CyberEvent Wijk bij Duurstede

Digitaal Veilig Ondernemen

2 oktober 2023

Ervaringsverhaal

Iris Meerts, burgemeester van Wijk bij Duurstede © Frank jansen

Hoe ook de moeder van burgemeester van Wijk bij Duurstede keihard werd opgelicht: ‘Ze is er ingetuind’

Welkom!

Veiligheid

1:8000

De kans op brand
in je bedrijf

1:250

De kans op inbraak
in je bedrijf

1:5

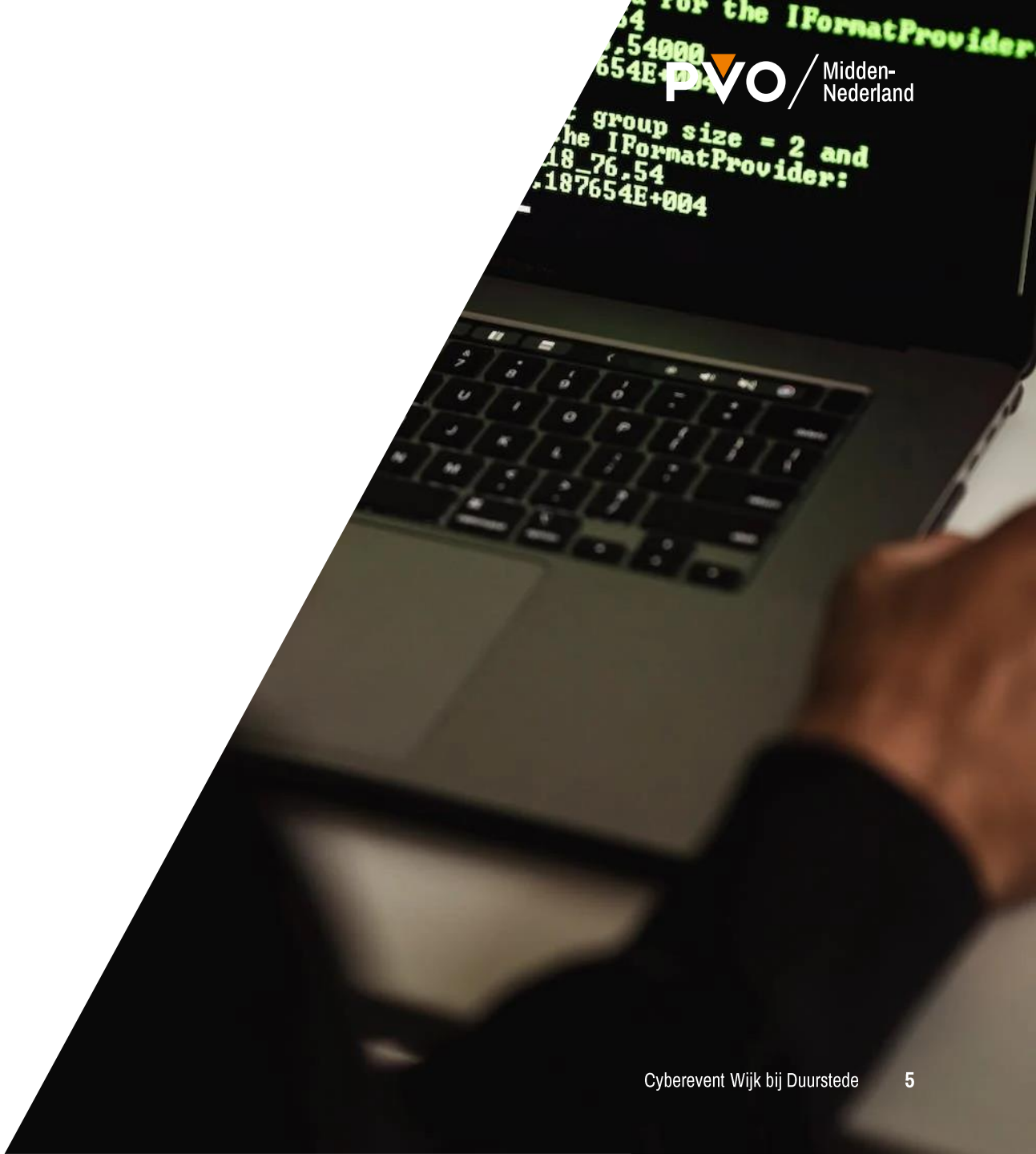
De kans op
een cyberaanval

Burgemeester Iris Meerts

- Welkom!
- Praktische mededelingen

Het programma:

- Gastheer Ernst-Jan Damen – van Vliet Duurzaamhout
- Ian van der Wurff – Tozetta
- Jaap van Driel – Digitale Wijkagent
- Merel Hurenkamp – themaspecialist cyberweerbaarheid
- Afsluiting en borrel (rondleiding door het pand)



Ernst-Jan Damen

VAN VLIET
DUURZAAMHOUT.NL

Ian van der Wurff - Tozetta

TOZETTA

Jaap van Driel – Digitale wijkagent

- digitaal-wijkagent.heuvelrug@politie.nl

POLITIE

Wat nu?

Merel Hurenkamp | Platform Veilig Ondernemen Midden-Nederland

2 oktober 2023

PVO / Midden-Nederland

Ik hoor jullie denken...

- Een cyberaanval overkomt mij niet;
- Mijn IT-leverancier regelt dat voor me;
- Wij zijn te klein;
- Ik weet dat ik er iets mee moet, maar waar moet ik beginnen?
- Wat moeten criminelen met onze gegevens?

Jij bent niet de enige die dat denkt...

Bakker Ineke

- Kleine bakkerij in Noord-Brabant
- Allergievriendelijke broden
- 50 klanten
- Bakfiets

Mail van de belastingdienst

- Al haar gegevens kwijt
- Bijzondere persoonsgegevens
- Boete van autoriteit persoonsgegevens
- Failliet

Iedereen kan slachtoffer worden van cybercriminaliteit!

5 basisprincipes van veilig digitaal ondernemen

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en malware

1. Inventariseer je kwetsbaarheden

Algemeen belang

- Inventarisatie kroonjuwelen
- Wie is er in jouw organisatie verantwoordelijk voor back-ups? Staat dat ergens zwart op wit?

- Als je niet weet wat je hebt, kan je het ook niet beveiligen

To do: Maak een risicoanalyse of inventarisatie. Bespreek verantwoordelijkheden en leg afspraken vast.

1. Inventariseer je kwetsbaarheden

Help! Ik ben gehackt!

- Wat nu?
- Hebben jullie een incident responsplan? Digitaal of fysiek?
- En back-ups? Doen die het ook?

“Autoverhuurbedrijf dagen lang stil door hack: incident responsplan ook versleuteld”

To do: Maak een calamiteitenplan en plan voor back-ups (patchbeleid). Bewaar deze goed!

Jouw gegevens zijn belangrijk voor jou en je bedrijfsvoering.

60% van de mkb’ers gaat na een hack binnen 6 maanden failliet.

PVO / Midden-Nederland

2. Kies veilige instellingen

Alles wat met het internet verbonden staat is te hacken

- Werken jouw medewerkers hybride?
- Hoe is het gesteld met de Wi-Fi thuis?

- Welke apparaten op kantoor staan verbonden met het internet?

“23 jarige jongeman uit Nederland hackt printers van universiteit in Amerika”

2. Kies veilige instellingen

Digitale poortwachter

- Wat is een firewall?
- Wat is loginformatie?

- Voorkomt ongeautoriseerde toegang
- Detecteert ongebruikelijke activiteit

To do: Vraag je systeembeheerder of IT-leverancier hoe en waar jouw loginformatie is opgeslagen? En of je een firewall hebt.

3. Voer updates uit

Stop met wachten tot vrijdagmiddag

- Wie stelt wel eens een update uit?

Bij updates lossen systemen kwetsbaarheden op in de software: ze verbeteren de sloten van openstaande deuren

3. Voer updates uit

Installeer ook de patches!

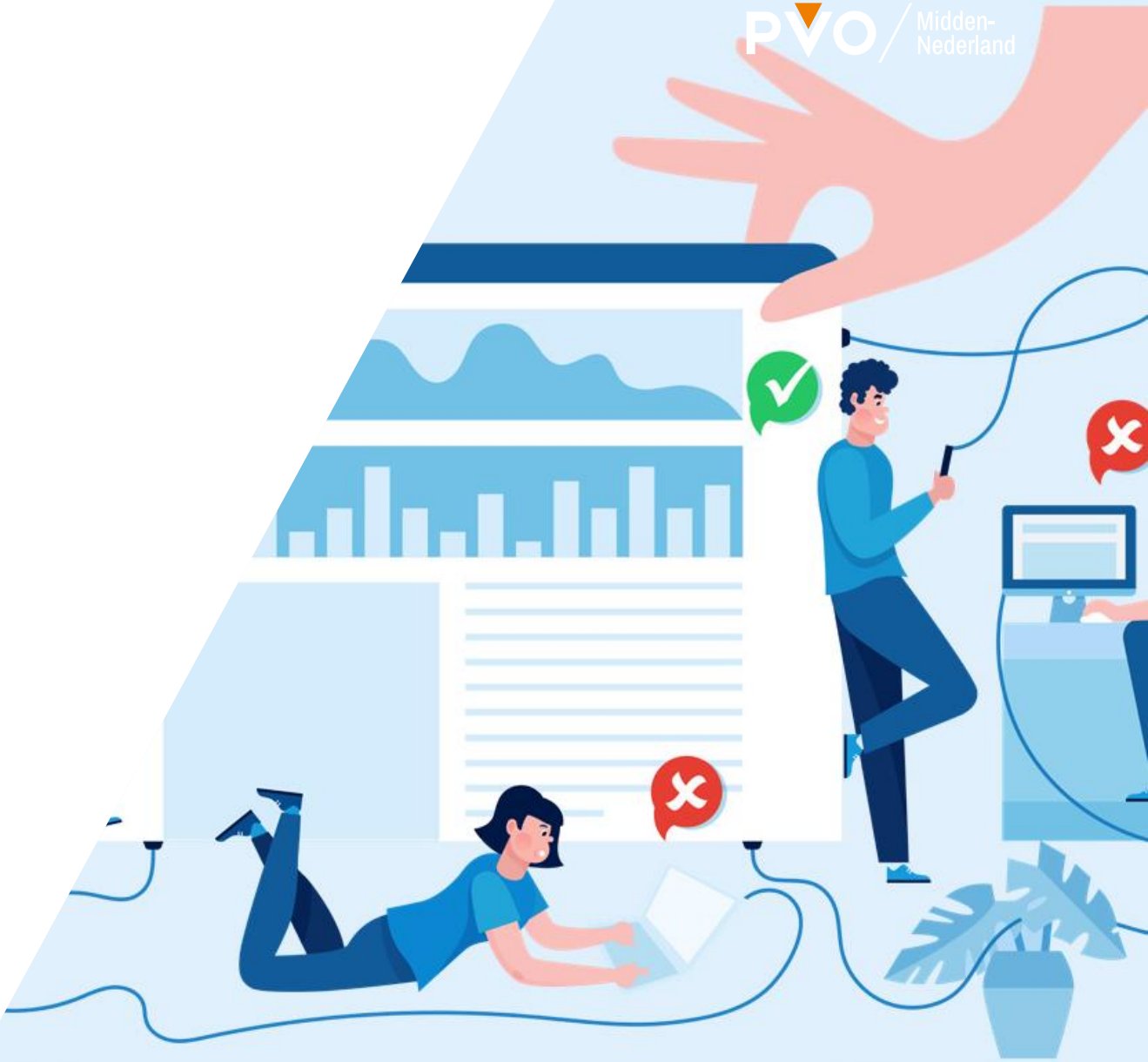
- Patches zijn letterlijk pleisters, kleine tussentijdse updates die worden gebruikt om kleine fouten te verbeteren
- Zijn de updates centraal geregeld of is de medewerker zelf verantwoordelijk?

To do: voer updates direct uit, zet automatisch updaten aan en bespreek de afspraken over updaten intern.

4. Beperk toegang

“U heeft geen toegangsrechten voor deze pagina”

- Hebben al jouw medewerkers dezelfde toegangsrechten?
- Wees kritisch op wie je welke rechten geeft
- Wat is het beleid als iemand stopt met werken?



4. Beperk toegang

“Welkom123”

- Hoeveel tekens is jullie wachtwoord?

- Dictionary attack, brute force, social engineering
- Zorg voor minimaal 18 tekens: wachtwoordzinnen
- Gebruik niet dezelfde wachtwoorden (passwordmanager)

Cybercriminelen zullen in geen 100 jaar mijn wachtwoord hacken!

5. Voorkom virussen en andere malware

Vormen

- **Virussen**
  - Trojan
  - Worm
- **Malware**
  - Ransomware

5. Voorkom virussen en andere malware

Bescherm je tegen virussen

- **Gedrag:** human factor en vergroot bewustwording
- **Techniek:** antivirusprogramma
- **Organisatie:** beperk installatiemogelijkheden apps en denk na over processen

To do: biedt cyberawareness aan voor je medewerkers, beperk installatiemogelijkheid van apps, inventariseer of en welk antivirusprogramma je hebt.

Cyberawareness

1 klik verwijderd van een cyberaanval

- Train / test jezelf en je personeel
- Neem het op als terugkerend onderwerp in interne meetings
- Neem het op in onboardingsproces
- Pas kracht van herhaling toe

In **80%** gevallen veroorzaakt menselijk handelen…

Iedereen kan slachtoffer worden van cybercriminaliteit!

5 basisprincipes van veilig digitaal ondernemen

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en malware

Wat ga je morgenochtend doen?

- Maak een back-up van je belangrijkste bestanden
- Stel Multi Factor Authentication (MFA) in
- Zet automatische updates aan
- Controleer de beveiligingsstandaarden van je e-mail
- Leer phishing herkennen (phishingbingo)
- Print een bellijst voor noodsituaties
- Plan een gesprek in met je IT-leverancier

Geef je cyberweerbaarheid een update…

PVO Midden-Nederland

Schaam je niet…

- Criminelen zetten in op emotie, stress, vertrouwen en kwetsbaarheid.
- Stress is een slechte raadgever: je hoofd stopt met nadenken.

Verifieer alles, neem een bekende in vertrouwen

Dan nu..

- Einde van het inhoudelijke programma
- Ernst Jan zal een rondleiding geven door het pand
- Vergeet de goodiebag niet als je naar huis gaat!
- Informatie over de quickscan van Tozetta in de goodiebag
- Vanuit het Platform Veilig Ondernemen Midden-Nederland lopen er mensen rond met wat vragen

- Jullie ontvangen nog een e-mail met daarin een samenvatting van de avond en alle tips en tricks op een rijtje

Afsluiting