Helpdesk

helpdesk@rc.rug.nl

Met dank aan de RC Servicedesk

Extra beveiliging van uw pc bij gebruik van een kabelmodem

Helpdesk is een vaste rubriek waarin vragen en problemen met betrekking tot computergebruik worden behandeld. Dit keer wordt het internetten via de kabel kritisch belicht.

Steeds meer mensen schakelen over op internet via de kabel. Een pc met een vaste internetverbinding zoals bij een kabelmodem loopt grotere risico's dan een pc die slechts een paar momenten per dag met een modem is ingelogd.
Ook het feit dat een pc met een kabelmodem meestal een vast internetadres heeft, maakt het risico groter. Wanneer u thuis een internetverbinding via de kabel heeft, is het daarom verstandig wat extra maatregelen te nemen.
Het grootste gevaar voor een ontregelde pc blijft het gedrag van de eigen gebruiker. Alle beveiligingsmaatregelen halen weinig uit als in het wilde weg programma's van het internet worden gedownload, e-mail attachments zonder meer worden opgestart en gekopieerde (gekraakte) programma's worden geïnstalleerd.

De risico's

Pc's die op internet zijn aangesloten via een kabelmodem zijn extra vatbaar voor de volgende risico's:

- Personen die zich via het internet toegang willen verschaffen tot uw pc. Dit kan zijn om uw gegevens te lezen, bestanden te beschadigen, te wissen of zelfs de pc onklaar te maken.
  Vaak worden ook pc's gebruikt als tussenstation om illegale activiteiten uit te voeren, bijvoorbeeld het kraken van grote computers, of het uitvoeren van gecoördineerde aanvallen op computersystemen. U kunt zonder het te weten verdacht worden van het plegen van een computermisdaad!
- Op uw pc kan een 'Trojaans Paard' zijn geïnstalleerd. Dit kunt u zelf hebben gedaan toen u dat leuke programmaatje installeerde! Met een dergelijk programma wordt een 'achterdeur' opengezet waarmee via het internet uw pc geheel kan worden overgenomen. Ook uw toetsaanslagen kunnen worden meegelezen; hiermee kunnen bijvoorbeeld uw wachtwoorden worden afgekeken. Ook kan uw pc plotseling een 'eigen leven' gaan leiden omdat iemand anders de bediening heeft overgenomen. Bekende voorbeelden zijn 'Back Orifice' en 'Netbus'. Het programmaatje kan natuurlijk ook gewoon uw harde schijf wissen.
- U loopt extra risico om een computervirus binnen te halen omdat downloaden zo lekker snel gaat. Tegenwoordig zijn het meestal macrovirussen in een Word-bestand. Vooral '.doc-bestanden' als e-mail attachment of e-mail in HTML-formaat vormen hier het grootste risico omdat hierdoor programma's van anderen op uw pc kunnen worden gestart.

Adviezen

Voor een kabelaansluiting zijn daarom de adviezen, die eigenlijk voor alle internetgebruikers gelden, nog iets belangrijker:

- Zet de *file- en printer-sharing* uit. Als u deze toch nodig hebt, zorg dan voor goede wachtwoorden en beperk de toegang zoveel mogelijk.
- Installeer een goede virusscanner en haal regelmatig (wekelijks) nieuwe virusbeschrijvingen op (dit kan eenvoudig met de visusscanner).
- Istalleer zonodig 'firewall'-software of andere speciale beveiligingsprogramma's.
- Is uw virusscanner of firewall een aantal jaren oud? Overweeg dan om een nieuwe versie van het programma te installeren. Door de ontwikkelingen op beveiligingsgebied worden antivirusprogramma's voortdu-

rend aangepast. Updaten is op een gegeven moment niet meer voldoende of niet meer mogelijk.

- Kijk regelmatig, met bijvoorbeeld 'Windows Update', of er 'reparaties' van Windows bestaan (speciaal wat betreft veiligheidslekken). Dit geldt met name voor gebruikers van het programma Outlook en Outlook Express.
- Werk veilig, d.w.z. start niet zomaar e-mail attachments op, let op van waar u software binnenhaalt van het internet. Bijvoorbeeld: gekraakte ('warez'-) software is verdacht. Deze en andere programma's kunnen virussen bevatten of Trojaanse Paarden, waarmee uw pc wordt voorzien van een 'achterdeur' waardoor men de pc totaal kan overnemen via het netwerk (Back Orifice, Netbus).
- Controleer bestanden die u van anderen krijgt of van het internet downloadt altijd voor het openen op virussen met de virusscanner.
- Zorg ervoor dat u uw belangrijke documenten en data regelmatig bewaart op een afzonderlijk medium: gebruik hiervoor diskettes of (re)writable cd's. Controleer *altijd* of de gemaakte *backup* zelf door uw computer kan worden gelezen: het is erg sneu wanneer je een backup nodig hebt, maar de backup zelf blijkt niet te kunnen worden gelezen. Zorg ervoor dat de *backup* is gemaakt *voordat* uw computer is gehacked. Zodra er is ingebroken in uw computer zijn alle bestanden in uw computer verdacht, en dienen ze te worden vervangen door nieuwe, verse bestanden.

Hulpmiddelen

Met slechts heel weinig hulpmiddelen kunnen al heel wat problemen worden voorkomen of tenminste op tijd worden ontdekt.

Een onmisbaar hulpmiddel is een goede virusscanner. Thuis-pc bezitters van de RUG hebben een virusscanner van MacAfee of Norton op hun pc. Gebruik de scanner zo nu en dan, bij voorkeur na downloaden nieuwe software. En haal ook regelmatig (wekelijks) nieuwe virusdefinities op. Heeft u ZoneAlarm geïnstalleerd dan moet u wel even toestemming geven aan dit programma om het internet te gebruiken.

Om de internettoegang tot uw pc af te sluiten bestaan zogenaamde persoonlijke *firewall*-programma's, bijvoorbeeld van Norton. Een ander praktisch programma is 'ZoneAlarm', waarmee u precies kunt aangeven welke programma's op uw pc het internet kunnen gebruiken en welke programma's aan anderen toegang tot de pc verlenen. Alle andere toegangsmogelijkheden worden dichtgezet en zijn niet zichtbaar vanaf het internet.

Ieder programma dat toegang tot het internet wil, zal eerst een vraag veroorzaken of dat wel mag. Het is duidelijk dat Netscape wel in orde is, maar als de screensaver dit vraagt dan moeten er wat alarmbellen gaan rinkelen.

U kunt het programma downloaden van **www.zonelabs.com** waar ook een uitleg te vinden is. Informatie over Zone Alarm en de installatie is ook te vinden op de Surfkit-website **www.surfkit.nl/instructions/firewall/home.html**. In verband met aanpassingen op deze website is het mogelijk dat de informatie op een andere plek terug te vinden is op de Surfkit-website.

Wilt u zich overtuigen dat een dergelijk programma echt nodig is, surf dan eens naar Gibson Research Corporation (http://grc.com) en klik op 'Shields UP!'. Hier kunt u testen hoe toegankelijk uw pc is.

Foute boel?

Heeft uw computer ondanks de voorzorgsmaatregelen toch een virus opgelopen? Verbreek dan de verbinding met internet om te voorkomen dat uw pc ellende bij anderen veroorzaakt. U kunt proberen met uw virusscanner het virus te verwijderen. Probleem hierbij is dat een virusscannner voor een eenmaal actief geworden virus niet altijd in staat is de eenmaal aangerichte schade geheel te herstellen.

Op de website van de leverancier van uw virusscanner kunt u kijken of er meer informatie beschikbaar is over het verwijderen van het virus (gebruik hiervoor wel een andere pc met internetverbinding!). Mocht u daar geen informatie kunnen vinden, dan kunt u bijvoorbeeld kijken op de website van 'VirusAlert', (**www.virusalert.nl**) waar veel informatie is te vinden over virussen en het verwijderen daarvan.

Uiteraard kunt u ook altijd contact opnemen met uw helpdesk (voor internetabonnees van de RUG is dat de RC Servicedesk: (050) 363 32 32).