



Cybersecurity

Dirk Tielens



Samen leren en groeien





Agenda

- 01 Waarom moet ik mij beschermen?
- 02 Wat kan er fout gaan?
- 03 Hoe bescherm ik mij tegen de gevaren?

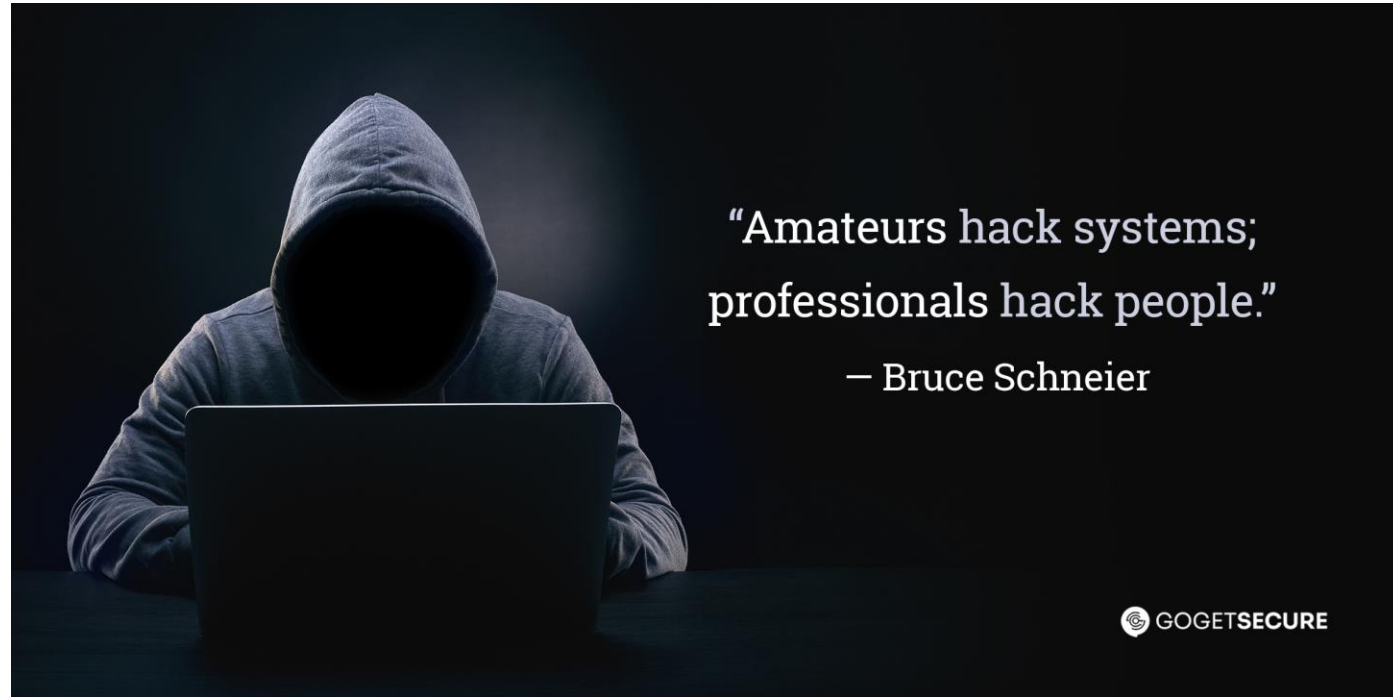


Waarom moet mij
beschermen?



Waarom moet ik mij beschermen?

- **Amateurs hacken systemen:** Ze richten zich op het binnendringen van computersystemen zonder veel diepgaand inzicht.
- **Professionals hacken mensen:** Ze gebruiken sociale manipulatie en psychologische tactieken om toegang te krijgen tot systemen.



“Amateurs hack systems;
professionals hack people.”

– Bruce Schneier

Waarom moet ik mij beschermen?

- Meer en meer data staat in de cloud
 - Interessant voor de eindgebruiker want die kan van overal aan zijn/haar data
 - Ook interessant voor de hacker want ook die kan van overal aan de data van de gebruiker
- We delen, al dan niet bewust, veel van onszelf (sociale media). Voor hackers is dit interessante info.



Waarom moet ik mij beschermen?

- 95% van alle cyberincidenten wordt veroorzaakt door menselijke fouten
- Phishing → AI gaat belangrijke rol spelen
- Zwakke wachtwoorden
- Verlies van apparaten
- Onvoldoende kennis
- Onveilig gebruik van openbare Wifi-netwerken
- ...



Waarom moet ik mij beschermen?

>> Concreet voorbeeld

>> Microsoft 365 schooltenant

>> 2800 leerlingen

>> 580 personeelsleden

>> Totaal: 3380 gebruikers

>> Log van mislukte inlogpogingen gedurende 5 minuten

>> 9u17 tot 9u22 op 20/5/24 - Pinkstermaandag



Microsoft 365

Waarom moet ik mij beschermen?

- Resultaat (Scantime 5 min – 3380 accounts)
 - 9797 mislukte inlogpogingen
 - Aantal getroffen accounts: 41
 - Hoogste aantal pogingen op 1 account: 1217
 - Aantal accounts met meer dan 1000 mislukte pogingen: 6 (5 personeelsleden, 1 directielid)
 - Aantal verschillende landen waaruit de pogingen kwamen: 108
 - Landen waaruit de meeste pogingen kwamen: China (3417), Zuid-Korea (994), USA (927), Hong Kong (566), VAE (531), ...





Wat kan er fout
gaan?



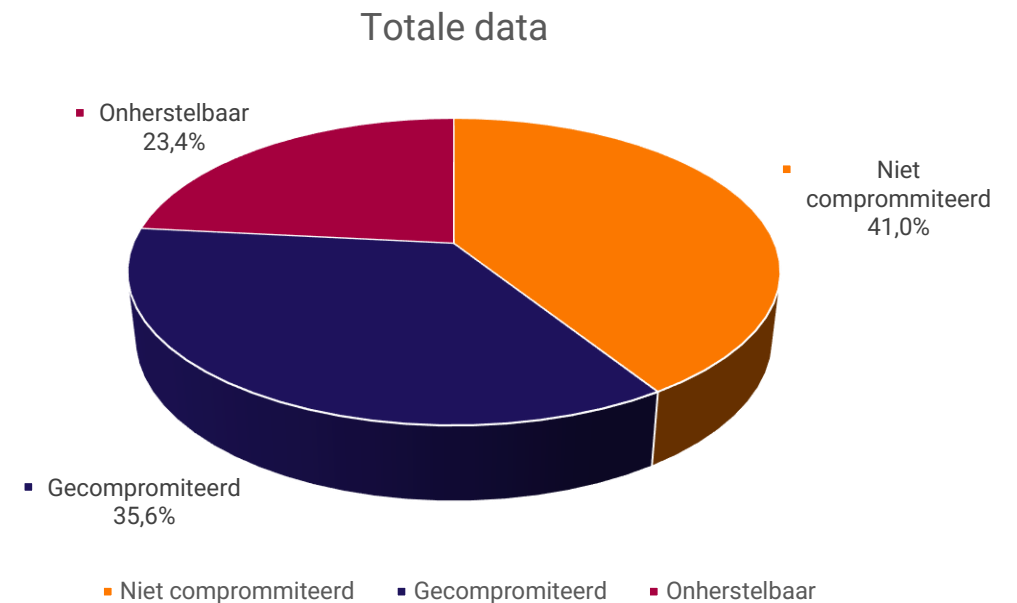
Wat kan er fout gaan?

- Verlies van data → **Ransomware**
- Ransomware: data versleutelen, sleutel in ruil voor losgeld
- Bekenste voorbeelden
 - Stad Antwerpen, Diest, Zwijndrecht
 - Duvel
 - ...



Wat kan er fout gaan?

- Veeam (backup software) organiseerde een enquête onder 12000 respondenten die slachtoffer werden van een cyberaanval.
- Daaruit blijkt dat 41% van de data bij aanvallen gecompromitteerd of versleuteld wordt en maar 57% hersteld kan worden.
- Enkele andere harde cijfers uit het onderzoek:
 - 81% van de getroffen bedrijven betaalde losgeld om data terug te krijgen
 - 1 op 3 slachtoffers kon hun data niet herstellen, zelfs na betaling



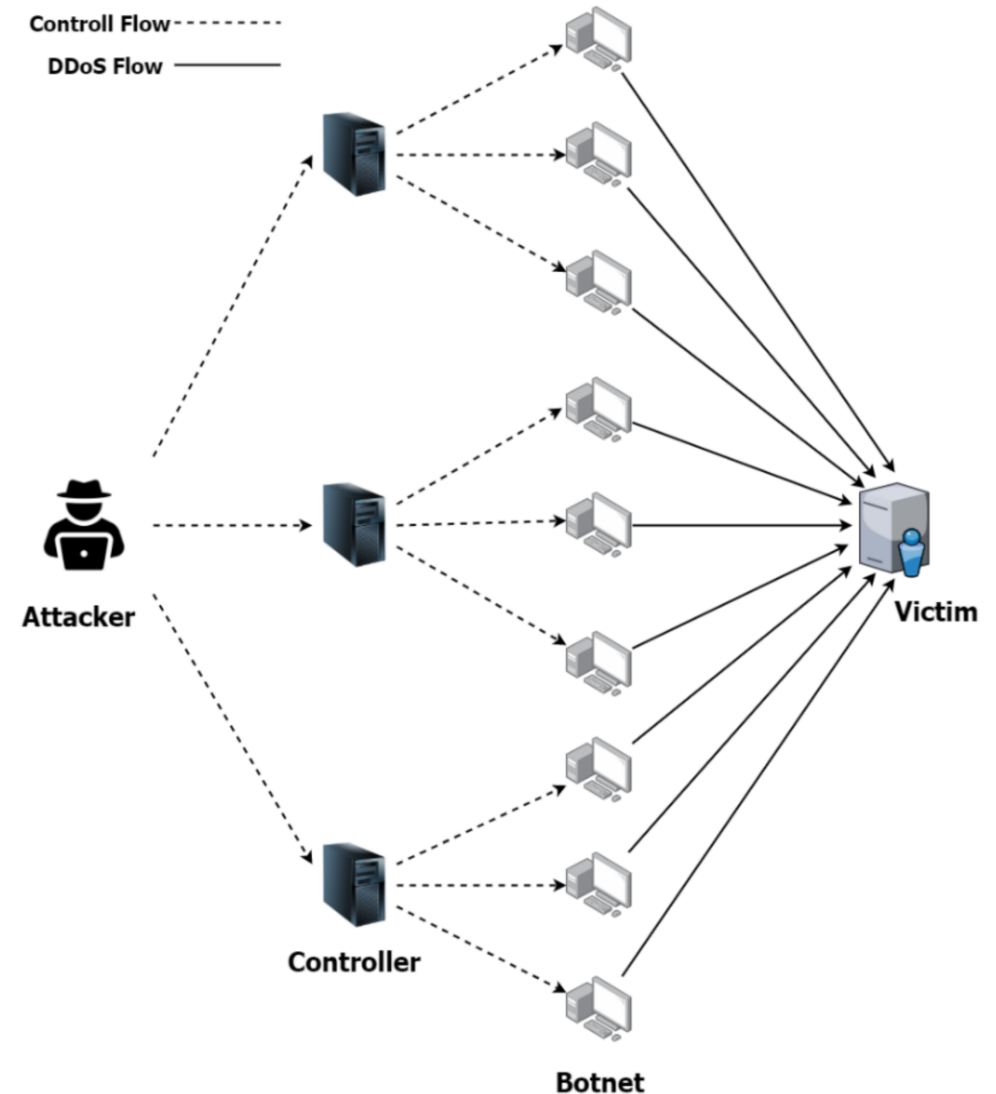
Wat kan er fout gaan?

- Ongeoorloofde verspreiding/toegang van data → **Phishing**
- **Phishing** = het “hengelen, vissen” naar gegevens
- **IA** gaat hier een belangrijke rol spelen
 - Stemmen nabootsen van ipv whatsapp berichten te sturen
 - Deep fake video's
 - Polyforme Malware: Malware die zichzelf “herschrijft” zodat het moeilijker wordt om te detecteren. De malware muteert als het ware zichzelf.



Wat kan er fout gaan?

- Lam leggen van systemen → **DDoS**
- Hacker stuurt ontzettend veel data naar zijn slachtoffer zodat zijn systeem onderuit gaat.
- Vaak worden besmette computers als “hulpje” ingezet (zgn. botnets)
- Zeer eenvoudig uit te voeren. Wordt vaak gedaan door “script kiddies”. Jonge kinderen/pubers die zich vervelen. Scholen hebben hier regelmatig last van.
- Bescherming hiertegen kan maar is behoorlijk duur



Wat kan er fout gaan?

- »» Insider threats (gevaren van binnenuit)
→ vb: **rancuneuze werknemer**
- »» Insider threats worden vaak vergeten
 - »» Vb: account van werknemer die niet wordt afgesloten na ontslag/vertrek
 - »» Medewerker die data openbaar deelt ipv met specifieke mensen ...
 - »» Tip: Vermijd gedeelde accounts / wachtwoorden





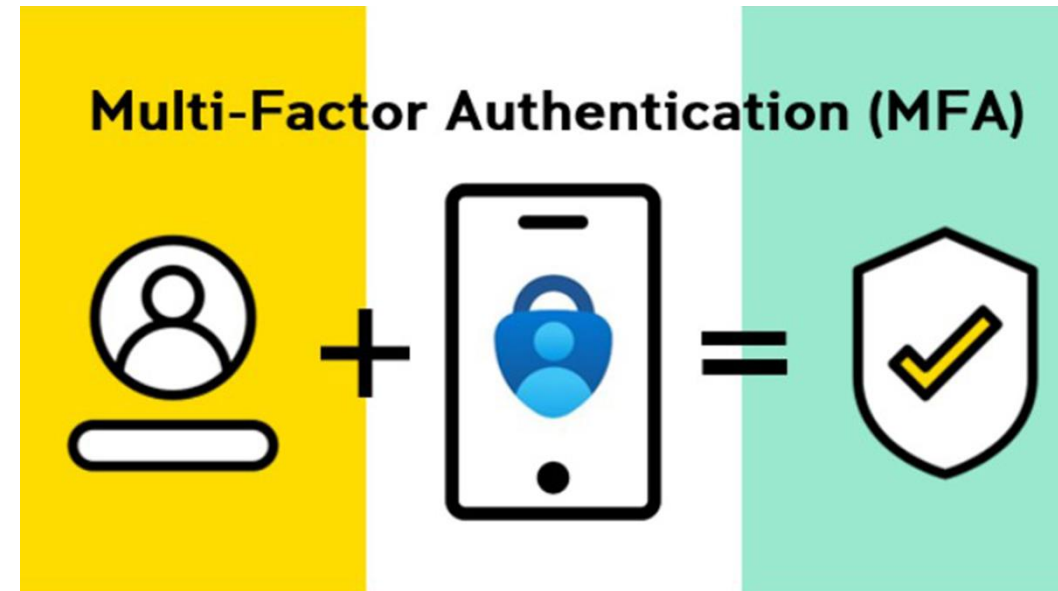
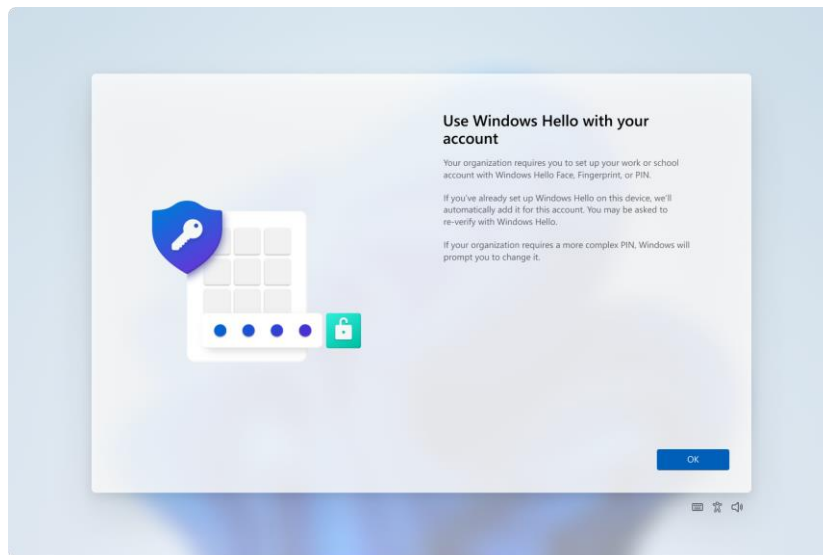
Hoe bescherm ik mij
tegen de gevaren?



Hoe bescherm ik mij tegen de gevaren?

>> MFA

- >> Microsoft Authenticator
- >> Google Authenticator
- >> SMS / Telefoon
- >> Windows Hello for Business



Hoe bescherm ik mij tegen de gevaren?

- Goede wachtwoordmanager
 - Lastpass, 1Password, Bitwarden, Keepass
 - Gebruik voor elke site een uniek, voldoende complex paswoord



Hoe bescherm ik mij tegen de gevaren?

- Gezond boerenverstand (herkennen van bv phishingmails)
 - Goede test: <https://safeonweb.be/>

DOE DE
Phishingtest
Herken jij verdachte berichten op tijd?

1 ONGELEZEN BERICHT

VANDAAG

250 Eur te winnen bij Delhaize via WhatsApp: Kijk: <http://delhaize-be.site> waardebonnen van €250 van Delhaize. Ze vieren hun verjaardag. Ik denk dat de aanbieding beperkt is. Ik heb de mijne al geclaimd. ❤️ 13:17

type a message

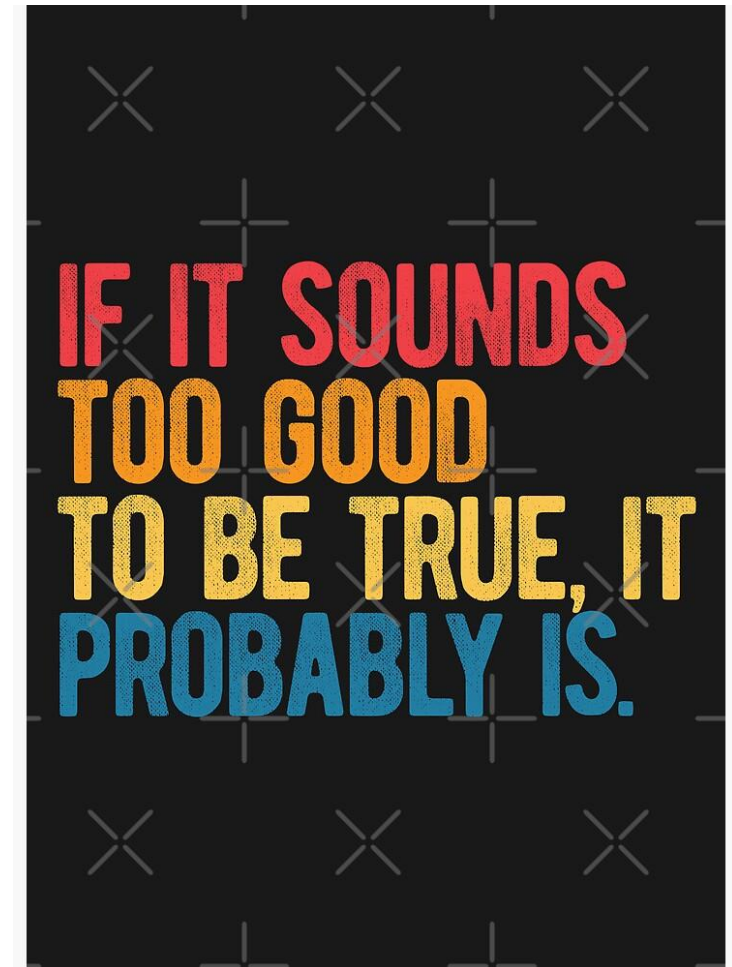
Promo Delhaize Vraag 1/6

Wat is er verdacht aan dit bericht? (meerdere antwoorden mogelijk)

- Het tijdstip van het bericht.
- De link naar de website (<http://delhaize-be.site>).
- Een promocampagne voor de verjaardag van Delhaize.
- Delhaize stuurt deze promo via Instant Messaging.
- Er staat een hartje aan het einde van het bericht.
- De promo is te mooi om waar te zijn.

Controleer

Safeonweb™



Hoe bescherm ik mij tegen de gevaren?

- » IT-gerichte hulpmiddelen
 - » Updates
 - » Antivirus
 - » Firewall
 - » ...



Ben ik zelf ooit gehackt?

- >> <https://haveibeenpwned.com/>
- >> Check je mailadres en/of paswoord in een gehackte database zit
- >> Meest gebruikte paswoord: “123456” (42542807 keer)
- >> Als je email of paswoord gevonden wordt → paswoord aanpassen

Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

..... pwned?

Oh no — pwned!

This password has been seen 42,542,807 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

 3 Steps to better security

[Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

    Donate

Internet connection monitoring

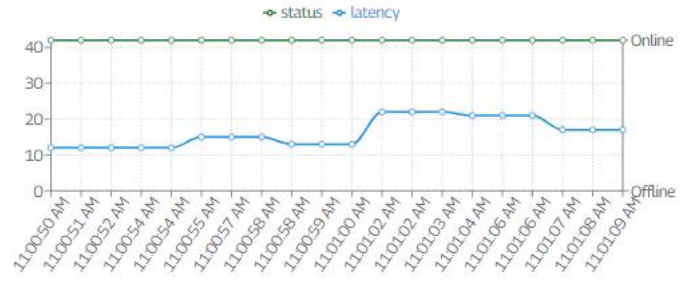
Print or Export to PDF | Reset realtime stats | [Connection log](#) | [Connection stats](#)

General stats

	Today	7 days	30 days	All time
Disconnects	0	0	0	0
Availability	100.00%	100.00%	100.00%	100.00%
Downtime	0	0	0	0

Now: 06/26/2024 11:01:09 AM
 Your IP:
 Online for: 0:02:57
 Latency: 17 ms

Realtime graph



Realtime data

Newer events are at the top. MAX log recording time: 3 hours. [Ping source setting request](#)

Date and time	Status	Latency	Ping source
06/26/2024 11:01:09 AM	Online	17 ms	google.com
06/26/2024 11:01:08 AM	Online	17 ms	google.com
06/26/2024 11:01:07 AM	Online	17 ms	google.com
06/26/2024 11:01:06 AM	Online	21 ms	google.com
06/26/2024 11:01:06 AM	Online	21 ms	google.com
06/26/2024 11:01:04 AM	Online	21 ms	google.com
06/26/2024 11:01:03 AM	Online	22 ms	google.com
06/26/2024 11:01:02 AM	Online	22 ms	google.com
06/26/2024 11:01:02 AM	Online	22 ms	google.com
06/26/2024 11:01:00 AM	Online	13 ms	google.com
06/26/2024 11:00:59 AM	Online	13 ms	google.com

STRESSER.ZONE

30

Method - Documentation

→ DNS | > ADVANCED PARAMETERS

SEND ATTACK | SCHEDULE

Manage attacks in progress | STOP ALL ATTACKS

HOST	PORT	REMANING TIME	METHOD	ACTION