Beveiliging van je ICT thuis

Bert van den Broek

PICTORA, ICT dienstverlening, gespecialiseerd in Oracle, business intelligence, service- en projectmanagement (bert@pictora.nl)

Inleiding

In vele huishoudens staat inmiddels een pc of laptop waarop driftig wordt gesurft op Internet, ge-emaild of gechat. Er wordt gewerkt met verschillende programma's, protocollen en netwerken. Dat dit de nodige bedreigingen met zich mee brengt is voor de professional een gegeven (denk ik), maar of ze zich in de praktijk daarna gedragen ...?. In hoeverre doorsnee gebruikers weet hebben van de gevaren, vraag ik me af. Vaak is er wel een virus programma operationeel, maar daar houdt het veel al mee op.

Het is meer dan eens gebeurd dat een computer niet goed meer werkte als gevolg van een hardware storing of, naar later bleek, een virus. Een back-up was in de meeste gevallen niet voorhanden. Een ander probleem waar pc gebruikers mee te maken kunnen krijgen is de vele ongewenste e-mail (ook wel spam genaamd) en zogenaamde cookies die naar de pc worden gestuurd. Ook hierin kunnen bedreigingen schuilen.

In dit artikel wordt nader ingegaan op de bedreigingen die een goede werking van de pc of laptop in de weg kunnen staan en welke maatregelen genomen kunnen worden om deze bedreigingen te reduceren.
In dit artikel wordt zo min mogelijk ingegaan op de techniek, maar meer op conceptueel niveau aanbevelingen gedaan. Getracht wordt zo eenvoudig mogelijk te beschrijven welke gevaren de werking van de pc in gevaar kunnen brengen of gegevens ontoegankelijk kunnen maken en daarmee waardevolle informatie voor de gebruiker verloren gaat.

Belangrijkste reden voor dit artikel is BEWUSTWORDING. Beveiliging thuis, op het werk, in het verkeer, etcetera is vanzelfsprekend. Beveiliging van de pc wordt vaak ten onrechte schouderophalend afgedaan of de gebruiker is zich onvoldoende bewust van de gevaren. Voor de ervaren, kritische computergebruiker zal dit artikel mogelijk weinig nieuws bevatten en zal de lezer veelal een 'déjà vue' gevoel hebben. Of deze lezer ook de nodige beveiligingsmaatregelen heeft genomen is echter nog de vraag.

Waartegen willen beveiligen?

Zoals vaker in het leven komen bedreigingen van alle kanten op je af; dit geldt ook voor bedreigingen voor de pc. Zonder daar nu van in paniek te raken, is het wel van belang bewust te zijn van deze bedreigingen. Op hoofdpunten zijn voor pc's de volgende bedreigingen:

- Ondoordacht bestanden verwijderen en daarmee de goede werking van de pc belemmeren of waardevolle informatie kwijt zijn.
- Hardware storingen, met als gevolg verlies van gegevens.
- Virussen die een pc volledig kunnen laten ontsporen en onverwachte dingen laten doen.
- Ongeautoriseerd toegang verschaffen tot en gebruik van gegevens.
- Afluisteren van de pc door onbevoegden.
- Ongewenste e-mails.

Beveiligingsmaatregelen

Alvorens te starten met het beveiligen van de pc, is het van belang eerst een aantal vragen te beantwoorden en maatregelen hierop af te stemmen. Een pc waarop slechts lokaal spelletjes worden gespeeld kan met minder beveiliging toe dan een pc met (bedrijfs-) kritische gegevens, al dan niet in combinatie met internet gebruik.

- Staan er belangrijke, eventueel privacy gevoelige gegevens op de pc?
- Wordt de pc gebruikt voor internet en/of uitwisseling van e-mails?
- Hebben verschillende personen toegang tot de pc en mogen allen afzonderlijk alle gegevens op de pc benaderen?
- Welke programma's worden gebruikt voor de verschillende toepassingen? Zijn deze programma's goed ingericht / geparametriseerd?

Voor elk type bedreiging zijn verschillende maatregelen te nemen.

1 Back-ups maken

Om gebruikers tegen zichzelf in bescherming te nemen en in geval een pc of laptop toch een keer stuk gaat, is het goed regelmatig een back-up te maken van de gegevensbestanden die op de harde schijf van de pc staan. Denk niet te snel: 'dat gebeurt mij toch niet', want maar al te vaak blijkt dit toch een tijdbom te zijn die onverwacht wel degelijk af kan gaan. En als het toch nog nooit gebeurt is, dan heb je gewoon geluk gehad of ben je pas begonnen met werken op een pc. Regelmatig (dagelijks, wekelijks, maandelijks) een back-up maken kost relatief weinig tijd en biedt een grote zekerheid dat je gegevens niet kwijt raakt. Het is niet noodzakelijk geavanceerde back-up software aan te schaffen om hiermee te werken; een reserve kopie maken, al dan niet gezipt, en deze op een rewritable cd of externe harde schijf [1] te schrijven, biedt vaak al voldoende waarborg voor de gemiddelde gebruiker. Eventueel kan gebruik worden gemaakt van de back-up service van het besturingssysteem. Slechts in geval van grote, professionele toepassingen met veel waardevolle gegevens, loont het de moeite om back-up software aan te

schaffen. Al moet je je in dat geval ook afvragen of de pc wel het meest geschikt is voor dit soort toepassingen.
Nadat een back-up is gemaakt is het raadzaam zo nu en dan even te proberen een restore (het terugzetten van een back-up) uit te voeren, zodat je zeker weet dat dit ook lukt als de nood echt aan de man is. Het is enkele keren gebeurd dat er, om uiteenlopende redenen, echt geen restore gedaan kon worden.

2 Antivirus software installeren

Antivirus software beschermt de pc tegen kleine programmaatjes die zich hechten aan allerlei bestanden of andere programma's waardoor deze onverwacht geactiveerd kunnen worden en schade kunnen toebrengen aan gegevens of geheime informatie kunnen achterhalen en via e-mail naar de afzender sturen. Deze virussen komen op de pc via internet, e-mail, 'logische kanalen' (poorten) waarmee het mogelijk is voor programma's om bijvoorbeeld client – server architectuur te werken en chatten. Belangrijk is de antivirus software up to date te houden en regelmatig de laatste wijzigingen te downloaden en te activeren. Alle bekende antivirus software is tegenwoordig zo gemaakt dat als er een verbinding met het internet is, de software zelf direct verbinding zoekt met de internet site van de leverancier en de wijzigingen automatisch ophaalt en activeert[2].

3 Firewall

Een firewall is software die onder andere poorten dichtzet en slechts gecontroleerd verkeer mogelijk maakt. Het is erg belangrijk deze software te activeren omdat hiermee een waarborg wordt verkregen tegen het ongeautoriseerd binnen komen of uitgaan. Firewall software is veelal onderdeel van de belangrijke antivirus software[2] en van het besturingssysteem[3].

4 Draadloze netwerken

Naast de hiervoor genoemde gevaren zijn draadloze netwerken een extra bedreiging voor de pc. Handige pc gebruikers kunnen, mits binnen een bepaalde straal, draadloze netwerken 'afluisteren' en toegang verkrijgen tot de gegevens op de pc. Door deze draadloze netwerken gecodeerd te laten werken, wordt dit gevaar sterk gereduceerd. Een en ander is wel afhankelijk van het gebruikte codeer protocol. Op dit moment is WPA de beste beveiliging voor draadloze netwerken.

5 Register bescherming

Sommige virussen installeren zichzelf in het registergeheugen. In dit gedeelte van het computergeheugen staan allerlei programma's en gegevens over die programma's die voor het besturingssysteem essentieel zijn en waarmee de goede werking wordt gewaarborgd. Virusprogramma's in het register kunnen allerlei waardevolle informatie verzamelen of programma's en gegevensbestanden onbruikbaar maken. Ze werken voor de gebruiker onzichtbaar, maar kunnen grote schade aanrichten.

Door een programma te installeren dat controleert op wijzigingen in het register en deze tegenhoudt, is weer een stap gezet naar een veilige omgeving.

6 Spam

Spam is ongevraagde e-mail die naar de geadresseerde wordt gestuurd. Hierin schuilt niet zozeer het gevaar van virussen, maar het is veelal ongewenst, kost tijd en ruimte en kan in sommige gevallen confronterend zijn[2].

7 Parametrisering

Beveiliging begint bij de inrichting van de pc. Nagenoeg alle programma's kennen wel een menukeuze Opties of Eigenschappen of Instellingen, of iets dergelijks. Hiermee kan al een begin worden gemaakt met het beveiligen van de pc door alle opties goed door te nemen en de juiste keuzes te maken. Bij twijfel kan de documentatie worden gelezen of informatie zoeken op internet (...). Wees in elk geval alert op keuzes om al dan niet cookies en wijzigingen in het register of het bestandssysteem toe te staan. Wees alert op het openen van macro's in programma's. Of beter: regel dit zoveel mogelijk op besturingsniveau.

Het loont absoluut hier in een vroeg stadium de nodige aandacht aan te geven. Ook al wordt al langere tijd zonder problemen met de pc gewerkt, het loont ook dan nog de moeite om hier aandacht aan te geven.

Kosten

De kosten voor het nemen van de bovengenoemde beveiligingsmaatregelen, zijn een fractie van de aanschafprijs van de pc, het internet abonnement en de software. Hiervoor hoeft het dus niet achterwege gelaten te worden. Denk ook aan de kosten bij verloren gaan van gegevens (derving, extra tijd en geld voor herstel, etc). Welke redenen zijn dan nog aan te voeren om niet (of gedeeltelijk) te beveiligen? Gemakzucht? Onwetendheid? Onverschilligheid? Tijdgebrek? Kortom: gewoon doen!

In tabelvorm ziet het er als volgt uit:

Bedreiging/ maatregelen	Gegevens bescherming	e-mails en internet gebruik	Verschillende gebruikers	Draadloos netwerk	Register wijzigingen
Backups	V				
Anti virus	V	V	V		V
Firewall	V	V	V		
Decodering	V			V	
Parametrisering	V	V	V	V	V

Baten

De baten zijn moeilijk in geld uit te drukken, maar iemand waarbij wel eens is ingebroken of iemand die een verkeersongeluk heeft gehad weet wat de autogordel kan betekenen. Of iemand die met -10 de straat op gaat, weet hoe fijn die dikke jas nu is. Het is niet zo dat daarmee alle ellende is te voorkomen. Inbraken worden nog steeds gepleegd, maar een goed beveiligde omgeving biedt hiertegen wel veel meer waarborgen.
Zo is het ook met beveiligingsmaatregelen op de pc. Je voorkomt tenminste een hoop gezeur, ergernis en onnodig tijdverlies. Het is goed hierover eerst na te denken: 'stel dat mijn adressenbestand nu corrupt raakt of ik mijn orderbestand per abuis heb verwijderd (stom, stom, stom, maar hoeveel tijd kost het me om een en ander te herstellen? En vooral: KAN het nog worden hersteld?) of een virus mijn pc onbruikbaar heeft gemaakt of geheime, privacy gevoelige gegevens worden gestolen en ik x dagen niet op mijn pc kan werken'? Het kan zelfs voorkomen dat je niet eens gemerkt hebt dat gegevens gestolen zijn en er onverwacht mee wordt geconfronteerd.

Toekomst

Het gebruik van internet, e-mail, (lokale) netwerken zal meer toenemen.
Nieuwe hardware en software zullen weer nieuwe bedreigingen met zich meebrengen waarvoor aanpassingen aan de huidige beveiligingssoftware en beveiligingsmaatregelen gerealiseerd zullen worden. Door goed op de hoogte te zijn met de software die op de pc is geïnstalleerd en te weten volgens welke protocollen gegevens worden verwerkt of verstuurd, kan al een eerste stap worden gezet naar beveiliging.

Voetnoten:
1. Een externe harde schijf is al verkrijgbaar vanaf € 70,– (30 GB).
2. Antivirus software is er vanaf € 34.95 voor een jaarabonnement. Er zijn ook internet security pakketten die niet alleen antivirus bieden maar ook antispam, firewall, antispy en parental control. Prijzen vanaf € 55,–.
3. Gebruik òf de één òf de ander, maar niet beide!

(Prijzenbron: Paradigit, Wageningen)