Mediawijsheid: bescherming

Team Mediawijsheid
l.legrand@hethooghuis.nl
Laatst gewijzigd 15 juli 2015

Webadres https://maken.wikiwijs.nl/47028/

Inhoudsopgave

Inleiding

Malware is een verzamelnaam voor allerlei soorten schadelijke of hinderlijke computerprogramma's die op jouw computer terecht komen zonder dat je daar toestemming voor hebt gegeven. Er zijn veel verschillende soorten. Sommige zijn alleen maar een beetje hinderlijk, maar andere kunnen heel gevaarlijk zijn.

Daarnaast gebruiken computercriminelen ook methoden om jouw wachtwoorden te 'kraken' zonder dat ze daarvoor software op jouw pc hoeven te zetten.

Deze les gaat over:

- **de veel voorkomende soorten malware:** virussen en phishing
- Het kraken van wachtwoorden
- Hoe je je computer en jezelf zo goed mogelijk kunt **beschermen**
- Wat je het **beste kunt doen** als je in aanraking komt met malware.

Virus

asistenta@clausweb.ro

Iedereen weet wel wat een virus is. Een virus is een organisme dat jou ziek kan maken. Zo'n virus kan zich vermenigvuldigen én hij kan ook overgaan op andere mensen. Zo kan het virus ook die andere mensen weer ziek maken.

En een computervirus?

Een computervirus is eigenlijk precies hetzelfde. Het is een computerprogramma dat geschreven is om je computer te vertragen, kapot te maken, of om te zorgen dat je gegevens verloren gaan. Mensen kunnen ook een virus schrijven dat misbruik maakt van jouw computer en bijvoorbeeld uit jouw naam allerlei mails gaat versturen. Je computer wordt er dus eigenlijk 'ziek' van. Net als in het echt is het ene virus erger dan het andere. Sommige virussen zijn een klein beetje vervelend maar andere kunnen heel gevaarlijk zijn.

En net als bij een gewoon virus kan een computervirus zich verspreiden en overgaan op andere computers. Zo worden die andere computers ook 'ziek'.

Hoe komt het op je computer?

In ieder geval komt zo'n virus op je computer terecht zonder dat je daar toestemming voor hebt

gegeven. Het virus zit verstopt.

Je kunt op allerlei manieren een virus krijgen. Een paar voorbeelden:

- Via een mail met een bijlage. Het virus zit dan in de bijlage. Als je de bijlage opent, komt het virus op je computer terecht en verstopt zich daar.
- via een zogenaamd 'lek' in de software die al op je computer zit. Vooral software die door heel erg veel mensen gebruikt wordt, zoals Windows wordt hiervoor gebruikt.
- via software die je installeert.
- via bestanden die je downloadt vanaf internet, bijvoorbeeld een mp3-bestandje
- Via een CD, DVD, USB-stick
- Via bluetoothverbindingen

Wat merk je er van?

Je computer werkt niet goed meer...

Sommige virussen willen je 'pesten' door je computer langzaam te maken of bestanden te verminken. Daar merk je in het begin meestal niets. Langzaam wordt je computer trager. Bestanden zijn niet meer te vinden of te gebruiken of bepaalde software doet het niet meer. Na een tijdje ga je denken dat je weleens een virus zou kunnen hebben.

Sommige van deze virussen zitten zo in elkaar dat ze op een bepaalde datum gaan werken: bijvoorbeeld op 1-1-2014 of op 11-11-2011.

Zo'n virus zit vastgeplakt aan een bestand. Ga je het bestand gebruiken, dan komt het virus in het werkgeheugen van de computer terecht. Ga je daarna met een ander bestand werken dan plakt het virus daar ook aan. Zo kan het virus zich door je computer verspreiden.

Internet/mail raakt verstopt: er wordt 'spam' gestuurd

Sommige virussen lezen je adresboek en sturen dan weer mails aan alle adressen uit jouw adresboek. Als zo'n virus zich snel verspreidt kun je bijvoorbeeld niet meer mailen of het gaat heel langzaam.

Zo'n virus heet een 'worm' en deze zit verstopt in de bijlage van een email. Als je de bijlage opent start het virus.

Je computer wordt gebruikt en/of je gegevens worden gestolen

Veel moderne virussen willen jouw computer niet kaptomaken maar **gebruiken**. Ze willen uit jouw naam dingen bestellen, gegevens van jouw pc doorsturen, taken uitvoeren waar jij niets van weet, jouw wachtwoorden stelen enzovoorts. Heel vaak weet je dan helemaal niet dat je computer een virus heeft.

Je hoort het dan pas als je gewaarschuwd wordt.

Bron afbeelding: Marsmett548 Tallahassee via Flickr.com

Voorbeeld

Botnet opgerold 2010 (schooltv)

Bekijk het filmpje.

De computercriminieel die dit heeft bedacht zorgde ervoor dat het virus Bredolab op je computer terecht kwam. Het virus installeerde daar schadelijke software. Die software zorgde ervoor dat de bazen van het netwerk jouw computer dingen kon laten doen waar je zelf niets van wist.

Gevaarlijk dus!

Hoeveel?

Hoeveel?

Hoeveel verschillende computervirussen denk jij dat er bestaan?

- honderden
- duizenden
- tienduizenden
- miljoenen

Het is heel belangrijk dat jezelf én je computer zo goed mogelijk beveilgd zijn tegen virussen. Voor jezelf, maar ook voor anderen. Als jouw computer een virus heeft, kun je vaak dat virus ook weer doorgeven aan allerlei andere computers.

Wat doe je als je een virus op je computer hebt?

Als je een virus op je computer hebt moet dat in ieder geval verwijderd worden voor het nog meer schade aanricht. Er zijn allerlei tools en mogelijkheden om een virus te verwijderen.

- vertel het in ieder geval tegen je ouders. Je kunt dan samen kijken wat je het beste kunt doen.
- Weet je hoe het virus heet? Typ de naam van het virus, samen met het woord 'remove manual' in op Google of een andere zoekmachine. Je vindt dan bijna altijd wel een site waar je een programmaatje kunt downloaden om het virus te verwijderen.
- Je kunt hulp vragen aan ICT en Media op school. ICT en Media plaatst dan een nieuw image op je pc. Je virus ben je dan kwijt maar de software die je zelf hebt geinstalleer en je bestanden ook! Zorg dus voor een backup.

Phishing

bron: flickr betacontinua

Bij 'phishing' proberen criminelen om persoonlijke informatie van jou te verzamelen. Het kan dan gaan om wachtwoorden, pincodes, inloggegevens en bankrekeningnummers van je bank enzovoorts. Ze doen dat door een mailtje te sturen dat aan jou vraagt om je gegevens door te geven. Zo'n mailtje lijkt echt van je bank of van gmail of iets dergelijks te komen, maar het is NEP!

Heel vaak willen de boeven die hierachter zitten je **bankrekeningnummer met je inloggegevens** te weten komen. Dat is natuurlijk heel gevaarlijk, want daarna kan je rekening worden geplunderd.

Banken proberen er dan ook van alles aan te doen om hun klanten te helpen om phishing-mails te herkennen.

Het kan ook gaan om het te weten komen van je **inloggegevens** op andere websites, zodat de criminelen uit jouw naam allerlei dingen kunnen doen die jij niet bedoeld hebt.

Klik maar een op deze link en daarna op de enveloppen die je te zien krijgt. Je ziet dan **voorbeelden** van phishingmails en je leert ook hoe je kunt zien dat het nep is.

Wat doe je als slachtoffer?

- **Waarschuwen** Kom je erachter dat je een phishingmail hebt gekregen en hebt beantwoord? Waarschuw altijd:
    - Je ouders. Laat zien wat je hebt gekregen en bespreek wat je het beste kunt doen
    - Het echte bedrijf. Stuur bovendien de tekst van de phishingmail naar ze op zodat er niet nog meer slachtoffers vallen.
- **Wachtwoord** Kom je erachter dat je een phishingmail hebt gekregen en heb je al wel je naam en wachtwoord doorgegeven? Ga direct naar de site waar het om gaat en verander je wachtwoord.
- **Bankgegevens.** Zijn er bankgegevens doorgegeven? Vertel dit direct tegen de bank.

Wachtwoord kraken

Hoe kraakt iemand een wachtwoord? (www.laatjeniethacken.nl)

Er bestaan computercriminelen die met behulp van speciale programma's op internet je wachtwoord proberen te achterhalen. In het filmpje heb je gezien hoe dat kraken in zijn werk kan gaan en hoe snel het kan gaan.

Als anderen je wachtwoord hebben kunnen ze uit jouw naam allerlei dingen doen die je niet bedoeld had.

Bescherming

Het is heel belangrijk dat je jezelf en je computer zo goed mogelijk beschermt tegen virussen, tegen phishing en tegen andere vormen van malware.

Maar: ook al pak je de bescherming goed aan, het is geen garantie! Het is altijd mogelijk dat er een virus tussendoor glipt of dat je een phishingmail niet op tijd herkent.

- Zorg voor een goede virusscanner
- Stel automatische updates in
- Firewall
- Let op met downloaden
- Goede wachtwoorden
- Geef je gegevens niet zomaar weg
- Maak backups!

Virusscanner

Wikimedia Commons Dave Mauroni

Wat doet je virusscanner?

- De virusscanner 'kijkt' naar de bestanden op je computer en **vergelijkt ze met een lijst met**

bekende virussen. Vindt je virusscanner een virus dan zal hij die **verwijderen** of 'in **quarantaine** plaatsen'. Dat laatste betekent dat de bestanden op een afgeschermd stukje van je pc worden gezet. Iedere dag komen er nieuwe virussen bij en de lijst met bekende virussen wordt dan ook vaak bijgewerkt. Het betekent dus wel dat je de virusscanner steeds moet **updaten**.

- De virusscanner zoekt naar 'verdacht gedrag' op je computer. Als programma's bijvoorbeeld gegevens gaan wegschrijven naar andere programma's kan dat een teken zijn dat het om een virus gaat.
- De virusscanner zoekt naar verdachte mails en gooit als dat nodig is de bijlage weg.

Als je virusscanner iets gevonden heeft, zal hij je waarschuwen en je vragen wat hij moet doen.

Belangrijk

- Zorg voor een goede virusscanner op je pc.Je laptop van school werkt standaard met **Windows Defender**.
- Zorg dat je virusscanner automatische updates uitvoert. Je laptop van school staat standaard zo ingesteld dat Windows Defender automatisch wordt geupdate.
- Als je virusscanner iets gevonden heeft en je vraagt wat er moet gebeuren, klik de melding dan niet gewoon weg, maar lees goed wat er staat en wat je moet doen.

Klik op de link hieronder om te zien hoe je Windows Defender bereikt.

Windows Defender: instellingen

Automatische updates

Je weet al dat het belangrijk is dat je virusscanner is ingesteld op 'automatische updates'. Maar dat geldt ook voor andere software.

Je weet ook al dat sommige malware op je computer terecht kan komen via zwakke plekken in de beveiliging van bepaalde software. Onze computers op school werken met Windows 7 en Windows 8. Windows probeert steeds eventuele beveiligingslekken op te sporen en te repareren om computercriminelen geen kans te geven. Andere grote software-ontwikkelaars doen dat ook. Dat betekent dat er ook vaak nieuwe versies van de software beschikbaar komen. Het is dus belangrijk dat jij die nieuwe versies van de software ook op je eigen laptop installeert, anders blijf jij zitten met een softwarelek en wordt je computer een gemakkelijke prooi voor malware.

Belangrijk

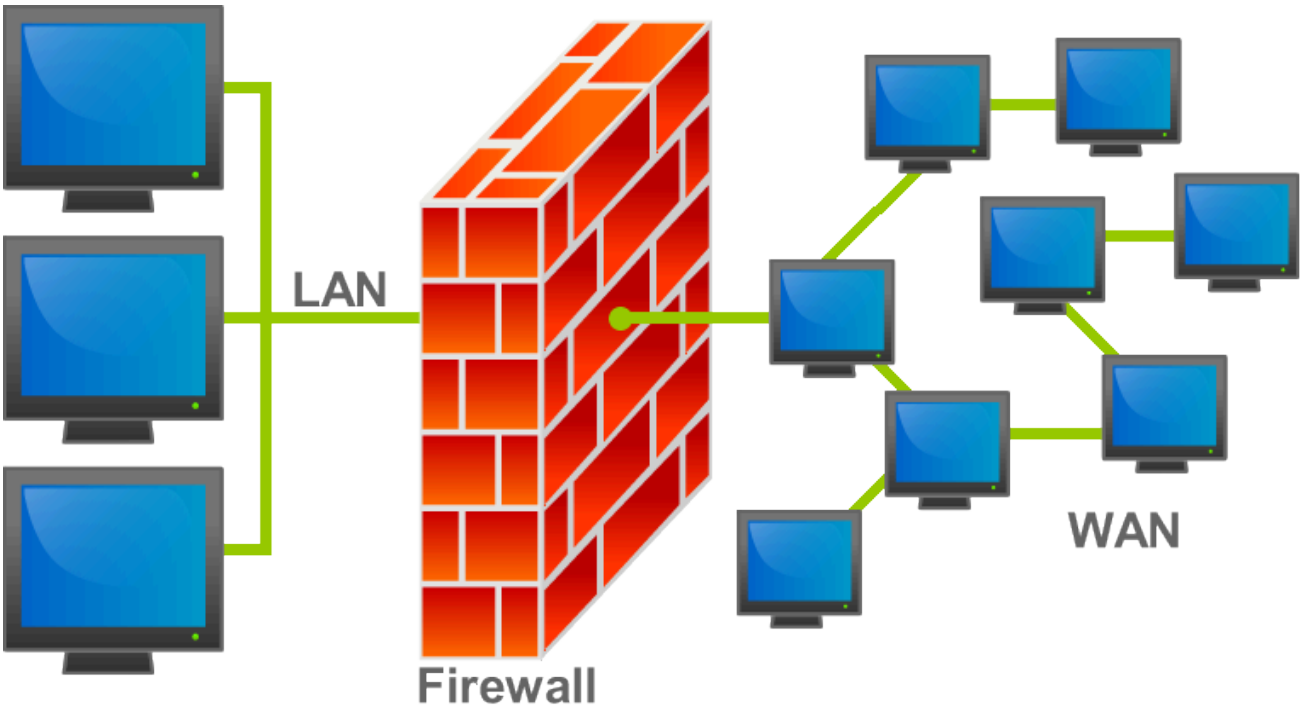
- Zorg dat je computer zo is ingesteld dat automatisch updates van belangrijke software wordt uitgevoerd (zoals Windows, Office, Adobe-productien, Flash) Je computer van school staat al standaard zo ingesteld.
- Krijg je een melding dat er een update klaarstaat van een softwarepakket dat jij gebruikt,

installeer de update dan ook.
- Controleer af en toe of je ook echt werkt met de laatste versie van je software.

Klik op de link hieronder om te zien hoe je de status van de 'automatische update' van Windows kunt bekijken.

Automatisch updaten Windows en andere Microsoft producten

Firewall



Wikimedia Commons Bruno Pedrozo

Met een **firewall** kun je zelf beslissen welke internetprogramma's toegang hebben tot je computer.

In Windows 7 en Windows 8 zit een ingebouwde firewall. Je kunt die firewall zelf inrichten en er zo voor zorgen dat alleen programma's die jij vertrouwt, toegang krijgen tot je pc.

Belangrijk

- Zorg voor een goed ingerichte firewall op je pc. Je pc van school maarkt gebruik van de firewall van Windows. Deze is standaard zo ingesteld dat wanneer je firewall iets blokkeert, hij je daarvan een **melding** geeft. Je kunt er dan voor kiezen om het programma op te nemen in de lijst van toepassingen die door de Firewall mogen.
- Standaard staat die firewall **ingeschakeld.** Het is heel belangrijk dat de firewall ook ingeschakeld blijft.
- Geef alleen programma's vanuit internet toegang tot je pc als je ze echt vertrouwt
- Weet je het niet zeker? Vraag het aan je ouders of aan ICT en Media

Firewall - extra informatie

Precies weten hoe het werkt?

Als je precies wilt weten hoe het in elkaar zit kun je dat In het filmpje bekijken. Sommige stukjes van de video zijn best lastig. Het is niet erg als je alles kunt volgen. Nieuwsgierig genoeg? Kijk naar de video:

Wat is een firewall en hoe stel je die in? - Explania

Opletten met downloaden

Als je bestanden downloadt, zoals een filmpje (mp4 of bijvoorbeeld avi) of muziek (mp3) kun je gemakkelijk een virus meeslepen. Een goede virusscanner is echt geen overbodige luxe.

Ook word je bij het downloaden nogal eens gevraagd om allerlei andere zaken mee te installeren. Kijk uit: want standaard is alles 'aangevinkt'. Je moet zelf goed opletten en waar nodig de vinkjes weer uitzetten. Lezen wat er gedaan moet worden!

Sterke wachtwoorden

Je hebt al gezien dat er boeven bestaan die met behulp van speciale programma's op internet je wachtwoord proberen te achterhalen. Lukt dat, datn kunnen ze zo toegang krijgen tot al je diensten. Het is dus belangrijk dat je werkt met goede wachtwoorden, of, nog beter, met **wachtzinnen.**

Bron: www.laatjeniethacken.nl

Belangrijk

- Zorg voor een goed wachtwoord dat niet gemakkelijk te kraken is. Een goed wachtwoord is **lang.** Een **wachtzin** is beter dan een wachtwoord. Gebruik geen bekende uitspraken, of persoonlijke informatie.
- Gebruik niet steeds hetzelfde wachtwoord of dezelfde wachtzin. Iemand die jouw wachtwoord dan kraakt, heeft meteen toegang tot al jouw diensten.
- En: deel je wachtwoord niet met anderen!

Geef je gegevens niet zomaar weg

Je kunt allerlei beveiligingsmaatregelen nemen, maar als je zelf je gegevens weggeeft, kunnen computercriminelen daar gemakkelijk misbruik van maken. Let dus op wat je doet.

Belangrijk

- Geef je e-mail adres niet zomaar aan iedereen, maar alleen aan mensen die je kent.
- Als je je e-mail adres wel op een internetpagina invult, moet je zeker weten dat het veilig is. Je kunt ook een apart emailadres gebruiken speciaal voor zulke internetpagina's.
- Geef alleen persoonlijke gegevens in e-mails en op webpagina's als je zeker weet dat het veilig is.
- Soms weet je niet zeker of iets echt is of nep. Bel dan naar het bedrijf of stuur een mailtje. Maar let op: vaak staan in de nepberichten ook netptelefoonnummers en nepmailadressen. Zoek dus een ANDER mailadres of telefoonnummer dan in je mail vermeld staat.

Maak een backup

Je hebt wel gezien dat er allerlei zaken kunnen gebeuren met de gegevens die op je computer staan. Het is het belangrijkste dat je zoveel mogelijk nare zaken voorkomt. Maar het is ook belangrijk dat je **backups** maakt van je (belangrijke) gegevens. Als er dan iets mis gaat zijn je gegevens tenminste niet verloren.

Een backup wil zeggen dat je je gegevens een keer **extra** opslaat. Je maakt een **kopie** van je gegevens.

Die kopie zet je **op een andere plek**. Logisch, want als je je backup op dezelfde computer zet, is die straks óók besmet of stuk. Een aantal mogelijkheden zijn:

- Veel mensen hebben thuis nog meer computers, soms in een netwerk. Vraag je ouders of je je backup op een andere computer thuis mag zetten. Je kunt dat (samen met je ouders) zelfs zo inrichten dat er bijvoorbeeld iedere avond automatisch een backup gemaakt wordt.
- Gebruik Skydrive als backup voor je belangrijkste gegevens. Voordeel is dat je je gegevens altijd ook vanaf een andere computer (met internetverbinding) kunt gebruiken. (ook heel prettig wanneer je laptop een keer kapot zou zijn). Geen Skydrive? Je kunt hulp vragen aan ICT en Media.
- Gebruik een usb-stick om een backup van je belangrijkste gegevens te maken.

Mindmap malware

Klik op de afbeelding om de mindmap te openen.

Opdrachten

Opdracht 1: Phishing

Een 66-jarige man uit Olst is voor bijna achtduizend euro opgelicht. Hij werd het slachtoffer van het zogeheten 'phishing'.

De man kreeg meerdere e-mails waar hij dacht dat ze van de Rabobank waren. In één van de mails zat een link naar een website waarop het slachtoffer vervolgens zijn gegevens heeft ingevuld. Later werd hij gebeld door een vrouw die zei dat ze medewerkster van de Rabobank was. De vrouw liet het slachtoffer verschillende codes invoeren en doorgeven. Later ontdekte hij dat er een groot geldbedrag was overgeboekt naar München in Duitsland. Het slachtoffer heeft aangifte gedaan bij de politie.

(bron: RTV-Oost, 2011 rtvoost.nl/nieuws/default.aspx?nid=128532)

Opdracht: Phishing

Klik op de link hieronder. Lees de informatie en kijk naar de schermprints. Dan begrijp je waarom deze meneer erin is getrapt....

http://www.pcbeveiligen.nl/informatie/phishing-email-rabobank/

Zoek zelf drie voorbeelden van phishingmails op internet. Maak er schermprints van en plak ze in een worddocument.

Opdracht 2: bescherming

Wat kun je doen?

Beschermt een goede virusscanner je tegen phishing? Waarom wel/niet? Overleg eventueel met je buurman/buurvrouw. Zet het antwoord in een worddocument.

Opdracht 3: Trojaans paard

Trojaans paard

Een bijzondere vorm van malware is een 'trojaans paard' (trojan horse).

a. Zoek op internet op

- wat een 'trojaans paard' is
- waarom het zo gevaarlijk is
- hoe je erachter komt dat er een trojaans paard op je computer zit

b. Wat moet je doen als je computer is geinfecteerd met een trojaans paard?

Zet je antwoord in je worddocument.

Opdracht 4: Zoeken

Zoeken...

a. Wat voor soort virus is ZeroAccess? Zoek het op internet op. Zet het antwoord in je worddocument

b. Zoek een site waar je informatie vindt over het verwijderen van ZeroAccess (tip: typ in Google als zoekwoorden: **ZeroAccess removal handmatig** in. Lees wat er staat. Kijk ook zo goed mogelijk of je wel op een betrouwbare site bent beland. Zoek anders een andere site. Kopieer de link naar je worddocument

Inleveren

Inleveren

Zet je naam boven je worddocument en lever het in.

Over dit lesmateriaal

Colofon

Team	Mediawijsheid l.legrand@hethooghuis.nl
Laatst gewijzigd	15 juli 2015 om 22:13

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Eindgebruiker	leerling/student

Bronnen

Botnet opgerold 2010 (schooltv)
http://teleblik.nl/embed/media/5419385/fragment?autoplay=0&start=518&end=659

Hoe kraakt iemand een wachtwoord? (www.laatjeniethacken.nl)
//www.youtube.com/embed/sCMotoEV3TY

Bron: www.laatjeniethacken.nl
//www.youtube.com/embed/6n-ZoFW-d_I?rel=0