Virusscanner biedt veiligheid, maar is ook een wapen

Als je net een virusscanner hebt geïnstalleerd, voel je je waarschijnlijk een stukje veiliger. En in veel gevallen is dat ook zo. Maar er is een keerzijde: antivirussoftware kan ook worden misbruikt door inlichtingendiensten en criminelen om je computer over te nemen of bestanden te stelen.

Dat blijkt ook weer nu de Nederlandse overheid waarschuwt voor de antivirussoftware van Kaspersky. De Rijksoverheid wordt zelfs volledig verboden om Kaspersky-antivirussoftware te draaien, uit vrees dat Kaspersky-software door de Russische overheid kan worden misbruikt voor spionage.

Waarom het kabinet daar overigens nu mee komt, is onbekend: de Amerikaanse en Britse overheden besloten afgelopen herfst al om Kaspersky in de ban te doen. Volgens het kabinet is er geen misbruik van de Kaspersky-virusscanner bekend.

Veel macht

Virusscanners zijn een interessante plek voor overheidshackers en criminelen om aan te vallen, omdat antivirussoftware zoveel macht heeft over de computer waarop hij draait.

Er zijn zelfs beveiligingsonderzoekers die ervoor waarschuwen om helemaal geen antivirussoftware te draaien. "Antivirussoftware werkt niet en maakt mensen onveilig voor gerichte aanvallen", schrijft de bekende beveiligingsonderzoeker Travis Ormandy bijvoorbeeld op Twitter.

Ik zou consumenten nog steeds adviseren om een antivirusscanner te installeren
Beveiligingsonderzoeker Maarten van Dantzig

Beveiligingsonderzoeker Maarten van Dantzig van beveiligingsbedrijf Fox-IT - dat zelf geen antivirussoftware maakt - noemt dat advies "zeer overdreven". "Ik zou consumenten nog steeds adviseren om een virusscanner te installeren", zegt hij.

Maar risico's zijn er wel. "Antivirussoftware zit redelijk diep in je besturingssysteem", zegt Van Dantzig. Antivirussoftware draait in de zogenoemde kernel van Windows en Mac OS X, in feite de motor van de computer. Zo kunnen ze ingrijpen als een virus zijn slag probeert te slaan. Een aanvaller kan daar misbruik van maken.

Analyses

"Als je een virusscanner installeert, onderschept die virusscanner alle programma's die worden uitgevoerd", zegt Mark Loman. Hij maakt zelf beveiligingssoftware voor het Britse bedrijf Sophos. "Voordat een bestandje wordt geladen, analyseert de virusscanner of er iets vreemds aan de hand is."

Een virusscanner om de tuin leiden betekent dus dat je heel veel macht hebt als aanvaller, meer dan wanneer je een ander programma zoals Word of Google Chrome weet te kraken. Vandaar dat Russische overheidshackers volgensonder meer The New York Times in systemen van Kaspersky zaten. In hoeverre Kaspersky daarvan wist, is onduidelijk: Kaspersky zelf ontkent dat.

Volgens Amerikaanse media blijkt de software van Kaspersky desalniettemin een krachtig wapen voor de Russische overheid. Dat komt doordat de Kaspersky-antivirussoftware, net als veel andere virusscanners, verdachte bestanden opstuurt naar servers van Kaspersky voor analyse.

Bestanden worden opgestuurd als ze aan een bepaald patroon voldoen en worden aangemerkt als schadelijk bestand. Volgens Amerikaanse media wisten Russische overheidshackers dat systeem te misbruiken en konden ze via software van Kaspersky zoeken naar geheime documenten en die vervolgens bemachtigen.

Dat zou onder meer zijn gebeurd met digitale wapens van de Amerikaanse inlichtingendienst NSA, die van de privécomputer van een medewerker werden gehaald en bij Kaspersky terechtkwamen. Kaspersky erkent dat, maar zegt dat zijn virusscanner simpelweg aansloeg op die wapens, die immers als virus werden herkend.

Het bedrijf zegt nooit informatie te hebben gedeeld met de Russische overheid - maar dat hoeft ook niet per se: die Russische overheidshackers kunnen ook hebben ingebroken bij Kaspersky om die gegevens te stelen.

Kaspersky is echter niet het enige bedrijf bij wie dat laatste zou kunnen gebeuren. "Volgens mij versturen de meeste virusscanners dit soort informatie", zegt Loman. "En meestal staat dat dan standaard aan." Zijn eigen software is terughoudender, bezweert hij.

Nieuwe bedreigingen

Dat gebeurt overigens met goede bedoelingen. "Op die manier kunnen ze virussen beter detecteren en nieuwe virussen ontdekken", zegt Van Dantzig.

Het is niet de enige manier waarop virusscanners gebruikt zouden kunnen worden: met enige regelmaat worden beveiligingsproblemen in virusscanners gevonden, die door kwaadwillenden zouden kunnen worden misbruikt.

Zo vond antivirusscepticus Ormandy beveiligingsproblemen in Kaspersky-software, maar ook in software van concurrenten als Malwarebytes, Microsofts eigen beveiligingssoftware Windows Defender en Sophos. Zelfs als een antivirusbedrijf dus niet samenwerkt met een buitenlandse inlichtingendienst, zouden overheidshackers dus hun slag kunnen slaan door beveiligingsproblemen in virusscanners te misbruiken.

"Als je inbreekt op antivirussoftware, kun je beter onder de radar blijven", zegt Van Dantzig. Dat is specifiek interessant voor gerichte aanvallen op gevoelige doelwitten, waarbij de kans om betrapt te worden zo klein mogelijk moet zijn.