WELKOM

Lokale besturen in de digitale wolk
Slotsessie Cyberveilige Steden en Gemeenten

29 april 2022 – 10.00 uur

vvsg
Vereniging van
Vlaamse Steden
en Gemeenten

We zenden uit via **MS Teams**. Volg via:

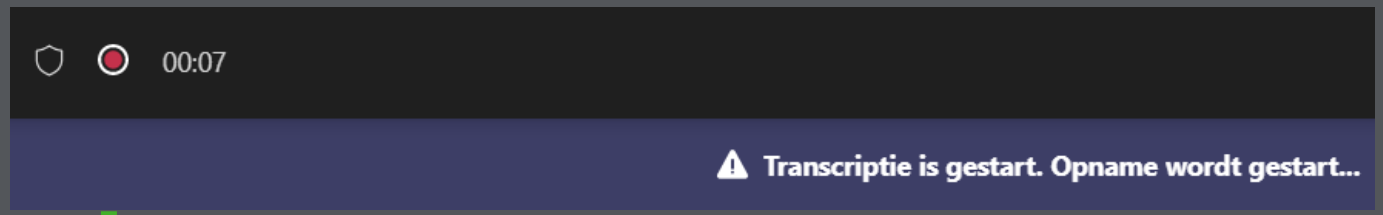
- Microsoft Teams App
- Browser (Chrome, Firefox of Edge)

Technische problemen?

- Mail naar **joke.jacobs@vvsg.be**
- Of zet een berichtje in de chat.

Praktische afspraken

Stel je vraag via de chat



Deze bijeenkomst wordt opgenomen.
Naderhand bezorgen wij je via het evaluatieformulier de opnames.

Kennismaking

Jolien Schoonooghe
Projectmedewerker Cyberveilige Steden en Gemeenten

jolien.schoonooghe@vvsg.be

0477/78.28.73

Kennismaking

- Voor deze slotsessie hebben er zich 179 personen ingeschreven, waaronder profielen zoals DPO’s, diensthoofden, projectcoördinatoren, preventieadviseurs en IT-medewerkers.

- Deze slotsessie is hoofdzakelijk bestemd voor lokale besturen in Vlaanderen.

Agenda

1. Inleiding en welkom
Gebracht door Jolien Schoonooghe, projectmedewerker Cyberveilige Steden Gemeenten - VVSG

2. Het belang van het Traject Ethisch Hacken
Gebracht door Jolien Schoonooghe, projectmedewerker Cyberveilige Steden en Gemeenten – VVSG

3. Inleiding 'Lokale besturen in de cloud'
Gebracht door Ward Van Hal, Stafmedewerker Innovatie en Digitale Transformatie - VVSG

4. 'Het lokaal bestuur in de cloud'
Gebracht door Eddy Willems, cybersecurity expert – G Data Cyberdefense

5. Pauze

6. Vragenronde 'Het lokaal bestuur in de cloud'

7. Vooruitblik op het verdere project
Gebracht door Jolien Schoonooghe, projectmedewerker Cyberveilige Steden en Gemeenten – VVSG

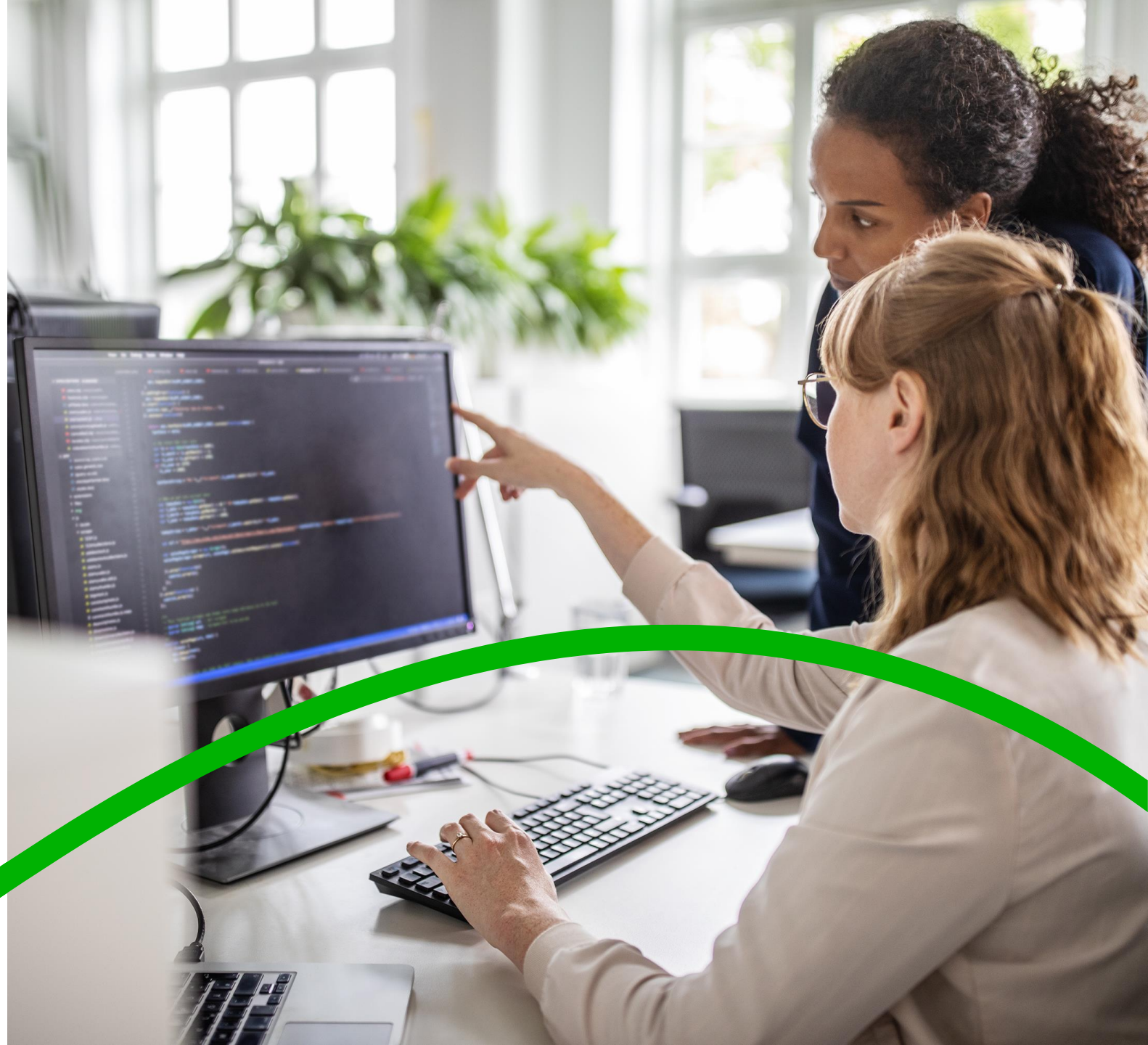
8. Afsluiting
Bart Somers, Minister van Binnenlands Bestuur
Jolien Schoonooghe, projectmedewerker Cyberveilige Steden en Gemeenten - VVSG

Cyberveilige Steden en Gemeenten

Het belang van Het Traject Ethisch Hacken

Jolien Schoonooghe
Projectmedewerker Cyberveilige Steden en Gemeenten - VVSG

vvsg



Project Cyberveilige Steden en Gemeenten

Naar aanleiding van de cyberaanval in Willebroek besloot de Vlaamse Overheid om 2,18 miljoen euro te investeren in de cyberveiligheid van lokale besturen op voorstel van **minister Bart Somers.**

Samen met het **Agentschap Binnenlands Bestuur**, **Audit Vlaanderen**, het **Facilitair Bedrijf** en **VVSG** werd een aanbod uitgewerkt voor lokale besturen:

Luik 1: De ontwikkeling van een Toolkit Cybersecurity

Luik 2 : Een Traject Ethisch Hacken in samenwerking met Howest, waarbij het mogelijk is om dit te combineren met ICT-veiligheidsaudits met co- financiering via Audit Vlaanderen

Luik 3: Bewustmaking en kennisdeling a.d.h.v. interactieve webinars en inspiratiesessies

Luik 1: De ontwikkeling van een Toolkit Cybersecurity

- In 2021 werkte VVSG samen met een taskforce van lokale besturen en externe professionals aan sjablonen, checklists en plannen voor steden en gemeenten.
- Hierbij werden er 12 tools ontwikkeld:
  - **Draaiboek Cybercrime**
  - **Sjablonen**
    - Business continuïteitsplan
    - Crisiscommunicatieplan
    - Checklist crisisbeheer
    - Beleid voor responsible disclosure
    - Register voor cyberincidenten
    - Procedure melding cyberincidenten
    - Interne en externe contactlijsten
    - Veiligheids- en opvolgingsplan
  - **Richtlijnen**
    - Richtlijnen Secure Software Development
    - Richtlijnen organisatiebeheersing
  - **Cybertips en –tricks**

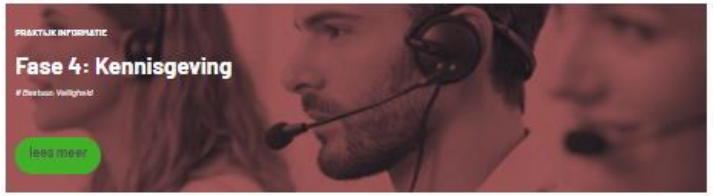
➢ Een cyberveiligheidskaart
➢ Overzicht aan inspiratie en leesvoer a.d.h.v. interessante bronnen i.v.m. cyberveiligheid

Draaiboek Cybercrime

- Het **bestrijden van cyberveiligheidsincidenten** is jammer genoeg geen rechtlijnig proces, maar een complexe oefening waarbij diverse acties door elkaar lopen, gaande van het detecteren van een incident tot het inperken van schade, het herstellen van de dienstverlening, het melden aan de bevoegde instanties en de slotbeschouwing. Er is een belangrijke rol weggelegd voor de ICT, maar eveneens voor interne en externe communicatie en organisatiebeheersing.

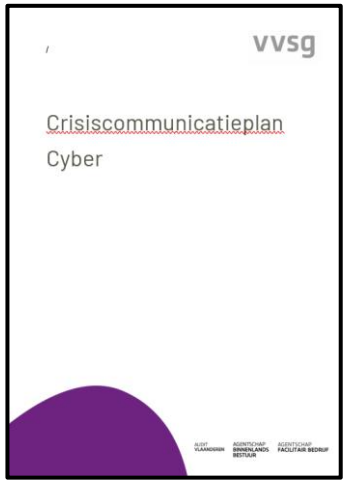
- Het opstellen van **een draaiboek op maat van je lokaal bestuur** is een stuk eenvoudiger indien reeds bepaalde plannen en leidraden voorhanden zijn.

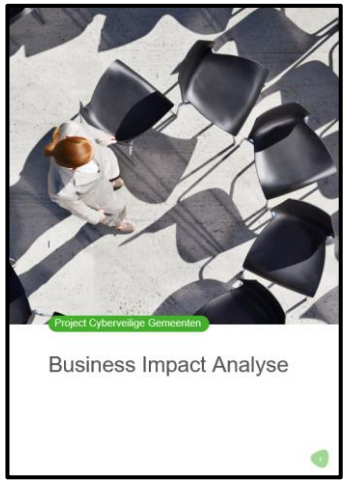
- We omschrijven de verschillende acties en keuzes die aan bod kunnen of zullen komen tijdens het bestrijden van een cyberveiligheidsincident, **aan de hand van 5 fases.** Hou hierbij in het achterhoofd dat sommige acties deze fases kunnen overstijgen, en dat elk incident een aanpak op maat vereist, met specifieke noden en oplossingen.



Sjablonen

- In het kader van het Project Cyberveilige Gemeenten werden talrijke sjablonen ontwikkeld op maat van lokale besturen:
  - Een business continuïteitsplan
  - Een crisiscommunicatieplan
  - Een checklist crisisbeheer
  - Een beleid voor responsible disclosure
  - Een register voor cyberincidenten
  - Een procedure melding cyberincidenten
  - Een interne en externe contactlijsten
  - Een veiligheids- en opvolgingsplan





Richtlijnen

- Richtlijnen Secure Software Development
- Richtlijnen organisatiebeheersing

Richtlijnen Secure Software Development

Richtlijnen organisatiebeheersing

Cybertips en -tricks

- We bundelden enkele interessante tips en lokale praktijken om cyberveiligheid in te bedden in de werking, cultuur en processen van steden en gemeenten.
    - Heeft jouw lokaal bestuur een inspirerende praktijkcase? Aarzel niet om contact op te nemen.

Kies voor een structurele aanpak met periodieke opvolging: Stad Geel

Sensibiliseringsmateriaal

- Cyberveiligheid is in sterke mate afhankelijk van gedrag. Het bewustzijn van medewerkers, mandatarissen, software- en IT-dienstenleveranciers rond informatiebeveiligingsrisico's is cruciaal en moet dus levend gehouden worden via structurele inbedding en periodieke controles op de naleving van gemaakte afspraken.

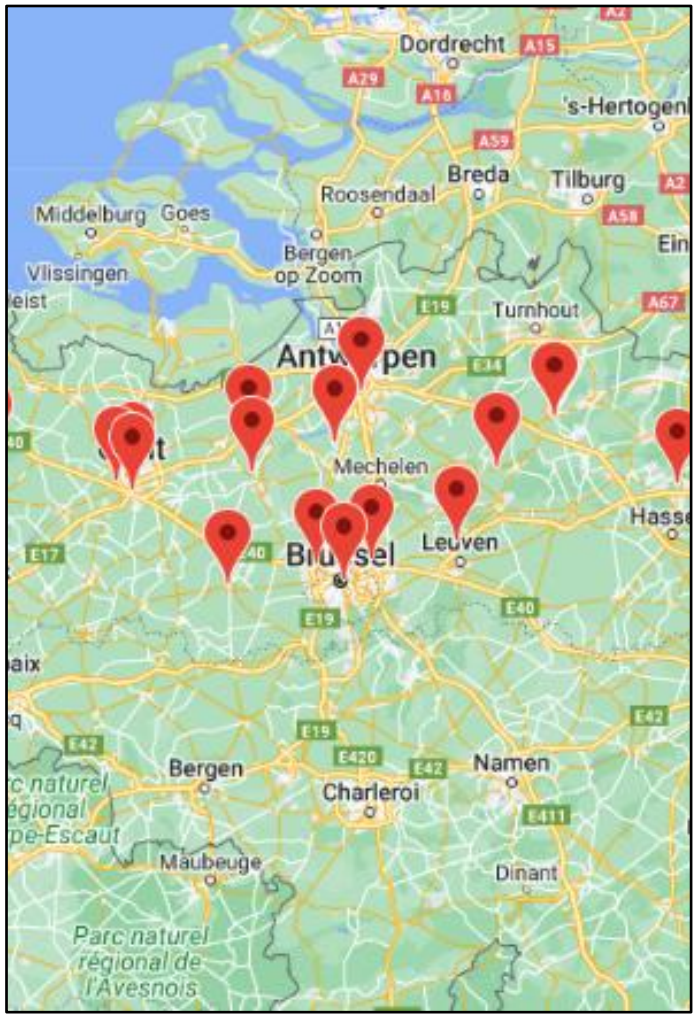
- Gelukkig is er al heel wat sensibiliseringsmateriaal voorhanden waarvan je gebruik kan maken als lokaal bestuur om je aanpak scherp te stellen:

  - Video's
  - Posters
  - Interessante bronnen:
    - Webinars over cyberveiligheid
    - Cyber Security KIT
    - E-learning modules
    - Safe on web testen
      - Campagnemateriaal Safe on Web
    - Bestaande campagnes vanuit De Vlaamse Overheid

Cyberveiligheidskaart

- Op zoek naar producten of diensten om de cyberveiligheid van je lokaal bestuur te verhogen?
  - De cyberveiligheidskaart wijst je de weg naar organisaties en bedrijven met een interessant aanbod op maat van lokale besturen.

Organisaties, bedrijven of kennisinstellingen met een interessant aanbod, kunnen een plaats op de kaart aanvragen via het online formulier



Luik 2: Een Traject Ethisch Hacken in samenwerking met Howest

- Ethische hackers van de Hogeschool West-Vlaanderen (HOWEST) nemen in kader van hun opleiding de lokale IT-omgeving kosteloos onder de loep gedurende minimaal 3 testdagen en formuleren aanbevelingen om de gevonden werkpunten aan te pakken.

- Een leerrijke werkervaring voor de studenten en een waardevolle bron van informatie voor de lokale besturen.

- Sinds 2020 lieten reeds **104 lokale besturen** hun ICT-omgeving doorlichten door ethische hackers van Howest.

Testen binnen het traject 1/2

Een Open-Source Intelligence test

- Waarbij informatie uit publieke bronnen wordt ingewonnen die het werk van hackers kan vergemakkelijken. Het kan hierbij onder andere gaan over gelekte inloggegevens en informatie over de netwerkstructuur of hosting van websites.

Een interne blackbox pentest

- Waarbij de studenten zich aansluiten op het interne netwerk om kwetsbaarheden op te sporen in de systemen, netwerken, applicaties of webplatformen, zonder enige voorkennis.

Een externe blackbox pentest

- Waarbij de studenten zoeken naar kwetsbaarheden in de systemen zonder zich te verbinden met het interne netwerk.

Testen binnen het traject 2/2

Een gestructureerd interview met de functionaris gegevensbescherming (DPO) of verantwoordelijke informatiebeveiliging (CISO)

- Op basis van een door Howest opgestelde vragenlijst, om inzicht te krijgen in de beveiligingsmaatregelen die het lokaal bestuur inzet.

Een vragenlijst naar lokale medewerkers

- De vragenlijst werd opgesteld door de Howest-lectoren en verspreid naar de lokale medewerkers door de studenten. De vragenlijst peilt naar het bewustzijn van ICT-veiligheidsrisico's, de aanwezige sensibilisering binnen het lokaal bestuur en de mate waarin de medewerkers goede praktijken toepassen.

Een social engineering campagne (Optioneel)

- Waarbij studenten kijken hoe medewerkers reageren op een phishingmail, impersonatie (waarbij de studenten onder een alias toegang proberen krijgen tot netwerken en systemen) of een USB-drop (waarbij gekeken wordt hoeveel medewerkers een USB die mogelijk malware bevat aansluiten).

Nuttige linken i.v.m. het Traject Ethisch Hacken

- Over het traject
- Ervaringen van deelnemers Traject Ethisch Hacken
  - https://vimeo.com/660682671 (Stad Leuven)
  - https://vimeo.com/660681993 (Stad Geel)
- Globaal analyserapport 2020
- ICT-veiligheidsaudits met cofinanciering

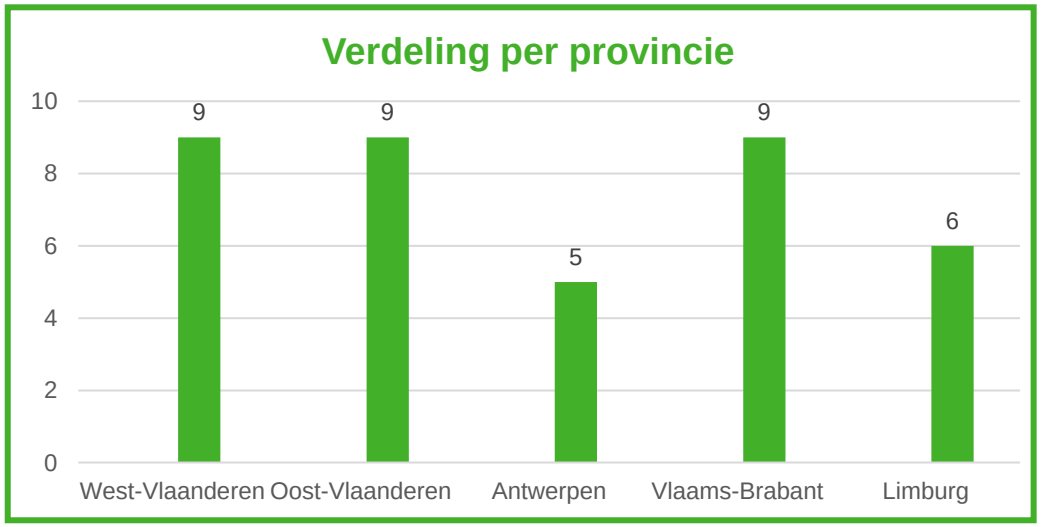
Luik 3: Bewustmaking en kennisdeling a.d.h.v. interactieve webinars en inspiratiesessies

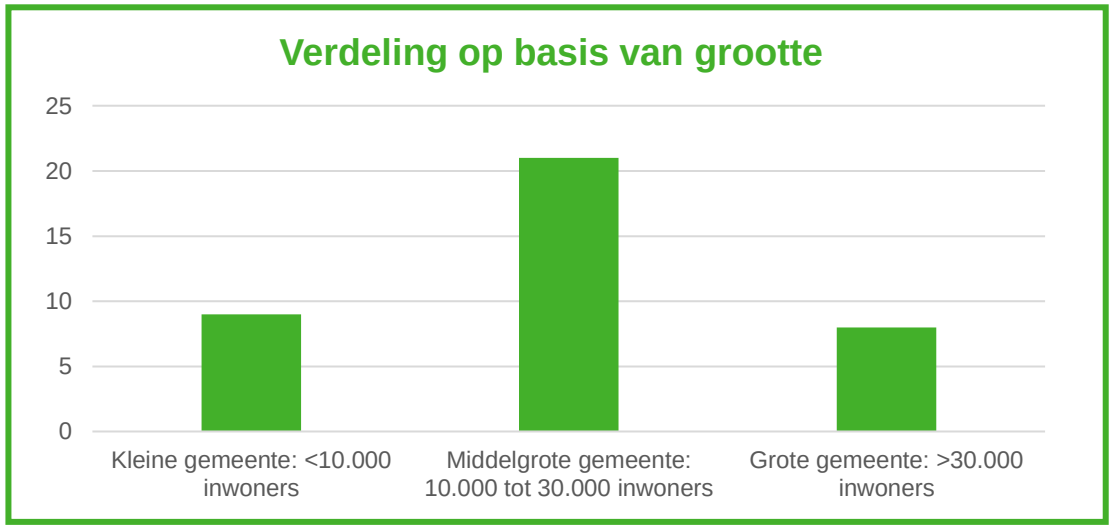
- Inspiratiesessie: ‘Sterke praktijken rond cyberveiligheid’
- Webinar ‘We worden gehackt, wat nu?’
- Presentatie ‘Cyberveiligheid, zoveel meer dan IT’
- Webinar ‘De Cyber Arena, cyberveiligheid voor niet-IT personeel’

➢ Te (her)bekijken op de projectpagina

Het Traject Ethisch Hacken 2021

- In **2021** kregen **38 steden en gemeenten** ethische hackers van de Howest-hogeschool over de vloer, die in kader van hun opleiding de lokale IT-systemen en toepassingen onder de loep namen en aanbevelingen formuleerden.





Het Traject Ethisch Hacken 2021

Het up-to-date houden van systemen en toepassingen is een belangrijke bouwsteen voor een cyberveilige organisatie.

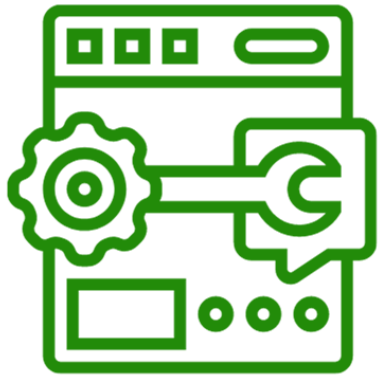
Gebruik geen verouderde systemen en toepassingen die niet meer ondersteund worden

Gebruik een geformaliseerd patchingproces voor infrastructuur

Werk een inventarisatie uit voor IT-gerelateerde objecten

Het vergeten aanpassen van **standaardinstellingen en wachtwoorden** maakt het eenvoudiger voor hackers om toegang te verkrijgen tot persoonlijke en/of gevoelige informatie.

Gebruik geen login of automatische login



Geef de standaard- of ontbrekende wachtwoorden geen toegang tot administrator-accountsmet hoge privileges.

Hernieuw regelmatig wachtwoorden

Het Traject Ethisch Hacken 2021

Het is aangewezen om **toegangs- en gebruiksrechten voor gebruikers** te beperkten tot het strikt noodzakelijke.

Geef geen te ruime toegang- en gebruikersrechten aan interne gebruikers

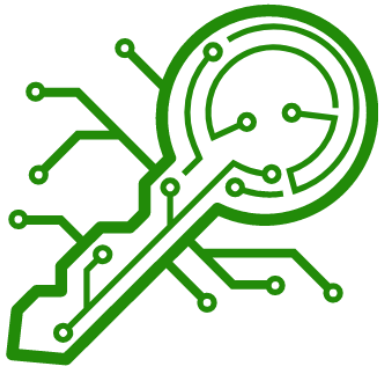
Maak gebruik van een identity and access management systeem

Pas een tweestapsverificatie of 2FA toe

Het Traject Ethisch Hacken 2021

Het is belangrijk om in te zetten op **manuele of automatische filtering** van de nodige sensibilisering rond **phishing.**

Vermijd het bestaan van communicatieprotocollen die onvoldoende of niet geëncrypteerd zijn



Zorg ervoor dat gevoelige informatie opslagen wordt met de nodige encryptie

Tracht zoveel mogelijk netwerken op te delen in segmenten

Traject Ethisch Hacken 2021

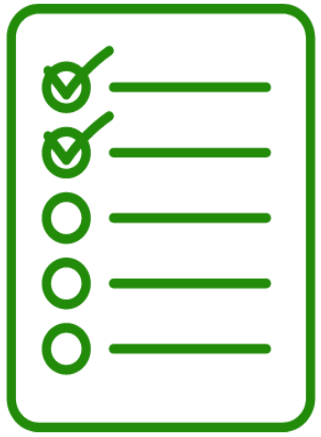
Het **gedrag van medewerkers** is een belangrijke bouwsteen om netwerken, systemen en applicaties veilig te houden.

Probeer medewerkers bewust te maken om goede praktijken rond cyberveiligheid te gebruiken

Zorg dat jouw lokaal bestuur bewustmaking rond cyberveiligheid voorziet rond voor haar medewerkers

Traject Ethisch Hacken 2021

Na een cyberaanval en/of ter preventie, is het cruciaal om de **nodige continuïteitsmaatregelen** te treffen om de dienstverlening en de werking operationeel te houden.



Zorg voor de opmaak van een plan dat helpt bij het herstel van de dienstverlening

Zorg voor de aanwezigheid van een back-up en herstelplan

Voorzie een goede back-up en herstelstrategie

Traject Ethisch Hacken 2022

- In het najaar van 2022 zal een herhaling van het traject ethisch hacken plaatsvinden. Indien jouw lokaal bestuur hier graag deel van wil uitmaken, kan je dit reeds melden via **cyberveiligheid@vvsg.be**

- Het vervolgtraject zal formeel aangekondigd worden via de VVSG-kanalen.

- Lokale besturen kunnen opnieuw via cofinanciering beroep doen op professionele ICT-veiligheidsaudits, gecoördineerd door Audit Vlaanderen.

  ➢ De audit kan gecombineerd worden met Het Traject Ethisch Hacken.

Vereniging van
Vlaamse Steden
en Gemeenten

Inleiding ‘Lokale besturen in de cloud’

Ward Van Hal, Stafmedewerker Innovatie en Digitale Transformatie - VVSG

Opstart denktank

- Binnen het project cyberveilige gemeenten richt de VVSG **een denktank op rond lokale cyberuitdagingen**.
  - Met deze denktank willen we tegemoetkomen aan de vraag bij de lokale besturen om in te zetten op kennisopbouw en visieontwikkeling rond relevante thema’s binnen het domein van cyberveiligheid.

- De thema’s die behandeld worden in de strategische denksessies, zijn afhankelijk van lokale noden en vraagstukken die aan bod komen binnen het bestaande netwerk. De denktank kent een wisselende samenstelling, afhankelijk van het vraagstuk dat voorligt.

- Het **eerste thema** dat de denktank zal behandelen gaat over **de transitie naar de cloud**.
  - Zijn de besturen die in de cloud werken beter gewapend tegen mogelijk IT-veiligheidsproblemen? Wat zijn de do's en de dont's bij deze transitie en hoe verhoudt deze transitie zich ten opzichte van het privacy-aspect?

- De oproep i.v.m. de opstart denktank rond cyberuitdagingen op de projectpagina.
- De oproep i.v.m. de opstart denktank rond cyberuitdagingen wordt ook nog verspreid via de VVSG-kanalen.

vvsg

Vereniging van
Vlaamse Steden
en Gemeenten

‘Lokaal bestuur in de cloud’

Eddy Willems

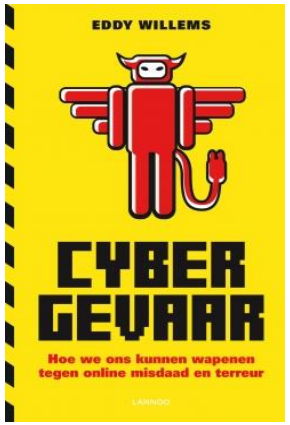
vvsg

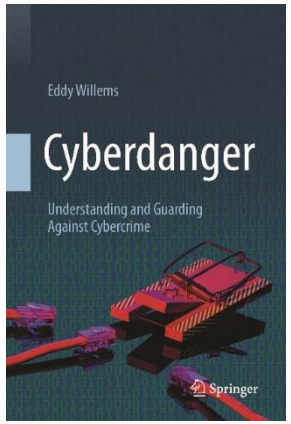
GDATA

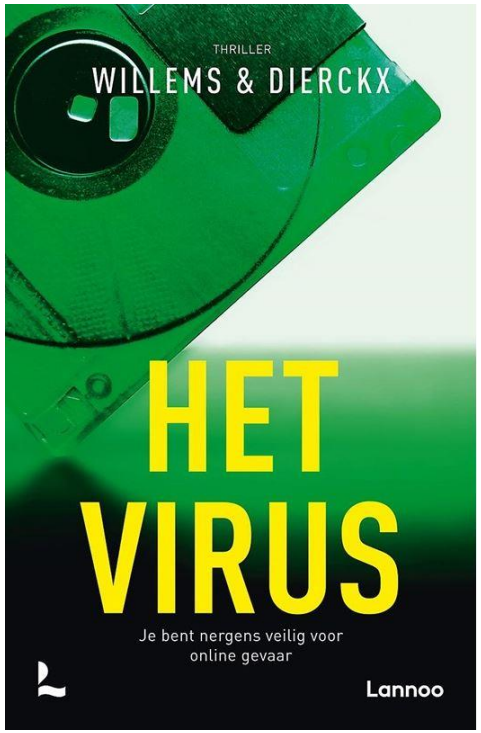
CYBERGEVAREN 2022 EN DE CLOUD

EDDY WILLEMS
SECURITY EVANGELIST
G DATA CYBERDEFENSE AG
TWITTER: @EDDYWILLEMS

WIE BEN IK







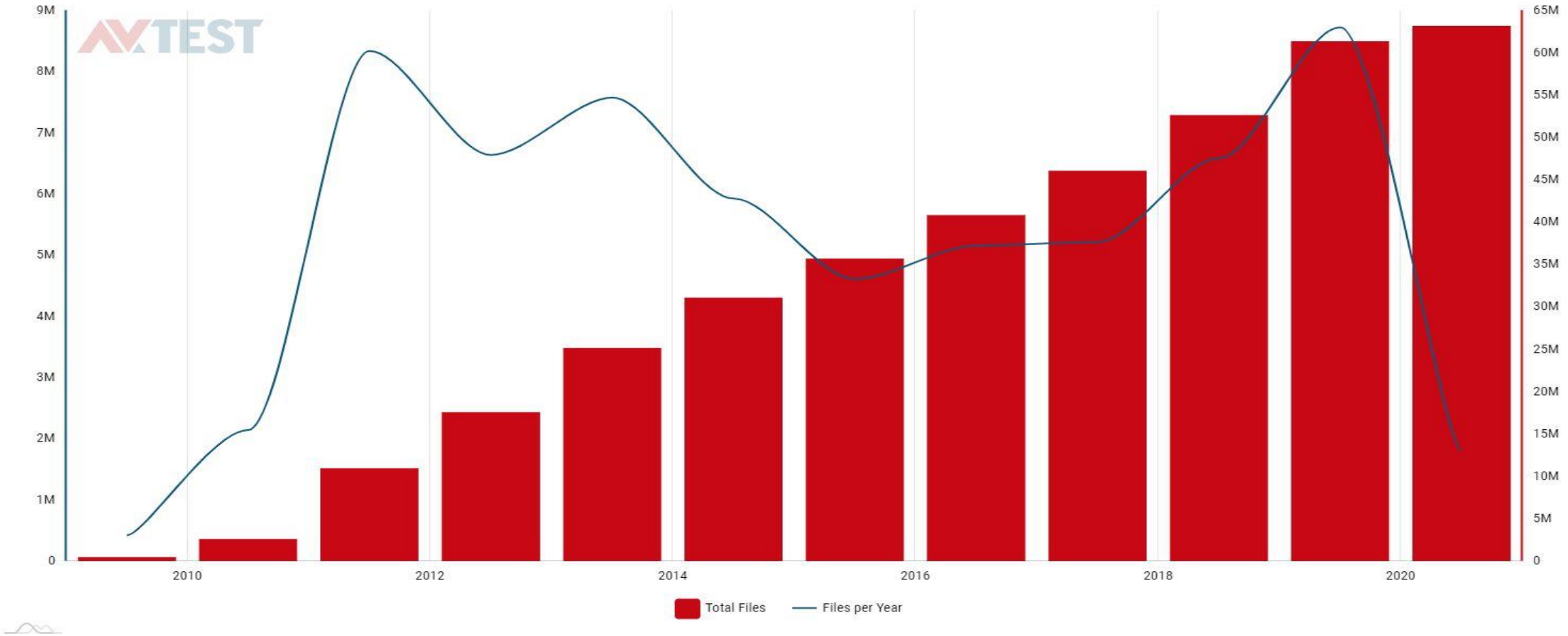
- **Security Evangelist** bij **G DATA CyberDefense AG**
- In de security industrie sinds 1989
- Vroeger: **Cyber Security Expert** bij CERT-org. en security bedrijven zoals Kaspersky, Westcon(NOXS), ..
- **Director** van **EICAR**(Co-founder)**, AVAR** en **LSEC**
- **Researcher/Technical Spokesperson** citaten in duizenden publicaties en media
- **Auteur** van Cybergevaar, Cybergefahr , Cyberdanger , Het Virus
- **TEDx** spreker: A Tale of Two Floppies

WERELDWIJD G DATA SECURITY-OPLOSSINGEN

- Bochum (Duitsland) in 1985 – Uitvinder antivirus
- HQ en R&D: Bochum en (R)Filippijnen
- Security oplossingen en online cursussen voor consumenten en bedrijven
- Beschikbaar in 90+ landen
- 500+ werknemers

MEMORIES

HEDENDAAGSE BEDREIGINGEN



400.000 nieuwe samples per dag

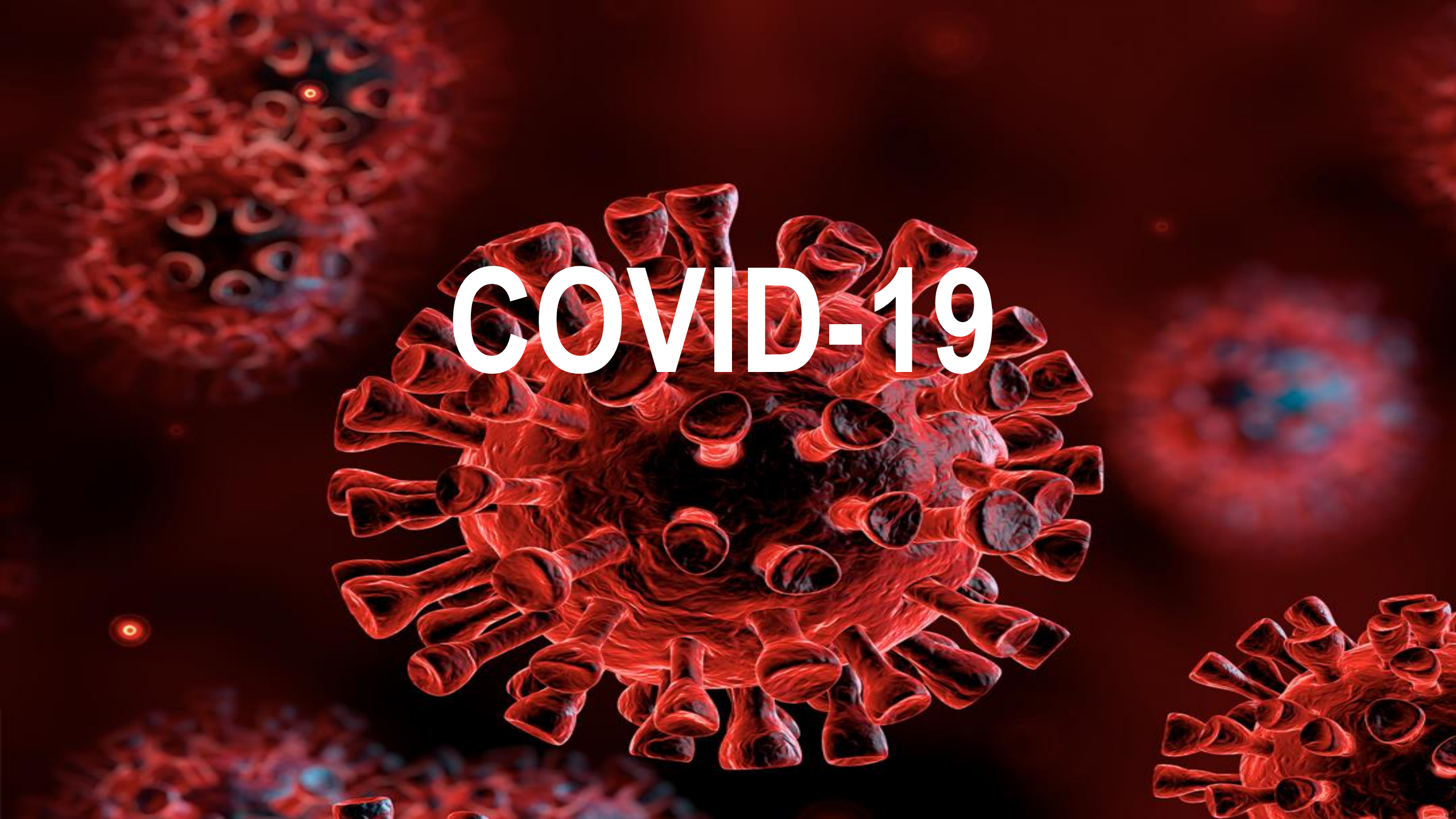
Ongeveer 900 miljoen malware samples => 99,9% onzichtbaar => GELD!

Gemeente Willebroek slachtoffer van cyberaanval met ransomware

25/01/2020 om 17:20 door msn

Burgemeester Eddy Bevers: 'Onze eerste prioriteit is het woonzorgcentrum, daarna bekijken we hoe de administratie kan heropstarten.' Foto: Joris Herregods

De gemeentelijke diensten van Willebroek zijn gehackt. De daders eisen losgeld in de vorm van bitcoins. De gemeente heeft een klacht ingediend bij de politie.


COVID-19

RANSOMWARE WAPENSTILSTAND?

Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

Go to home

RANSOMWARE AAANVAL TIJDENS CORONA

Snake ransomware leaks patient data from Fresenius Medical Care

By Ionut Ilascu

May 20, 2020 02:36 PM 0

Medical data and personally identifiable information belonging to patients at a Fresenius Medical Care unit are currently available online on a paste website.

Fresenius is a large private hospital operator in Europe and its systems were compromised as part of a massive campaign from Snake ransomware that targeted organizations across all verticals.

RANSOMWARE AANVAL TIJDENS CORONA

Cognizant

Industries Services Latest Thinking About

PRESS RELEASES CONTACT

Search Newsroom

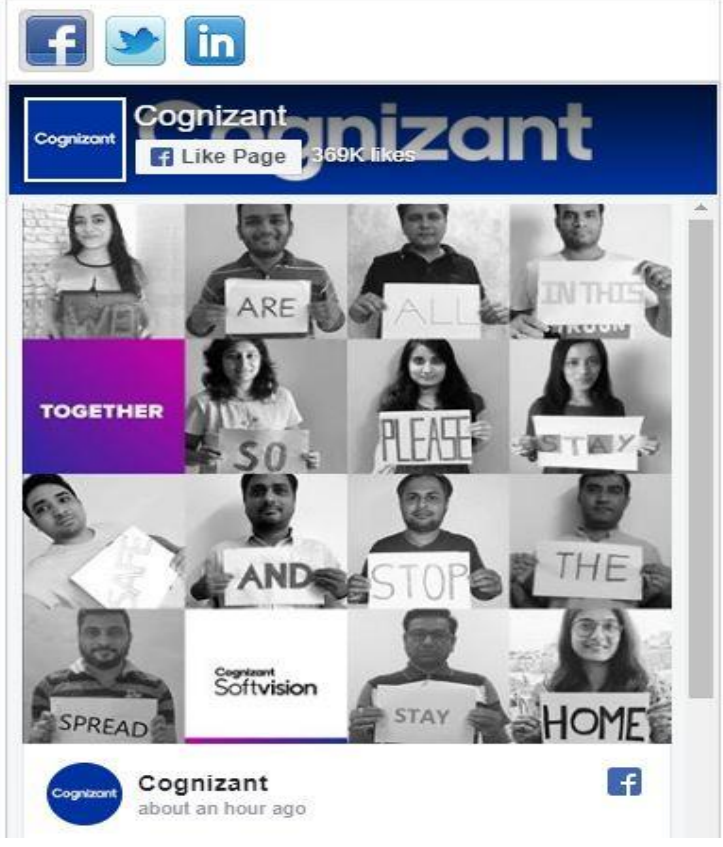
Cognizant Security Incident Update

April 18, 2020

Cognizant can confirm that a security incident involving our internal systems, and causing service disruptions for some of our clients, is the result of a Maze ransomware attack.

Our internal security teams, supplemented by leading cyber defense firms, are actively taking steps to contain this incident. Cognizant has also engaged with the appropriate law enforcement authorities.

We are in ongoing communication with our clients and have provided them with Indicators of Compromise (IOCs) and other technical information of a defensive nature.




Marktleider digitaal onderwijs wil van zijn laptops af


De QR-fauteuil van streetartkunsternaar Pantone


Nyrstar boekt negende verliesjaar op rij


Zelensky wil Kremlingezinde oppositieleider ruilen voor Oekraïense gevangenen

Miko slachtoffer van hackers


©Katrijn Van Giel

KURT VANSTEELAND | Vandaag om 07:59

De koffiespecialist zegt 'snel gehandeld' te hebben en werkt hard om weer volledig operationeel te zijn.

Meest gelezen

1 Raad van State doorkruist Brussels prestigeproject Immobel
2 Poetin zinspeelt op langdurig conflict in Oekraïne
3 Automerken beperken speelruimte dealers
4 Belgische vastgoedmarkt koelt af
5 Fondsenreus vloert Europese grootbanken met salvo blokverkopen

2022 – 1
Ransomware
en Supply Chains

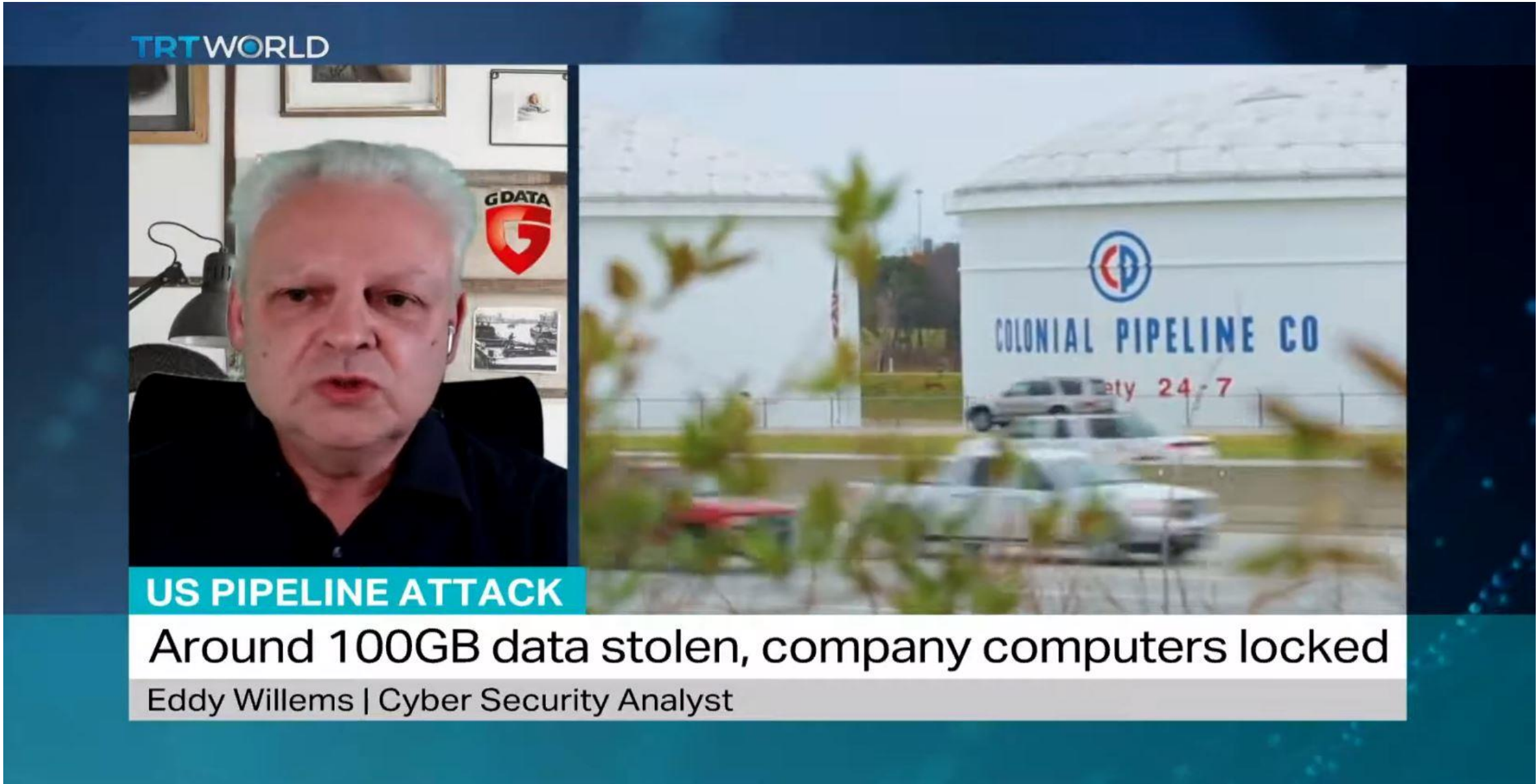
SOLARWINDS HACK

SolarWinds attack explained: And why it was so hard to detect

A group believed to be Russia's Cozy Bear gained access to government and other systems through a compromised update to SolarWinds' Orion software. Most organizations aren't prepared for this sort of software supply chain attack.

By Lucian Constantin
CSO Senior Writer, CSO | DEC 15, 2020 3:44 AM PST

US OLIEPIJPLIJN AANVAL 2021



KASEYA MSP AANVAL 2021

Business

Ransomware attack struck between 800 and 1,500 businesses, says company at center of hack

Kaseya's software touches hundreds of thousands of firms, but company says vast majority were unaffected

Listen to article 3 min

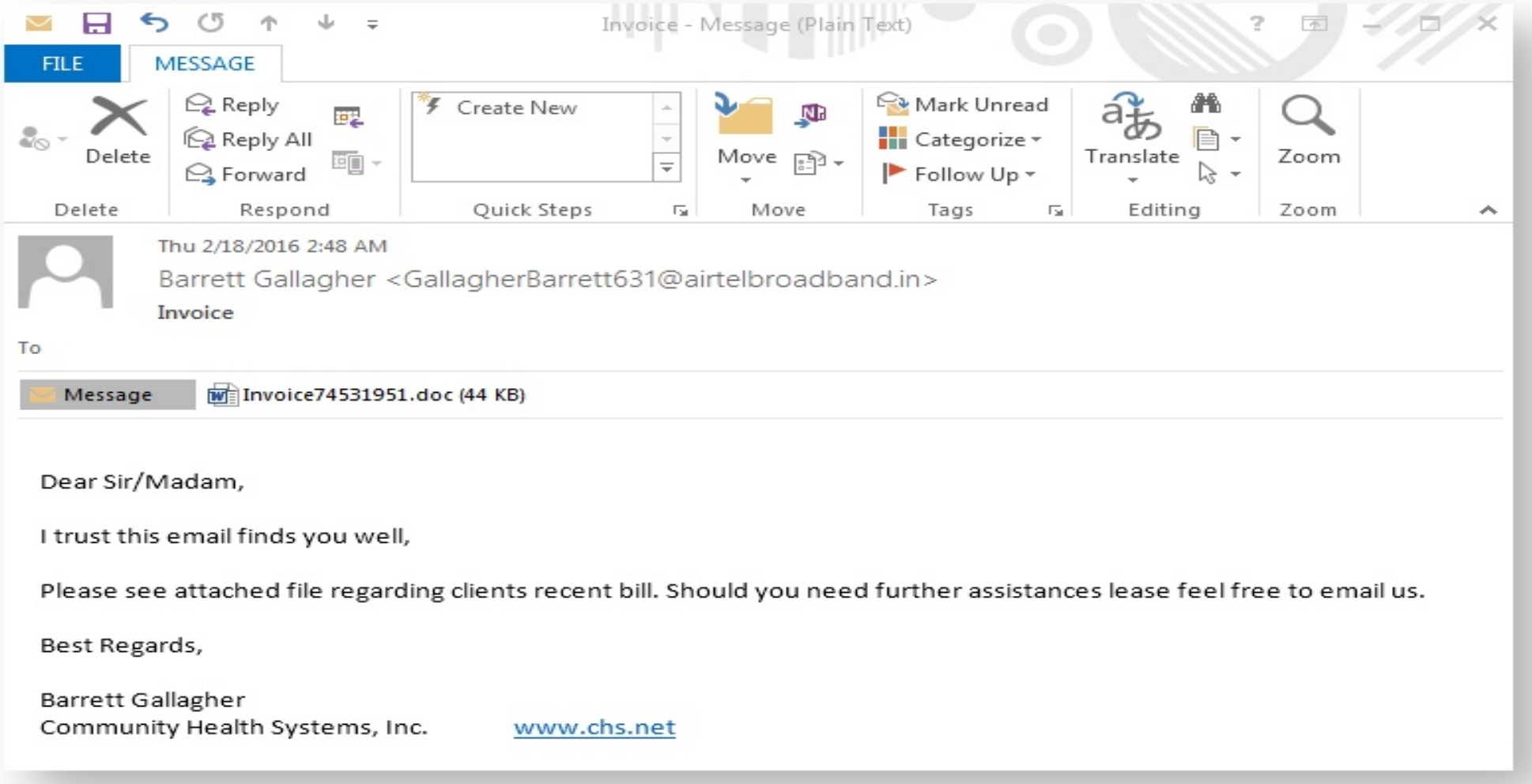

To pay
or
not to pay?
Cryptocurrency?!

2022 – 2
Social Engineering
En Phishing

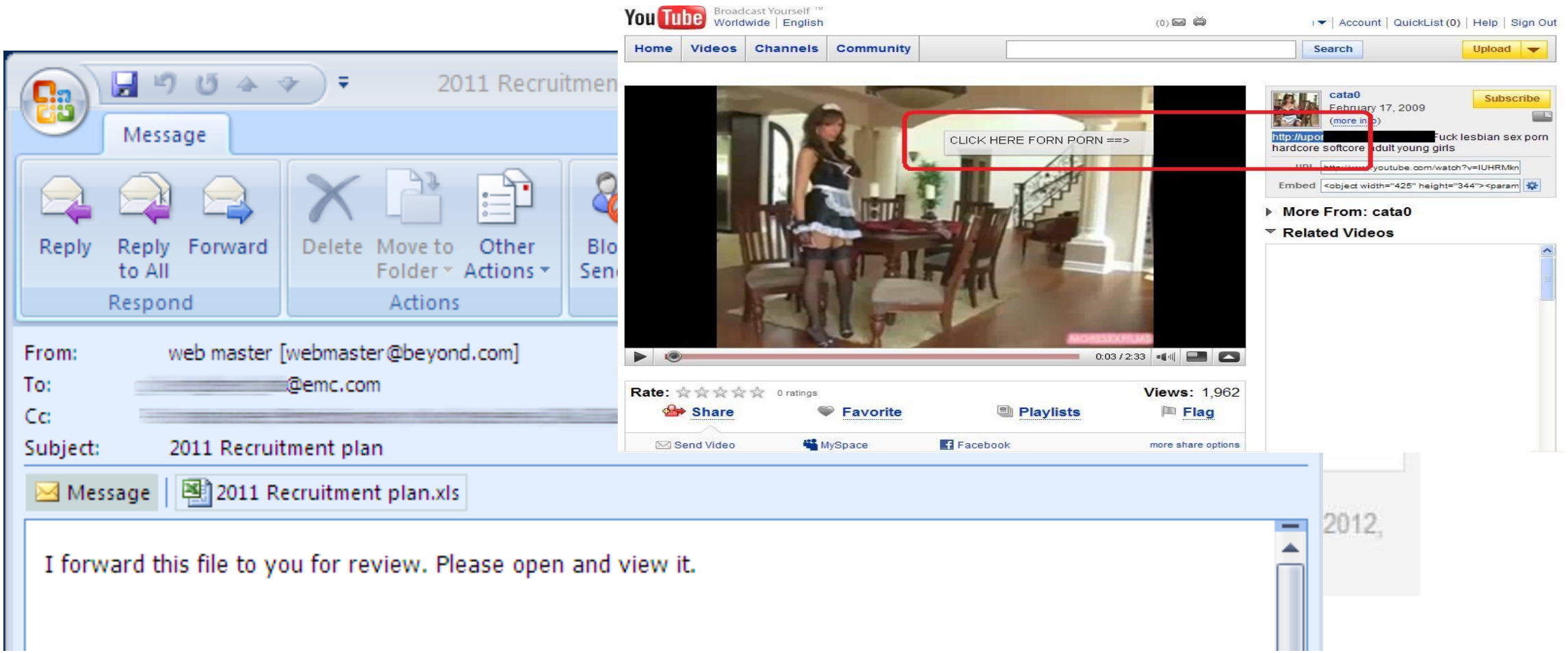
HOE GERAAKT JE COMPUTER OF NETWERK IN DE PROBLEMEN?

A. De gebruiker

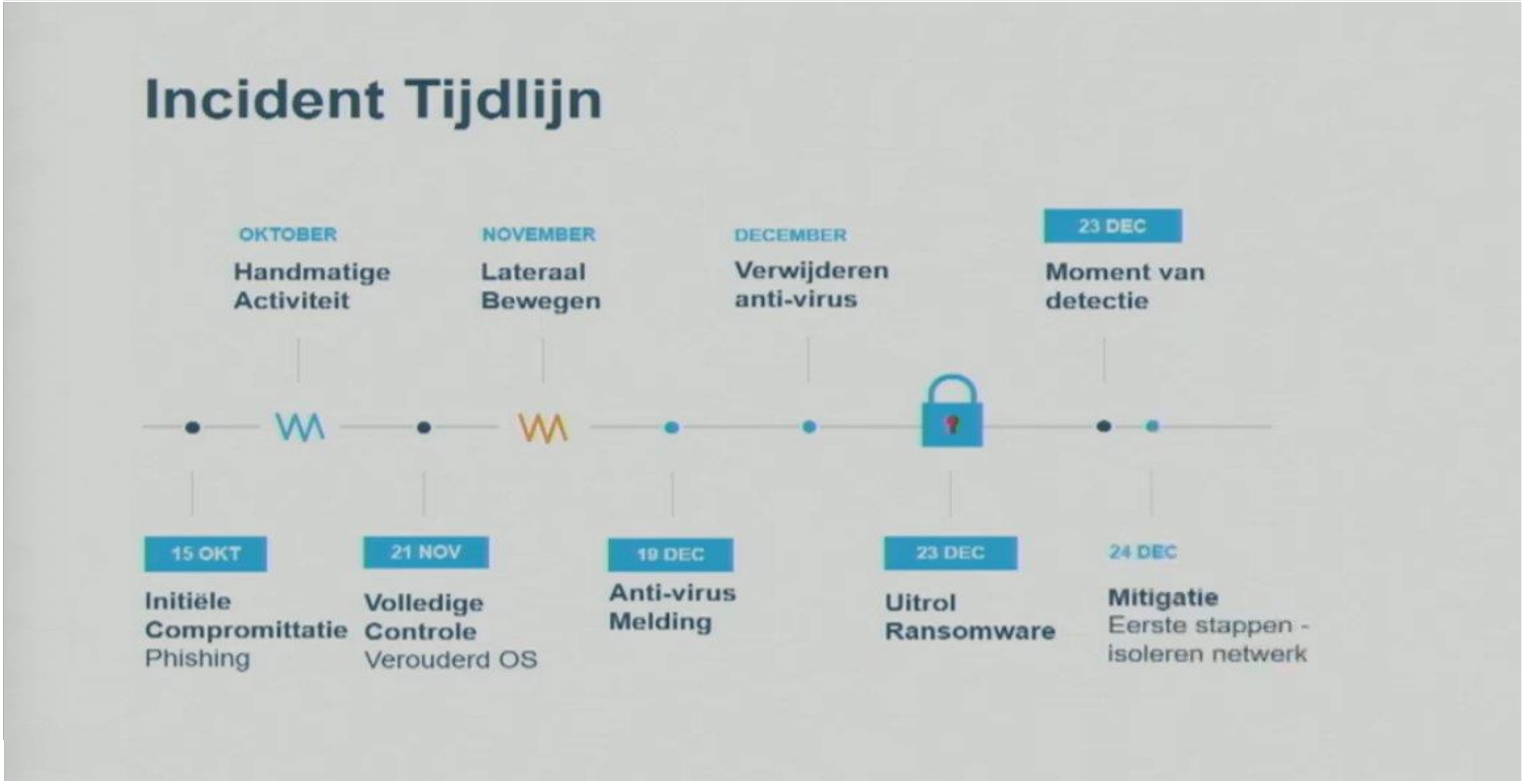
MAILS MET DOCS, ZIP, JAVASCRIPT, ETC…



DE MENSELIJKE FACTOR



ENKELE VOORBEELDEN



SPEAR PHISHING

Mon 20-Jan-20 11:27

Thierry Goeman <Thierry.Goeman@nieuwsblad.be>

Het Nieuwsblad.pdf

To Thierry Goeman

You forwarded this message on 21-Jan-20 10:34.

Thierry Goeman has shared a PDF document with you on One Drive for Business

Dank en beste groeten
Thierry Goeman
Het Nieuwsblad
0475 89 09 83

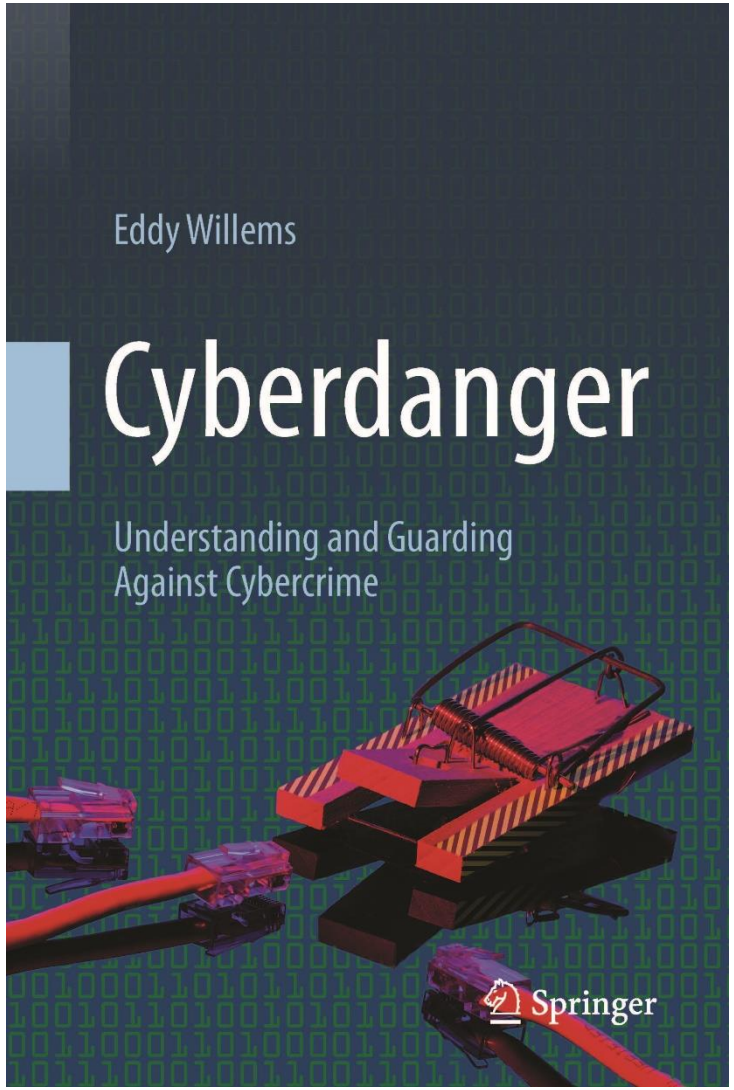
DE TWEEDE WET (VAN WILLEMS) : DE BASIS VAN SECURITY

CBP = TF x MF

CBP = Cybersecurity Probleem

TF = Technologische Factor

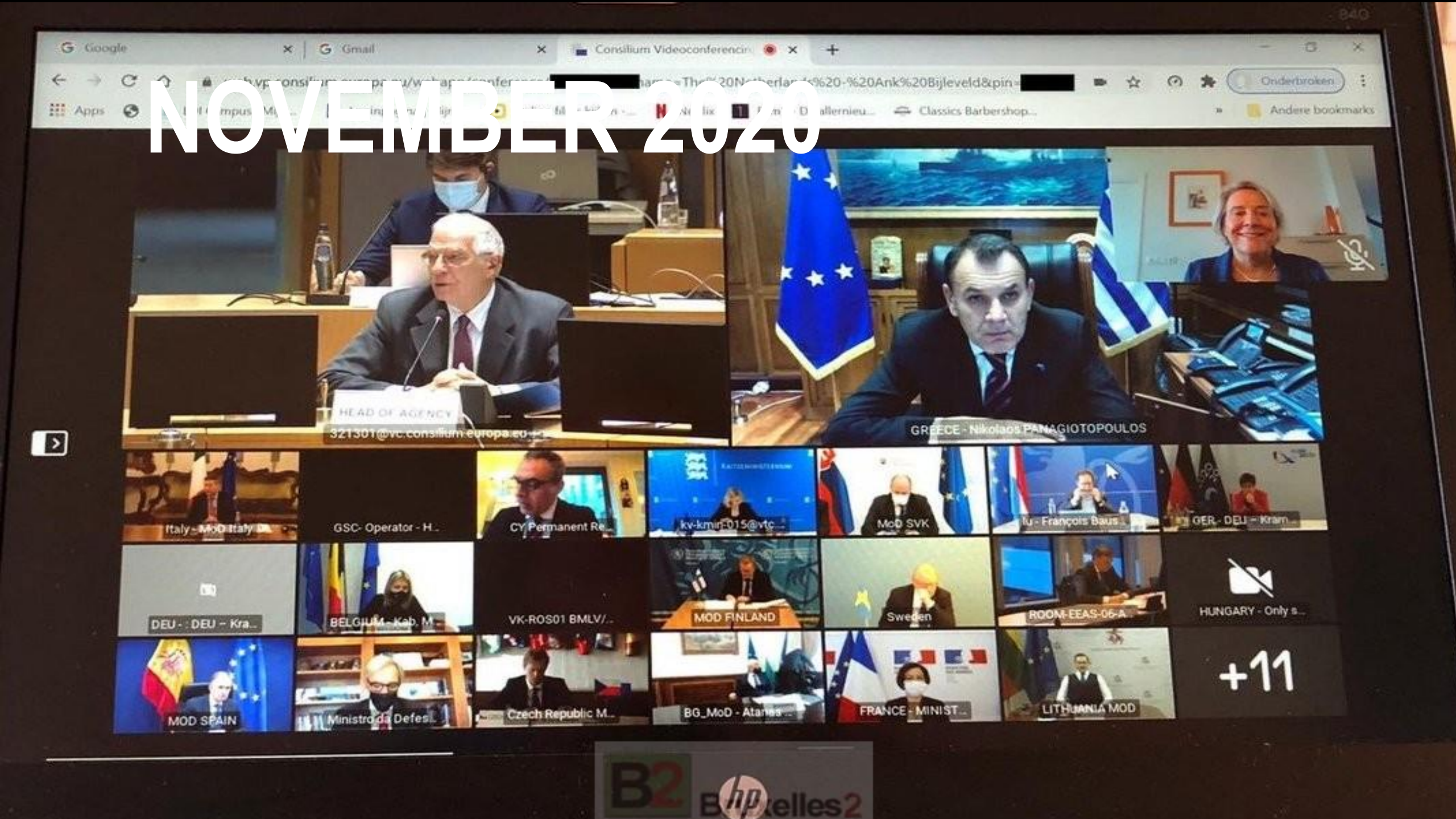
MF = Menselijke Factor




COVID-19


Zoom Meeting ID: 539-544-323
Speaker View
Participants (35)
Find a participant
Cabinet Room (Host, me)
PM
Defra SoS
Alister Jack - Scottish Secretary
Amanda Milling
Anne-Marie Trevelyan
Ben Gascoigne
Brandon Lewis (SoSNI)
Cabinet Secretariat (Emily Card...
Chancellor of the Exchequer
chris whitty
Dom Raab
Ed Lister
Grant Shapps
Home Secretary
iPhone
Mute All
Unmute All
More
Zoom Group Chat
PM
Cabinet Room
Jacob Rees-Mogg
Home Secretary
Simon Hart
Nat
Robert Jenrick, MHCLG
Liz Truss
SharmaA
markspencer
Dom Raab
Matt Hancock
Anne-Marie Trevelyan
Chancellor of the Exch...
Therese Coffey
Defra SoS
SoS Department for E...
Brandon Lewis (SoSNI)
michael.gove739
Alister Jack - Scottish S...
Suella Braverman
Press Team HQ
Lord Chancellor
1/2
1/2
Mute
Stop Video
Invite
Manage Participants
35
Share Screen
Chat
Reactions
End Meeting
BBC NEWS
ENG
11:20
31/03/2020

NOVEMBER 2020



B. De beheerder (Software/Hardware)

OVH hosting provider goes down during planned maintenance

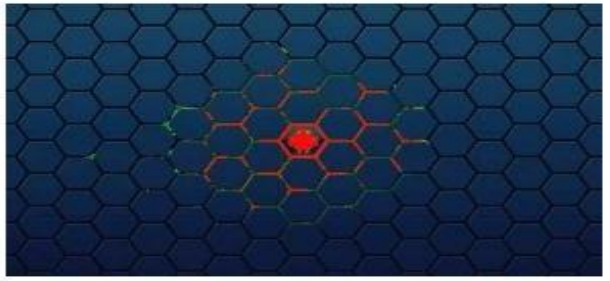
By Sergiu Gatlan

October 13, 2021 04:32 AM 0

OVH, the largest hosting provider in Europe and the third-largest in the world, went down earlier today following what looks like routing configuration issues during planned maintenance.

OVH has 32 data centers with over 300,000 servers on four continents and a total of 20 Tbit/s global network capacity.

POPULAR STORIES



Study reveals Android phones constantly snoop on their users

Emergency Apple iOS 15.0.2 update fixes zero-day used in attacks

2022 – 3

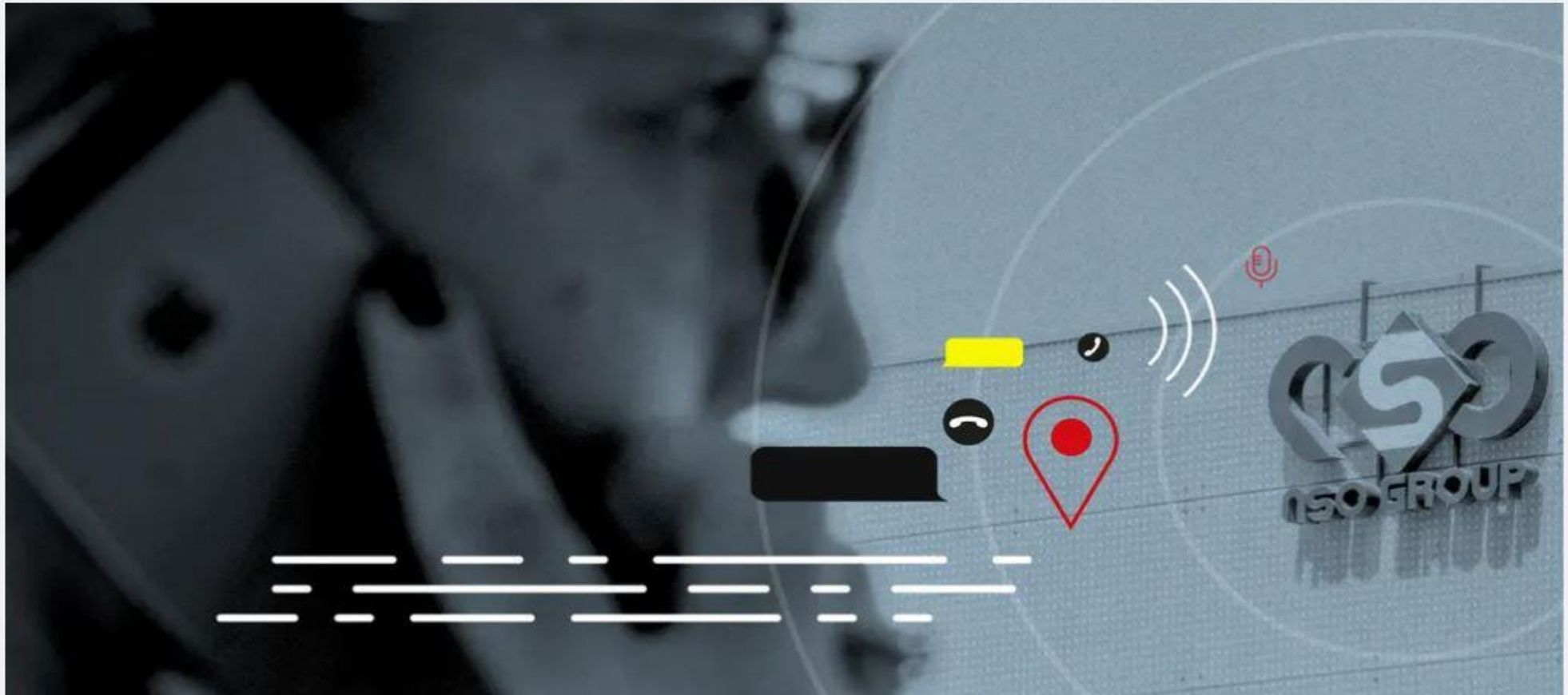
APT’s bij overheden, journalisten en NGO’s

The Pegasus project
Surveillance

What is Pegasus spyware and how does it hack phones?

David Pegg *and* Sam Cutler

Sun 18 Jul 2021 17.00 BST



MUST READ: Tech jobs are booming, and hybrid working sees more women join the industry

This is why the Mozi botnet will linger on

The botnet continues to haunt IoT devices, and likely will for some time to come.

By Charlie Osborne for Zero Day | September 1, 2021 | Topic: Security

It has been two years since the emergency of Mozi, and despite the arrest of its alleged author, the botnet continues to spread.

Mozi was discovered in 2019 by 360 Netlab, and in the two years since, has grown from a small operation to a botnet that "accounted for an extremely high percentage of [Internet of Things] IoT traffic at its peak."

According to Netlab (translated), Mozi has accounted for over 1.5 million infected nodes, of which the majority -- 830,000 -- originate from China.

Mozi is a P2P botnet that uses the DHT protocol. In order to spread, the botnet abuses weak Telnet passwords and known exploits to target networking devices, IoT, and video recorders, among other internet-connected products.

The botnet is able to enslave devices to launch Distributed Denial-of-Service (DDoS) attacks, launch payloads, steal data, and execute system commands. If routers are infected, this could lead to Man-in-The-Middle (MITM) attacks.

SECURITY

Windows 10 is a security disaster waiting to happen. How will Microsoft clean up its mess?

This malware could threaten millions of routers and IoT devices

Costco customers complain of fraudulent charges, company confirms card skimming attack

Exchange Server bug: Patch immediately, warns Microsoft

Average ransomware payment for US victims more than $6 million

RELATED

Now Iran's state-backed hackers are turning to ransomware
Security

The ransomware threat is getting worse. But businesses still aren't taking it seriously
Security

Why are you still using QWERTY? 2021's most common passwords revealed
Security

BIZTECH NEWS

Ukraine war: Ukrainians announce the launch of an 'IT army' to fight off Russian cyberattacks

As well as protecting against cyberattacks, Ukraine's 'IT army' would also target Russian cyberspace. - Copyright Canva

By **Euronews and Reuters** • Updated: 27/02/2022 - 03:45

Most viewed

1 St Javelin and the missile that's now an icon of Ukraine's resistance

2 Elon Musk moves Starlink satellites over Ukraine after vice PM's plea

3 Has the ISS become a new front in Russia's war in Ukraine?

4 Russia's Central Bank scrambles to deal with sanctions, falling rouble

5 A balanced fight? This is how the armies of Russia and Ukraine compare

Cloudflare blocks an almost 2 Tbps multi-vector DDoS attack

13-11-2021

Omer Yoachimik

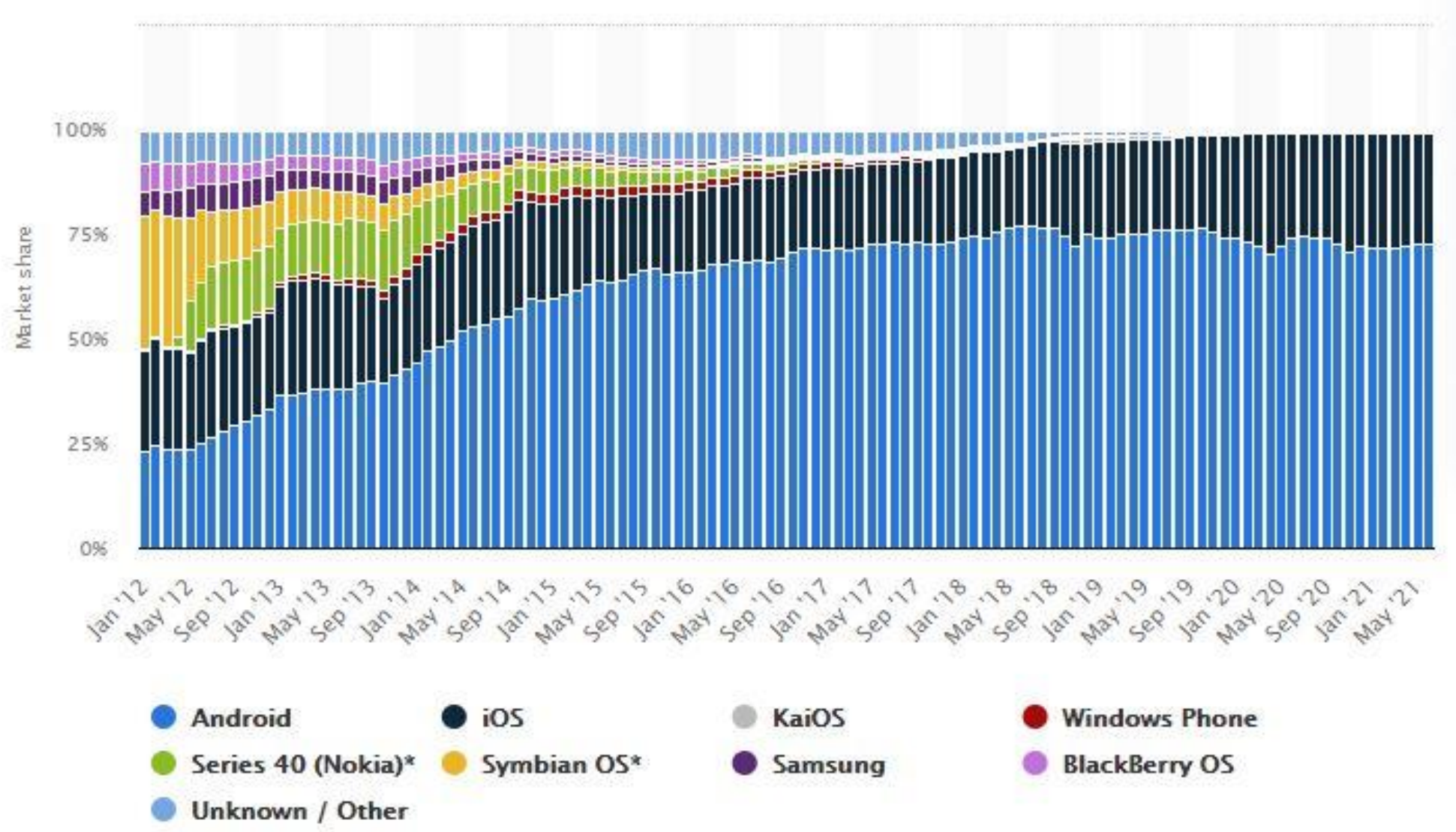
Earlier this week, Cloudflare automatically detected and mitigated a DDoS attack that peaked just below 2 Tbps — the largest we've seen to date. This was a multi-vector attack combining DNS amplification attacks and UDP floods. The entire attack lasted just one minute. The attack was launched from approximately 15,000 bots running a variant of the original Mirai code on IoT devices and unpatched GitLab instances.

2022 – 6
Innovatieve Mobiele Malware

HET ECHTE PROBLEEM : WAAR STOPT HET NETWERK?

GLOBAAL MARKTAANDEEL MOBIEL OS

STATISTA 2021



MOBIELE MALWARE SITUATIE ...

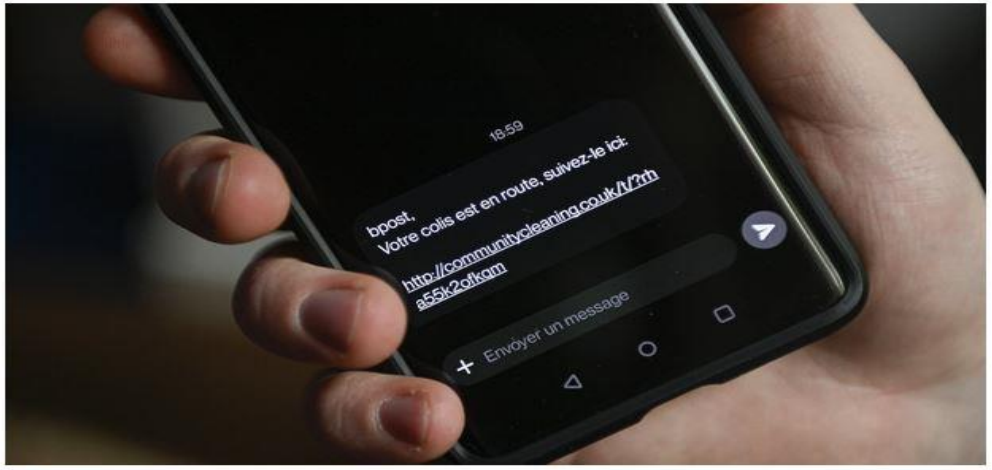
MOBIELE MALWARE

DataNews Rubrieken Het magazine Voordelen voor abonnees Abonneren Eddy Onze magazines

'Virus op meer dan 9.000 smartphones via valse bpost-sms'en'

12/05/21 om 15:27 Bijgewerkt op 14/05/21 om 11:35 Bron : Belga

Al zeker 9.000 smartphones zijn met een virus besmet geraakt doordat gebruikers een app installeerden via een sms die zogezegd van bpost kwam. Dat zeggen het Centrum voor Cybersecurity (CCB) en telecomwaakhond BIPT.



© Belga

Het gaat om een gevaarlijk virus, FluBot, dat veel schade aanricht en dat zich bovendien snel verspreidt naar de telefooncontacten van het slachtoffer, zeggen de overheidsinstanties.

"Door te experimenteren en te leren van 'mislukkingen', kan het development team beter worden dan de dag ervoor.

- Craig McLuckie

Meest gelezen


1 Reisapplicatie Covidsafe.be beschikbaar vanaf 17 juni


2 BIPT: er is ruimte voor vierde mobiele operator, maar...


3 Proximus blijft marktleider op vast en mobiel


4 Simac haalt raamovereenkomst bij Provincie Vlaams-Brabant binnen


5 Proximus mag Mobile Vikings overnemen

Data News Jobs

2022 – 7
Meer Data Lekken

Robinhood says millions of customer names and email addresses taken in data breach

Zack Whittaker @zackwhittaker / 2:14 PM GMT+1 • November 9, 2021


EMOTET

Afpersingsgroep Lapsus$ Ofwel ‘Kidsplay’

- Redline password stealer
- Kopen van credentials/tokens
- Doorzoeken public code repositories
- Betalen werknemers van geviseerde bedrijven
- Sim swapping

MICROSOFT \ TECH \ WINDOWS

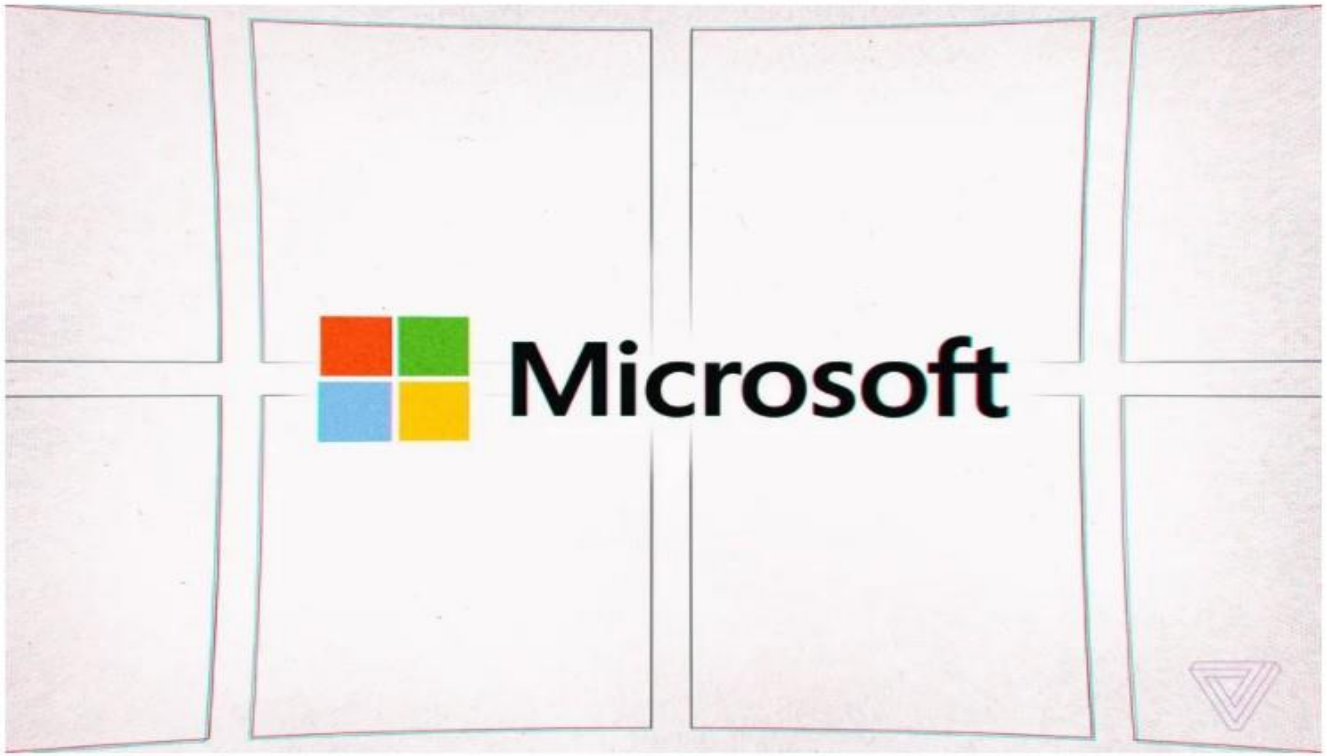
13

Microsoft confirms Lapsus$ hackers stole source code via 'limited' access

Lapsus$ says it has accessed data from Okta, Nvidia, Samsung, and Ubisoft

By Mitchell Clark, Richard Lawler, and Jay Peters | Mar 22, 2022, 7:06pm EDT

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.



Malware makers have already exploited other certificates released by Lapsus$. | Image by Alex Castro / The Verge


IN-THE-CLOUD
TRANSITIE
DEEL VAN DE
OPLOSSING?

CLOUD COMPUTING VOORDELEN

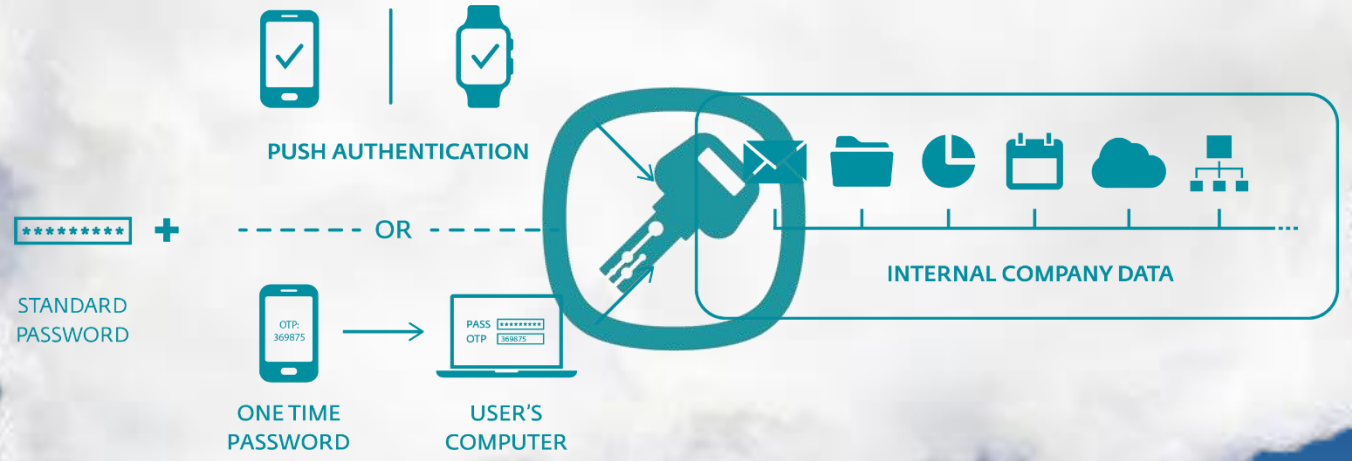
- Voordelen van het opschalen (smart scaling)
- Gestandaardizeerde (default) interfaces
- Gemakkelijke audits
- Betere timing, effectieve en efficiënte updates
- Betere monitoring
- Automatische backups
- En veel meer …

IN-THE-CLOUD SECURITY : WAAROP LETTEN?

Gebaseerd op VB Willems-Zwienenberg whitepaper: ‘Fool us or is it us fools?’
https://vblocalhost.com/conference/presentations/fool-us-or-is-it-us-fools-11-fools-years-later/

BEVEILIG ALLE TOESTELLEN NIET IN DE CLOUD (ENDPOINT) + VRAAG IN-DE-CLOUD PROVIDER

MFA AUTHENTICATIE WAAR HET KAN




PATCH MANAGEMENT
ALLE SOFTWARE EN FIRMWARE
OP ELK TOESTEL
UP-TO-DATE
+ VRAAG IN-DE-CLOUD PROVIDER


BACKUPS! ONLINE
OOK OFFLINE..
VERSCHILLENDE LOCATIES?
HOE GEREGELD IN-DE-CLOUD?


NA HET ETHISCH HACKEN …
VRAAG HULP
EN DOE EEN CHECKUP
CONTROLEER
DE CONSULTANTS


WAT ZIJN JOUW
KROONJUWELEN?
CREATIE VAN EEN SECURITY
POLICY EN ACTIEPLAN!
TEST HET UIT!!!
(Business Continuïteitsplan)

GDPR VS CLOUD ACT
ISSUES
MAW
WAAR ZIT JE DATA?


LET OP VOOR:
DATA LEKKEN

LET OP VOOR:
INSIDER ABUSE

LET OP VOOR:
UNKNOWN RISK PROFILE

Hardening/Patching? Wie heeft toegang tot wat? Procedure bij security indic

LET OP VOOR:
FINANCIËLE DDoS

LET OP VOOR: CRIMINEEL GEBRUIK VAN SERVICES

Not In-The-Cloud Tips

- Limiteer beheerdersrechten
- Hang niet alles aan het internet ((RDP en CITRIX) + VPN)!
- Beheer ook BYOD systemin
- Segmentatie Netwerk
- Monitoring!!!!!!
- Wie is verantwoordelijk voor IT security?!
- Gebruik encryptie
- Buzzwords: EDR (Endpoint Detection Report), XDR (Extended …) and Zero Trust (Never trust, always verify)

DE MENS?!

MAAK GEBRUIK VAN SECURITY AWARENESS TRAININGS

GRATIS – BEPERKT AANBOD

Cybersecurity online - OFO IFA

ofoifa.belgium.be/nl/fiche/cybersecurity-online

Apps | Suggested Sites | Web Slice Gallery | Customize Links | Imported From IE

NL FR

Andere informatie en diensten van de overheid

NEWSFLASH : Network Innovation: volgende bijeenkomst op 15 juni

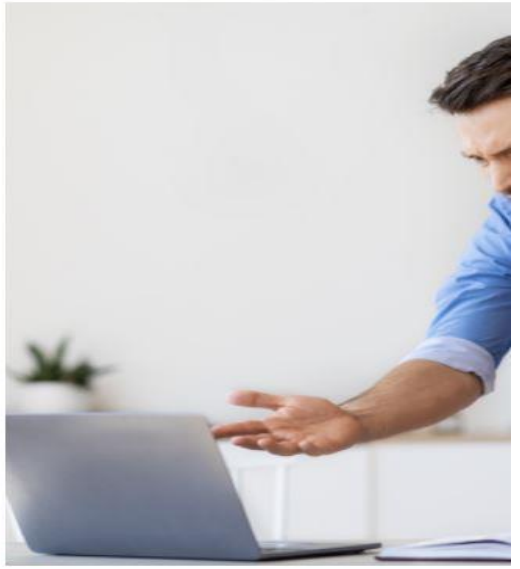
Aanbod **Evenementen** **Praktisch** **Nieuws** Voor HR-diensten Voor opleiders

CYBERSECURITY ONLINE

ZELFSTUDIE | VOOR INDIVIDUELE AMBTENAREN

IT | Cybersecurity

Je moet professionele informaticagegevens en -systemen beveiligen? Je moet de cyberweerbaarheid vergroten? In deze online opleiding leer je hoe je problemen en aanvallen kan detecteren en hoe defensieve technieken kan gebruiken om je systemen te beveiligen.



⊖ Pluspunten

Deze online opleiding is een individuele zelfstudie en bestaat uit 16 lessen.

Je kan **stap voor stap** de verschillende lessen **op je eigen ritme** ontdekken

⊖ Voor wie?

- Voor alle ambtenaren die gegevens en systemen willen beveiligen
- Voor alle ambtenaren die cybercriminaliteit willen voorkomen of stoppen.

⊖ Op het programma

Praktische info

De opleiding is vrij toegankelijk :

- meld je aan op ecampus.ofoifa.be

BEDANKT!
VRAGEN?

How QR codes are made:
QR codes aren't always safe!

Pauze

Lokale besturen in de digitale wolk
Slotsessie Cyberveilige Gemeenten
29 april 2022

vvsg
Vereniging van
Vlaamse Steden
en Gemeenten

Vragenronde ‘Het lokaal bestuur in de cloud’

Stel je vraag via de chat

vvsg

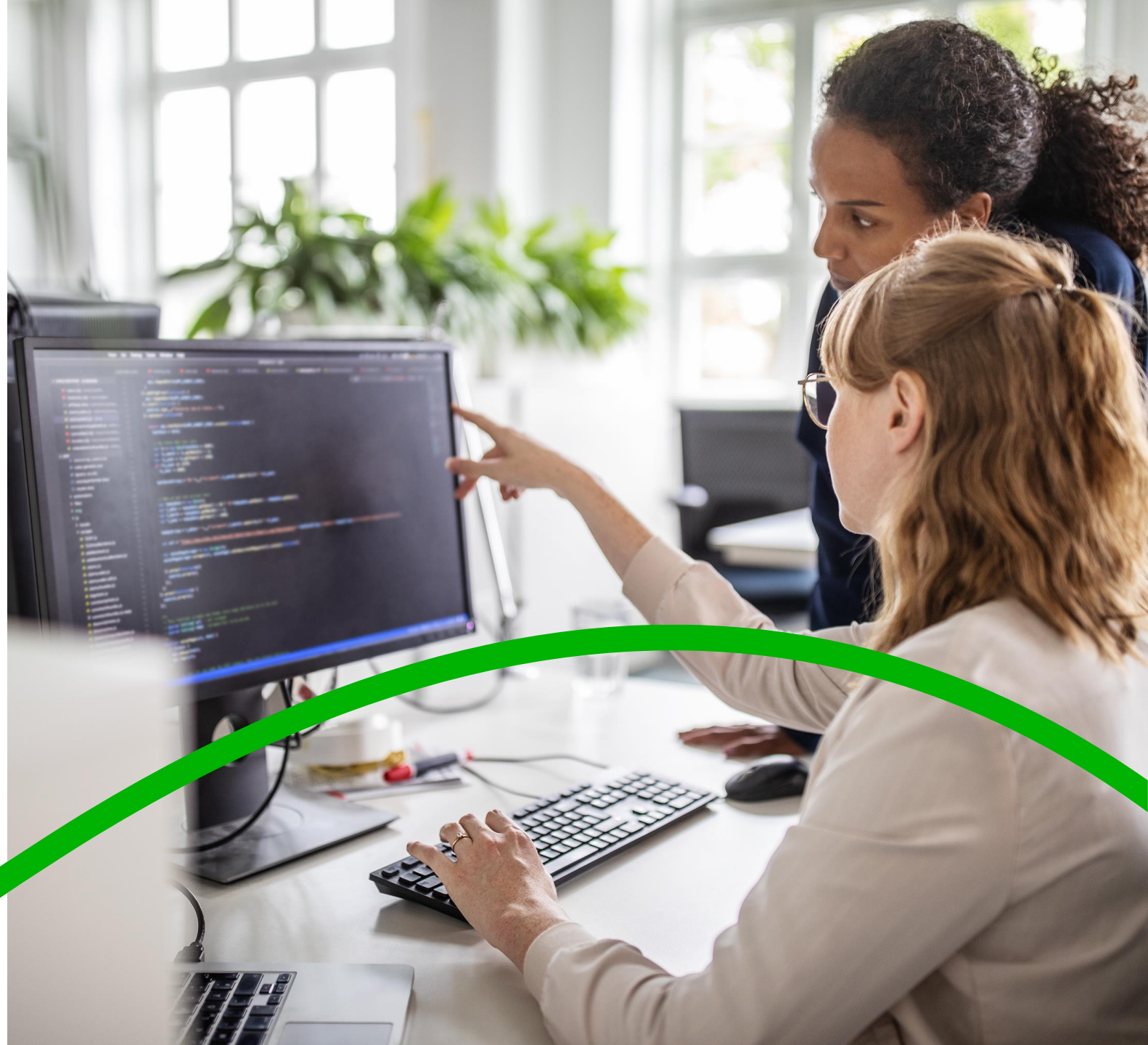
Vereniging van
Vlaamse Steden
en Gemeenten

Cyberveilige Steden en Gemeenten

Vooruitblik op het verdere project

Jolien Schoonooghe
Projectmedewerker Cyberveilige Steden en Gemeenten - VVSG

vvsg



Vooruitblik op het verdere project

In dit project schuiven we 3 sporen naar voren:

Spoor 1: Verspreiding en actualisatie van de digitale toolkit Cybersecurity
Spoor 2: Verderzetting van het Traject Ethisch Hacken in samenwerking met HOWEST
Spoor 3: Kennisopbouw en bewustmaking

Organisatie van 6 interactieve webinars

- Elk webinar gaat dieper in op één of meerdere tools uit **de digitale toolkit Cybersecurity** en de wijze waarop deze **geïmplementeerd kunnen worden.** Deze tools worden steeds gekoppeld aan **een inspirerende praktijkcase**, met een toelichting door een of meerdere (ervarings)deskundigen.

- De **zes thema's** die behandeld zullen worden tijdens de interactieve webinars:

    - Incident response
    - Business continuïteit
    - Cyber awareness
    - Informatiebeveiliging
    - Veilige software en detectie
    - Monitoring.

- **De opnames** van de webinars worden achteraf ter beschikking besteld **op de centrale projectpagina**.

2022

- Organisatie eerste en tweede webinar gebeurt tussen april en juni 2022
- Organisatie derde webinar gebeurt in het najaar van 2022

2023

- Organisatie van de vierde en de vijfde webinar gebeurt tussen april en juni 2023
- Organisatie van de zesde webinar gebeurt in het najaar van 2023

Spoor 1: Verspreiding en actualisatie van de digitale toolkit Cybersecurity

- Publicatie van 3 artikels in het VVSG-magazine Lokaal
  - Gedurende de periode van het project

- Uitrol van een communicatie- en sensibiliseringscampagne rond cybersecurity-oefeningen
  - Voorzien tussen september en november 2023

Traject Ethisch Hacken 2022

- Opstart traject: in het voorjaar van 2022
  - Officiële aankondiging via de VVSG-kanalen
  - Publicatie van de oproep gebeurt in juni 2022
- Lokale besturen die interesse hebben, kunnen zich al aanmelden via cyberveiligheid@vvsg.be

- Uitvoering van de audits door de studenten bij de lokale besturen
  - Tussen oktober en eind december 2022

- Analyseren en communiceren van de resultaten
  - Tussen januari en april 2023

Spoor 3: Kennisopbouw en bewustmaking

- **Organisatie van een omvattende bewustmakingssessie naar lokale medewerkers**
    - Deze sessie gaat dieper in op onveilig gedrag en praktijken die hen kunnen helpen om zichzelf en het lokaal bestuur te beschermen tegen de dreigingen die cybercriminaliteit met zich meebrengt. De bewustmakingssessie wordt opgenomen, zodat deze ook later door lokale besturen gebruikt kan worden voor interne vormingen en training.
        - Deze sessie zal doorgaan in 2022
- **Organisatie van een bewustmakingssessie aan die zich richt tot lokaal management en mandatarissen**
    - Deze sessie legt de focus op technische en organisatorische maatregelen die de cyberveiligheid van het lokaal bestuur ten goede kunnen komen. De sessie is laagdrempelig van opzet, zodat deelnemers aan het einde een duidelijk en behapbaar overzicht hebben van maatregelen die geïntroduceerd kunnen worden om stappen vooruit te zetten. Ook voor deze sessie zorgen we voor een opname, die nadien op onze website wordt gedeeld met andere geïnteresseerde lokale besturen.
        - Deze sessie zal plaatsvinden in 2023

Nuttige informatie i.v.m. het Project Cyberveilige Steden en Gemeenten

Het **Traject Ethisch Hacken** kadert binnen het **Project Cyberveilige Steden en Gemeenten** dat gecoördineerd wordt door de VVSG, met ondersteuning van de Vlaamse Overheid. Voor meer info bij het project en de verschillende luiken kan je terecht op **de website van VVSG**. Op deze pagina zijn ook tools te vinden die gebruikt kunnen worden om de lokale aanpak te versterken, zoals een sjabloon voor een business continuïteits-en crisiscommunicatieplan en een inspirerende infosessies.

In **de conclusie van het analyserapport** wordt verwezen naar de rapporten die Audit Vlaanderen uitwerkte in kader van de Thema-audits Informatiebeveiliging 2017-2018 en 2020. Beide documenten zijn te raadplegen op **de website van Audit Vlaanderen**. Audit Vlaanderen coördineert ook het aanbod van professionele ICT-veiligheidsaudits met cofinanciering in het kader van het Programma Cyberveilige gemeenten. **Hier** vind je meer informatie bij het aanbod en de bestelprocedure.

Voor diverse aanbevelingen uit dit analyserapport bestaan reeds goede praktijkvoorbeelden bij lokale besturen.
Op de website van de Vlaamse Overheid staan een twintigtal praktijken die kunnen helpen bij het uitwerken van de eigen lokale aanpak.

Het Traject Ethisch Hacken kwam tot stand door een samenwerking met studenten toegepaste informatie van Howest. Voor meer informatie bij de opleiding en afstudeerrichtingen kan je terecht op **de website van de hogeschool.**

In het **najaar van 2022** zal **een herhaling van het traject ethisch hacken** plaatsvinden. Indien je lokaal bestuur hier graag deel van wil uitmaken, kan je dit reeds melden **via mail**. Het vervolgtraject zal formeel aangekondigd worden via de VVSG-kanalen.

vvsg

Vereniging van
Vlaamse Steden
en Gemeenten

Afsluiting

Minister Bart Somers

Vereniging van
Vlaamse Steden
en Gemeenten

Vragen?

Keynote spreker | Eddy Willems – eddy.willems@gdata.de

VVSG | Jolien Schoonooghe – jolien.schoonooghe@vvsg.be

vvsg Vereniging van Vlaamse Steden en Gemeenten

Hartelijk dank voor de aandacht en hopelijk tot ziens!

VVSG vzw • Bischoffsheimlaan 1-8 • 1000 Brussel • T +32 2 211 55 00
info@vvsg.be • www.vvsg.be