
HACKERSPACE
DRENTHE
INTERNETVEILIGHEID

Internetveiligheid

Door Rein Velt (rein@velt.org) voor de presentatie op 8 april 2025 in Hackerspace Emmen

Disclaimer: Het geven van presentaties is niet mijn hobby of werk. Maar ik doe mijn best.

Onderwerpen

Inleiding

Wat zijn de meest voorkomende risico's ?

Phishing en datalekken grootste bedreiging - https://www.bsi.bund.de/DE/Service-Navi/Publikationen/DVS-Bericht/dvs-bericht_node.html

- Diefstal en misbruik van persoonlijke gegevens: gebruikersnaam, email, wachtwoord, creditcard-info, BSN, telefoon, persoonlijke info
- Geen toegang meer tot je eigen email-account/Google/Facebook/Instagram
- Misbruik van je creditcard/bankrekening
- Misbruik van je foto's (cyberpesten)
- Misbruik van je computer (virussen,botnets)

Meestal gaat het om diefstal van identiteit, gegevens (geld)

Wat kan ik daar tegen doen?

1. Gebruik sterke, unieke wachtwoorden en multi-factor authenticatie (MFA)
2. Houd software en apparaten up-to-date
3. Wees voorzichtig met het klikken op links of het downloaden van bijlagen. (CHECK DE BRON)
4. Gebruik antivirussoftware en een firewall.
5. Geen openbare Wi-Fi (of neem een VPN)
6. Maak regelmatig extra back-ups van belangrijke/persoonlijke gegevens

Hoe komen hackers aan je gegevens?

Datalekken

- Datalek: Hof van Twente besmet door ransomware
- https://tweakers.net/nieuws/233220/mailinglijst-blog-have-i-been-pwned-oprichter-gelekt-door-phishingmail.html
- Phishing aanval op klanten van creditcard
- https://haveibeenpwned.com/

Brute force attacks

Cyber criminelen gebruiken jouw gegevens uit datalek en gaan dan automatisch wachtwoorden raden.

Daarom is het ook belangrijk om een goed wachtwoord te kiezen! *

Phishing

Cyber criminelen gebruiken gegevens uit datalek en vragen jou om aanvullende informatie.

- Email spam
- Fake websites
- Nep login-schermen
- Nep betaal-sites

** We gaan hier later verder op in met voorbeelden*

Wachtwoorden

Test wachtwoordkraken

Hoe veilig is jouw wachtwoord?

https://veiliginternetten.nl/wachtwoordkraaktest/

De meest gebruikte wachtwoorden in 2024

- 123456 (10,37%)
- 123456789 (3,49%)
- 12345678 (1,94%)
- password (1,85%)
- qwerty (0,95%)
- adobe123 (0,91%)
- 1234567 (0,69%)
- 111111 (0,67%)
- 12345 (0,61%)
- 1234567890 (0,51%)

Moeilijke wachtwoorden en PassPhrases

- ~~admin~~ (0.03 seconden)
- ~~4e7dfG!@~~ (7 dagen)
- ~~WoordenboekWoorden~~ (30 dagen)
- MoeillijkWachttwooord007$#^& (5 *10^12 jaar)
- 2Sch3l3Ol!fant3nOntsn4pt!n020#@! 9*10^18 jaar)

HACKERSPACE DRENTHE

Langer is beter

Langer is meestal beter, maar zorg voor altijd voor afwisseling met nummers, accenten, symbolen, tekens, hoofd- en kleine letters. Wees creatief.

Tekens	Mogelijke combinaties	Tijd nodig
1	62	<1 seconde
2	3.844	<1 seconde
3	238.328	<1 seconde
4	14.776.336	< 1 seconde
5	916.132.832	42 seconden
6	56.800.235.584	43 minuten
7	3.521.614.606.208	44 uur
8	218.340.105.584.896	115 dagen
9	13.537.086.546.263.600	20 jaren
10	839.299.365.868.340.000	12 eeuwen
11	52.036.560.683.837.100.000	750 eeuwen
12	3.226.266.762.397.900.000.000	46500 eeuwen
Aantal mogelijke karakters: 62 (A-Z, a-z, 0-9) Aantal passwords per minuut +/- 22.000.000		

```
Mijn tante heeft een kat. Haar naam is Poekie. Poekie is wit en heeft
3.1415927 zwarte plekjes op haar rug. Eén vlekje heeft de vorm van een *.
Poekie is heel lief!
```

Omdat je dat niet allemaal wilt onthouden hebben we de **wachtwoord manager**!

HACKERSPACE DRENTHE

Wachtwoordmanagers

- Lange en ingewikkelde wachtwoorden zijn beter maar erg moeilijk te onthouden.
- Zeker als deze per site/login verschillend moeten zijn

Daarom is de wachtwoordmanager een handige tool:

- Door je browser (web)
- Met een app/programma (keeppass, lastpass)
- Wie vertrouw jij je wachtwoorden toe?

- Geen enkele wachtwoordmanager is 100% veilig
- maar meestal veiliger dan zonder wachtwoordmanager
- Kijk wat voor jou prettig werkt

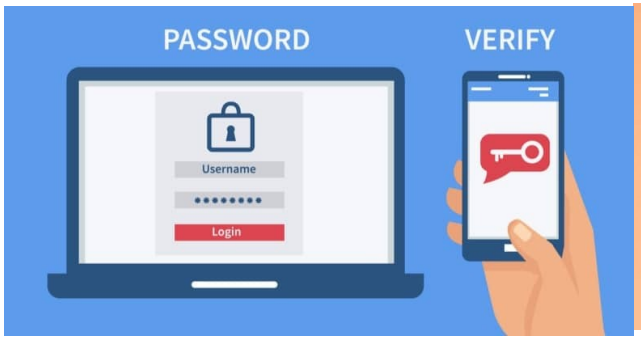
	Lastpass	KeePass	1Password	Dashlane	Passwordstate
Offline Mode	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓		✓	✓
Browser Integration	✓	✓	✓	✓	✓
Password Capture	✓			✓	✓
Password Changes	✓			✓	✓
Security Alert	✓		✓	✓	
Portable Application	✓	✓		✓	
Mobile Application	✓		✓	✓	✓
Security Audits	✓		✓	✓	✓
Import	✓	✓	✓	✓	✓
Export	✓	✓	✓	✓	✓
Throwaway Passwords	✓		✓	✓	✓
Password Sharing	✓	✓	✓	✓	✓
Integrated Database	✓		✓	✓	✓

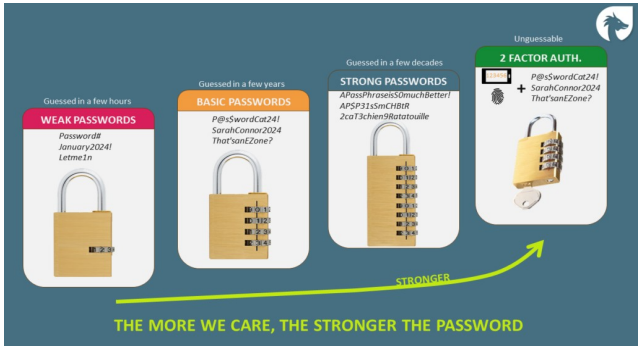
HACKERSPACE DRENTHE

Tweefactorauthenticatie/(2FA / MFA)

Bij tweefactorauthenticatie (2FA) of multifactor authenticatie is er een tweede veiligheidslaag (en soms zelfs een derde laag) voor toegang tot een applicatie. Bijvoorbeeld een extra pincode via een ander apparaat.

- Altijd aanzetten als het kan
- Met een app op je telefoon
- Met een electronische token
- https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=nl





Phishing en social engineering

Test Dontclick

https://dontclick.certifiedsecure.org/

Hoe phishing werkt

Voorbeeld 1: Brief van DIGI-D

In je brievenbus ligt een envelop met daarin een brief.

DigiD
Digitale Identificatie

DigiD
Postbus 96810
2509 JE Den Haag
www.digid.nl

Helpdesk DigiD
T 088 123 65 55
info@digid.nl

Openingstijden Helpdesk
Werkdagen: 08:00 - 22:00 uur
Zaterdagen: 09:00 - 17:00 uur

Datum: 04-03-2025
Betreft: Heractivering van uw DigiD- toegang

Geachte heer/mevrouw,

Om uw gegevens te beschermen, moet uw DigiD-toegang opnieuw worden geactiveerd. Dit is een standaard veiligheidsmaatregel om ongeautoriseerde toegang te voorkomen. Volg de instructies in de brief om uw toegang te herstellen.

Stappen om uw gegevens te bevestigen

1. ***Scan met uw mobiele apparaat de onderstaande QR-code en klik op de link die wordt weergegeven.***
   Deze link brengt u naar een beveiligde pagina waar u uw gegevens kunt bevestigen.

2. ***Volg de stappen die u op de pagina ziet.***
   De instructies zijn eenvoudig te volgen en helpen u bij het snel en veilig bevestigen van uw gegevens.

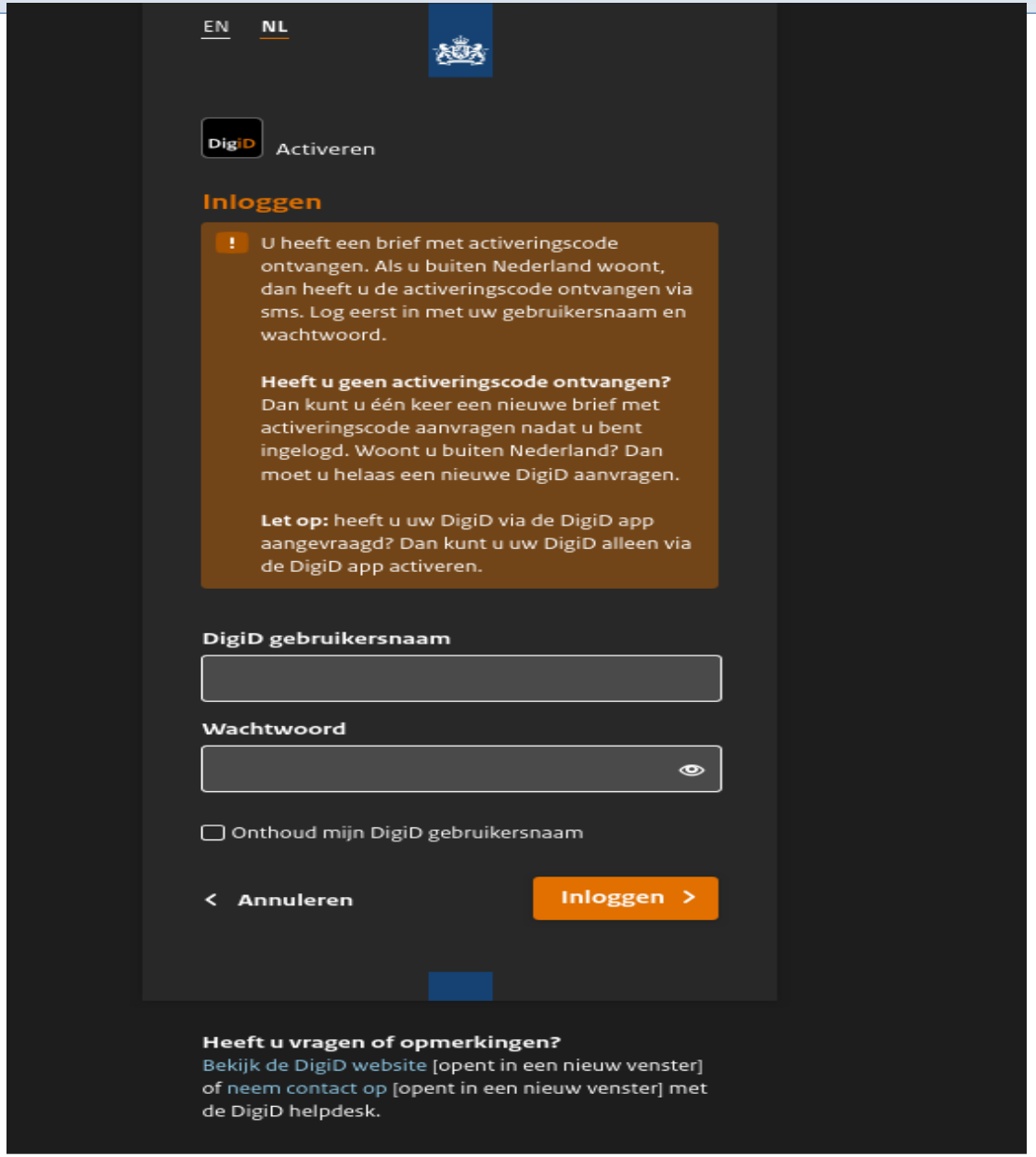
DigiD

Gegevensbevestiging afgerond
Nadat u alle stappen hebt voltooid, worden uw gegevens bevestigd. Indien alles correct is, kunt u zonder verdere onderbrekingen gebruik blijven maken van uw DigiD-account.

Met vriendelijke groet,

Dylan Kuijpers
Veiligheidsadviseur
DigiD, Den Haag

Je scan de QR code en gaat naar de website



Oplichting!

Meer phishing voorbeelden

Rabobank

NEP

Geachte heer/mevrouw,

Uw huidige Rabo Scanner voldoet niet meer aan de standaard eisen van de Rabobank en komt hierdoor binnenkort te vervallen.
We adviseren u om uw nieuwe Rabo Scanner **binnen** 2 werkdagen op te vragen om een blokkade te voorkomen.

Is uw scanner al geblokkeerd?
Dan kunt u in de tussentijd niet inloggen of betalen.

Kosten nieuwe scanner
Om uw nieuwe Rabo Scanner geheel kosteloos te ontvangen heeft u uiterst 2 dagen de tijd om de aanvraag in te dienen.
Dit kunt u doen door hier te klikken.
Na de genoemde datum brengen we 24,95 euro in rekening per Rabo Scanner.

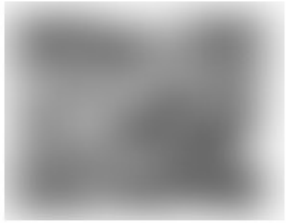
Uit mijn gmail spambox.

Belangrijke Update voor Uw Beveiliging

Geachte ,

Volgens onze administratie is uw e-mailadres (@) nog niet gekoppeld aan de nieuwste update van ons beveiligingssysteem. Sinds 1 maart 2025 maken wij gebruik van een verbeterd beveiligingsprotocol. Wij verzoeken u vriendelijk uw instellingen te actualiseren om de werking van uw account te optimaliseren.

U kunt de QR-code hieronder scannen om naar het beveiligingsportaal te gaan en de update door te voeren. Hier kunt u ook aangeven welke app u gebruikt, zodat we de juiste instellingen kunnen toepassen.



Het vernieuwde systeem verhoogt uw online veiligheid en biedt extra bescherming tegen ongeautoriseerde toegang. Voor extra gemak kunt u overwegen de ICS-app te installeren, waarmee u snel en veilig uw betalingen kunt goedkeuren.

Hartelijk dank voor uw medewerking. Heeft u nog vragen, dan helpen wij u graag verder.

Met vriendelijke groet,
ICS Services IT-Team

Speciale aanbieding van ANWB Veilig uw exclusieve korting op geselecteerde artikelen!

ANWB Noodpakket

Gefeliciteerd!

Je bent geselecteerd om de kans te krijgen om een gloednieuw product te krijgen

Auto Noodpakket

Neem slechts 2 minuten de tijd om onze korte enquête in te vullen en ontvang een exclusieve speciale korting op Medicare Kit!

Deze aanbieding is beperkt geldig en de voorraad is beperkt, dus wees er snel bij en profiteer van uw bod voordat het te laat is. Wees een van de weinigen die kunnen genieten van premiumkwaliteit voor een fractie van de prijs. Wees er snel bij, want de voorraad raakt snel op!

Ontvang uw cadeau met exclusieve korting!

Phishing via WhatsApp

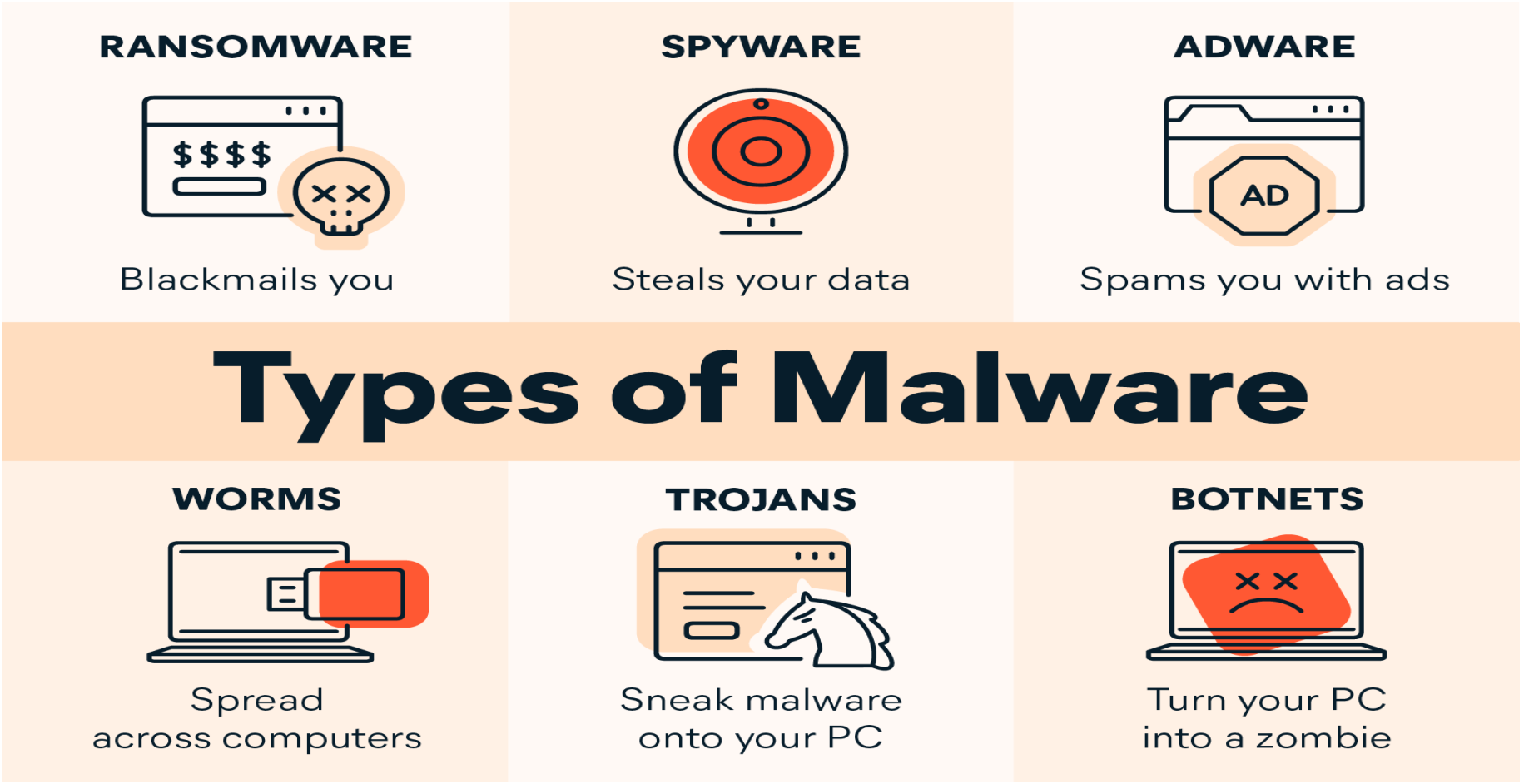
HACKERSPACE DRENTHE

Wat kun je doen tegen phishing?

- **Zero trust principe** = never trust, always verify
- Check de bron / domeinnaam / URL / SSL-slotje
- In geval van twijfel: zeg NEE
- KLIKKEN =BETALEN = BALEN
- Anderen nooit toegang geven tot je computer of smartphone
- Geef nooit je pincode of wachtwoord aan anderen
- Kijk goed uit waar je inlogt en of de site echt is.

- Bij schade: aangifte doen bij de politie en melding doen bij het bedrijf/instelling
- Cyber verzekeringen
- https://digihulp.nl (Digihulplijn: 0800-1508)

Spyware, virussen, trojans, worms,...



Spyware

Programma dat jou bespioneert en gegevens doorstuurt.

Meestal voor Windows/Internet Explorer

Spyware kopieert zich zelf meestal niet

Voorbeelden:

- Kazaa
- DivX (behalve voor de betaalde versies en de 'standaard'-versie zonder de encoder)
- eXeem™
- Morpheus
- Grokster
- Messenger Plus!
- BSPlayer (de gratis variant)
- KMSPico.

HACKERSPACE DRENTHE

Virus

Programma dat zichzelf kopieert **in een ander programma** en verspreid (eerste in 1970)

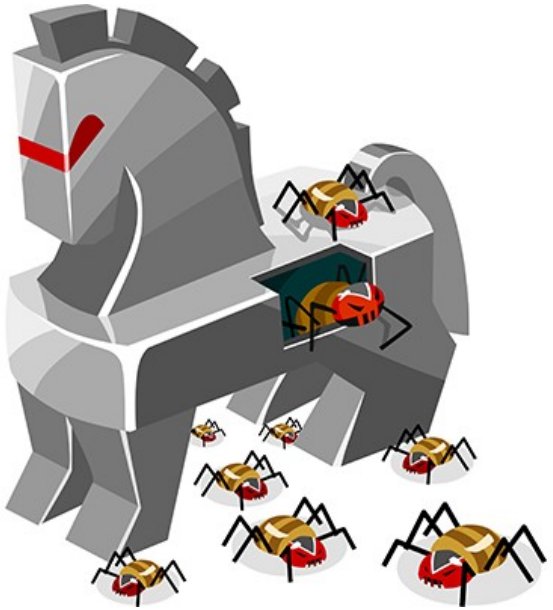
- Meestal voor MS-Windows (grootste doelgroep / veel oude versies / veel onervaren gebruikers / onbeschermde computers)
- Minder voor Mac en Linux

Voorbeelden van manieren waarop een virus in een computer kan doordringen zijn:

- Websites ,USB-sticks ,diskette , geheugenkaarten, cd-rom, dvd ,e-mail
- misbruik van bugs (vulnerabilities) in software
- Open netwerkpoorten en slechte wachtwoorden
- Windows Update (Flame./ Man-In-The-Middle en het gebruik van valse certificaten, die gegeneerd konden worden door zwakheden in het md5-algoritme.)

Trojan

Virus/mallware/spyware die binnen komt via een vermomming (paard van Troje)



Met een Trojaans paard wordt de pc opengezet voor andere gebruikers (cyber criminelen). Dit geeft hun de mogelijkheid om de hele computer over te nemen en alles af te luisteren en door te sturen:

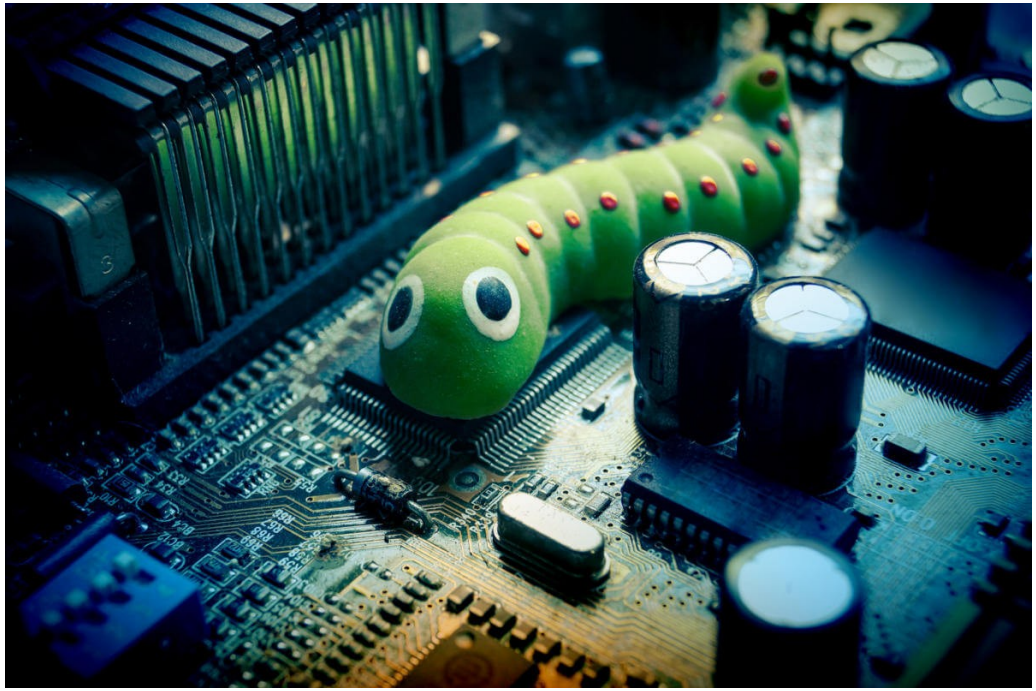
- Wachtwoorden en gebruiksnamen op het systeem te achterhalen.
- De harde schijf te gebruiken om bestanden te delen, wijzigen of verwijderen.
- De pc gebruiken in een DDoS-aanval (Distributed Denial of Service).
- Spammails te versturen vanaf de pc. Men noemt zo'n pc dan een spambot of zombie.
- Creditkaartnummers en bankgegevens te verzamelen.
- De computer lid maken van een zogenaamd botnet.

HACKERSPACE DRENTHE

Worm

Een soort virus dat zich snel verspreid en kopieert via (verschillende) computer protocollen en netwerken.

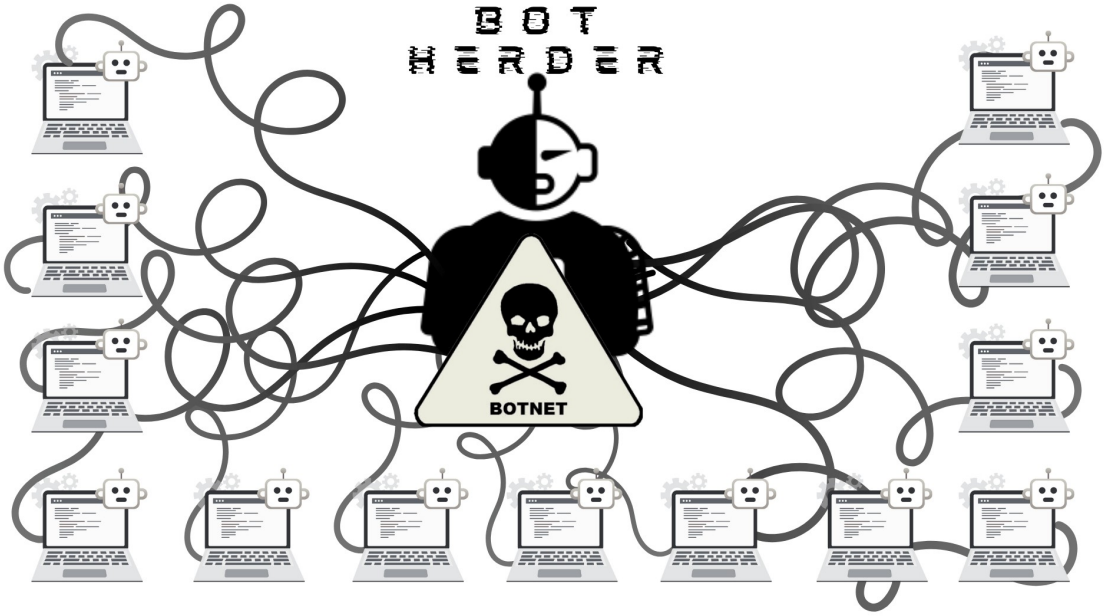
- Geen programma nodig om te verspreiden
- Probeert alle poorten en netwerk ingangen en maakt gebruik van aanwezige services
- Veel bandbreedte / traag netwerk.
- Gegevens verwijderen, aanpassen of ander malware binnen halen.



HACKERSPACE DRENTHE

Botnet

Een heleboel besmette computers die samen (als computer leger) ingezet kunnen worden voor criminele activiteiten. Deze worden vaak aangestuurd via een centrale computer.



Ransomware

Jouw computer wordt gegijzeld en alle bestanden worden gecodeerd. Tegen betaling van losgeld kunt u de decodeer-sleutel krijgen en anders bent u alles kwijt.

Wat kun je er tegen doen?

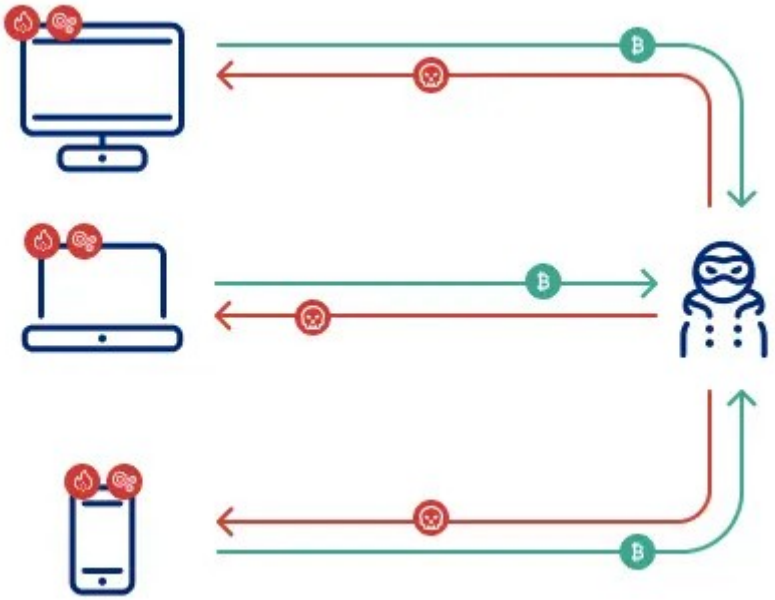
- Zorg dat je altijd meerdere goede backups hebt van belangrijke/persoonlijke/onvervangbare data .
- Software is meestal wel te herstellen door alles opnieuw te installeren.
- Installeer altijd software van de bron (fabrikant) en nooit via vage websites
- Sommige virusscanners kunnen ransomware detecteren

Wat kun je doen als het is gebeurt?

- Aangifte doen / melden
- Harde schijf formatteren, alles helemaal opnieuw (laten) installeren .

Cryptojacking

Jouw computer wordt stiekem gebruikt door anderen om bitcoins te minen. Dat kost veel stroom en maakt de computer langzaam.



Updaten en beveiligen van apparaten

HACKERSPACE DRENTHE

Test software updates

https://www.datalekt.nl/quizzen/quiz-updates-en-patch-management/

Beveiliging van apparaten

1. **Geef anderen geen toegang**
2. **Geen software installeren uit dubieuze bron,**
3. **Gebruik altijd een beveiligde verbinding (HTTPS/SSL/VPN)**
4. **Updaten van software en besturingssystemen is belangrijk!.**

Dus...

- Altijd afmelden/uitloggen als je weg gaat bij je computer (zie regel 1)
- Pas op met USB-sticks die je krijgt (zie regel 2)
- Zorg voor goede wachtwoorden (zie regel 1)
- Geef nooit je telefoon of laptop af als deze niet is gelocked (zie regel 1)
- Altijd VPN bij openbare WIFI (beveiligde gecodeerde verbinding, privacy)
- Belangrijke sites altijd met HTTPS (beveiligde verbinding, privacy)

Tips:

- Browser instellingen. (adblockers en privacyplugins)
-

Gegevens in de cloud

Risicos van cloudopslag

- Google kan ook stuk (gegevensverlies, datalekken)
- Staat het er over 30 jaar nog steeds? Wil je dat? Of wil je dat juist niet?
- Misbruik van persoonlijke data (cyberpesten, phishing)

Maatregelen

- Maak altijd gebruik van tweefactor authenticatie
- Maak altijd lokale backupS van belangrijke, persoonlijke en onvervangbare data
- Foto's kun je laten afdrukken in een fotoalbum (en kado geven). Dan kun je ze zelfs nog bekijken als de stroom uitvalt
- Hoe gegevens in de cloud te beveiligen
    - Deel alleen wat je wilt delen!
    - rechten, permissies, privé of openbaar, alleen vrienden of iedereen? Let daar goed op!
    - Ruim op en gooi weg (zelfcensuur)

HACKERSPACE DRENTHE

Vragen?

HACKERSPACE DRENTHE

• Links

- https://www.politie.nl/informatie/checkjehack.html
- https://haveibeenpwned.com
- https://www.datalekt.nl
- https://digihulp.nl (Digihulplijn: 0800-1508)
- https://www.autoriteitpersoonsgegevens.nl