De enorm bedroevende toestand van cybersecurity

Bert Hubert
bert@hubertnet.nl


Universiteit Leiden
KIESRAAD
Toetsingscommissie Inzet Bevoegdheden
Autoriteit online Terroristisch en Kinderpornografisch Materiaal
POWERDNS
TU Delft
FOX-IT
FOR A MORE SECURE SOCIETY
POWERDNS
POWERDNS
TU Delft

Toetsingscommissie Inzet Bevoegdheden

En, hoe is het met de cybersecurity?

NOS Nieuws • Vrijdag 27 september, 15:19 •
Aangepast vrijdag 27 september, 18:17

Datalek bij politie, hackers bemachtigen contactgegevens alle politiemedewerkers

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.

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.

6 min 115

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.

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 ▸

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.

> **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.

!!

Met deze brief informeer ik uw Kamer over de verdachte activiteiten rondom de informatievoorziening bij het NFI donderdagavond 7 november 2024.

Door het detectiesysteem van het NFI zijn verdachte activiteiten waargenomen op een account van een medewerker van het NFI. Uit voorzorg heeft het NFI besloten om alle internetverbindingen van het systeem te verbreken.

Een extern forensisch onderzoeksbureau is gelijk donderdagavond 7 november 2024 ingeschakeld om nader onderzoek te verrichten. Het onderzoek is enerzijds gericht op het veiligstellen van informatie en anderzijds om te beoordelen wat er precies aan de hand is.

Het eerste resultaat van het onderzoek heeft geen aanwijzingen opgeleverd wat betreft infiltratie van buitenaf. Zodra meer resultaten bekend zijn van het lopende onderzoek wordt bekeken of en welke maatregelen getroffen kunnen worden. Het NFI is nog in staat om forensische onderzoeken uit te voeren, maar wordt door deze situatie helaas wel enigszins belemmerd. Het NFI werkt er hard aan om alle systemen weer zo snel mogelijk in gebruik te kunnen nemen.

Ik zal uw Kamer informeren zodra er meer bekend is over de situatie en het onderzoek bij het NFI.

Het NFI heeft alle medewerkers hierover ook geïnformeerd.

The Shadow Brokers

From Wikipedia, the free encyclopedia

The Shadow Brokers (**TSB**) is a hacker group who first appeared in the summer of 2016.[1][2] They published several leaks containing hacking tools, including several zero-day exploits,[1] from the "Equation Group" who are widely suspected to be a branch of the National Security Agency (NSA) of the United States.[3][4] Specifically, these exploits and vulnerabilities[5][6] targeted enterprise firewalls, antivirus software, and Microsoft products.[7] The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA's Tailored Access Operations unit.[8][9][10][4]

EternalBlue [edit]

Main article: EternalBlue

Over 200,000 machines were infected with tools from this leak within the first two weeks,[26] and in May 2017, the major WannaCry ransomware attack used the ETERNALBLUE exploit on Server Message Block (SMB) to spread itself.[27] The exploit was also used to help carry out the 2017 NotPetya cyberattack on June 27, 2017.[28]

ETERNALBLUE contains kernel shellcode to load the non-persistent DoublePulsar backdoor.[29] This allows for the installation of the PEDDLECHEAP payload which would then be accessed by the attacker using the DanderSpritz Listening Post (LP) software.[30][31]

Enorme incidenten, hoe komt dat dan?

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

A A A A

Multiple Critical Vulnerabilities in Microsoft Products

Download

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

A A A A

Multiple Critical Vulnerabilities in Microsoft Products

Download

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.

“Patches” voor meer dan 100 grote software fouten per week

Die fouten zaten er meestal al JAREN

Het is niet dat we nu bijna klaar zijn met fixen, er komen minstens net zoveel nieuwe fouten voor terug!

localhost:8040/SetupWizard.aspx/

CONNECTWISE ScreenConnect

1 2 3 4

WELCOME

TO SCREENCONNECT

This setup wizard will configure basic settings for ScreenConnect.

GitLab Community Edition

Username or email

bert@hubertnet.nl

Password

Remember me

Forgot your password?

Sign in

Don't have an account yet? Register now

Stappen

1. Check email adres in formulier: is dit wel een gebruiker van ons?
2. Zo ja, start “stuur wachtwoord reset procedure”

3. Wachtwoord reset procedure maakt een link voor een nieuw wachtwoord
4. Kijkt in het formulier waar die link heen gestuurd moet worden
5. Verstuurt

GitLab Community Edition

Username or email

bert@hubertnet.nl

Nog een keer!

Username or email

Enge-Hacker@example.com

Password

Remember me

Forgot your password?

Click!

Sign in

Don't have an account yet? Register now

Stappen

Van boven naar beneden

1. Check email adres in formulier: is dit wel een gebruiker van ons?
2. Zo ja, start “stuur wachtwoord reset procedure”

3. Wachtwoord reset procedure maakt een link voor een nieuw wachtwoord
4. Kijkt in het formulier waar die link heen gestuurd moet worden
5. Verstuurt

Van beneden naar boven!

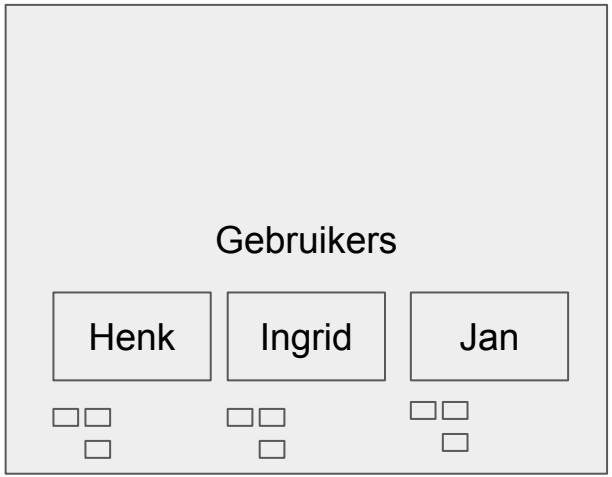
```
GET /api/v1/totp/user-backup-code/../../license/keys-status/<url_encoded_python_reverse_shell>
HTTP/1.1 Host: <IP_Vulnerable_Ivanti_Product>
```

V:\Gebruikers\Henk\rapport.docx

Ivanti Workspace Control 2022.3

Composer (10.10.0.0)

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



ivanti

Patents | ivanti.com

V:\Gebruikers\Henk\..\Ingrid\geheim.docx

Nieuws

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'

274 12 345 678

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.

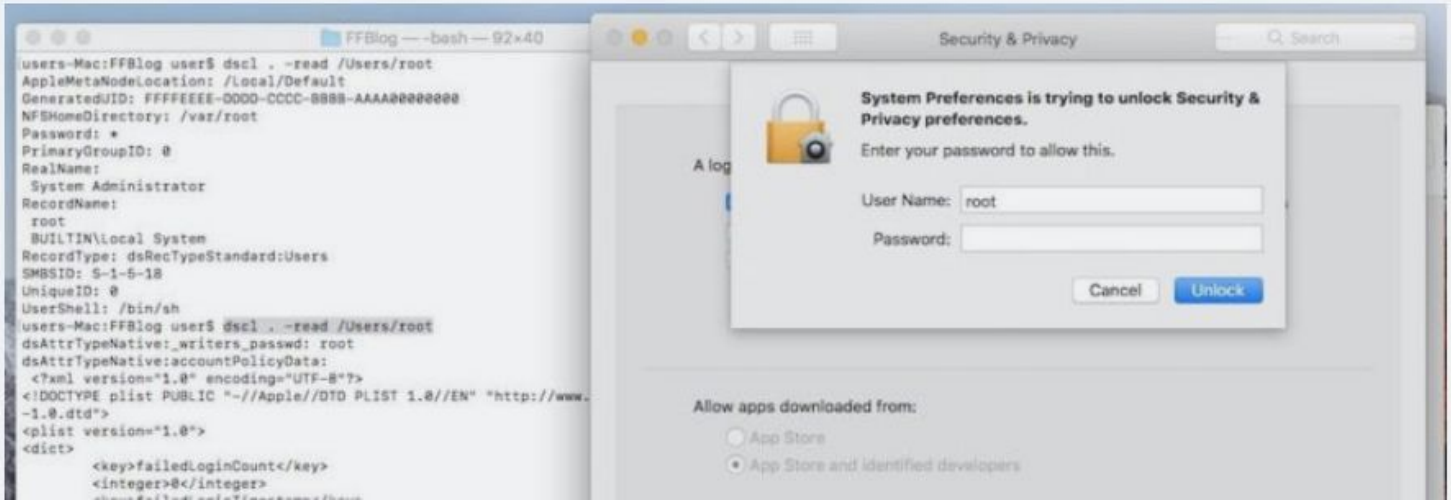
Voor vergaderingen op afstand gebruiken veel Nederlandse overheidsorganisaties het programma Webex, van de Amerikaanse techgigant Cisco. Het programma zou veiliger zijn dan andere populaire videobel-programma's als Zoom en Microsoft Teams. Toch lukte het Eva Wolfanger, techjournalist bij Die Zeit, maandenlang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

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

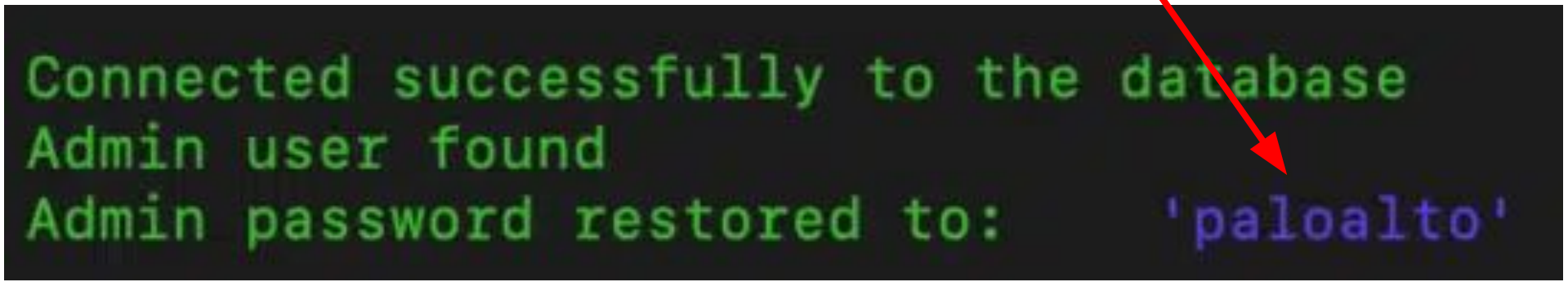


Palo Alto Networks: Leader in Cybersecurity Protection

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'
```

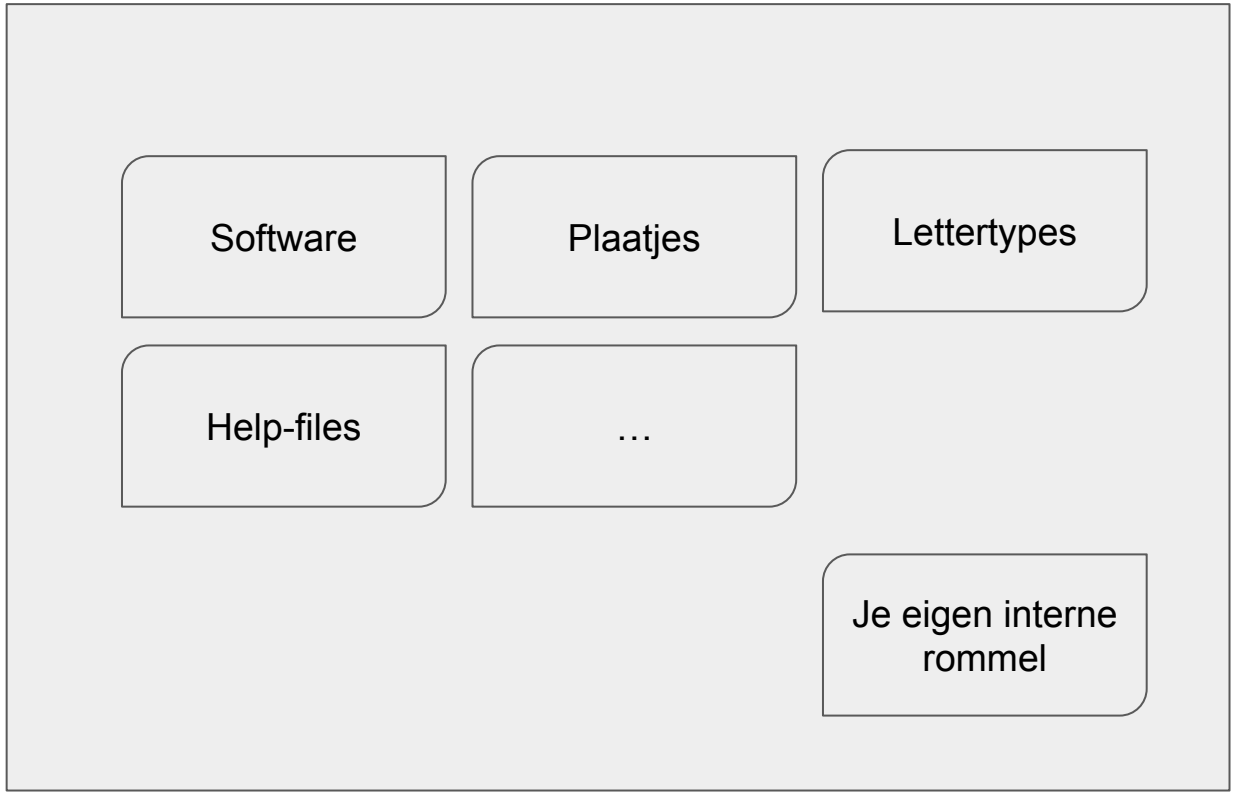


Beveiligingsrisico's OSV naar aanleiding van melding opgelost

Nieuwsbericht | 12-09-2023 | 15:30

Eind juni ontving de Kiesraad de melding dat er meerdere kwetsbaarheden zijn gevonden in de module Politieke Partijen van de Ondersteunende Software Verkiezingen (OSV2020). Deze melding werd gedaan door onafhankelijk beveiligingsexpert Maarten Boone van Zerocopter. De geconstateerde risico's zijn inmiddels door de leverancier opgelost.

Installatiepakket



De kwetsbaarheden zijn ontdekt in de installer, de software waarmee de software wordt geïnstalleerd op computers. In de installer zijn inloggegevens gevonden van de leverancier. Ook was in de installer het pad te vinden naar de private sleutel op het interne netwerk van de leverancier plus de gebruikersnaam en het wachtwoord hiervan. Deze gevonden kwetsbaarheden samen leveren een risico op voor de integriteit van de software. De kwetsbaarheden zijn verholpen voordat politieke partijen de software konden downloaden ten behoeve van de Tweede Kamer verkiezingen op 22 november.

Het is niet te doen!
Maar we geven de gebruikers de schuld

NIEUWS

De zwakste schakel binnen cybersecurity is nog steeds de mens

27 oktober 2023

In 2003 werd oktober uitgeroepen tot de Cybersecurity Awareness Maand. Inmiddels zijn we twintig jaar verder maar deze bewustwording blijft nodig. Technieken blijven innoveren, aanvallen worden strategischer en bedrijven zijn nog steeds kwetsbaar. Neem daarom de tijd om stil te staan bij dit onderwerp en stel jezelf de volgende vraag: zijn alle aspecten van cybersecurity binnen mijn bedrijf eigenlijk wel op orde?

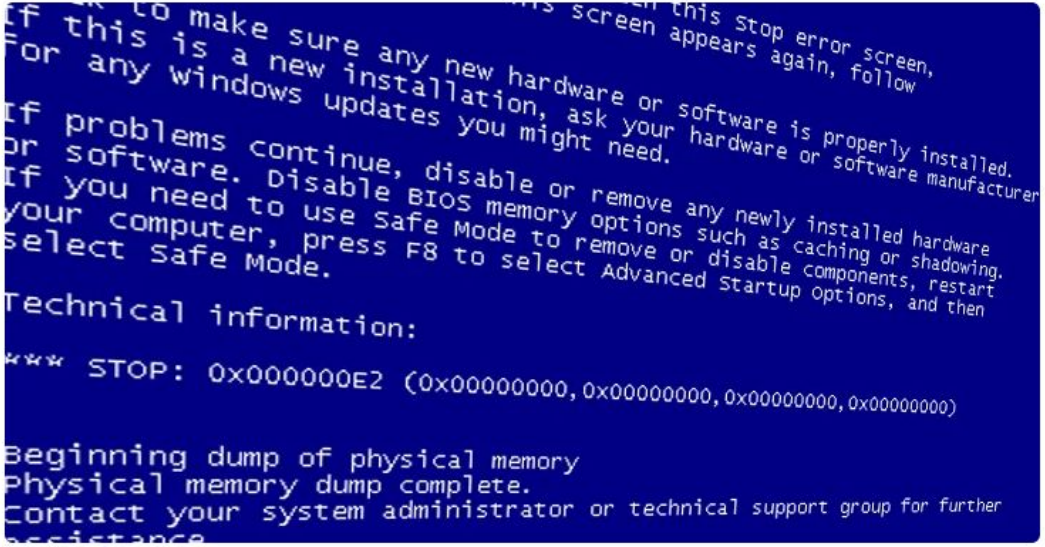
"Unfortunately we have fallen prey to the myth of techno exceptionalism. **We don't have a cyber security problem – we have a software quality problem**. We don't need more security products – **we need more secure products**."

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

Naar de cloud dan maar?

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

Sep 07, 2023 Newsroom Cyber Attack / Email Hacking



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

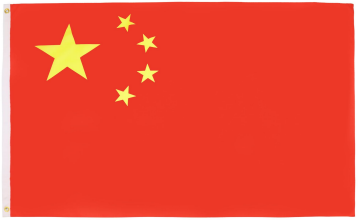
Microsoft faulted for ‘cascade’ of failures in Chinese hack

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

10 min 240

A woman walks by the Microsoft office building in Beijing on July 20, 2021. (Andy Wong/AP)

After years of touting the strength of its cybersecurity, Microsoft — the world's most valuable company — has been beset by recent embarrassing breaches. In early 2021, Chinese government-sponsored hackers compromised Microsoft Exchange email servers, putting at risk at least 30,000 public and private entities in the United States along with at least 200,000 worldwide.



In January, Microsoft detected an attack on its corporate email systems by the Russian foreign spy service, the SVR. The company said the spies broke into a testing unit, moving somehow from there into emails of senior executives and security personnel. Microsoft alerted its customer Hewlett-Packard Enterprise that it had been hacked as part of that campaign, and U.S. officials told The Post last month that there were dozens of other victims, including Microsoft resellers.

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.'

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.

Cybersecurity is echt rampzalig. En als je het oursourcet is het ergens anders rampzalig, alleen zie je het miner

Confidentiality
Integrity
Availability

Vertrouwelijkheid, klopt het nog, beshikbaarheid

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

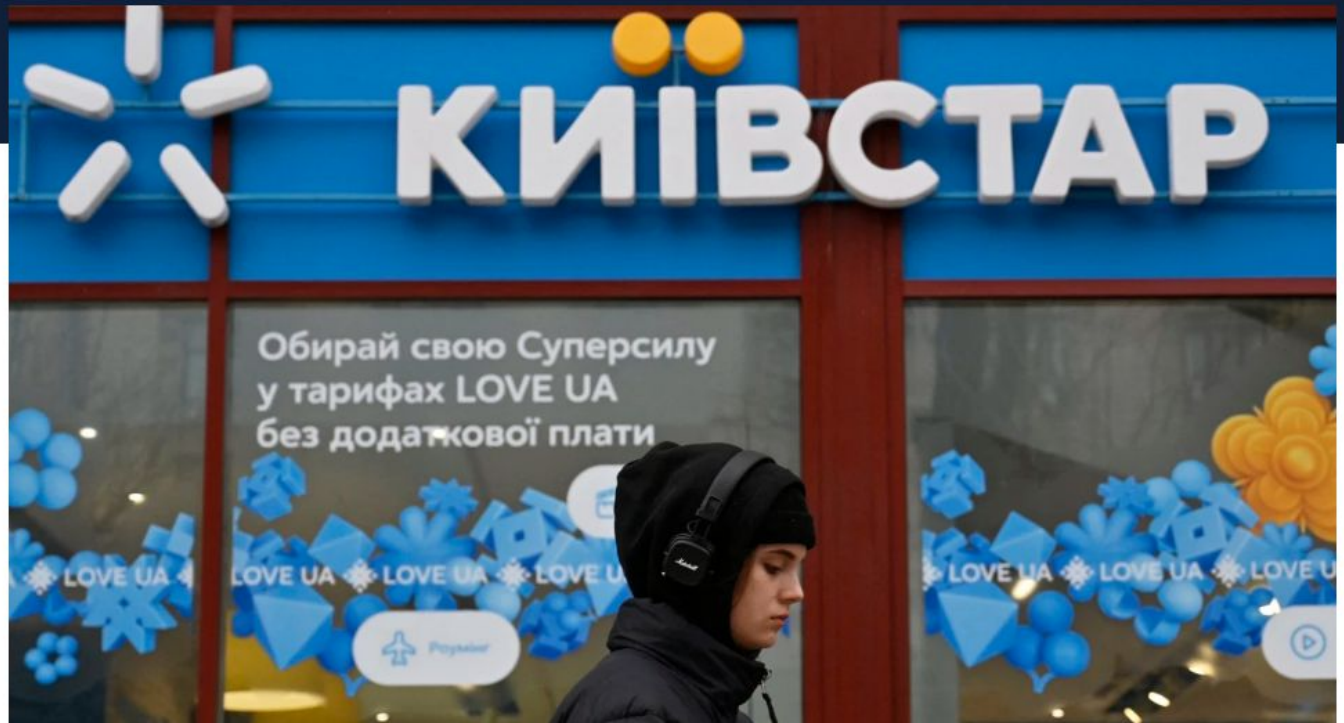
EPA's help desk is available 24/7 and responds to water cyber inquiries within two days. The help desk provides guidance to help prevent, detect, respond to and recover from cyber incidents.

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

OT: Operationele Technologie

- Pacemaker, hartbewaking, beademingsapparatuur, raffinaderijen, luchtverkeersleiding, gemalen, afsluitdijken, bruggen, verkeerslichten, zelfrijdende auto’s, electriciteitscentrales, kerncentrales, LNG terminals, oliepijpleidingen, kaasbedrijven
  - We hebben er allemaal wel een gevoel bij: als dit gehacked wordt zijn we de sigaar
- Industriële systemen leefden vroeger totaal gescheiden van normale IT:
  - Loonstrookjes, printers, de website, email, agendasystemen, spelletjes
- Voor OT golden echt andere regels. Gescheiden netwerken, grotere en zwaardere apparatuur (stoplichtkast als voorbeeld), dikkere kabels, drie lagen beveiliging
- Die scheiding is aan het verdwijnen & dat is bijna niet meer tegen te houden

Moet alles op internet?

Nederlandse communicatieinfrastructuur wordt grotendeels beheerd vanuit verre buitenlanden, waarvan de meeste geen bondgenoten zijn.

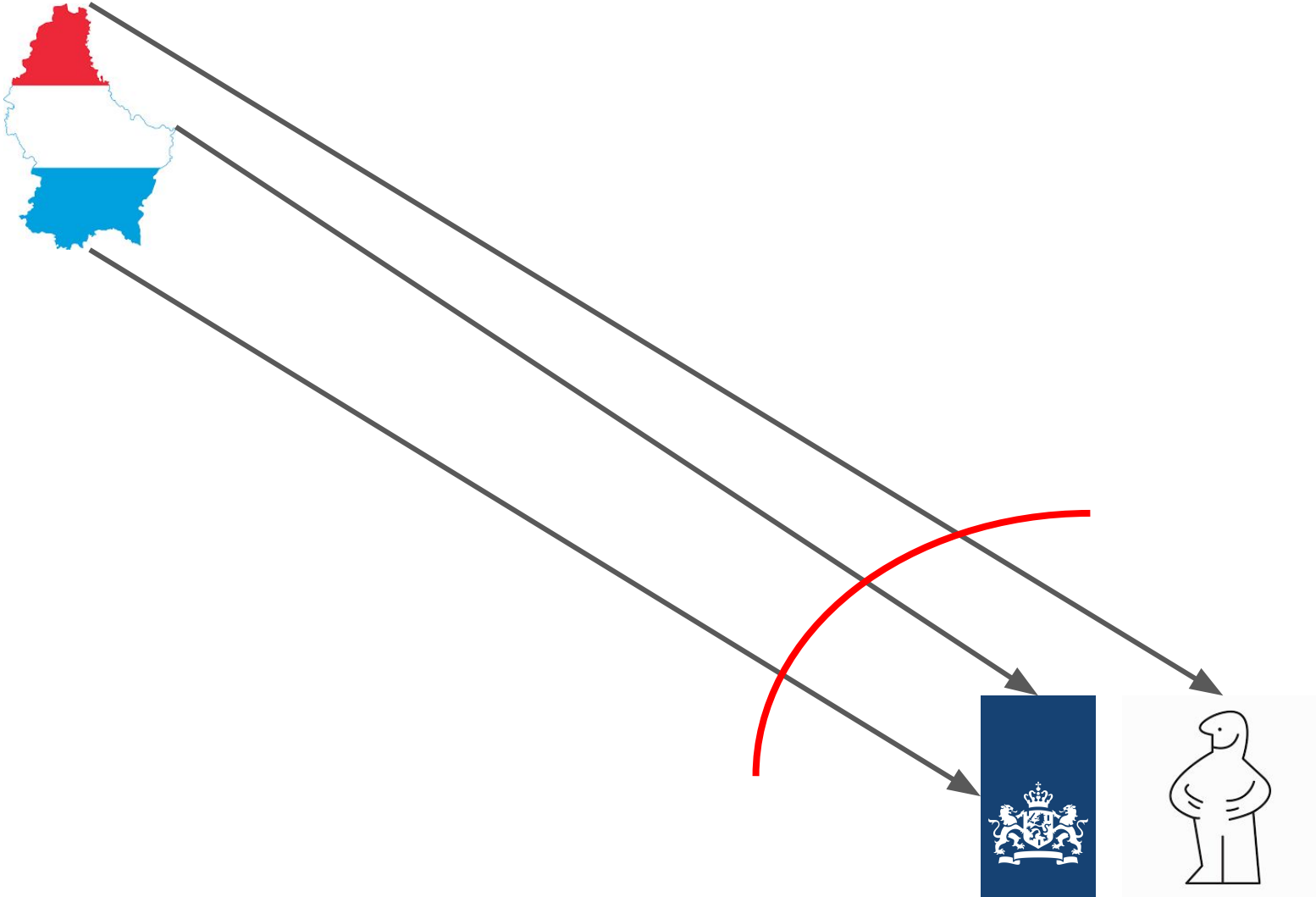
Hoe is het zover gekomen?

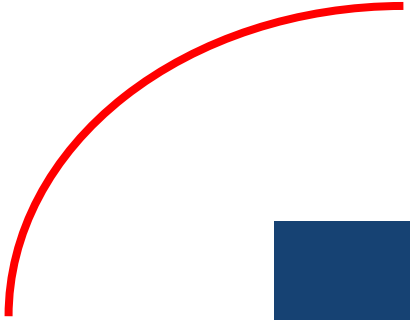
- Voor gevaarlijke stoffen, fabrieken, apparaten bestaan strenge vormen van regelgeving
  - Ontwikkeld over afgelopen **eeuwen**
  - Voor de Titanic kon iedereen een boot maken bijvoorbeeld
- **IT is sneller uitgerold dan we wisten hoe dat veilig moest**
  - En we weten het nu grotendeels nog niet
- Uit zichzelf staat veiligheid nooit bovenaan (niet zichtbaar, niet mee te scoren)
- Raden van bestuur zijn in Nederland bijzonder en in Europa algemeen vrijwel geheel ontdaan van technische kennis
- Moeilijke keuzes worden daarom liever uitbesteed of niet serieus genomen

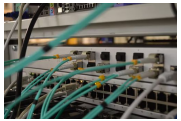
Wie ZIJN die hackers dan?

Actoren

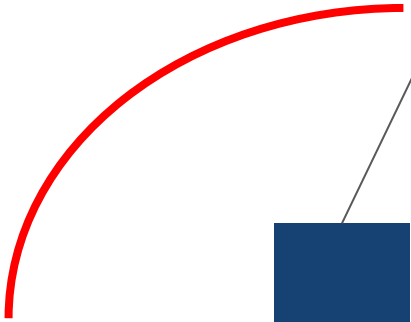
- Totaal wilde westen!
  - **Onderdruk de neiging het netjes in te willen delen**
- Het is een mix van:
  - Staatshackers (ambtenaren, militairen): zo doen wij het doorgaans
  - Bestaande criminele organisaties met ingehuurde hackers
  - Hackers die criminele organisaties worden
  - Hackercollectieven die getolereerd worden door hun land (“zolang je maar niet hier hackt, en af en toe iets op ons verzoek doet”)
  - Semi-staatsbedrijven die hacken in opdracht
  - Bedrijven die tooling en infrastructuur maken tbh bovenstaande groepen
- De grenzen tussen deze werelden zijn fluide
- Het is vaak wel mogelijk technisch aan elkaar gerelateerde aanvallen te groeperen in “APTs”
- Maar nogmaals: grote duidelijkheid is hier (bewust) niet te vinden
  - Desondanks wordt het veel geprobeerd








Synology



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.

Wat moeten we dan doen?

- Software die je niet draait wordt ook niet gehacked
  - Zet oude spullen uit
  - En als je iets nieuws doet, moet het echt online?
- **Hou op met merken/apparatuur die steeds in het nieuws is**
- Data die je niet hebt wordt ook niet gestolen
  - Verzamel het niet, hou het niet vast
- Partners die je niet hebt worden ook niet gehacked
  - Moet alles met iedereen gedeeld worden?
- **Blijvend succesvol:**
  - **Updaten updaten updaten**
  - **Geen “alleen wachtwoord nodig” meer**
  - **Monitoren, monitoren, monitoren**
- **Verwacht niet dat software of een apparaat je veilig houdt**

1. Hebben we backups?
2. Nee echt serieus, hebben we backups?
3. Laat eens zien dan?
4. Oh staan de backups op het normale systeem!

Samenvatting

- De toestand van cybersecurity is huilen
  - Maar we accepteren het
  - Zelfs de top van de top krijgt z’n spullen niet veilig
- Meer en meer *operationele* technologie gaat ook naar “gewone computers”
  - Die we daarna outsourcen
- Er zijn wetten aan de horizon die dit moeten verbeteren
  - Schoorvoetend…
  - We hebben betere software nodig!
- Best practices blijven werken

De enorm bedroevende toestand van cybersecurity

Bert Hubert
bert@hubertnet.nl