljard dollar per jaar uit aan spioneren. Foto van de NSA. Waar ik ooit geweest ben. In hun museum. Aanrader overigens dat museum.

International criminal court

This article is more than **2 months old**

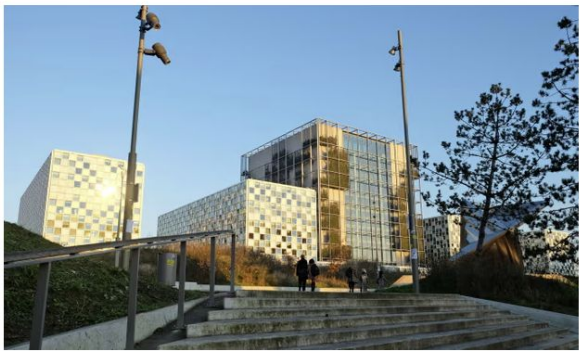
ICC braces for swift Trump sanctions over Israeli arrest warrants

Leadership at international criminal court fears new US administration will move quickly to shut it down

Harry Davies

Mon 20 Jan 2025 15.03 CET

Share



Exterior view of the international criminal court in The Hague, Netherlands. Photograph: Mike Corder/AP

The international criminal court is bracing itself for Donald Trump to launch aggressive economic sanctions against it this week, amid fears such a move could paralyse its work and pose an existential threat.

Multiple sources in the prosecutor's office said Microsoft's Azure cloud platform is critical to its operations and suspending access would paralyse its investigations. **"We essentially store all of our evidence in the cloud,"** one said.

Court authorities are understood to have been rapidly reviewing the ICC's suppliers and have **ended some commercial relationships in an effort to reduce its exposure**.

https://www.theguardian.com/law/2025/jan/20/international-criminal-court-icc-braces-swift-trump-sanctions-over-israeli-arrest-warrants

Exclusive: US could hit entire International Criminal Court with sanctions soon

By **Anthony Deutsch**, **Humeyra Pamuk** and **Stephanie van den Berg**

September 22, 2025 6:42 PM GMT+2 · Updated 2 hours ago

People stand outside the International Criminal Court (ICC) as the United States is considering imposing sanctions as soon as this week against the entire International Criminal Court, in The Hague, Netherlands, September 22, 2025. REUTERS/Piroschka van de Wouw Purchase Licensing Rights

The order to halt all cyber operations against Russia marks a stark departure from the previous administration's cybersecurity strategy. | Photo: Ismail Enes Ayhan via Plattform Unsplash | Unsplash Lizenz

US Halts Defensive Cyber Activities Against Russia: A Digital 'Withdrawal' from Europe

13. März 2025 Thomas Reinhold

Gaan de Amerikanen hun clouds in Europa nog wel verdedigen voor ons?

What Is the Insurrection Act of 1807?

Legal experts regard the act as a major exception to the law that generally forbids the use of the military for domestic law enforcement.

Ondanks oproep Kamer

Belastingdienst zet e-mail tóch bij Amerikaanse clouddienst Microsoft

Door Wouter van Dijke · 2 oktober 2025 · Aangepast: 3 oktober 2025

RTL Z

We zijn echt overgeleverd!

Maar hoe gaat het hier met de cybersecurity?

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.

History:

- *18/08/2025 --- v1.0 -- Initial publication*

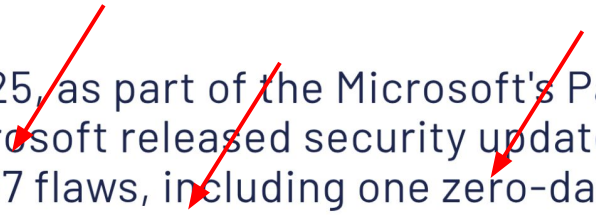
Summary

On August 13, 2025, Microsoft released its August 2025 Patch Tuesday advisory addressing 111 security flows in various products among which 16 are rated as critical [1].

It is recommended updating as soon as possible, prioritising public facing and critical assets.

- *09/07/2025 --- v1.0 -- Initial publication*

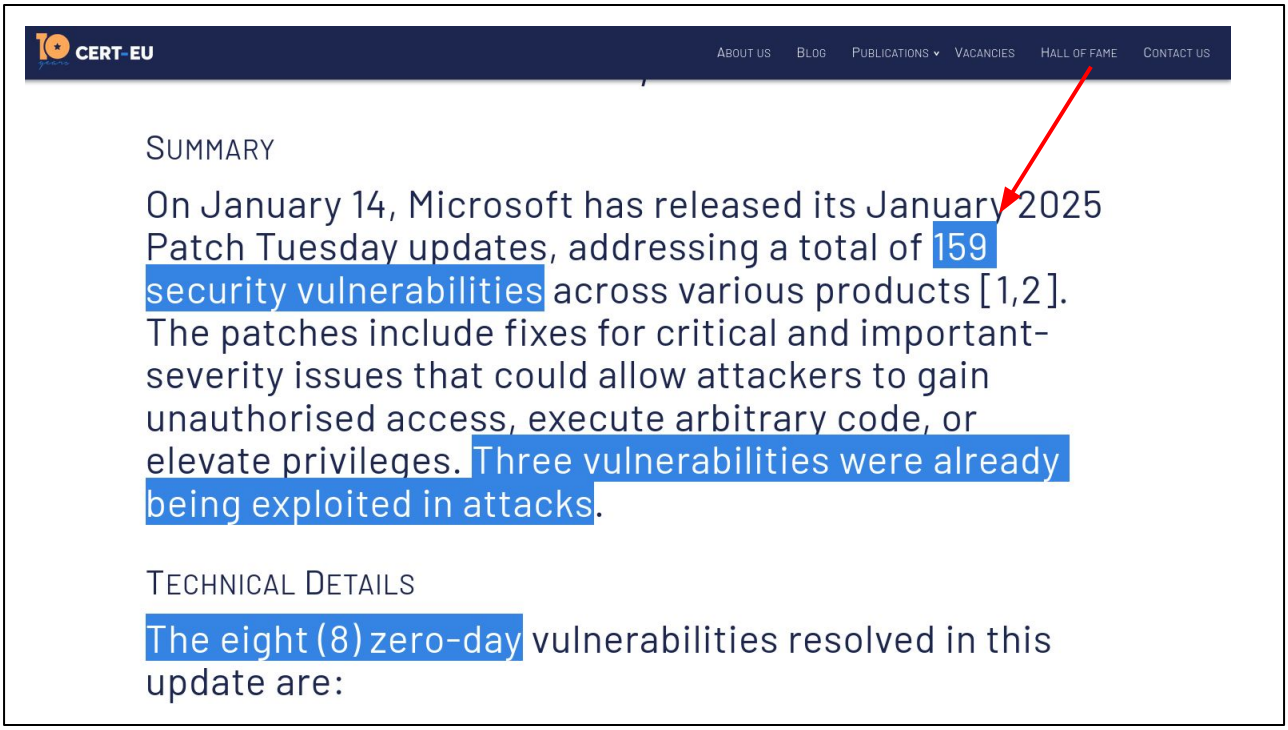
Summary



On July 8, 2025, as part of the Microsoft's Patch Tuesday, Microsoft released security updates addressing 137 flaws, including one zero-day vulnerability and fourteen critical vulnerabilities [1].

It is recommended updating as soon as possible, prioritising public facing and critical assets.

Technical Details

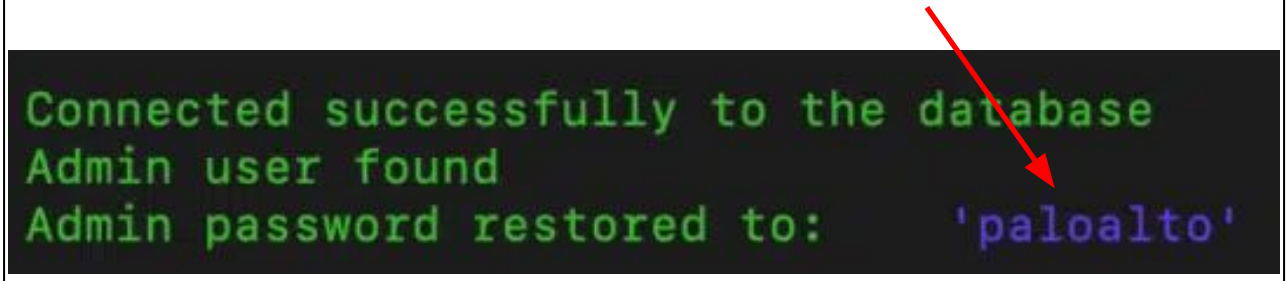

CERT-EU
About us
Blog
Publications
Vacancies
Hall of fame
Contact us
Summary
On January 14, Microsoft has released its January 2025 Patch Tuesday updates, addressing a total of 159 security vulnerabilities across various products [1,2]. The patches include fixes for critical and important-severity issues that could allow attackers to gain unauthorised access, execute arbitrary code, or elevate privileges. Three vulnerabilities were already being exploited in attacks.
Technical Details
The eight (8) zero-day vulnerabilities resolved in this update are:

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'
```



https://www.horizon3.ai/attack-research/palo-alto-expedition-from-n-day-to-full-compromise/

2025-019: Critical Vulnerabilities in Fortinet Products

Tuesday, May 13, 2025 08:11:21 PM CEST

On 13 May 2025, Fortinet released a security advisory addressing several vulnerabilities in their products, two of which are rated as critical.
It is recommended updating as soon as possible.

2025-018: Zero-Day Vulnerabilities in Ivanti EPMM

Friday, May 16, 2025 07:55:33 PM CEST

On May 13, 2025, Ivanti released a security advisory addressing two zero-day vulnerabilities in their EPMM products. An attacker could chain those vulnerabilities to achieve unauthenticated remote code execution on the vulnerable device. These vulnerabilities have been exploited in a limited number of cases.
[New] The analysis conducted by WatchTowr provides significantly more information than the advisory issued by Ivanti in two key aspects:
- WatchTowr attributes the vulnerabilities to code owned by Ivanti, whereas Ivanti asserts that they are related to third-party libraries.
- Additionally, WatchTowr questions the validity of the reported authentication bypass vulnerability, disagreeing with Ivanti's assessment.
CERT-EU strongly recommends applying the update as soon as possible, prioritising Internet facing devices.

PATCHES

14

Cisco scores a perfect 10 - sadly for a critical flaw in its comms platform

The second max score this week for Netzilla - not a good look

Iain Thomson

Wed 2 Jul 2025 // 22:33 UTC

If you're running the Engineering-Special (ES) builds of Cisco Unified Communications Manager or its Session Management Edition, you need to apply Cisco's urgent patch after someone at Switchzilla made a big mistake.

Cisco Unified Communications Manager (CM) consolidates IP telephony, high-definition video, unified messaging, instant messaging, and Presence status indicators. Its Session Management Edition centralizes dial-plan and trunk aggregation across multi-site deployments.

However, the ES builds of both packages have hardcoded credentials baked in, and they cannot be changed or deleted, meaning an unauthenticated, remote attacker can quickly get themselves full root control of a system if they know where to look. There's no workaround, and the only solution is to upgrade to the newest code for Unified CM, Cisco said.

DoublePulsar

Cybersecurity from the trenches, written by Kevin Beaumont. Opinions are of the author alone, not their employer.

Follow publication

Citrix forgot to tell you CVE-2025–6543 has been used as a zero day since May 2025

Kevin Beaumont Follow 5 min read · 2 hours ago

6

Back in late June, Citrix posted a patch for CVE-2025–6543, which they described as “Memory overflow vulnerability leading to unintended control flow and Denial of Service”. Denial of service? Piff the magic dragon, who cares.

Honderden grote gaten worden gedicht per week

Zo’n gat was er vaak al JAREN

Het komt nooit af, honderden NIEUWE gaten per week

De software waar we op bouwen is GEHEEL LEK

(ook in de cloud, maar daar zie je het niet zo)

https://doublepulsar.com/citrix-forgot-to-tell-you-cve-2025-6543-has-been-used-as-a-zero-day-since-may-2025-d76574e2dd2c

Kallisti 🎃
@kallisti@infosec.exchange

@da_667
At least once a week, looking at the state of InfoSec, I ask myself:"Why do we still have running water, electricity, an economy, infrastructure?"

And a few minutes later I remember the ever same answer:"Because nobody cared enough to take it from us yet."

Oct 06, 2025, 05:28 PM ·

12 boosts · **0** quotes · **18** favorites

Stuxnet, Photo by [Tasos Mansour](#) on [Unsplash](#)

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.

Drie storingen in zes weken: kan Odido het vertrouwen in zijn netwerk redden?

Door Ir
Redact
Feedba

AD NIEUWS REGIO SPORT SHOW KIJK PODCAST PUZZEL 9-2025 • 06:00

Mijn Gemeente Praat mee Auto Geld Koken & Eten Wonen Gezond Achter de Schen

Klanten van Odido hadden het de afgelopen weken niet altijd makkelijk met hun internetverbinding. In anderhalve maand kampte de provider meerdere keren met een langdurige storing. Klanten tastten vaak uren in het duister over de oorzaak en het moment waarop hun verbinding hersteld zou worden.

Op 15 en 16 juni ondervonden gebruikers problemen door een storing in de DNS-servers. Een dag later hadden klanten in delen van Zeeland, rond Rotterdam en op plaatsen in Noord-Holland minder tot geen bereik door een kabelbreuk. Op 25 juni, rond de NAVO-top, had Odido meerdere storingen op zijn mobiele netwerk. Op 1 augustus volgde de zwaarste storing: een deel van de klanten was 15 uur offline.

Voor die laatste storing besloot Odido zijn klanten twee euro compensatie te geven. Dat ligt boven het wettelijk minimum van één euro, maar volgens veel klanten is het een schamele vergoeding voor de problemen die zij eind juni tot begin augustus ondervonden. Veel tweakers voelen zich. in reacties en op

▲ © REUTERS

Uren geen Teams, Outlook en Office 365 door storing Microsoft, ook problemen bij Nederlandse overheden

Rijkswaterstaat Verkeersinformatie
@RWSverkeersinfo

Translate post

De afritten Delft op de #A13 zijn dicht door een pinstoring bij de nabijgelegen Ikea. Alle winkelbezoekers vertrekken namelijk tegelijk, wat voor veel drukte zorgt. Het verkeer op de snelwegen kan een afrit verderop en binnendoor alsnog naar bestemming (tenzij dat de Ikea was).

Storing verkeersleidingspost Utrecht opgelost

Lees voor

5 juni 2024

CROWDSTRIKE

NOS Nieuws • Vrijdag 19 juli 2024, 21:32

Hoe een softwarefoutje luchthavens, media en ziekenhuizen kon platleggen

“OT mensen: ‘zijn jullie GESTOORD’”

NOS Nieuws • Vrijdag 19 juli 2024, 09:00 • Aangepast vrijdag 19 juli 2024, 12:37

Wereldwijd problemen door computerstoring: onder meer luchthavens en ziekenhuizen getroffen

Kustwacht
In nood: 0900-0111
Geen spoed/pechhulp

Choose language NL Zoeken

Home / Nieuws / Kustwacht getroffen door grootschalige storing

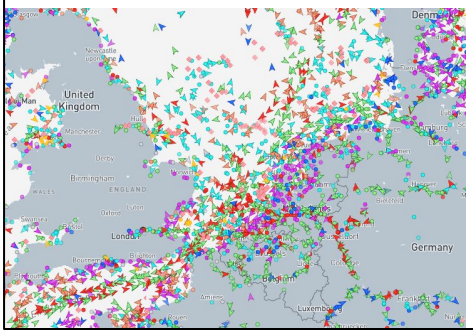
Nieuws

Eenvoudige w
Le

Kustwacht getroffen door grootschalige storing

28-08-2024 18:25 uur

Dinsdagavond werd de Kustwacht geconfronteerd met een storing. Hierdoor was het Kustwachtcentrum tot woensdagmiddag niet bereikbaar via de marifoon en telefoon. In de loop van de ochtend werd duidelijk dat er sprake was van een grootschalige, landelijke storing.



Grote storing: defensienetwerk blijkt essentieel voor overheidsdiensten

Netwerkstoring Verschillende overheidsdiensten werden woensdag getroffen door een grote netwerkstoring bij het ministerie van Defensie. Op Eindhoven Airport konden geen vluchten landen of opstijgen. Systemen van de kustwacht en de marechaussee, maar ook van 112 en DigiD, lagen eruit. Hoe kon dit gebeuren?

SD **Steven Derix** en **Rik Wassens**

28 augustus 2024 • Leestijd 4 minuten

Luisteren Leeslijst

Ook minister David van Weel (Justitie) liet van zich horen. Hij zei dat de storingen vooral voor ongemak zorgen. "Ook bij Defensie kan er een storing zijn", zei hij. "Het hoeft dus ook geen aanval te zijn.

Get used to it, zou ik zeggen."

De reacties vanuit de overheid schoten in het verkeerde keelgat bij Bert Hubert techexpert en oud-toezichthouder van de inlichtingendiensten. De overheid heeft de ernst van de situatie niet in de gaten, zegt hij. Volgens Hubert is het heel erg wat er aan de hand is. "Maar de reactie erop is nog veel erger. Zo van dit gebeurt weleens."

https://www.nu.nl/tech/6326175/zorgelijke-wen-er-maar-aan-reactie-van-overheid-op-storing-zien-ernst-niet-in.html

Op de werkvloer werkt cybersecurity in **niets** zoals in het afgevinkte rapport staat.

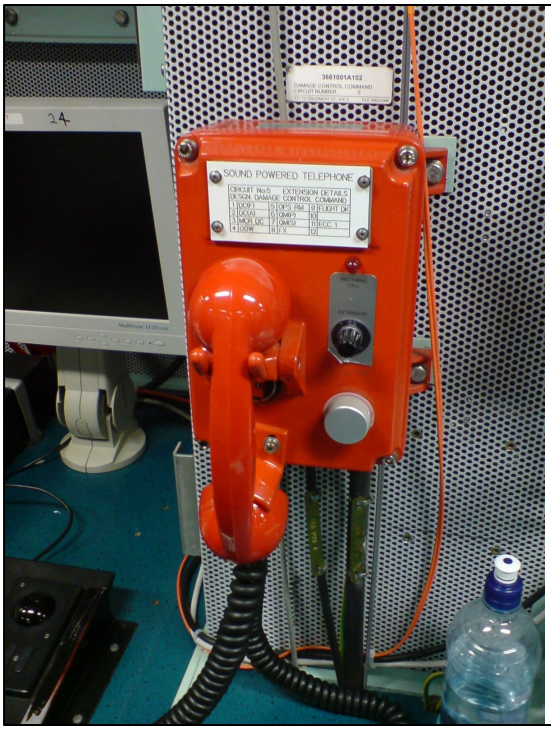
Daarom gaat het toch mis ondanks alle goedgekeurde en geaccordeerde plannen.

“IT”

“Where we like our stuff complex & enterprise-grade”

“OT”

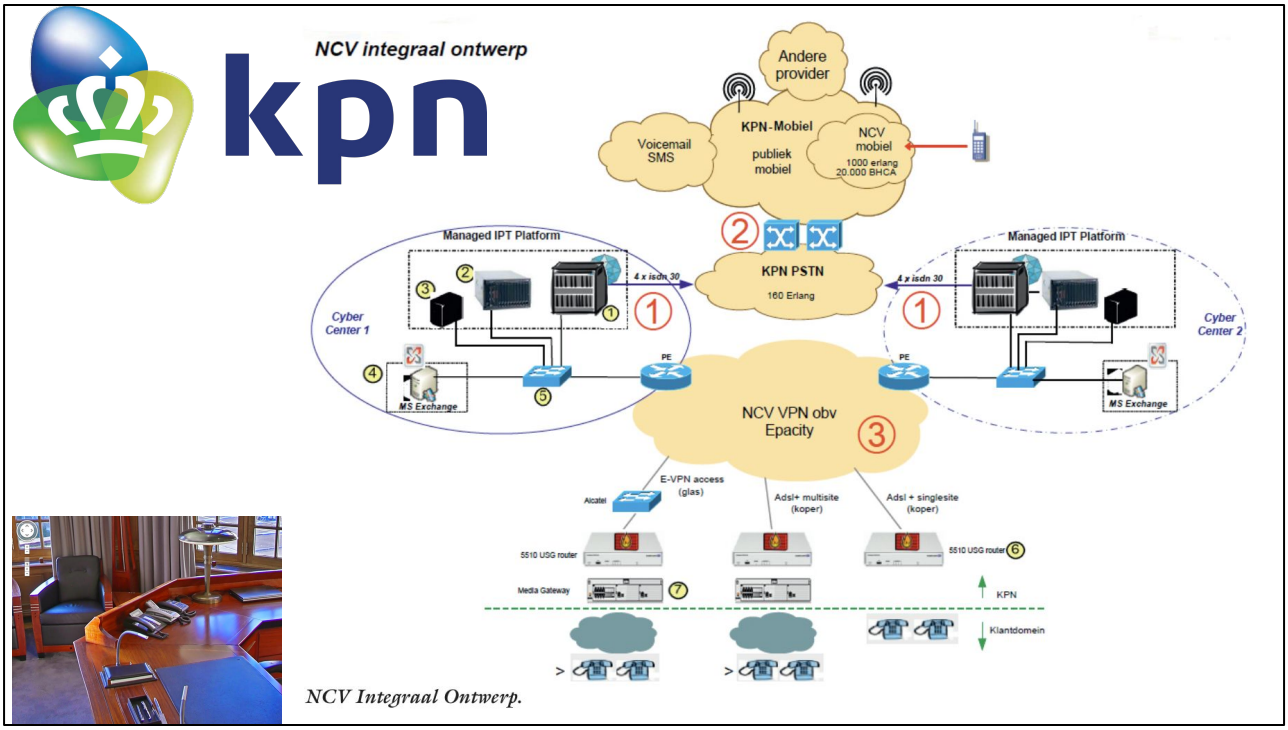
“Where reliability and safety should be king”



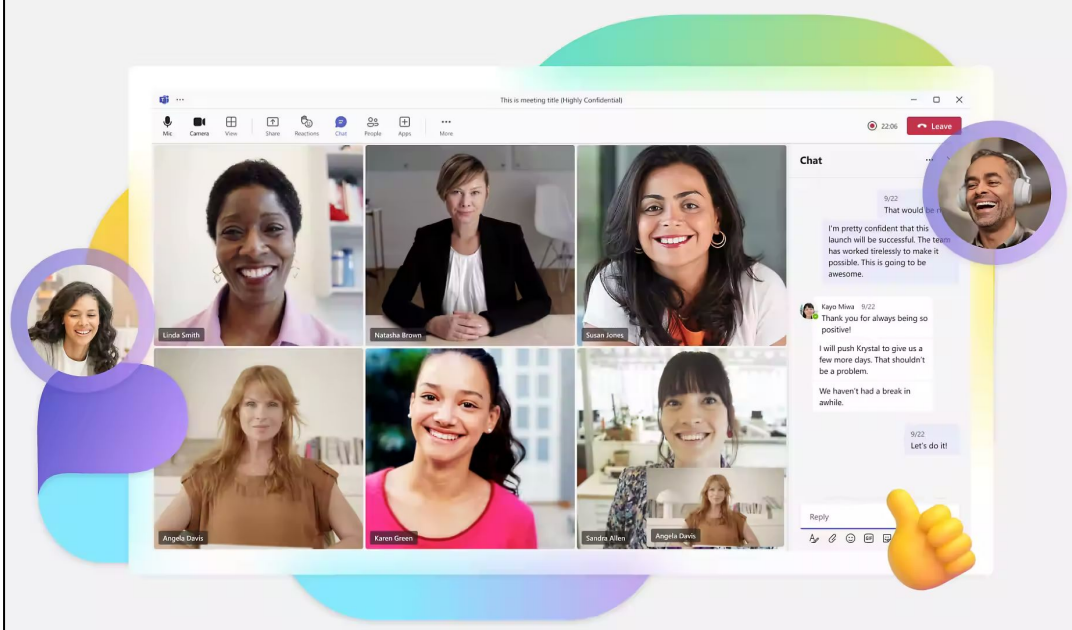
“Many different types of equipment have attempted, **but have largely failed**, to replace the incredibly simple sound-powered telephones on ships. Due to the rugged, reliable and **power-free** nature of this equipment, it remains in use on all US military vessels.”

https://en.wikipedia.org/wiki/Sound-powered_telephone - ALWAYS works. Can do 50 kilometer distance.

https://www.gld.nl/nieuws/8135427/kijken-mag-nu-want-geheime-atoombunker-voldoet-alleen-nog-als-erfgoed



https://vovklict.nl/intercom/2013/1/38__41.pdf -
https://www.nctv.nl/binaries/nctv/documenten/publicaties/2023/03/20/koepelnotitie-crisiscommunicatie-bij-uitval-van-elektriciteit/Koepelnotitie+comm.+elektra.pdf



Microsoft Teams as fixed-line telephony replacement for government use!

No kidding!

More like Microsoft M364

Dit is allemaal onacceptabel.

Honderden nieuwe securityproblemen per week

Maar we vinden het best

Vliegvelden, kustwacht, ziekenhuizen vallen om als je er naar blaast

Iedereen blijft dezelfde lekke spullen kopen

En we gaan onze telefoons vervangen door Teams en kunnen alleen nog maar communiceren via Donald Trump

Hoe kan dat nou?

1) De wereld wordt enger en enger (Merz, Tusk)

2) We zijn in de Amerikaanse aap gelogeerd met de bulk van onze maatschappij (cloud)

3) Al onze cybersecurity is lek als een mandje **in de praktijk**

En toch heeft iedereen er voor getekend dat het wel goed is zo

We zijn hier niet op security-congres.nl…

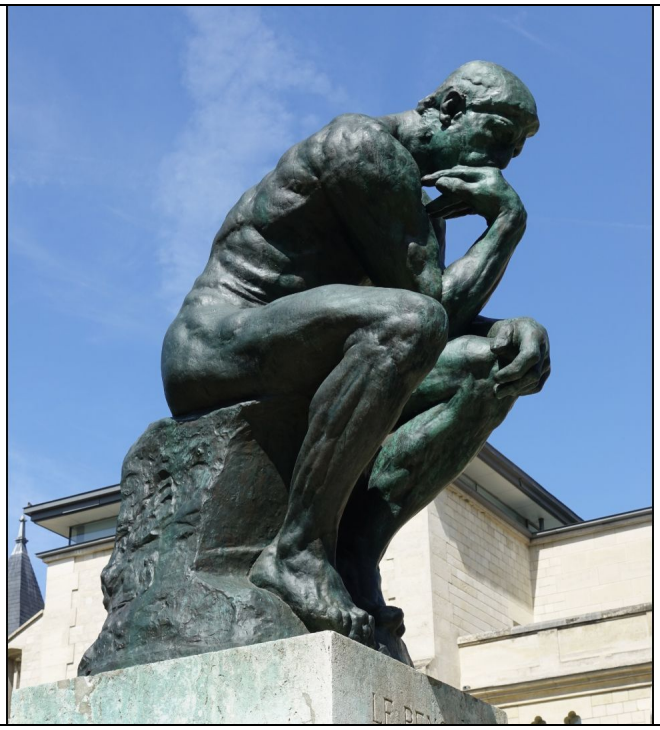
We zijn op **compliance-congres.nl!**

Compliance != Security

Je kunt een spinnenweb van outsourcingsovereenkomsten over diverse continenten niet “veilig complyen”!

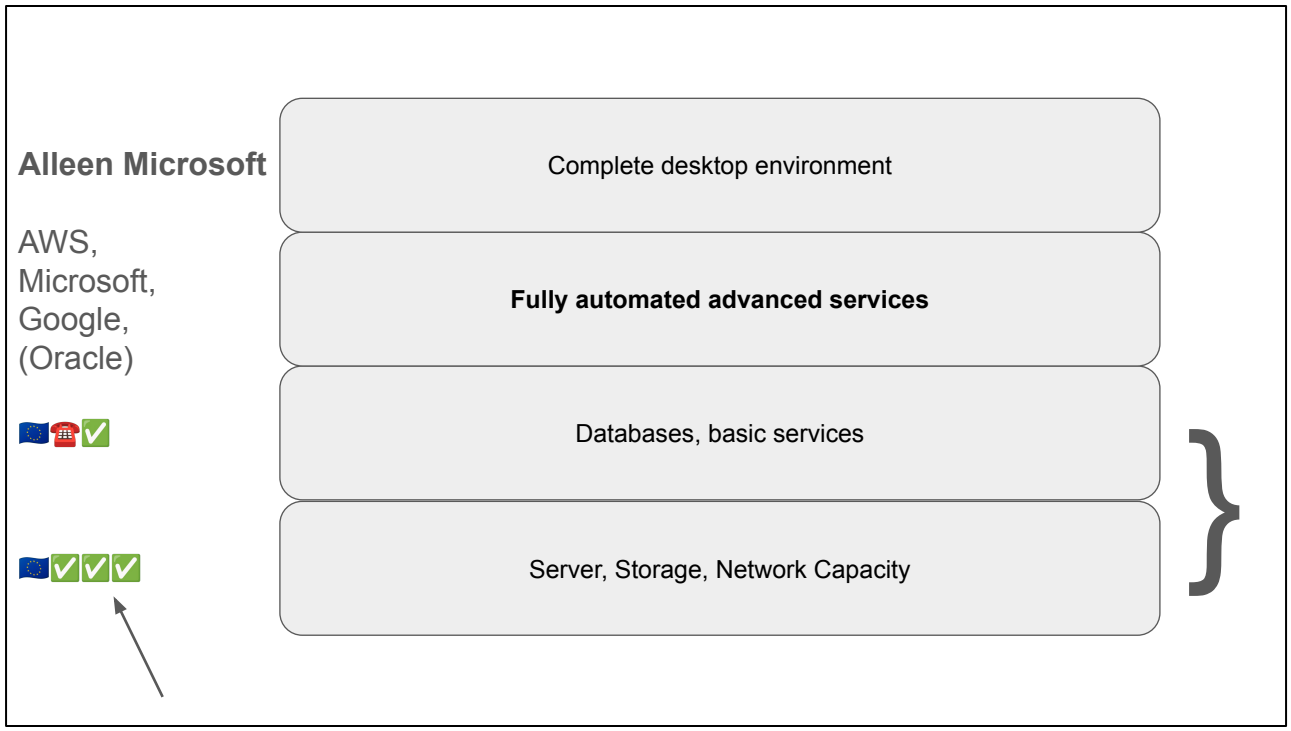
Security is een INTEGRALE uitdaging!

(en eenmaal gehacked blijkt alles ‘on the ground’ heel anders dan je dacht)



De weg terug omhoog - onze eigen clouds en onze eigen cybersecurity


Ongeveer 100% van nieuwe diensten
“Jouw probleem om te maken en beheren”
Product
S3
RDS
SQS
R53
Cognito
Google
aws


Alleen Microsoft
AWS,
Microsoft,
Google,
(Oracle)
🇪🇺☎️✅
🇪🇺✅✅✅
Complete desktop environment
Fully automated advanced services
Databases, basic services
Server, Storage, Network Capacity

Hosters verkopen hout, klanten willen meubels

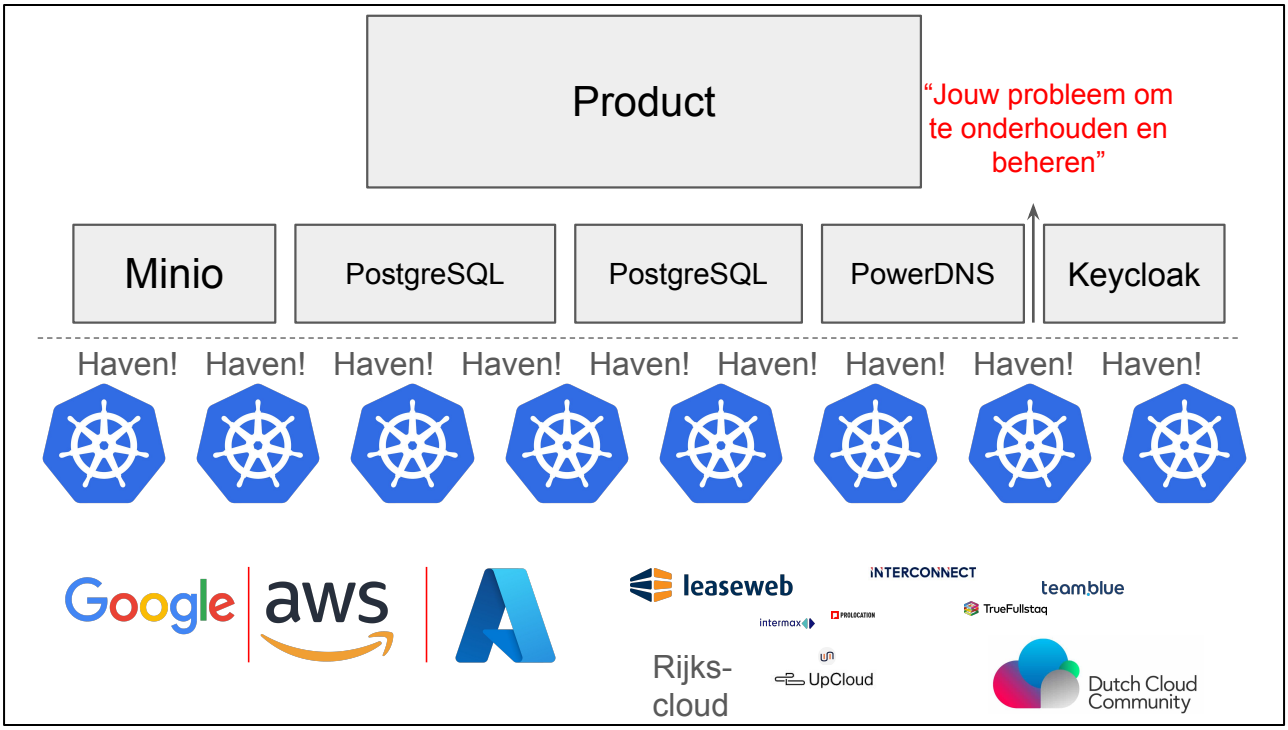
Mar 17 2025

Eerder schreef ik dat er niet één soort cloud is, het loopt van servers verhuren tot kant en klare kantoorsoftware as a service.

Een relevant soort cloud is wat informeel wel 'cloud native' wordt genoemd. Ik schreef daarover dat een 'cloud native programmeur' niet werkt op basis van servers. Als je virtuele servers verhuurt en je noemt jezelf een cloudbedrijf, dan snapt die cloud native programmeur daar niets van. Die kan niet uit de voeten met computers, die heeft diensten nodig.

Vanuit de klassieke serverbusiness vindt men zo iemand helaas nogal sneu, heeft hulp nodig bij alles, kan geen database draaien zelf, heeft geen idee wat een nameserver is. "Zo'n programmeur kookt met pakjes en zakjes maar kan nog geen ei bakken zelf".

Maar omgekeerd, heb je weleens goed gekeken naar die pakjes en zakjes van de cloud? Daar zitten echt PRACHTIGE dingen tussen. Naast complete databases waar je nooit naar om hoeft te kijken zitten er grote bouwblokken bij die problemen voor je oplossen die anders enorm veel werk zouden zijn om goed te doen.


Product
“Jouw probleem om te onderhouden en beheren”
Minio
PostgreSQL
PostgreSQL
PowerDNS
Keycloak
Haven!
Haven!
Haven!
Haven!
Haven!
Haven!
Haven!
Haven!
Haven!
Google
aws
leaseweb
INTERCONNECT
teamblue
TrueFullstaq
intermax
PROLOCATION
Rijks-cloud
UpCloud
Dutch Cloud Community

Je kunt, **met wat goede wil**, op Europese cloudproviders draaien.

Vroeger konden we dat ook namelijk (“**5 jaar geleden**”)

Maar inmiddels is het gewoon veel makkelijker om dat niet te doen, zelfs voor je belastingdata

En een van de grote redenen? **Compliance**

De auditors zijn zo goed aan boord met Microsoft

Zelfde geldt voor niet-Ivanti, niet-Citrix, niet-Cisco cybersecurity

De auditors vinden het al ok

Informatiebeveiliging is ineens een stuk meer dan een theoretisch iets.

En u bent onderdeel van onze verdediging!

Aan de repressie kant: accepteer geen oplossingen meer die 100 security fixes per jaar nodig hebben die steeds in het nieuws zijn.

Aan de positieve kant: sta positief ten op zichte van Europese leveranciers die nog niet alle vinkjes kunnen zetten op compliance. Misschien nog niet nodig.

En kijk tegelijk ook eens kritisch naar de scope van de compliance vinkjes van de grote Amerikaanse aanbieders!

Succes!

Digitale autonomie & Cybersecurity

Bert Hubert / bert@hubertnet.nl
https://berthub.eu/security-congres