Novel T

CYBERSECURITY IN DE ZORG

WIE, WAT, WAAROM en HOE?

28 juni 2022

UNIVERSITY OF TWENTE. SAXION provincie Overijssel Gemeente Enschede regio Twente

SAXION
UNIVERSITY OF APPLIED SCIENCES

Hack_Right

IT visibility
we make it run like clockwork

Centrum voor Veiligheid en Digitalisering
Centrum voor Veiligheid en Digitalisering is een kenniscentrum voor en van ondernemers en publieke instellingen.
Information Technology & Services · Apeldoorn · 800 followers
Niki works here · 1 employee
✓ Following | Learn more | More
Home | About | Posts | Jobs | People | Events | Videos

FME

▲ Liesbeth Holterman, manager van de cybersecurity hub van Novel-T. © Frans Nikkels Fotografie

Treurig gesteld met cyberveiligheid in Twentse maakindustrie

ENSCHEDE - Vrijwel geen van de veertig Twentse maakbedrijven die meededen aan een vrijwillige check, heeft de cybersecurity op orde. Af en

CYBERVEILIG NEDERLAND

Novel T

NEDERLAND ICT
VOOR DE DIGITALE ECONOMIE

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

deVolkskrant

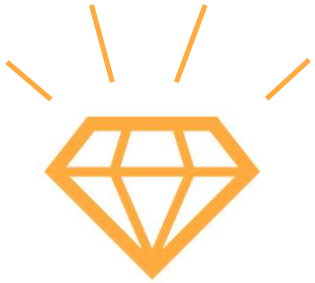
Volgens Liesbeth Holterman van Cyberveilig Nederland, een brancheorganisatie van cybersecuritybedrijven en betrokken bij het initiatief, zijn bedrijven de afgelopen maanden slachtoffer geworden van een cyberaanval die voorkomen had kunnen worden als bekend was dat hun IP-adres of andere indicator was gecompromitteerd. Holterman: 'Het NCSC deelt nu vanuit de wettelijke taak alleen risico en dreigingsinformatie met bedrijven die tot de doelgroep horen, daar gaat het mis.'

Het platleggen van transportbedrijf Bakker Logistiek, waardoor er geen kaas in winkels van Albert Heijn lag, was bijvoorbeeld het gevolg van een kwetsbaarheid in Microsoft Exchange die al langer bekend was.

Den Haag

ORGANISATIE

1



Kroonjuwelen in kaart

2

Risicomanagement

3

Beleid en proces

Beschikbaarheid
(hoe erg is het dat een systeem het niet meer doet?)

Integriteit
(hoe erg is het dat bepaalde gegevens niet juist zijn?)

Betrouwbaarheid
(hoe erg is het dat gegevens naar buiten lekken?)

Kans \ Impact	niet merkbaar	klein	gemiddeld	groot	desastreus
dagelijks	gemiddeld	hoog	hoog	kritiek	kritiek
wekelijks	gemiddeld	gemiddeld	hoog	kritiek	kritiek
maandelijks	laag	gemiddeld	hoog	hoog	kritiek
jaarlijks	laag	gemiddeld	gemiddeld	hoog	hoog
> jaarlijks	laag	laag	gemiddeld	gemiddeld	hoog

Cybersecurity Dreigingsbeeld Zorg 2021

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

ZZ CERT

Inhoud

Potential impact on society

Insiders

Disruptie, informatie diefstal

Script kiddies

Disruptie, informatie diefstal

Hacktivisten

Disruptie, informatie manipulatie

Statelijke actoren

Spionage, disruptie, informatie diefstal

Criminelen

Disruptie, informatie diefstal

Terroristen

Sabotage

Note:Towards a new cyber threat actor typology – Van Eeten, Hernández Gañán en Pieters

AFSPRAKEN MET JE IT

https://www.digitaltrustcenter.nl/gesprek-met-it-dienstverlener

TECHNIEK

Er zijn veel informatieve kennisproducten (zie bijv. https://www.ncsc.nl/documenten en https://www.digitaltrustcenter.nl/informatie-advies)
Cybersecuritybedrijven kunnen passend advies geven over benodigde maatregelen

BRON:
file:///C:/Users/liesb/Downloads/NCSC+Cybersecuritymaatregelen+def.pdf

MENS

1

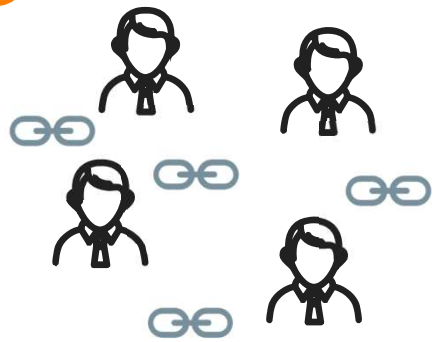
☺ ☺ ☺

Positieve cultuur

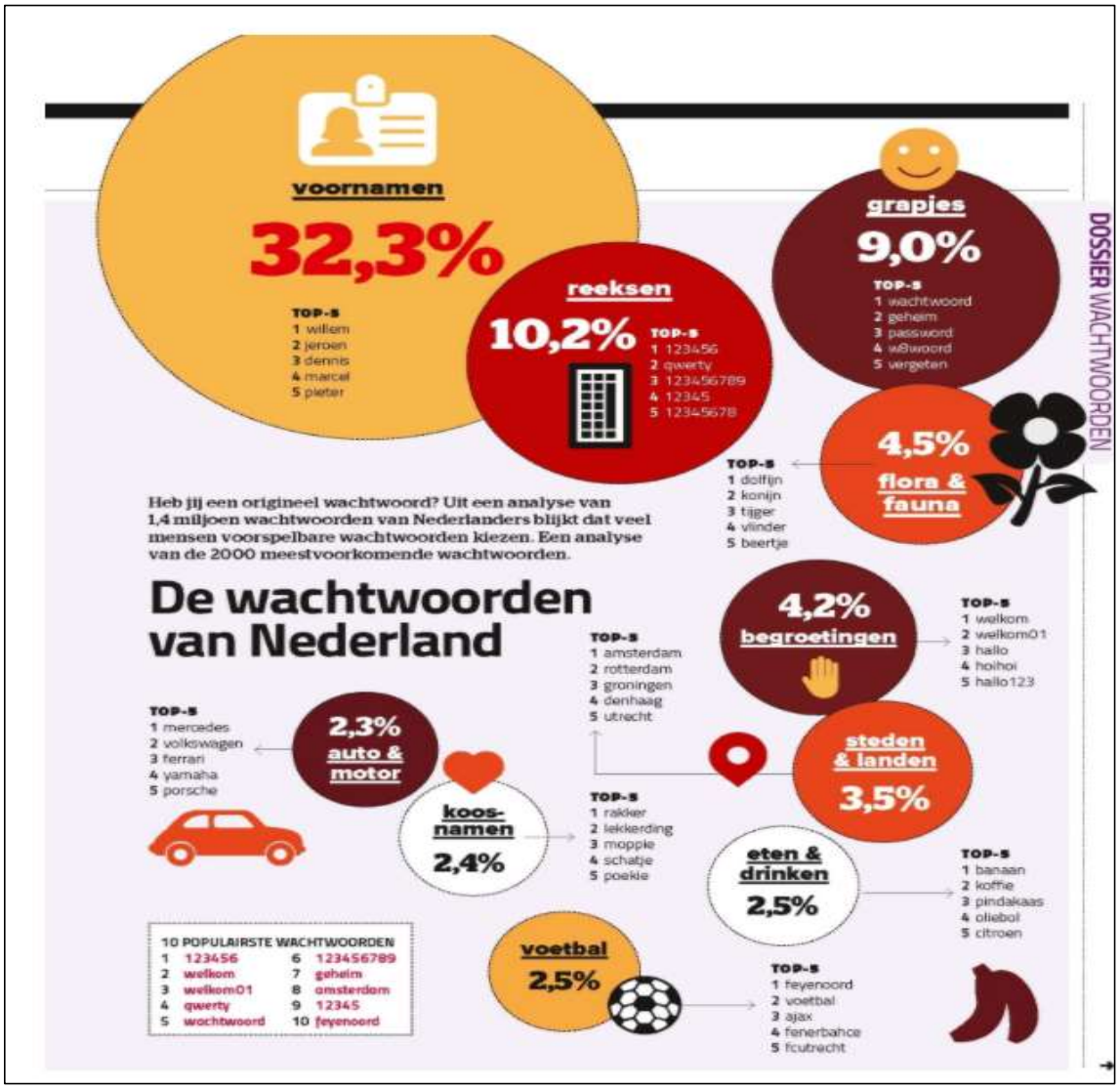
2

Awareness

3



Trainen crisis



Novel T

SAXION UNIVERSITY OF APPLIED SCIENCES

Beantwoord de volgende vragen

1 Hoe lang is jouw wachtwoord? (Tel alle letters, cijfers en/of andere tekens op.)

‹ › 5 karakters

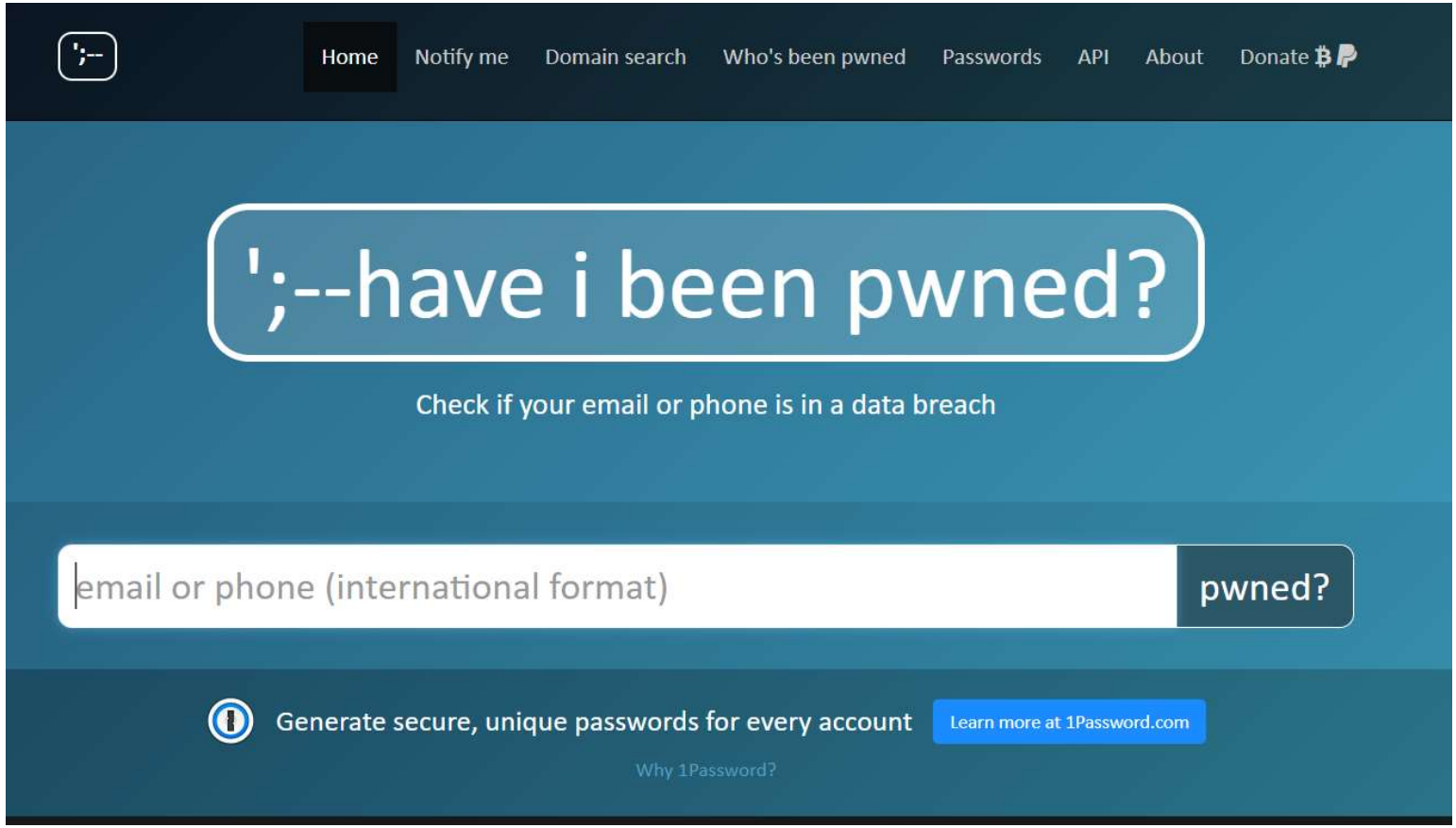
2 Welke karakters staan er in jouw wachtwoord? (Meer opties mogelijk.)

- ☐ Kleine letters (a-z)
- ☐ Hoofdletters (A-Z)
- ☐ Cijfers (0-9)
- ☐ Speciaal (#,&,!)

OMG! Directe hack! Jouw wachtwoord is in 1 minuut gekraakt!

Je loopt gevaar! Met een veel te kort wachtwoord ben je direct te hacken en liggen je persoonlijke bestanden, bank- en inloggegevens in feite op straat…Je wachtwoord moet echt veel langer, minimaal 12 karakters, liefst nog langer.

https://veiliginternetten.nl/wachtwoordkraak-test/



https://haveibeenpwned.com/

AANDACHTSPUNTEN...

Gebaseerd op de uitvoering van ongeveer 75 cybersecurity scans bij bedrijven in Overijssel (variërend tussen 12 en 200 FTE)

- IT-beheer vaak uitbesteed, maar zonder afspraken
- Geen rollen en verantwoordelijkheden vastgesteld
- Patchen (updaten) blijft aandachtspunt
- Back-up (ook productie-omgeving) wordt vaak vergeten
- Digitalisering productieomgeving in de kinderschoenen
- Weinig afspraken in de supply-chain
- Geen 2-factor authenticatie ingesteld

NovelT

CALL TO ACTION

- Deel ervaringen met elkaar. Een incident kan grote impact hebben
- Denk na over je kritische assets en neem maatregelen
- Weet waar je afhankelijkheden in de keten zitten: maak afspraken
- Zorg dat iedereen in en buiten de organisatie weet wie waarvoor verantwoordelijk is
- Train je medewerkers

Novel T

VRAGEN, OPMERKINGEN, SUGGESTIES?

Liesbeth Holterman
E-mail: l.holterman@novelt.com
Website: novelt.com/cybersecurity
Tel: +31(0)6 36 26 89 57

Henk van Ee
E-mail: h.m.vanee@saxion.nl
Website: saxion.nl
Tel: +31(0)6 22 67 48 04