Anti-inbraaktips voor computers

- Inbraak in uw computersysteem kan in belangrijke mate worden voorkomen, indien men de computer uitrust met een z.g. Firewall (brandmuur). Deze software controleert elke informatie vanaf het internet/intranet die naar binnen komt. De goede Firewalls controleren ook het uitgaande verkeer (uitbraakbeveiliging Trojaans Paarden). ZoneLabs geeft gratis Firewalls uit (ZoneAlarm). Deze Firewall controleert in- en uitgaand verkeer;
- Een goede Firewall dient z.g. aanvals-handtekeningen te bezitten. Wanneer een dergelijke aanval op uw systeem wordt uitgevoerd, blokkeert de Firewall de ingaande communicatie met de inbreker;
- Inbrekers zijn niet alleen hackers, maar ook computervirussen (wormen) die proberen een zwak beveiligde computer te vinden via het internet en vervolgens proberen binnen te komen;
- Installeer ook een virusscanner. Voor bedrijven worden virusscanners aanbevolen die een ICSA-lab certificatie hebben. Hierdoor is een garantie afgegeven dat het afvangpercentage voor virussen 100% is. Zie daarvoor de website van ICSA-lab. Een zeer goede virusscanner is NOD32, die vooral via de z.g. heuristische methode kwaadaardige software kan afvangen;
- Controleer via het software programma Microsoft Baseline Security Analyser (Windows platform) of uw systeem kwetsbaar is. De BSA geeft dan richtlijnen hoe de beveiliging van uw computersysteem verbeterd moet worden;
- Installeer ten slotte een aantal goede spyware-scanners. Deze scanners kunnen voorkomen dat uw computer door spyware, dialers, highjackers en andere malware kan worden overgenomen;
- Zorg ervoor dat u altijd de nieuwste virusdefinities ophaalt van het internet en deze installeert in uw virusscanner. Dit geldt ook voor de spyware-scanners. Zonder een actueel databestand van virus-handtekeningen is uw computersysteem kwetsbaarder. Controleer of er geregeld updates of upgrades zijn voor uw Firewall;
- Maak altijd voldoende back-ups om uw computersysteem (na een virusaanval of inbraak) te herstellen. Kopieën van uw klantenbestand, voorraadbeheer, leveranciers en financiële administratie moeten altijd gemaakt worden;
- Controleer of uw besturingsysteem een nieuwe update nodig heeft. Updates zijn belangrijk, omdat er kritieke lekken kunnen worden dichtgegooid. Digitale inbrekers zijn vaak genoeg op zoek naar zwakheden in computersoftware en gebruiken die om binnen te komen. Wie een Windows-platform heeft kan de nieuwste updates downloaden via Windows Update.