EDDY WILLEMS
is malware researcher, met meer dan 20 jaar ervaring op zijn actief. Hij is security evangelist bij securityspecialist G-Data, en is directeur informatie en pers van EICAR (European Institute for Computer Anti-Virus Research).

Het testen van malware en veiligheid in een zure regenwolk

Ik stootte met mijn hoofd tegen mijn nieuw bureau toen ik er vanonder kroop. De volgende dagen ontsierde een nare buil mijn hoofd, maar gelukkig waren de vier interne netwerken bij mij thuis volledig geherstructureerd en voorzien van de laatste nieuwe beveiligingssnufjes. Dat is een onderdeel van mijn beveilingsbeleid en zo'n beleid is zowat het allerbelangrijkste dat een bedrijf zou moeten hebben. Blijkbaar is dat echter nog niet het geval, zo leert EICAR (European Institute for Computer Anti-Virus Resaerch) ons, tenzij je gaat kijken bij de grotere bedrijven zoals banken en verzekeringsfirma's.

Maar we zitten hier in België wel met meer dan 90% bedrijven (volgens KMO-IT) die onder de noemer kmo vallen. En raad eens hoeveel er daar een 'beveiligingsbeleid' hebben? Volgens statistieken van EICAR komen we hier op een goede 10% uit. Een beveiligingsbeleid is immers meer dan het installeren van een anti-virus pakket en een firewall. Die software en hardware is overigens wel broodnodig, want vandaag kijken we aan tegen een berg van 50 miljoen malware. Een torenhoog probleem waar de cybercrime aan de basis van ligt en dat zal zo blijven in de komende jaren.

Het internet maakt het voor iedereen te makkelijk om foute dingen te doen. Voor velen wordt de grens tussen goed en kwaad ook heel erg dun. Wanneer ga je over de streep? Als je op YouTube laat zien hoe je makkelijk een beveiligingspakket in de luren kan leggen? Of als je zelf een deel van een botnet gekocht hebt om wat mails te versturen naar mogelijke klanten? Beide mogelijkheden zijn niet goed te praten, maar dat standpunt lijken nog slechts enkelingen te delen, lijkt het soms. Momenteel zorgen tientallen botnets, met miljoenen pc's in de macht van de underground, voor de meeste problemen. En dan spreken we nog niet over het probleem dat veel *command-and-control centers* draaiden of draaien bij isp's van een buurland van ons: Nederland. Normvervaging, laksheid of vrijheid, waaronder zouden we dat klasseren?

Vaak wordt me gevraagd hoe infecties nog mogelijk zijn, nu iedereen toch een deftige beveiliging heeft? Het volgende voorbeeld volstaat. Op drie van de vijf events waar ik verleden jaar aanwezig was, bleken geïnfecteerde usb-sticks de ronde te doen. In alle opzichten is de usb-stick dus echt wel de vervanging van de floppy en zelfs met goede maatregelen kunnen langs deze weg heel wat problemen zich aandienen. Ook hier is een strikt nageleefd beleid belangrijk. Het menselijk gedrag in goede banen leiden, is dan ook een sleutelfactor in een solide beleid. De beveiligingsproblemen van sociale netwerksites zijn ondertussen volop gekend en het einde is ook daar nog niet in zicht. Aanvaard jij alle applicaties op jouw Facebook? Ik alleszins niet! Wees ook voorzichtig met alle mogelijke plugins voor Firefox, met oudere Flashversies of niet up-to-date Adobe Acrobat Reader software.

We willen ook allemaal te snel aan informatie geraken. Twitter is hiervan een prachtig voorbeeld. De grootste dreiging gaat evenwel uit van geïnfecteerde websites, ook legitieme, door malware als Gumblar – een plaag die gestaag uitbreiding vindt. Slechte paswoorden en slechte beveiliging van netwerken zijn hiervoor medeverantwoordelijk. Technieken als virtualisatie, in-the-cloud protectie en whitelisting worden wel steeds beter. Het gevaar is dat onze 'wolken' steeds meer worden aangevallen tot ze oplossen in 'zure' regen.

Het gevaar is dat onze 'wolken' steeds meer worden aangevallen tot ze oplossen in 'zure' regen.

Onafhankelijke testers van dat alles zullen dan ook nog aan belang winnen in de toekomst. Veel bedrijven hechten dan groot belang aan goede testen en advies over deze technieken, evenals soft- en hardware. Dit is precies één van de opdrachten van AMTSO, de Anti-Malware Testing Organisation (zie www.amtso.org). Ik meen dat er vandaag teveel testen zijn die compleet irrelevant zijn om een goed beeld te schetsen van een voldoende beveiliging. AMTSO wil een leidraad bieden voor correcte testen die een goede vergelijking mogelijk maken. Het testen van soft- of hardware is immers niet hetzelfde als het correct testen van een securitypakket of -appliance. Journalist-testers moeten de AMTSO-richtlijnen maar eens doornemen, want zo helpen ze bedrijven en toekomstige gebruikers om de wereld wat veiliger te maken. Ik raad iedereen aan om dit van nabij te volgen. Belangrijk is ook het advies van security consultants, zelfs als je niet echt zeker bent of dit wel geheel objectief is. Het is in ieder geval een aanrader als je niet wil dat je netwerk of je bedrijf een nare buil oploopt.#