OUCH! | December 2014

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Wat is antivirus?

Overzicht

Antivirus is een beveiligingsprogramma dat je op jouw computer of mobiel toestel installeert om het te beschermen tegen malware infecties. Het begrip 'malware' is een verzamelnaam voor verschillende vormen van schadelijke software zoals virussen, worms, Trojans en spyware. De oorsprong van het woord malware komt van de woorden malicious en software. Als jouw computer geïnfecteerd is met malware, dan kan een cyberaanvaller bijvoorbeeld al jouw toetsaanslagen registreren, jouw documenten stelen of zelfs jouw computer gebruiken om anderen aan te vallen. In tegenstelling tot wat vele mensen geloven, kan ieder besturingssysteem, zelfs Mac OS X en Linux, geïnfecteerd geraken.

Gastredacteur

Jake Williams is de oprichter van Rendition Infosec (**www.renditioninfosec.com**) en is een gecertifieerde SANS-instructeur en cursus auteur. Hij is actief op Twitter als **@MalwareJake** en schrijft een blog op **malwarejake.blogspot.com**.

Je kan antivirus software kopen als een alleenstaande oplossing, maar vaak maakt het deel van uit van een beveiligingspakket. Het probleem is dat antivirus niet langer cyberaanvallers kan bijbenen, aangezien er voortdurend nieuwe types en versies malware worden uitgebracht. Dagelijks worden er zoveel nieuwe versies malware uitgebracht, dat geen enkel antivirusprogramma dit kan detecteren of jou beveiligen tegen alle types malwares. Om dit beter te begrijpen, kijken we naar hoe de meeste van deze programma's werken.

Hoe antivirus werkt

Er zijn twee manieren waarmee antivirus software malware opspoort, signature detectie en gedragsdetectie. Signature detectie werkt zoals het menselijk immuniteitssysteem. Het scant jouw computer voor bepaalde tekenen of signatures van bekende schadelijke software. Dit gebeurt doordat er een woordenboek met gekende malware wordt geraadpleegd, indien iets op de computer overeenkomt met een patroon in het woordenboek, probeert het programma dit te neutraliseren. Net als bij het menselijk immuniteitssysteem, vereist het woordenboek updates, zoals griepvaccins, om bescherming te bieden tegen nieuwe malware varianten. Antivirus beschermt enkel tegen datgene wat bekend is als schadelijk. Het probleem is dat cyberaanvallers snel nieuwe malware varianten uitgeven zodat antivirus producenten ze niet meteen kunnen bijhouden. Hierdoor is er, ongeacht hoe recent jouw antivirus werd geupdated, altijd een nieuwe malware variant die mogelijk jouw antivirus software omzeilt.

Wat is antivirus?

Met gedragsdetectie, probeert de antivirus de malware niet te identificeren, maar wordt er eerder gekeken naar het gedrag van geïnstalleerde software op jouw computer. Wanneer een toepassing verdacht gedrag toont, zoals het raadplegen van een beschermd bestand of het wijzigen van een andere toepassing. Dan zal de gedragsbaseerde antivirus het verdacht gedrag opmerken en dit aan jou melden. Deze aanpak voorziet beveiliging tegen nieuwe soorten van malware die nog niet in een woordenboek zijn opgenomen. Het probleem met deze aanpak is dat er valse meldingen kunnen optreden. Jij, de computergebruiker, kan hierdoor verward worden over wat je precies mag en wat je niet mag toestaan en zo ben je op de duur niet meer vatbaar voor deze meldingen. Hierdoor kan je in de verleiding komen om op 'Accept' te klikken bij iedere waarschuwing, waardoor jouw computer een doelwit is voor aanvallen en infecties. Bovendien, tegen de tijd dat de aanval is opgemerkt, zal de malware allicht op jouw machine zijn uitgevoerd en weet je mogelijk niet welke acties de malware heeft uitgevoerd alvorens dat jouw antivirus programma dit heeft opgemerkt.

Antivirus is een belangrijk deel van jouw beveiliging, het kan niet alle aanvallen detecteren of stoppen. Uiteindelijk ben jijzelf de beste verdediging en niet enkel de technologie.

Antivirus is een belangrijk onderdeel om je computer en mobiele toestellen te beveiligen, we raden aan om het te installeren en actief te gebruik indien mogelijk. Alhoewel, het belangrijkste punt om te herinneren is dat ongeacht hoe je antivirus werkt, het jou nooit volledig kan beschermen tegen alle types malware. Uiteindelijk ben jijzelf en niet de technologie de sterkste verdediging tegen cyberaanvallers.

Antivirus Tips

1. Haal jouw antivirus enkel bij gekende, vertrouwde bronnen en verkopers. Cyberaanvallers verdelen heel vaak valse antivirus programma's dat in feite malware is.
2. Verzeker je ervan dat je de laatste versie van jouw antivirus programma hebt geinstalleerd. Dat je jouw jaarlijks abonnement betaald en actief is en dat jouw antivirus is ingesteld om zichzelf automatisch te updaten. Indien jouw computer gedurende een tijd offline of uitgeschakeld is geweest dan moet jouw antivirus zichzelf updaten wanneer je het terug inschakelt of verbindt met het Internet. Stel deze updates niet uit.
3. Zorg ervoor dat jouw antivirus automatisch draagbare media scant, zoals USB sticks en verzeker je ervan dat real-time bescherming is ingeschakeld.
4. Besteed aandacht aan waarschuwingen en meldingen van jouw antivirus toepassing. De meeste meldingen bieden de mogelijkheid tot meer informatie of bevatten een aanbeveling over wat je moet doen. Indien je een melding krijgt op jouw werkcomputer, contacteer dan onmiddellijk de helpdesk of jouw leidinggevende.
5. Deïnstalleer of schakel jouw antivirus programma niet uit omdat je het gevoel hebt dat het jouw computer vertraagt,

Wat is antivirus?

een website blokkeert of jouw ervan weerhoudt om een app of toepassing te installeren. Door jouw antivirus uit te schakelen ga je jezelf blootstellen aan onnodige risico's, met mogelijk een serieus security incident tot gevolg. Indien er problemen zijn op een werkcomputer, contacteer dan jouw helpdesk. Indien er problemen zijn op een persoonlijke computer, contacteer dan de antivirus leverancier, bezoek hun website voor meer informatie of vervang jouw antivirus door een ander product.

6. Installeer geen meerdere antivirus toepassingen op jouw computer. Dit zorgt ervoor dat de programma's zullen conflicteren met elkaar en kunnen de beveiliging van jouw computer mogelijk verminderen.
7. Herken de waarschuwingen van jouw antivirus toepassing. Cyberaanvallers kunnen mogelijk schadelijke websites opzetten die realistische antivirus meldingen posten en bieden 'hulp' aan om jouw computer te repareren. Het klikken op links of knoppen van zulke websites zullen schade aanbrengen aan jouw computer.

Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Anti-Virus Product Comparisons:	http://www.av-test.org/en/
Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Email Phishing Attacks:	http://www.securingthehuman.org/ouch/2013#february2013
I'm Hacked, Now What?:	http://www.securingthehuman.org/ouch/2014#may2014

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers