Neuer VR-Computercheck schützt vor Drive-by-Angriffen

In den letzten Monaten hat sich auf dem Feld der Online-Kriminalität viel getan. Infizierte Dateianhänge und konventionelles Phishing sind heute aus der Mode. Moderne Trojaner-Angriffe erfolgen fast ausschließlich auf bekannte Schwachstellen von Browser und Multimediakomponenten – zwei Einfallstore, die der neue VR-Computercheck jetzt schließen kann.

Kiel/Bonn, 22. November 2010 - Im letzten Jahr hat die Zahl der Personalcomputer in Deutschland erstmals die Zahl der zugelassenen Pkw überstiegen. Das Internet ist vom Tummelplatz für Computerfreaks zum Online-Medium für alle Bürger geworden. Eine Bestellung bei Amazon oder eine Überweisung im Online-Banking sind heute genauso einfach wie Autofahren. Leider hat der große Erfolg der Online-Geschäftsprozesse auch seine Schattenseiten: Mit jedem umgesetzten Euro und mit jedem online bestellten Artikel wird der private PC mehr und mehr zum Lieblingsziel von Computerkriminellen. Dabei ist der so genannte Drive-by-Angriff heute die wichtigste Technik, um private PC’s zu infizieren.



Drive-by-Angriffe sind schwer zu erkennen

Drive-by beschreibt einen "Angriff im Vorbeifahren". Kriminelle präparieren dazu vermeintlich harmlose Internetseiten mit Trojanern, die schon beim Betrachten der Seite den PC infizieren. Technisch werden hierzu Sicherheitslücken in Browsern und Browser-Plugins ausgenutzt. Noch tückischer ist es, wenn die Internet-Mafia bekannte Webseiten hackt und diese dann zur Verbreitung von Schadcode missbraucht. So etwas ist schon renommierten Websites, wie dem Hamburger Abendblatt oder dem Handelsblatt passiert. Man braucht also keine

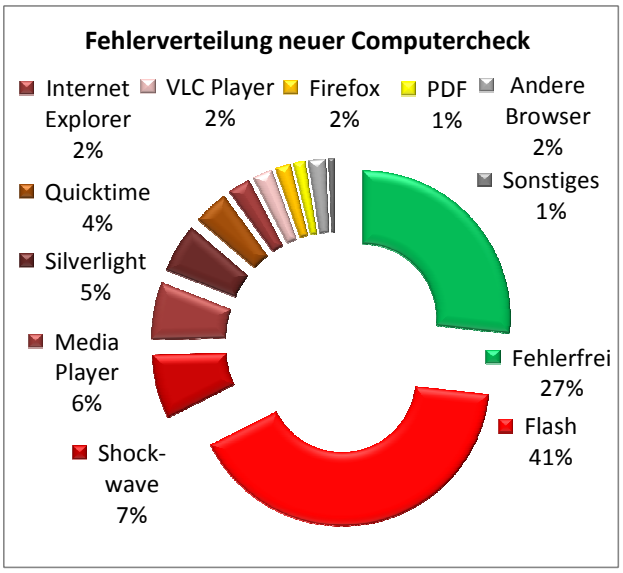
„Schmuddelseiten“ mehr zu besuchen, um sich im Netz zu infizieren. Ähnlich tückisch ist die Methode, speziell präparierte Suchseiten für beliebte Suchbegriffe zu manipulieren. Laut Spiegel landen bereits 20 % aller Suchanfragen nach dem Wort „free music download“ auf Seiten von Internetkriminellen. Als dritte drive-by Methode verwenden Angreifer Internetseiten mit Tippfehlern in der Adresse. Ein kleiner Zahlendreher oder das Vertauschen von zwei Buchstaben reicht dann meist aus, um auf einer manipulierten Seite zu landen.

Schutz durch Aktualität

Für Privatkunden ist diese Situation extrem gefährlich, da alte Verhaltensregeln für das Internet nicht mehr gültig sind. Früher hieß es „besuchen Sie keine dubiosen Webseiten“, heute sind vor allem seriöse Anbieter betroffen. Die Weisheit, „klicken Sie nicht auf unbekannte Dateianhänge“ bringt wenig, wenn die Infektion bereits beim reinen Betrachten der Internetseite ausgelöst wird. Hinzu kommt, dass der eigentliche Hacker-Angriff nicht mehr als solcher wahrgenommen wird, denn die Trojaner verhalten sich auf dem infizierten PC so lange still und leise, bis tatsächlich Geld gestohlen werden soll. Gegen dieses Vorgehen hilft nur die ständige Aktualisierung von Browser, Betriebssystem und allen Media-Plugins, um Drive-by-Infektionen von Anfang an zu verhindern.

So hilft der neue VR-Computercheck

Um diesen neuen Gefahren begegnen zu können, wurde der neue VR-Computercheck in den vergangenen Monaten technisch stark verbessert. Der Check arbeitet jetzt mit allen Internet-Browsern von Internet-Explorer bis Google Chrome zusammen. Er erkennt Sicherheitslücken in den Browsern und Multimedia-Erweiterungen wie Flash oder Quicktime. Der Computercheck erkennt bei mehr als der Hälfte aller privaten PCs gravierende Sicherheitslücken, noch bevor diese ausgenutzt werden können. Natürlich bleibt der Check seinem Konzept treu und bietet für jedes erkannte Sicherheitsloch eine ausführliche Anleitung zur Fehlerbeseitigung sowie eine technische Email-Hotline für alle weiter-



führenden Fragen. Machen Sie doch auch einmal wieder den Test, Sie werden überrascht sein, wie sehr Ihnen der neue Computercheck helfen kann. Der Check wird seit vielen Jahren von über 500 Volksbanken Raiffeisenbanken in ganz Deutschland erfolgreich eingesetzt. Die neue Version können Sie unter http://www.coronic.de/vr-computercheck auf der Homepage des Herstellers CORONIC GmbH kostenlos testen.

Die CORONIC GmbH ist seit vielen Jahren im Bereich Sicherheit und Datenschutz von Internetanwendungen sowie der vollautomatischen Auditierung und Absicherung von PC-Systemen aktiv. Wir sind Technologiepartner vieler Volksbanken und Raiffeisenbanken und betreiben diverse Sicherheitsportale für Finanzdienstleister.

Weitere Informationen: CORONIC GmbH., Schauenburgerstraße 116, 24118 Kiel, Tel.: 0431 530 237 10, E-Mail: info@coronic.de, Web: www.coronic.de