COMPUTER BEVEILIGING

(18-12-2012)
Gerrit van Eijndhoven
http://www.gerritentiny.nl/

Inhoud

Algemeen
Een computer is een medium waarbij veelvuldig gebruik wordt gemaakt van informatie die door diverse bronnen kan worden toegeleverd.
De meest voorkomende bronnen zijn:

- floppydisk (is aan het verdwijnen)
- CD- en DVD-rom
- Geheugenstick
- Geheugenkaart
- Internet (surfen en emailen)

De informatie op die media zal meestal betrouwbaar zijn maar kan ook vervuild zijn door moedwillig aangebrachte miniprogrammaatjes met het doel je computer of je software te beschadigen of om vertrouwelijke gegevens vanaf jouw computer te verkrijgen.
De meeste vervuiling komt via Internet, maar ook de andere bronnen kunnen narigheid binnenbrengen.
Dus als je floppies, cd's, dvd's, geheugenkaarten of sticks krijgt die je niet helemaal vertrouwd, scan ze dan eerst op ongerechtigheid.

Risico-categorieën

De belangrijkste risico-categorieën zijn:

- Virussen.
  Deze beschadigen of wijzigen bestanden op je computer zodanig dat programma's of de gehele computer niet of nauwelijks functioneren.
  Ook kunnen ze schade aan de hardware toebrengen, schijven of schijfinhoud beschadigen en meer van die ongein.
  Je krijgt ze vooral binnen via besmette websites en email-bijlagen.
- Spyware
  Spyware zijn ongewenste, verborgen programmaatjes die door derden via Internet op je computer geïnstalleerd worden. De bedoeling is dat ze vertrouwelijke gegevens, zoals b.v. gebruikersnamen wachtwoorden doorgeven aan de maker van het spywareprogramma.
  Je krijgt het vooral binnen via besmette websites en email-bijlagen.
- Spam
  Spam is opgedrongen reclame die als email wordt aangeboden.
  Meestal gaat het over reclame voor dubieuze zaken.
  Spam kan ook besmet zijn met virussen en spyware.
- Phishing
  Meestal gebeurt phishing door het ontvangen van een email met een link. Die email lijkt verstuurd te zijn door je bank maar is een vervalsing.
  Klik je op de aangeboden link dan kom je op een valse webpagina van je bank terecht waarin vertrouwelijke informatie zoals wachtwoord e.d. wordt gevraagd. Die info komt dan bij oplichters terecht.
  Let er op !! Je bank zal NOOIT naar wachtwoorden e.d. vragen. Wordt je toch gevraagd dan is het oplichting.
- Cookies
  Cookies zijn kleine tekstbestandjes, met de extensie .txt, die sommige bezochte sites op je computer plaatsen.
  Cookies worden op vaste plaatsen op je computer opgeslagen.
  Bij Windows XP en Vista in:
  C:/Document and Settings/<*gebruikersnaam*>/Cookies
  Bij Windows 7 liggen ze wat verder weg in :
  C:/users(gebruikers)/<*gebruikersnaam*>/AppData/Roaming/Microsoft/Windows/Cookies

De inhoud van deze directories is alleen maar zichtbaar als men in de Verkenner via Extra – Mapopties – Weergave, *de inhoud van Systeemmappen weergeven* heeft aangevinkt.
Cookies zijn bedoeld als hulpjes bij een hernieuwd bezoek aan de betreffende site.
Een bekend voorbeeld is het bewaren van een gebruikersnaam, zodat die automatisch wordt ingevuld als je een site opnieuw bezoekt.
Doordat het alleen maar simpele tekstbestanden zijn kunnen ze geen virussen of andere schadelijke software bevatten.
Ze zijn dus nagenoeg altijd onschuldig en kunnen geen virussen op je computer installeren, schade aanrichten of informatie naar buiten sturen..
Een uitzondering zijn de z.g. tracking cookies.
Deze kunnen weliswaar geen schade aan je computer toebrengen maar wel persoonlijke gegevens zoals b.v. surfgedrag, naar de sitebeheerder doorsturen.
Wil men dat risico niet lopen dan kan men in Internet Explorer deze tracking-cookies blokkeren.
Ga daarvoor als volgt te werk:

- Open IE
- Klik op Extra
- Klik op Internet opties
- Klik op Privacy
- Klik op Geavanceerd
- Plaats een vink bij ‘Automatische cookie-verwerking opheffen’
- Selecteer Blokkeren bij Indirecte cookies

Wil je meer weten over cookies dan kun je o.a. eens kijken op:
http://www.jawwi.nl/artikelen/cookies.html
Ook al zijn cookies vrij onschuldig dan verdient het toch aanbeveling om ze regelmatig eens op te ruimen.
Het kunnen er in de loop der tijd honderden worden, nemen daardoor schijfruimte in beslag en kunnen je computer vertragen.
Opruimen kun je m.b.v. Schijfopruiming van Windows of met een onderhoudsprogramma als CCleaner.
Het verwijderen van Cookies richt geen schade aan.
Na het opruimen zullen dan soms wel je vooringevulde gegevens niet meer beschikbaar zijn tot je ze opnieuw hebt ingevuld.

Wat kun je er aan doen?

- Provider
  Nagenoeg alle providers van internet controleren passerende email zelf al op spam en virussen. Soms moet je er voor betalen.

- Virusscanner
  Installeer een goede virusscanner op je computer.
  Er zijn veel goede tegen betaling verkrijgbaar, maar er zijn ook een aantal gratis te downloaden van zeer goede kwaliteit.
  - Avast
    Een uitgebreid programma.
    Test ook email.
    Belast het systeem aanzienlijk.
    Surfresultaten worden in zeer beperkte mate getest.
    De gratis versie is te downloaden op:
    http://www.avast.com/nl-nl/free-antivirus-download

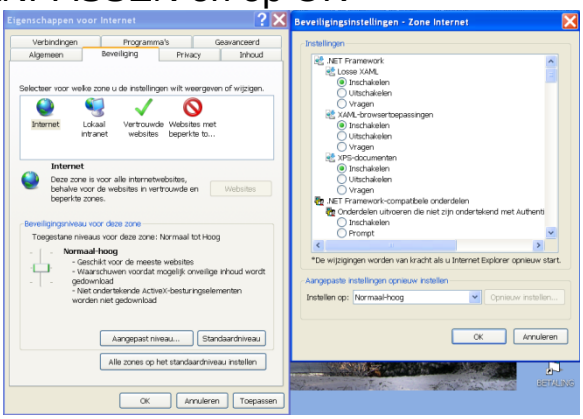
  - AVG-antivirusprogramma
    Een zeer uitgebreid programma.
    Test ook email en surfresultaten.
    Belast het systeem aanzienlijk.
    Het zeer frequent updaten en upgraden is soms erg hinderlijk.
    De gratis versie is te downloaden op:
    http://free.avg.com/nl-nl/startpagina
    of op:
    http://www.avgantivirus.nl/
    De gratis versie vind je daar bij *downloads* nummer 16.

  - Microsoft Securety Essentials
    Dit is een eenvoudig no-nonsens programma dat maar een minimale belasting op het systeem legt.
    Scant geen email en surfresultaten.
    Desalniettemin echt een aanrader.
    Te downloaden op:
    http://windows.microsoft.com/nl-NL/windows/products/security-essentials

- Firewall
  Windows en Vista hebben een goede Firewall.
  Zie het als een waakhond die aan de ingangspoorten ligt en er voor zorgt dat geen ongewenst volk (besmette programma's e.d.) ongemerkt op je computer binnen komt.

Een werkbare en veilige instelling is de volgende:

- Klik op START
- Klik op CONFIGURATIESCHERM
- Klik op BEVEILIGINGSCENTRUM
- Controleer of de Firewall INGESCHAKELD is
- Je kunt het beveiligingsniveau voor de verschillende zone's van de Firewall zelf instellen. Als je alle niveaus op HOOG instelt, zullen veel pagina's op Internet niet goed meer werken.
  Ga voor het instellen als volgt te werk:
- Klik op INTERNETOPTIES
- Klik op BEVEILIGING
- Selecteer evt. het icoon INTERNET
- Klik op AANGEPAST NIVEAU
- Kies bij "instellen op" NORMAAL-HOOG
- Klik op OK
- Klik op AANPASSEN en op OK



- Spamfilter
  - Spamfighter
    Installeer een spamfilter b.v. Spamfighter om je inkomende maar ook uitgaande mail op spam te scannen.
    Het is te downloaden op:
    http://www.spamfighter.com/Lang_NL/Download_Download.asp

- Surfen op Internet
  Als je op het internet surft kan het voorkomen dat je er bij de gevonden treffers een aantal links zijn die dubieus zijn. Als je die opent bestaat er een behoorlijk risico je virussen of spam binnenhaalt.
  Om dat te voorkomen zijn er diverse linkscanners die de gevonden sites scannen op ongerechtigheid en een advies geven over het risico.
  Om veilig te surfen installeer één van onderstaande linkscanners.
  - McAfee SiteAdvisor
    Deze controleert of de sites, die b.v. bij het zoeken met Google worden aangeboden, safe zijn. Dat wordt dan aangegeven door bij die site een gekleurd kenmerk aan te geven.
    Rood = onveilig
    Geel = wees voorzichtig!
    Groen = safe
    Grijs = niet getest
    Bij wat beperkte processors (netbook e.d.) veroorzaakt het wel een aanzienlijke traagheid bij tijdens het surfen.
    Dat wordt veroorzaakt door het scannen van alle gevonden resultaten.
    McAfee SiteAdvisor is te downloaden op:
    http://www.siteadvisor.com/download/ff.html

  - BitDefender TrafficLight
    Met dit programmaatje kun je bij het googlen controleren of een gevonden website veilig is. Na het installeren van TrafficLight wordt elke gevonden veilige site gemerkt met een groen vinkje. Dubieuze sites krijgen rood vinkje.
    Gebruik je de Explorer-browser installeer dan de Beta-versie. Voor andere browsers kun je een bijbehorende versie installeren.
    Opmerking:

Doordat het programma alleen de sites op de vertoonde pagina scant legt het nagenoeg geen beslag op de processor en veroorzaakt nauwelijks traagheid tijdens het googlen als de processor en/of geheugen wat beperkt zijn.
(zie ook McAfee SiteAdvisor)
http://trafficlight.bitdefender.com/extensions.html

- Computer scannen
  - CCleaner

    Laat regelmatig je anti-virusprogramma je gehele computer scannen op ongerechtigheid, b.v. 1x/mnd.
    Ook kun je je computer geheel laten controleren door goede gratis te downloaden onderhoudsprogramma's zoals CCleaner.
    Dit werkt zeer eenvoudig, je kunt er ook het register mee opschonen en geïnstalleerde programma's afdoende de-installeren.
    CCleaner kun het gratis downloaden op:
    http://www.piriform.com/ccleaner/update?v=2.23.993&l=1043

Wachtwoorden
Wachtwoorden zijn een noodzakelijke plaag.
Noodzakelijk, omdat een computer zonder wachtwoorden even (on)veilig is als een huis zonder sloten.
Een plaag, omdat ze niet of nauwelijks te onthouden zijn en je er in de loop der tijd tientallen van verzamelt.

Wachtwoorden zijn codes die je nodig hebt om toegang te krijgen tot bepaalde afgeschermde persoonlijke digitale informatie bv. bij het internetbankieren of de gegevens van je OV-kaart bekijken.
Als je toegang wilt hebben tot die gegevens. moet je telkens opnieuw je wachtwoord invoeren
Wachtwoorden worden soms ook gebruikt om delen van je computersysteem af te schermen.
Meestal wordt het wachtwoord aan een gebruikersnaam gekoppeld.
Enige toepassingsvoorbeelden:

- Een wachtwoord kan worden gebruikt bij het opstarten van je computer.
  Dat is niet noodzakelijk maar kan handig zijn als meerdere gebruikers op de computer werken.
- Een wachtwoord kan worden gebruikt om als Administrator toegang te krijgen tot bepaalde instellingen op je computer. Ook dit is dikwijls niet nodig.
- Een wachtwoord + gebruikersnaam in je e-mailaccount. Dit is altijd noodzakelijk om je inkomende email te kunnen ontvangen.
- Een wachtwoord kan ook worden gebruikt om bv. Word- of Excelbestanden af te schermen.
- Een wachtwoord + gebruikersnaam heb je nodig om te kunnen internetbankieren.
- Als je de eerste keer inlogt op een niet-free WiFi-verbinding wordt ook om een wachtwoord gevraagd. Meestal is dat de WPA-code van je router of modem.
  Buitenshuis wordt dat wachtwoord verstrekt door het bedrijf waar je inlogt, bv. in een hotel.
  Bij free-WiFi wordt meestal geen wachtwoord gevraagd.
- Heel veel instanties hebben een persoonlijke site met je gegevens. Bv. Mijn Ziggo, Mijn VISA, Mijn ING, Mijn Essent, Mijn OV, Mijn CBR, Mijn SVB, de Belastingdienst en nog veel meer.
  Ook veel webwinkels bieden een persoonlijke account aan.
  Om in te kunnen loggen heb je voor elke site een persoonlijk wachtwoord nodig.

Als je via internet een account aanmaakt bij een bedrijf of instantie wordt dikwijls een wachtwoord verstrekt voor éénmalig gebruik. De bedoeling is dan dat je na de eerste keer inloggen dat wachtwoord wijzigt in een eigen wachtwoord.
Een wachtwoord behoort uniek te zijn en moeilijk te kraken. Daardoor zijn ze meestal moeilijk te onthouden.
Dat is nog lastiger doordat sommige wachtwoorden periodiek moeten worden veranderd.
Enige adviezen:

- Neem minimaal 8 karakters.
- Neem in een wachtwoord cijfers, hoofdletters en kleine letters op bv. 13Lu7a. Ook leestekens zijn meestal toegestaan.
- gebruik een wachtwoord maar voor één toepassing.
- De consequentie hiervan is dat je wel tientallen verschillende wachtwoorden moet onthouden. Dat is ondoenlijk.
  Daarom is het noodzakelijk dat je ze noteert en bewaart.
  Je kunt dat schriftelijk doen in een lijst die je op een veilige plaats bewaart maar laat ze niet rondslingeren.
  Een ander hulpmiddel kan een digitale kluis zijn zoals het databaseprogramma Keepass. Je kunt het gratis downloaden op: http://keepass-password-safe.nl.softonic.com/
  In die database kun je al je wachtwoorden en bijbehorende informatie opslaan. Het programma is alleen maar te openen met een zelf te bepalen eigen wachtwoord, dat je uiteraard wel goed moet onthouden.

Als je wachtwoorden invoert worden ze meestal gemaskeerd met bolletjes of sterretjes. In sommige toepassingen kun je dat maskeren uitschakelen.
Soms kunnen gebruikersnamen en/of wachtwoorden in het invoervenster worden onthouden. Ben daar voorzichtig mee.
Er bestaan ook programma's om gemaskeerde wachtwoorden te kunnen lezen. Dat lukt niet in alle situaties, dus verwacht daar niet te veel van

Er bestaat ook software waarmee a.h.w. over je schouder mee kan worden gekeken welke toetsen je indrukt, een beetje vergelijkbaar met het over je schouder mee gluren tijdens pinnen.
Die malware kan door criminele figuren via internet ongemerkt op je computer worden geïnstalleerd, zodat zij in het bezit kunnen komen van je wachtwoorden.
Dat soort software wordt een Keylogger genoemd

Dit is zeker een reden om te zorgen dat je anti-virusprogramma altijd up-to-date is.
Ben je een wachtwoord kwijt dan zul je een nieuw aan moeten vragen bij de betreffende instantie.
Wordt soms alleen schriftelijk verstrekt en kost dan enige tijd.
Geef nooit een wachtwoord door aan anderen, zeker niet als er telefonisch om gevraagd wordt.

Nationaal Cyber Security Centrum
Het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie heeft een speciale site met het laatste nieuws betreffende de veiligheid op Internet.
Je vindt er ook veel tips en wetenswaardigheden over het veilig gebruiken van Internet.
De moeite waard om regelmatig in te snuffelen.
Klik op:
http://www.waarschuwingsdienst.nl/

Een goede raad.
Misschien slaat je bij het bovenstaande de schrik om het hart.
Dat is niet nodig.
Als je voor bescherming zorgt zoals hierboven aangegeven en je gedraagt je zoals hieronder staat aangegeven, is het onwaarschijnlijk dat je met rommel geconfronteerd wordt.

Open nooit een bericht van een onbekende en open nooit een bijlage waarvan je niet zeker weet of die veilig is.

Ben voorzichtig met het openen van emails en bijbehorende bijlagen als het een doorgestuurde mail is.
Deze zijn dikwijls een hele reeks computers gepasseerd (vergelijk het met een kettingbrief) en kunnen daar vervelende virusinfecties oplopen.

Stuur ook zelf geen pret-emails (met seks, humor e.d.) door aan anderen. Je kunt hen ongewild veel schade aan computer, software of bestanden berokkenen.

Krijg je regelmatig pretbijlagen van iemand toegestuurd, vraag hem dan om daarmee te stoppen. Die pretbijlagen vormen een zeer groot risico.

Als je op het internet surft, bezoek alleen degelijke sites.
Kijk in ieder geval of ze door een linkscanner zijn goedgekeurd.
Bij twijfel niet openen.

Ga je slordig met Internet om dan zullen ongetwijfeld computervirussen op je computer terecht komen.