Malware - Virussen

Diagnose

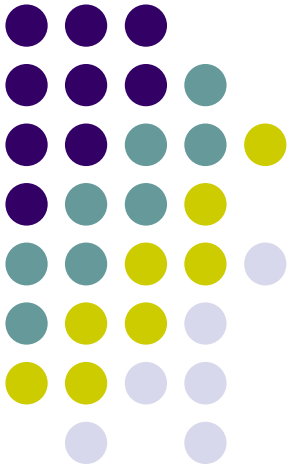
Preventie

genezing

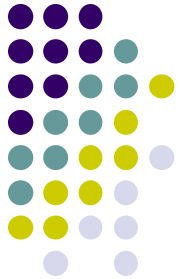
Defintie

“Malware is alle software die zonder expliciete toestemming van de gebruiker op de computer van de gebruiker wordt geïnstalleerd, die tot doel heeft de functie van de computer in het nadeel van de gebruiker en/of in het voordeel van de maker te veranderen.”

dr. Jaap-Henk Hoepman, Institute for Computing and Information Sciences, beveiliging en toegepaste cryptografie

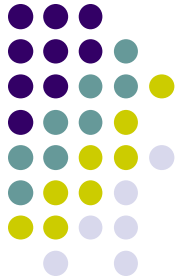


Wat?



- Ransomware
- Adware
- Spyware
- Trojans
- Keyloggers
- Toolbars

Wat doet het?

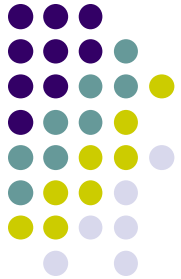


- hacking *(door openzetten van een poort waardoor men je computer kan controleren)*

  Doel: bepaalde acties op de pc uit voeren zoals

  - toetsenbordaanslagen vastleggen (om bijvoorbeeld wachtwoorden te ontdekken),
  - het openen en/of verwijderen van software en andere bestanden, enz…
  - inzetten van je PC in een crimineel botnet bij het massaal spammen, DoS (Denial-of-service)-aanvallen, enz
- Je gegevens gijzelen

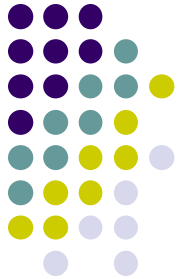
Ransomware: De belangrijkste dreiging op dit moment



je ontvangt een mailtje van een ogenschijnlijk bekende afzender en je opent ter goeder trouw de bijlage of klikt op een link. Het bericht is echter afkomstig van een cybercrimineel

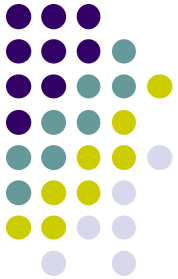
- enige tijd later wordt de toegang tot de computer geblokkeerd
- alle persoonlijke bestanden zijn versleuteld.
- De afperser belooft de gijzeling weer ongedaan te maken na een betaling

Voorkom de ellende



- Maak regelmatig een back-up
- let wel op: alle toegankelijke bestanden kunnen gegijzeld worden, dus ook de back-upbestanden op een aangesloten externe schijf. Schakel de backup schijf uit nadat de back-up klaar is en sluit hem zeker niet aan op een besmette computer.

Besmet met ransomware?



- Zet je wifi uit of trek je internetkabel uit.
- Koppel onmiddellijk alle andere toestellen los, zoals een externe harde schijf of een USB-stick.
- Vooral niet betalen! Ook al zou je eraan toegeven, er is geen enkele garantie dat de bestanden na de betaling weer toegankelijk worden.

Besmet met ransomware?

- Laat je toestel helemaal opnieuw installeren en gebruik achteraf een back-up of reservekopie om je gegevens terug te zetten.
- Heb je geen back-up, dan kan je gaan kijken op de website www.nomoreransom.org of er een tool bestaat om de gegevens terug te halen.

phishing


Anmeldung
Benutzername:
Wolfgang Müller
Kennwort:
OK
© zt-prentner.at

phishing

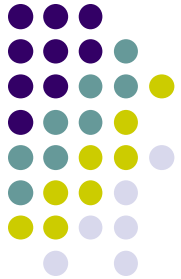
- oplichter probeert je persoonlijke gegevens zoals je bankcode, visakaartnummer, enz...te verkrijgen door gebruik van e-mail
- Probeert je te doen klikken op een link om Randsomware te installeren
- De mail kan ook een url bevatten waardoor je omgeleid wordt naar een website die tijdens je bezoek automatisch spyware naar jouw computer downloaden. Is je computer niet voldoende beschermd, dan wordt hij besmet. Niet alleen slecht bekend staande sites kunnen die hebben, maar ook sites met een goede reputatie kunnen slachtoffer worden van hackers en zo computers besmetten.

Doe de Phishingtest

- Herken jij verdachte berichten op tijd?
- https://www.safeonweb.be/nl/quiz/phishingtest

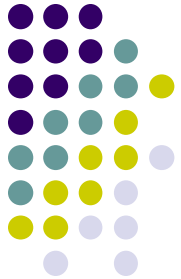
- Zie ook https://www.cybersimpel.be/nl

Adware - Spyware



- Adware is enkel reclame
- Spyware houdt op de achtergrond je surfgedrag bij. Aan de hand daarvan stuurt men je dan “gerichte” reclame. Kan van lichte hinder naar zeer schadelijk gaan

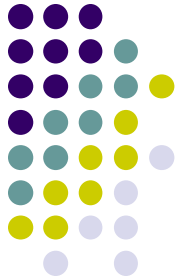
Hoe voorkomen?



- Vermijd sites met:
  - Overdreven veel reclame er op, goksites, porno, gekraakte software,…
- Pas op
  - met p2p
  - Gratis programma's
- Een adblocker installeren
- https://adblockplus.org/nl/
  - Kan tracking, malwaredomeinen, banners, pop-ups en videoadvertenties blokkeren

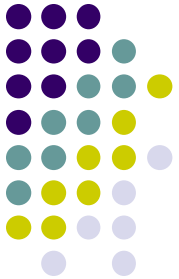
- Lees waarmee je akkoord gaat wanneer je software installeert
- Bekijk mails met bijlagen voor je ze opent. Zet de preview af.
  Outlook: beeld → leesvenster → uit
  Denk na over je wachtwoorden (gebruik acroniemen)
- Geef geen vertrouwelijke info door via e-mail, sociale media, …
- Antwoord nooit op spam, kettingbrieven...

Je systeem up-to-date houden



- Zorg ervoor dat je steeds de laatste versie van je besturingssysteem staan hebt.
- bij Windows 10 Home (de versie die op de meeste thuiscomputers staat) is het om veiligheidsredenen onmogelijk updates te verbergen zodat de installatie wordt uitgesteld of voorkomen.
- Vertrouw echter nooit pop-ups op het internet die jou vertellen dat er iets hapert aan je computer.

Internet en Java



- Zorg ervoor dat je browser veilig is
- softwareonderdelen die de mogelijkheden van Internet Explorer vergroten
  - Oudere versies van Java kunnen lekken hebben

Virusscanners

https://www.test-aankoop.be/hightech/internet/koopgids/koopgids-firewall-en-antivirussoftware

Het gratis antivirusprogramma (Microsoft Security Essentials voor Windows 7, Defender voor Windows 8 en 10) en de Windows 7-firewall is voor een gewone computergebruiker meestal voldoende

Gratis:

- **Avast (www.avast.com/uninstall-utility)**
- **AVG (www.avg.com/nl-nl/utilities)**
- **Avira (www.avira.com/en/support-for-home-knowledgebase-detail/kbid/902)**
- **Betalende:**
- **De gratis scanners hebben ook een betalende versie. Die Bieden meer dan de gratis versies. Daar is o.a. ook een firewall bij inbegrepen.**

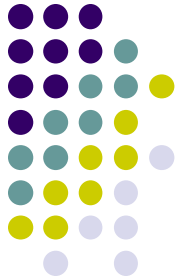
De firewall

- Er wordt vaak gedacht dat een virusscanner de computer voldoende beschermt.
- een goede firewall is net zo belangrijk!
- Een firewall wordt gebruikt om het (internet)verkeer tussen de computer en het netwerk/internet in de gaten te houden en waar nodig onbekend verkeer te blokkeren. Daarnaast zorgt de firewall ervoor dat de computer onzichtbaar is in het netwerk of op het internet, zodat wordt voorkomen dat onbevoegden toegang tot persoonlijke gegevens kunnen krijgen. De firewall maakt de internetverbinding dus een stuk veiliger.

Anti-Spyware

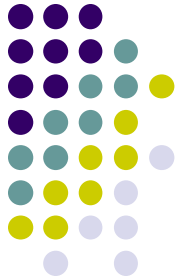
- Wordt je computer opeens traag, krijg je ongevraagd reclame en/of popups, krijg je extra toolbars, dan is er kans dat je computer met spyware besmet is.
- www.malwarebytes.org/antimalware/)
- Spybot – Search & Destroy: https://spybot-search-destroy.nl.softonic.com/

Spam vermijden



- Niet slordig omspringen met je e-mail adres
- Gratis e-mail adressen
- Tijdelijke e-mailadressen
  - www.spammotel.com
  - www.spamgourmet.com
  - http://www.10minutemail.com/10MinuteMail/index.html

draadloze netwerken



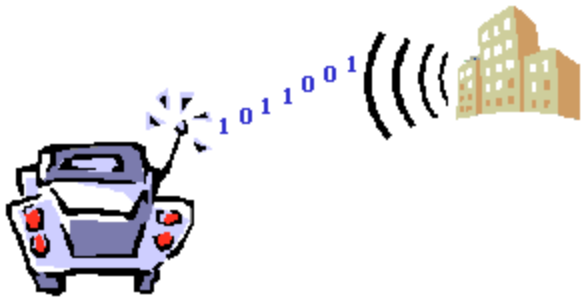
- Niet beveiligde draadloze netwerken zijn ook voor buren en voorbijgangers toegankelijk!
- Let op met openbare wifi
- https://www.cybersimpel.be/nl/onderwerpen/hoe-kan-ik-mezelf-beschermen-wanneer-ik-openbare-wifi-gebruik

Hoe beveiligen?

- De beveiliging gebeurt in het configuratiescherm van de router. Het menu benader je via je browser door een IP-adres in te typen, gevolgd door een routerpaswoord (Zie handleiding). Heb je moeilijkheden, roep hulp in van een expert. Gebruik een combinatie van:
  - WPA (WPA/WPA2) encryptie; WEP is zeer zwak en kan in 5 minuten ontcijferd worden. WPA, of Wifi Protected Access, is makkelijk aan te vinken in de instellingspagina's van een router of modem.
  - en een sterk router wachtwoord; Vaak is dat heel eenvoudig te doen via de veiligheidsinstellingen van het apparaat.

Conclusie

- geen reden tot paniek – wel voorzichtigheid
  - Vraag je af of je wireless echt nodig hebt. Kabels blijven sneller en veiliger. Een bekabeld netwerk is fysiek beter afgeschermd voor vreemden. Een netwerk waarbij de gegevens vrijelijk door de lucht worden getransporteerd, is kwetsbaarder
  - http://datanews.knack.be/ict/nieuws/dit-moet-u-weten-over-het-wifi-lek-met-wpa2/article-normal-913165.html

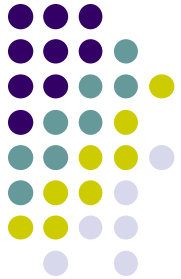


Veilig betalen 

- PC-banking en de betaalservices pay-pal en ogone zijn betrouwbaar. Het dataverkeer bij telebankieren wordt zwaar versleuteld. Als je een verbinding maakt met PC-banking doe je dat via SSL.

- Controleer of je wel op een https-site zit. **S** staat voor secure. Een authentieke veilige https-website herken je aan het hangslotje in de statusbalk, onderaan je browser Klik je daarop, dan heb je de mogelijkheid om een veiligheidscertificaat te controleren.

Mobile banking



- https://www.zichtrekeningen-vergelijken.be/mobile-banking-applicaties
- https://www.topcompare.be/nl/blog/bankieren-vanop-uw-smartphone
- https://www.topcompare.be/nl/blog/betalen-met-smartphone

Zie ook de site van febelfin

- https://www.febelfin.be/

Jouw privacy

- https://www.privacycommission.be/
- Zie www.e-privacy.be (Prof. dr. Michel Walrave)
- Controleer je privacy instellingen op sociale media
  - https://www.facebook.com/help/325807937506242/?locale=nl_NL