WWW.MINDYOURSTEP.INFO

Beveiligingssoftware

waar beschermt het je eigenlijk wel en waar niet tegen?

De vraag

Wanneer je computer is aangesloten op het internet is beveiligingssoftware tegenwoordig noodzakelijk om veilig gebruik te kunnen maken van je computer. Zelfs wanneer je zeer oplettend bent en denkt een betrouwbare website te bezoeken, kan er malware op je computer komen omdat deze 'betrouwbare' website zelf is gehackt. Malware is software die is ontworpen om schadelijke en ongewenste handelingen te verrichten. Computervirussen zijn de meest bekende vorm van malware. Maar ook Wormen, Spyware en Troyan Horses vallen in de categorie malware. Je kunt je dus terecht afvragen of een virusscanner nog wel voldoende beveiliging geeft. Wanneer je van onveilige bronnen software download, deze zonder controle installeert en daarbij je beheerderswachtwoord invult omdat de installatie daar nou eenmaal om vraagt, dan kan zelfs de beste virusscanner je niet helpen bij het voorkomen van infiltratie door malware. Kortom, je moet zelf oplettend blijven en kunt helaas niet klakkeloos vertrouwen op je beveiligingssoftware. Want ook wanneer je niets 'doms' doet, kun je gemakkelijk geïnfecteerd raken door malware. Beveiligingssoftware is er in verschillende soorten en maten. Een virusscanner, Anti Spyware, Anti Rootkit of een Firewall zijn voorbeelden van beveiligingssoftware die zich op verschillende soorten van besmetting van je computer richten. Het verschilt in bescherming, betrouwbaarheid, gebruikersgemak, functies en mogelijkheden, stabiliteit, hulp, support en niet onbelangrijk, het verwijderen van ongewenste data. Welke beveiligingssoftware heb je nodig en waar beveiligt het tegen?

De uitdaging

Besmetting door een virus is misschien niet eens het meest spannende waar je beveiligingssoftware je tegen moet beschermen. Voor criminelen is het verkrijgen, delen en gebruiken van je persoonlijke data, zoals je bankgegevens het meest interessant. Een virusscanner alleen is tegenwoordig dus niet meer genoeg. Anti Spyware, Anti Rootkit, Firewall en gegevensbescherming zijn geen overbodige luxe meer.
Anti Spyware software controleert je computer op schadelijke bestanden die onder andere gegevens van jou en je gebruik op je computer opslaan en doorsturen. Vaak komt Spyware door de beveiliging van je virusscanner heen. Anti Spyware software is speciaal ontworpen om deze vorm van malware wel te detecteren. Anti Rootkit software zoekt naar schadelijke, verborgen data op je computer of naar andere malware die de data verborgen wil houden. Criminelen proberen malware namelijk te verstoppen, waardoor deze niet wordt gedetecteerd door beveiligingssoftware. Anti Rootkit software helpt bij het opsporen hiervan.
Een goede firewall controleert de inkomende en uitgaande data van je computer naar het internet. Een firewall helpt dus te voorkomen dat een crimineel data van of naar je computer stuurt.

Voor gegevensbescherming bestaan geen of nauwelijks softwareprogramma's. Wees dus zelf bewust van welke persoonlijke gegevens je op je computer opslaat en wie daar allemaal toegang toe heeft. Maar besef je ook dat via malware ook achter je persoonsgegevens gekomen kan worden, zonder dat die op je computer staan opgeslagen. Bijvoorbeeld via het hacken van je webcam of via het in je mail vragen om je bankgegevens en verwijder (identiteits)gegevens op oude computers en telefoons.

De oplossing

De beste virusscanner ben je natuurlijk zelf. Maar oplettendheid alleen is niet meer genoeg. Onderstaande tips helpen je bij een zo veilig mogelijk computer- en internetgebruik.

- Ken de functies van je beveiligingssoftware. Lang niet elke virusscanner controleert bijvoorbeeld je e-mailverkeer. En ook het onschadelijk maken van malware kan per beveiligingssoftware verschillen.
- Gebruik originele versies van software. Juist de illegaal te downloaden beveiligingssoftware bevat vaak malware.
- Update je beveiligingssoftware zodra een update mogelijk is. Deze bevat de nieuwste beveiliging. Criminelen ontdekken vaak in verouderde software de zwakke plekken. Beveiligingssoftware die zichzelf elke dag automatisch een update geeft, heeft de voorkeur.
- Wijzig bij de aanschaf van onder andere een router, acces point of webcam de standaard gebruikersnaam en het wachtwoord. Criminelen kennen de standaard inloggegevens.
- Stel Wi-Fi Protected Acces (WPA) in op je access point of wireless router. Dit verbetert de beveiligingsfuncties van de standaard versleuteling, die voorkomt dat andere gebruikers verbinding kunnen maken met je draadloze netwerk.
- Beperk de rechten van gebruikers, inclusief die van jezelf. Niet de hackers zelf, maar gebruikers veroorzaken de meeste fouten door (onbewust) onveilige software te installeren.
- Gebruik een 'privacy filter' en webcamcover. Een privacy filter is een dun velletje dat je voor je beeldscherm plaatst waardoor de inkijkhoek verkleint wordt en alleen jij op je beeldscherm kunt kijken. Een webcamcover voorkomt ongewenst meekijken van criminelen.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak. Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.