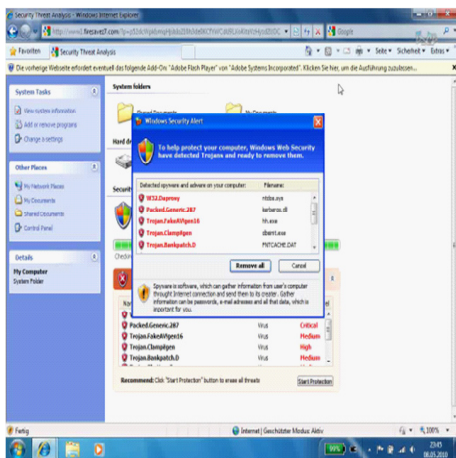


SCAREWARE

Gefahr im Internet

In den letzten Wochen haben die Meldungen über Scareware stark zugenommen. Dabei wird versucht, dem Benutzer mit einer gefälschten Virenwarnung Angst zu machen und ihn zum Besuch einer Webseite oder zum Download einer Software zu bringen.



AUTOR: ANDREAS WISLER

Bei der Suche nach Informationen im Internet erscheint plötzlich ein Fenster mit einer Virenwarnung. Das Fenster zeigt den gewohnten «Eigene Dokumente»-Ordner mit einem vorgelagerten, laufenden Virenscanner mit Virenfunden. Die erste Reaktion ist sicherlich ein grosser Schreck auf die unerwartete Meldung. Da liegt es nahe, auf den Button «Remove all» zu klicken.

ZUM AUTOR



Andreas Wisler [Tel.: 052 320 91 20,] Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Im Rahmen des Swiss Security Days ist er für die Schulungen an der Klubschule Winterthur zuständig.

Mit dem Klick auf diesen Button wird in der Regel eine Bestellseite für ein, meist nutzloses, Antivirentool geöffnet. Bevor dieses heruntergeladen werden kann, muss aber zuerst die eigene Adresse und natürlich die Kreditkarte angegeben werden.

Schauen wir uns die erscheinende Meldung etwas genauer an. Beim genauen Hinsehen ist ersichtlich, dass auch der Hintergrund im Web-Browser (hier Internet Explorer) läuft. Somit ist diese gefälscht, zeigt aber sehr schön, was mit etwas HTML-Kenntnissen möglich ist. Allenfalls wäre es auch aufgefallen, dass auf einem deutsch installierten Betriebssystem alle Meldungen auf Englisch erscheinen. Doch im ersten Schreck fällt dies in der Regel nicht auf.

11'000 verdächtige Seiten

Diese Art von Fehlermeldungen wird Scareware genannt: Scare (Schrecken) und ware von Software. Um an neue Opfer zu gelangen, versuchen die Betrüger, die Suchergebnisse von Suchmaschinen zu beeinflussen. Dazu orientieren sie sich gezielt an Begriffen, welche häufig gesucht werden und erscheinen dann in den normalen Suchergebnissen relativ weit oben. Erst kürzlich hat Google seinen Suchindex (über 240 Millio-

Die Software klammert sich hartnäckig an den PC, ...

nen Einträge) durchsucht und dabei 11'000 verdächtige Webseiten gefunden, welche Scareware verbreiten.

Mit Scareware wird reales Geld verdient. Es geht diesen Leuten nicht um „Hacker-Kunst“, sondern um den eigenen Profit. Da es hier um viel Geld geht, ist Scareware in der Regel hervorragend programmiert, auch wenn die Software schlussendlich keinen Mehrwert bietet. Einmal installiert, ist es sehr aufwendig, diese wieder zu entfernen. Die Software klammert sich hartnäckig an den PC, oft sogar hartnäckiger als ein Wurm. Immer öfter geht Scareware gegen potenzielle Gegner vor, schaltet Windows-Features und Schutzfunktionen aus.

Viele Antivirenprogramme haben Mühe, Scareware zu erkennen. Scareware kann sich sehr gut tarnen und somit vor den richtigen Antivirenprogrammen verstecken. Ein weiteres Problem ist, dass der

betrügerische Akt ausserhalb der Software-Funktion liegt. Das Opfer zahlt ja freiwillig für diese Software. Die Vertriebsmethode ist das eigentliche Verbrechen. Auf der Software-Seite gibt es in der Regel keinen Unterschied zwischen einer schlechten Antivirensoftware, welche keine Viren entfernen kann, und einer Scareware.

Sie können sich gut davor schützen, wenn Sie bei unerwartet erscheinenden Fenstern nicht der Aufforderung folgen, etwas zu installieren. Dies ist immer ein Indiz, dass etwas nicht stimmt. Werden Sie besonders misstrauisch, wenn im Web etwas, das wie ein Virenschanner aussieht, erscheint, obwohl Sie überhaupt keinen Online-Virenschanner besucht haben. Ist es bereits zu spät und es befindet sich Scareware auf dem eigenen Rechner, sollte dieser mit einer Antiviren-CD gestartet und so die störende Software entfernt werden. Dies ist oft der einzige Weg, die störende Software wieder loszuwerden. ♦

... oft sogar hartnäckiger als ein Wurm.

Blickpunkt:KMU

Success for your Business



Ihr Unternehmerportal im Netz: www.blickpunktkmu.ch