Trends en uitdagingen in cybercriminaliteit

Een wake-up call

Mathieu Verschraege

.mediavista

vvsg Vereniging van Vlaamse Steden en Gemeenten

Overzicht

- Trends in het cyberlandschap
  - Nationaal
  - Europees
  - Globaal
- Kwetsbare steden en gemeenten
  - Legacy systemen
  - Human factor
- Impact van de ‘human factor’
- Uitdagingen voor de toekomst

Trends

Evoluties in het cyberlandschap

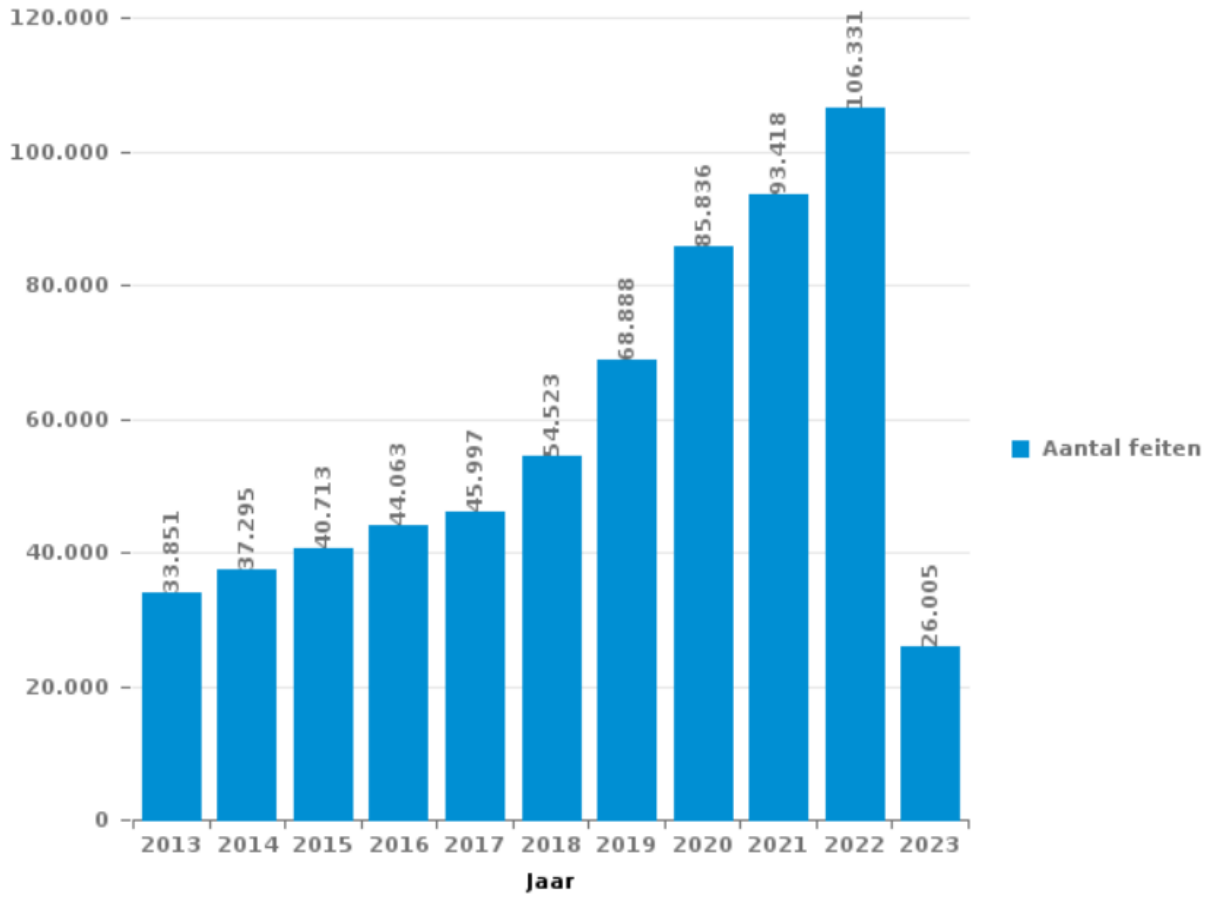
Trends

https://www.politie.be

BELGIË

Totaal aantal misdrijven met een ICT/online element sinds 2013

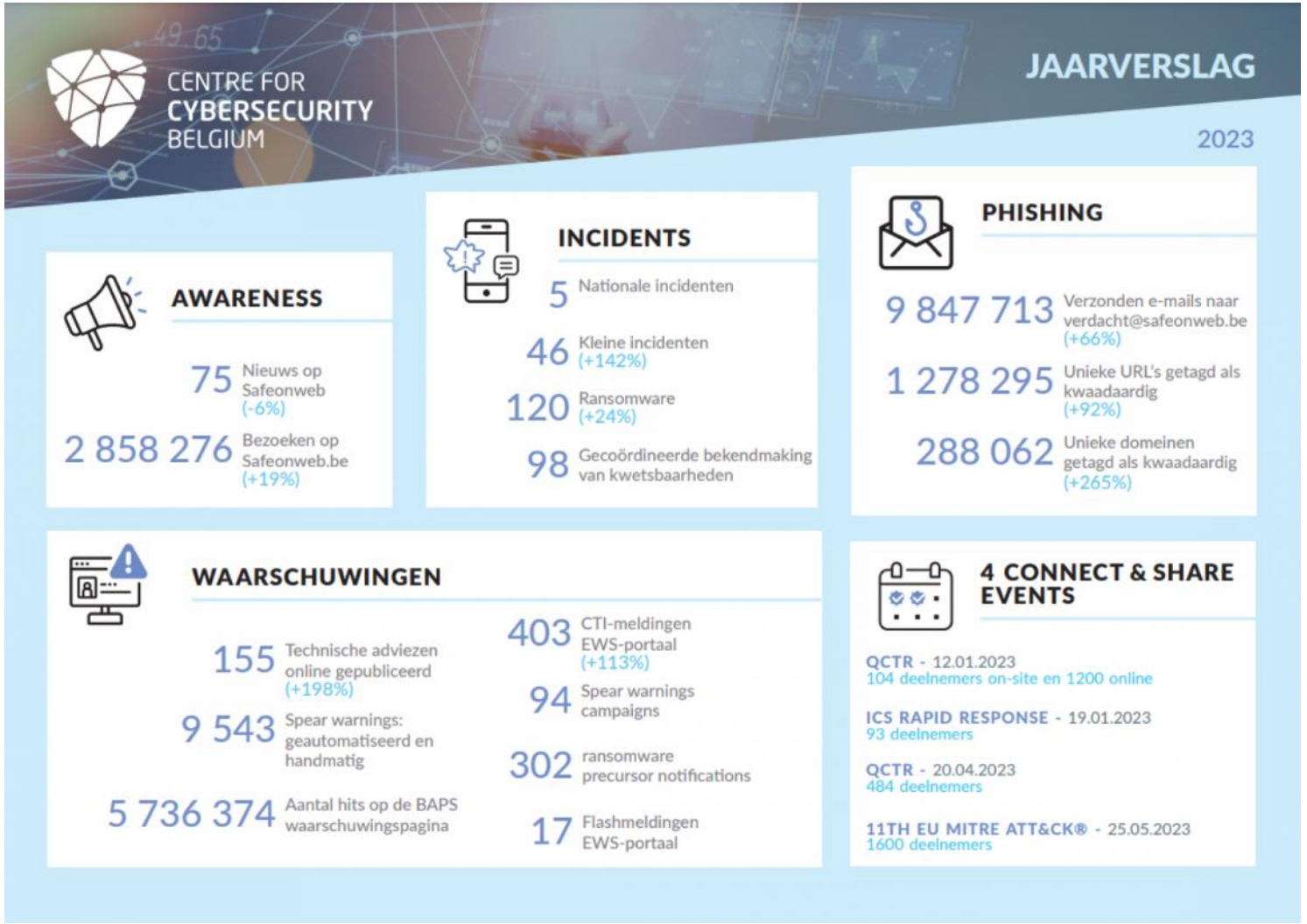
(deze cijfers kunnen een onderschatting zijn, dit afhankelijk van vattingspraktijken en technische beperkingen)



Trends

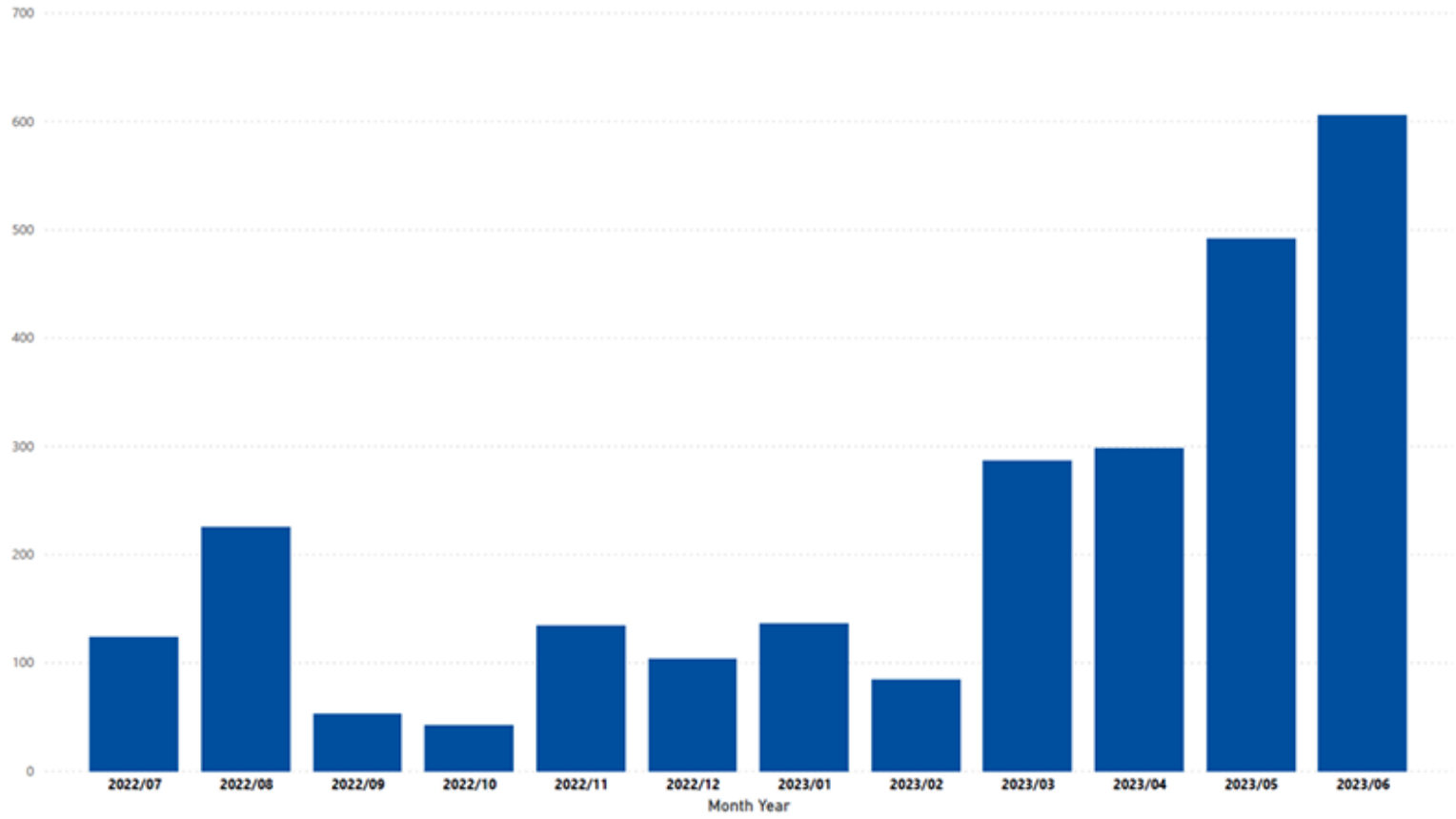
CENTRE FOR CYBERSECURITY BELGIUM

https://ccb.belgium.be



Trends

Figure 4: Timeline of EU events (count of number of observed incidents per month)

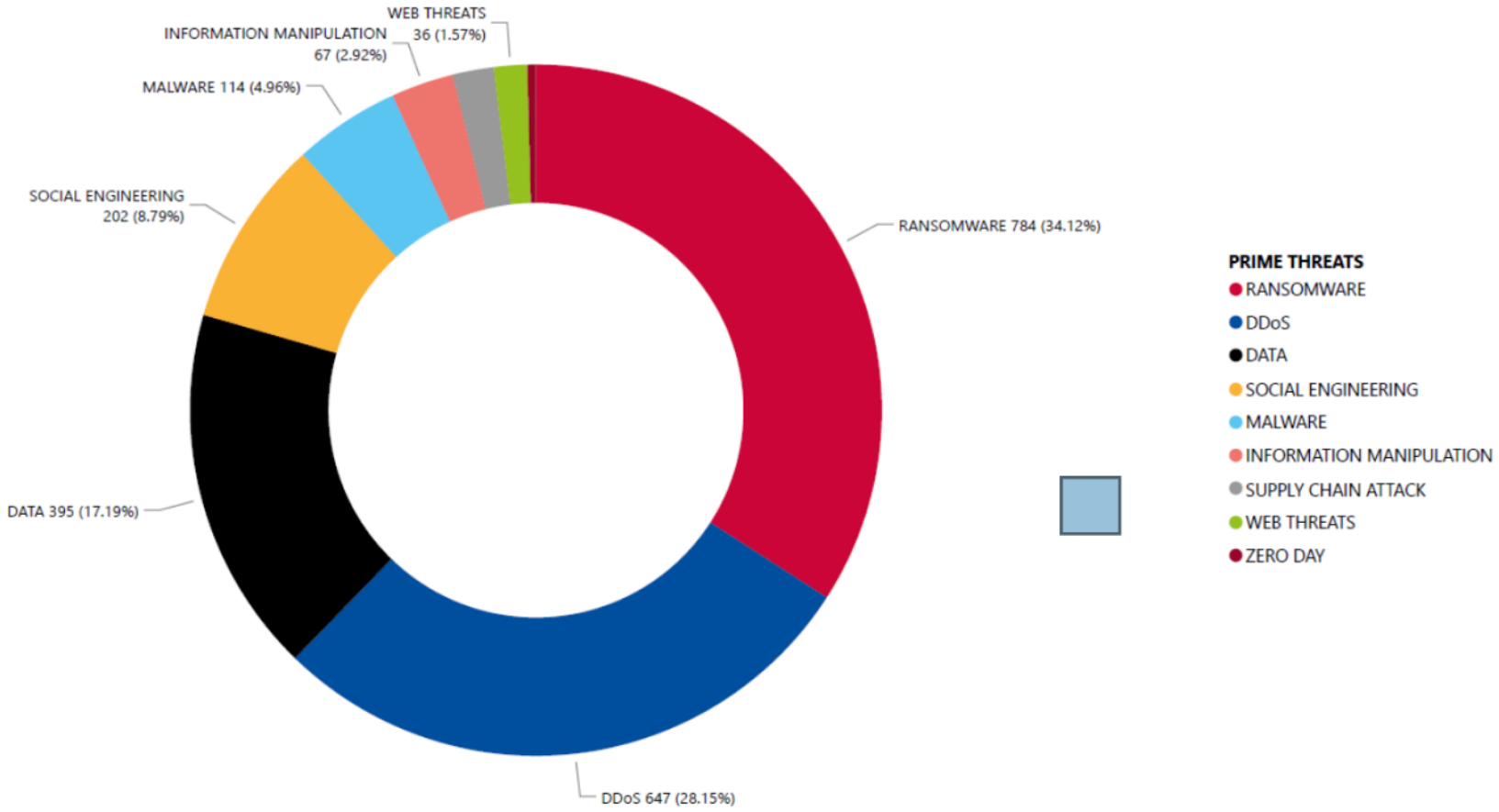


enisa
European Network and Information Security Agency

https://www.enisa.europa.eu

Trends

Figure 5: EU breakdown of number of threats by threat group

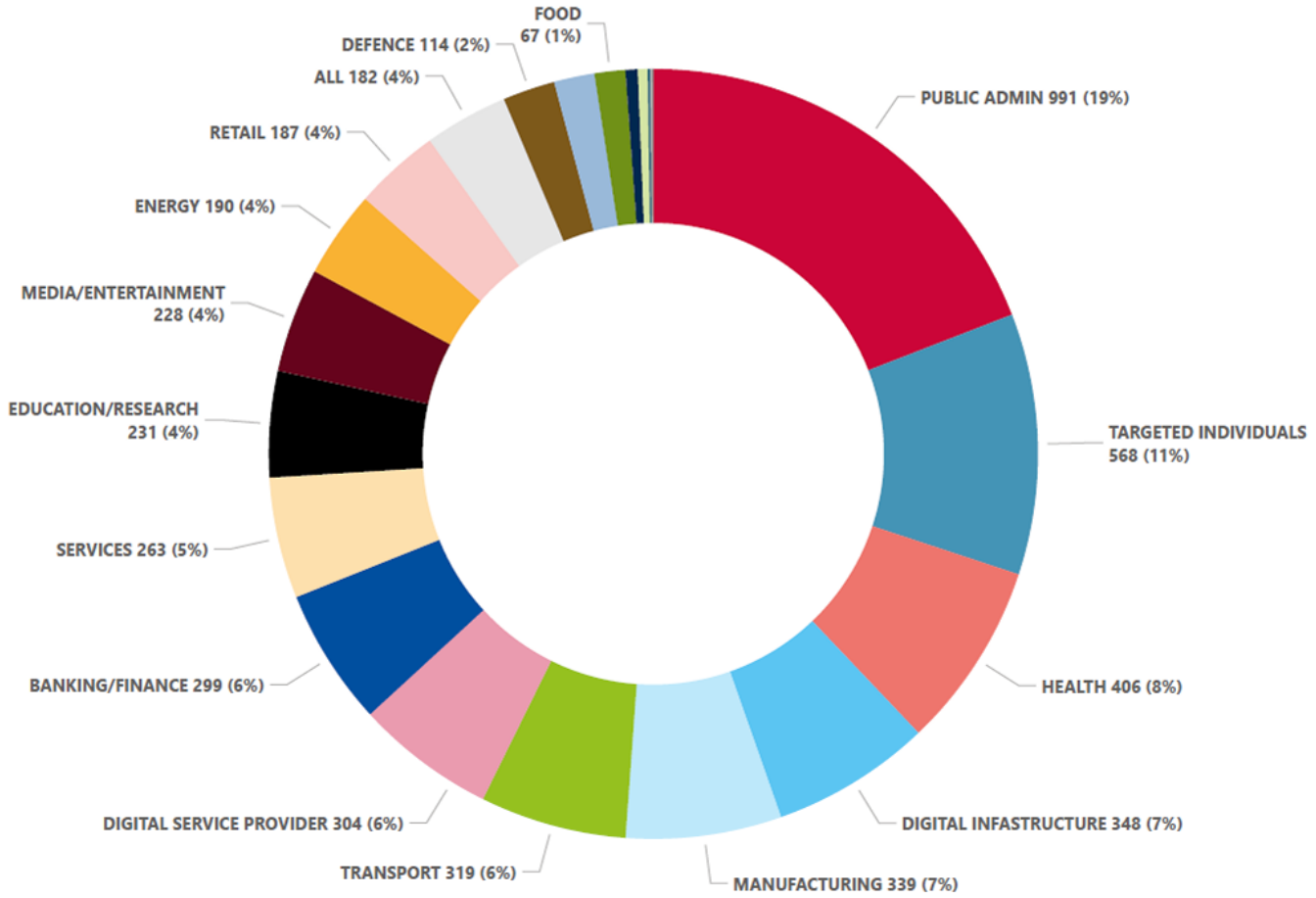


enisa
European Network and Information Security Agency

https://www.enisa.europa.eu

Trends

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



enisa
European Network and Information Security Agency

https://www.enisa.europa.eu

Kwetsbare steden en gemeenten

- Legacy systemen
- Human factor

Legacy systemen

- Nieuwe systemen: kwaliteitsstandaarden
- Opgelet met verouderde systemen
  - Kwetsbaarheden (patches, updates, …?)
  - Oude authenticatiemethoden
  - Problematische koppelingen met databanken
  - …
- Case: digitaal loket via *rijksregisternummer*

Legacy systemen

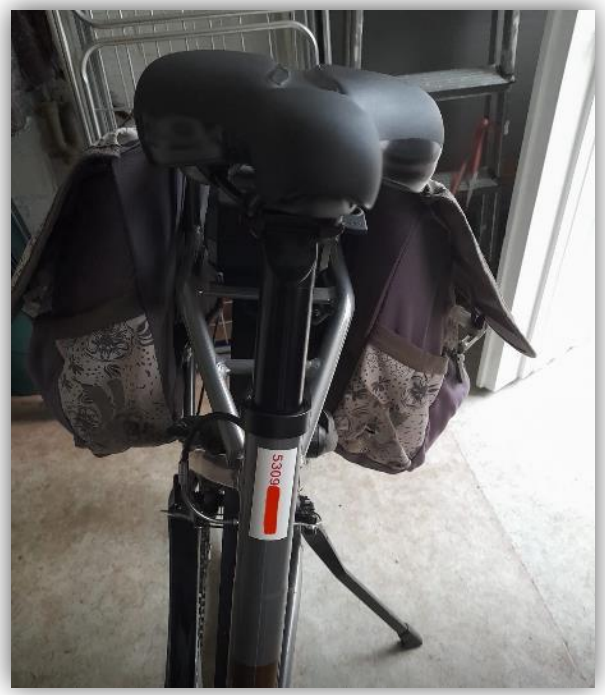
- Rijksregisternummer?

Nieuw, landelijk systeem voor fietsmarkering op komst: hoe zal het werken?

Wie zijn fiets wil laten markeren, zal vanaf volgend jaar gebruik kunnen maken van een nieuw, landelijk systeem. Wie dat wil, zal een moeilijk te verwijderen sticker kunnen krijgen met daarop een unieke QR-code. Wie die code met de smartphone scant, komt te weten of een fiets al dan niet gestolen is. In tegenstelling tot traditionele fietsmarkeringen geeft het nieuwe systeem geen persoonsgegevens vrij.

Denny Baert, Saskia De Schutter
za 20 aug 2022 15:25

vrt nws



Human factor

- Case: technische beveiliging vs. gebruikers
- Investeer in
  - technische oplossingen
  - continue professionalisering van **IT-medewerkers**
  - cyberbewustzijn van **alle medewerkers**
- Gedeelde verantwoordelijkheid

Impact van de ‘human factor’

Cyberweerbare medewerkers

De mens als sterke schakel

Versterk de cyberweerbaarheid van medewerkers

- Kennis van *actuele cybercrimefenomenen* en *manipulatieve technieken* verhogen met *awareness-sessies* en *nieuwsberichten*
  - (Spear) phishing i.c.m. MFA fatigue
  - CEO-fraude
  - Vishing (voice phishing) - helpdeskfraude

De mens als sterke schakel

Versterk de cyberweerbaarheid van medewerkers

- Geef inzicht in het waarom van een *e-policy*
  - Intrinsieke i.p.v. extrinsieke motivatie
  - Van ‘omdat het moet’ naar ‘omdat ik de organisatie help’
  - Heldere, eenvoudige communicatie

De mens als sterke schakel

Versterk de cyberweerbaarheid van medewerkers

- Betrek iedereen bij *simulaties* van cyberaanvallen
  - Wat verwacht je van individuele medewerkers in geval van een aanval?
  - Niet enkel grote rampscenario's, ook organisatiebrede phishingsimulaties
  - Ga actief aan de slag met resultaten en statistieken

De mens als sterke schakel

Versterk de cyberweerbaarheid van medewerkers

- Geef *duiding* bij de *actualiteit*
  - Leer samen uit de berichtgeving over cyberaanvallen op openbare besturen e.a.
  - Wees kritisch waar nodig

Uitdagingen voor de toekomst

Wat staat ons te wachten?
Hoe wapenen we ons?

Uitdagingen voor de toekomst

- AI-gestuurde aanvallen
  - Manipulatieve GenAI i.k.v. phishing en andere vormen van fraude
  - Automatisering, geografische spreiding en variabele aanvalspatronen

- Ransomware (en Ransomware-as-a-Service – RaaS)
  - Maximaliseer een Zero Trust-beleid

Uitdagingen voor de toekomst

- Internet of Things (IoT)-kwetsbaarheden
  - Enorme toename van het aantal apparaten en systemen die met internet verbonden zijn
  - Bv. verkeersregeling, energiebeheer, afvalbeheer, bewaking, …
- Supply Chain attacks
  - Kwetsbare toeleveringsketen = kwetsbare stad of gemeente
  - Koppeling van systemen kan criminelen via de toeleveringsketen toegang geven

Hoe wapenen?

- Zet blijvend in op **sensibilisering** van je **medewerkers**
  - Phishingsimulaties
  - Preventiesessies
- Investeer in **professionalisering** van **IT-ondersteuners**
- Zie **NIS2** als een **opportuniteit**
- Hanteer het **Cyber Fundamentals Framework** van het CCB
- **Begeleiding** en **ondersteuning** via VVSG, ABB, Vo-CRT, CCB

Hoe wapenen?

Cybercriminaliteit kent geen (gemeente)grenzen.

Bron: geopunt.be

Bedankt!

Mathieu Verschraege
mathieu@mediavista.be
www.mediavista.be