(On)veilige websites

Dagelijks kraken criminelen zo'n 1200 websites. Hoe weet u welke websites veilig zijn om te bezoeken, en is uw eigen homepage nog wel veilig? Twee beveiligingsexperts geven antwoord op 10 brandende vragen.

1 Welke sites zijn meestal doelwit?

Elke website die niet veilig is geprogrammeerd, of waarvan de software verouderd is, loopt risico. Bij recente aanvallen ging het om het 'injecteren' van kwaadaardige SQL-code. Een aanvaller kijkt dan niet naar het soort website, maar zoekt naar een beveiligingslek in de programmatuur. Verder wordt geprobeerd bezoekers van sociale netwerken en forums naar besmette websites te lokken.

2 Hoe weet ik of ik een site veilig kan bezoeken?

Dat is nooit met honderd procent zekerheid te zeggen. Websites weten vaak zelf niet dat ze gehackt zijn. Goed nadenken en gezond verstand zijn het belangrijkst. Klik niet zomaar op een link en pas op met het openen van bestanden. Helaas kan uiteindelijk zelfs een legitieme website besmet blijken.

3 Kan mijn virusscanner helpen?

Veel viruspakketten hebben een lijst met gevaarlijke websites die worden geblokkeerd. Ook zoekmachines als Google waarschuwen bij gevaar. Het is geen garantie dat het nooit fout gaat, dus blijf goed opletten en uw systeem up-to-date houden. Een virusscanner is de laatste schakel in uw defensie.

4 Vangt mijn virusscanner drive-by downloads op?

Een ongevraagde download kan worden onderschept, want die komt op uw pc terecht. In virusscanners zit intelligentie die probeert om nieuwe bedreigingen te herkennen, maar ook hackers zitten niet stil. Het blijft een race tegen de klok.

5 Een site wil iets op mijn pc installeren, is dat verstandig?

Door websites voorgestelde installaties zijn een risico. Hebt u bijvoorbeeld Java of Flash nodig, dan kunt u die het best ophalen op de website van de fabrikant zelf.

6 Kan ik na een vakantie wel veilig surfen en e-mailen?

Wacht altijd een paar minuten met surfen en e-mailen totdat alle updates van Windows en de virusscanner binnen zijn. Bij overige software kunt u controleren of u de meest recente versie hebt, of ze doen dit automatisch.

7 Loopt mijn website gevaar bij mijn provider of hoster?

De provider kan problemen voorkomen door de aangeboden software up-to-date te houden en onveilige systeeminstellingen uit te schakelen. Controleer ook of u zelf actie moet ondernemen (bijvoorbeeld een nieuwe versie activeren).

8 Moet ik mijn website veiliger maken?

Veel hangt af van de hulpmiddelen die u gebruikt. Hoe meer intelligentie, hoe meer er fout kan gaan. Bijvoorbeeld vanwege lekken in de software. Een site met alleen html-code; daar kan een hacker weinig mee, zolang deze goed beveiligd is. Programmeert u zelf, verdiep u dan in richtlijnen voor veilig programmeren.

9 Kan ik zien of mijn site besmet is?

Google controleert regelmatig of websites kwaadaardige code bevatten. Providers voeren ook controles uit en krijgen klachten als een website besmet is. Verder kan uw virusscanner alarm slaan, er kan ongewoon veel dataverkeer op de site zijn, of er verschijnen dingen die er niet thuishoren.

10 Wat moet ik dan doen?

Zoek uit om welke pagina's het gaat en hoe de aanvallers zijn binnengekomen. Haal de site direct offline, verwijder de gevaarlijke code en dicht het lek. Daarna kan de site weer online. Misschien hebt u hulp van de provider nodig. ■

De experts:

- Eddy Willems, IT Security Evangelist bij Kaspersky Lab Benelux BV.
- Joran Polak, hoofdredacteur van Security.nl