Das miese Geschäft mit Softwarelücken

Hacker und Regierungen müssen für Cyberattacken die neuesten Sicherheitslecks kennen. Um dieses Wissen feilschen sie auf einem unkontrollierten Markt

Von Claudio Müller

Am zweiten Dienstag eines jeden Monats beginnt für PC-Nutzer ein so vertrautes wie nerviges Ritual. Microsoft veröffentlicht an diesem Tag Updates für Windows, Office, Internet Explorer und Co. Meistens bremsen an diesem Patch Day zehn oder mehr Patches beim Download die Internetverbindung und bei der Installation den Rechner. Diese Updates schließen Sicherheitslücken, oft auch besonders sicherheitskritische, wie kürzlich im November. In den Office-Versionen 2003 bis 2010 konnten Angreifer einen Fehler ausnutzen, der bei der Darstellung von TIFF-Grafikdateien auftrat, und darüber Malware auf dem angegriffenen PC installieren.

Bevor es zu solchen Angriffen kommt, tobt auf den digitalen Handelsplätzen ein harter Kampf um die neuesten Softwarelücken und Exploits – das sind kleine Programme, die diese Lücken ausnutzen, um darüber etwa Malware auf einen Rechner zu schleusen. An diesem Wettbieten beteiligen sich Sicherheitsforscher, Hacker und spezialisierte Exploit-Dealer, aber auch Softwarehersteller und Regierungsbeamte. Jeder verfolgt dabei seine eigene Agenda: Profitgier, Angriffsoptionen für den Cyberwar oder das Vermeiden von schlechter PR. Die Sicherheit der Anwender haben sie dabei nicht im Blick – oder bestenfalls nachrangig.

Dieser Handel auf Kosten der User kann nur florieren, weil Software-Entwickler fehlerhaft programmieren. So schätzt Ex-Microsoft-Mitarbeiter Steve McConnell in seinem Bestseller „Code Complete“, dass in 1.000 Zeilen Programmcode zwischen 15 und 50 Fehler enthalten sind (zum Verständnis: Windows 7 besteht aus etwa 40 Millionen Zeilen Code). Die meisten Fehler richten nie Schaden an, weil sie nie entdeckt werden, andere führen lediglich zu kleineren Programmfehlern oder Abstürzen. Einige jedoch sind ein enormes Sicherheitsrisiko: Diese Lücken unterscheidet man etwa danach, ob ein Angreifer sie nur direkt am Gerät ausnutzen kann (lokal) oder über eine Internetverbindung (remote). Zudem gibt es verschiedene Angriffsarten. Eine typische Methode ist die Code Execution, mit der ein Angreifer eigene Programme auf dem Zielsystem ausfüh-

FOTOS: HEWLETT-PACKARD/JONATHAN ANDERSSON; ISTOCKPHOTO/GREMLIN

Softwarefehler finden

Um am Millionenmarkt der Sicherheitslücken reich zu werden, suchen Hacker die vielen Fehler in beliebten Programmen

ren kann. Bei einer sogenannten Remote Code Execution geschieht das übers Internet. Dies ist der typische Weg von Malware-Attacken und Cyberwar-Angriffen.

Suche nach der Nadel im Codehaufen

Bevor man mit Softwarefehlern Geld verdienen kann, muss man sie im Programmcode suchen. Dafür gibt es sogar Wettbewerbe auf offener Bühne. Zum Beispiel die Hackerveranstaltung Pwn2Own, die zuletzt im November auf der Konferenz PacSec Applied Security in Tokio stattfand. Bei der von HP gesponserten Veranstaltung fanden Teilnehmer neue Lücken in iOS 7, im Chrome-Browser für Android sowie im IE 11 für Windows 8.1. Mit denen konnten sie Fotos von einem iPhone auslesen sowie die Kontrolle über ein Google Nexus 4, ein Samsung Galaxy S 4 und ein Microsoft Surface RT übernehmen.

Die Methoden der Hacker beschrieb Donato Ferrante vom IT-Sicherheitsunternehmen ReVuln auf dem Hacker-Event ShmooCon 2013. Erstens: Fuzzing. Das ist ein Verfahren für Softwaretests, bei dem ein Tool alle denkbaren Eingaben für eine Software oder Webanwendung ausprobiert, um zu sehen, wie sie damit umgeht. Zum Beispiel: Was macht der Browser, wenn man in die URL-Zeile keine URL, sondern JavaScript-Code einfügt? Ferrantes Urteil zum Fuzzing: Geringer Aufwand, aber die damit gefundenen Lücken sind meistens schnell gepatcht, also wenig lukrativ. Zweitens: Code Review. Das ist die minutiöse Prüfung eines bekannten Programmcodes, etwa bei Open-Source-Tools oder geleakten Quellcodes. Ferrante sagt: Mittelschwer, aber generell eine gute Investition, wenn man Lücken finden will. Drittens: Reverse Engineering einer Software, deren Code nicht offenliegt. Dabei versucht man, die Entwicklungsschritte einer Software rückwärts nachzuvollziehen, um herauszufinden, wo die Schwachstellen liegen. Ferrante: Sehr schwierig und aufwendig, aber die gefundenen Lücken halten sich oft sehr lang. Diese Methode wenden Hacker manchmal auch bei den Sicherheitspatches an. „So versuchen sie, herauszufinden, welcher Fehler behoben wurde, um dann all die angreifen zu können, die den Patch nicht installiert haben“, sagt Sean Sullivan, Sicherheitsforscher von F-Secure.

Wer auf diesen Wegen neue Sicherheitslücken findet, ist nur noch einen Schritt vom großen Geld entfernt. Die Frage lautet: Von wem lässt man sich dieses Wissen vergolden?

Finderlohn für Softwarefehler

Ein naheliegender Interessent für eine Softwarelücke ist der Hersteller der Software selbst. Einige locken dafür mit einer Belohnung, der Bug Bounty. Zwischen 1.000 und 20.000 US-Dollar zahlen die Firmen im Rahmen solcher Projekte meist für einzelne Sicherheitslücken (siehe Seite 24). „Solche Programme geben Forschern einen Anreiz, ihre Entdeckungen nicht im Untergrund, sondern bei den Firmen selbst zu verkaufen“, sagt Christian Funk, Virenanalyst bei Kaspersky. „Und die Preise sind nicht unbedingt geringer als im Untergrund.“ Seit Juni 2013 öffnet auch Microsoft seine Kassen und zahlt seitdem für neu gefundene Lücken in Windows 8.1 bis zu 100.000 US-Dollar.

Schon deutlich länger nutzen Google und Facebook solche Verfahren. Google hat seit 2010 auf diesem Weg von über 2.000 Lücken erfahren und dafür mehr als zwei Millionen US-Dollar gezahlt. Auch Facebook hat in den vergangenen zwei Jahren mehr als eine Million US-Dollar an über 300 Sicherheitsforscher ausgeschüttet. Zwei von ihnen arbeiten inzwischen sogar für das Sicherheitsteam von Facebook. „Bug-Bounty-Programme sind ein essenzieller Teil unserer Sicherheitsbemühungen“, sagt auch Johnathan Nightingale, Vice President, Firefox Engineering, bei Mozilla. Nicht nur, weil sie Entdeckungen belohnen. Sondern auch, so Nightingale, weil sie den Forschern garantieren, dass ihnen keine juristischen Konsequenzen drohen, wenn sie die Software auseinanderpflücken. „Aber die Bug Bounties sind kein Allheilmittel“, weiß Nightingale. Denn sie kämpfen gegen zahlungskräftige Gegner auf einem freien Markt.

Anders als die Softwarehersteller sind Käufer auf dem freien Markt nicht nur auf Sicherheitslücken aus, sondern auch auf die Exploits. Darüber kann man Malware verbreiten, was sie für Cyberkriminelle attraktiv macht. Aber auch Geheimdienste und das Militär brauchen Exploits, denn sie sind die Munition im Cyberwar. Und zwischen all diesen Parteien stehen meistens Exploit-Broker. Diese Mittelsmänner kaufen von Hackern und Forschern Sicherheitslücken und Zero-Day-Exploits (also solche zu noch ungepatchten Lücken) und verkaufen sie an den Meistbietenden weiter.

„Dieser Markt existiert etwa seit Ende der Neunziger“, erklärt Candid Wüest, Sicherheitsforscher bei Symantec. „Aber sowohl die Zahl der gehandelten Exploits als auch die dafür gezahlten Preise sind zuletzt gestiegen.“ Ausschlaggebend sind teils die zunehmenden Cyberwar-Aktivitäten einzelner Staaten. Aber auch der veränderte Malwaremarkt hat dazu beigetragen. „Vor allem, weil Drive-by-Downloads →

Was bedeuten Exploit, Zero-Day und Co.?

- Sicherheitslücke: Programmierfehler im Code einer Software oder Webanwendung, über den Malware-Attacken laufen
- Zero-Day: Offene Sicherheitslücke, die angegriffen wird und noch nicht durch einen Sicherheitspatch geschlossen wurde
- Exploit: Schadprogramm, das Sicherheitslücken ausnutzt, um darüber andere Malware auf dem PC zu installieren
- Patch: Software-Aktualisierung, die bekannte Fehler behebt und automatisch oder manuell installiert wird

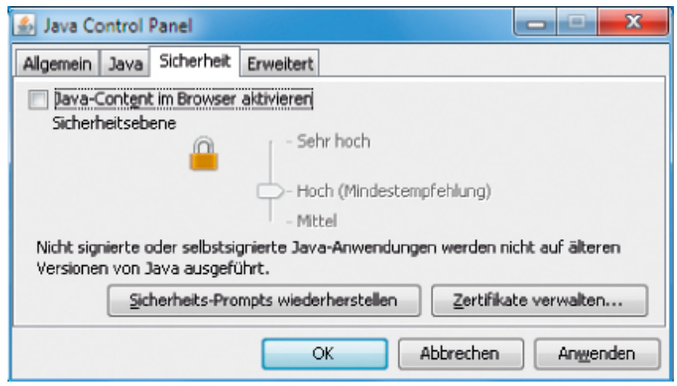
Die Software mit den meisten Fehlern

Im Vorjahr (Stand: 29.11.2013) wurden in folgenden Anwendungen und Betriebssystemen die meisten Sicherheitslücken bekannt:

Programme	
Oracle Java	180
Google Chrome	168
Mozilla Firefox	136
Microsoft Internet Explorer	120
Mozilla Thunderbird	106

Betriebssysteme	
Linux Kernel	177
Windows Server 2008	98
Windows 7	95
Windows Vista	92
Apple iOS	90

Quelle: CVE Details/MITRE, Zahlen für 2013



Das Java-Browser-Plug-in hat sehr viele Sicherheitslücken, lässt sich aber im Control Panel von Java deaktivieren

zum Standardangriff geworden sind", so Christian Funk. Und für diesen Angriff braucht man eben Exploits, die über eine manipulierte Website ungepatchte Softwarelücken im System des Seitenbesuchers finden und darüber Malware auf dem Rechner installieren.

Die Gefahr dieses Marktes ist, dass nur wenige von solchen Exploits wissen. „Deshalb bleiben die Lücken lange offen und können nicht gepatcht werden", erklärt Candid Wüest von Symantec. Und mit genau dieser Exklusivität verdienen die Exploit-Broker ihr Geld. Bis zu 250.000 US-Dollar ist zum Beispiel ein Exploit für iOS wert, verriet Grugq, ein anonymer, von Bangkok aus operierender Exploit-Broker, dem US-Magazin Forbes. Laut eigener Aussage verkauft er Exploits hauptsächlich an die US-Regierung – aber nur, weil Russland und China nicht genug zahlen. In China etwa würden zu viele Hacker exklusiv an die dortige Regierung verkaufen und so die Preise drücken.

Neben Einzelgängern wie Grugq gibt es viele Exploithändler, die von ihrer Nähe zum US-Militär profitieren. Dazu zählen die Firma Endgame, für die der Ex-NSA-Direktor Kenneth A. Minihan arbeitet, die Rüstungskonzerne Raytheon und Northrop Grumman und die US-Firma Netragard (Motto: „Wir schützen Sie vor Leuten wie uns."). Netragard ist spezialisiert auf Penetration Testing, das heißt, sie hacken Firmen in deren Auftrag, um dort Sicherheitslücken zu finden. Im Jahr 2000 startete Netragard zudem das Exploit Aquisition Program (EAP), wobei sie für 20.000 US-Dollar aufwärts Zero-Day-Exploits von Sicherheitsforschern und Exploit-Entwicklern kaufen. „Die müssen sich dabei persönlich identifizieren und bei uns registrieren, bevor wir etwas von ihnen kaufen", sagt Netragard-Gründer Adriel Desautels. Das gilt auch für die Auswahl der Käufer. „Wir verkaufen Exploits ausschließlich an Kunden in den USA", bekundet Desautels. „Der Verkauf von Exploits an andere Länder ist aus unserer Sicht juristisch fragwürdig. Denn würde damit ein Angriff auf unser Land stattfinden, könnten wir wegen Beihilfe angeklagt werden."

Die zahlungskräftigsten Käufer: Staaten

Adriel Desautels ist einer der wenigen Exploit-Broker, die an die Öffentlichkeit treten. Aus seiner Sicht ist ein derart kontrollierter Handel legitim und verhindert sogar, dass Exploits in die falschen Hände geraten, also in die von Cyberkriminellen oder Unrechtsstaaten. Doch Desautels ist ein einsamer Rufer, denn im Moment legt jeder Exploit-Broker eigene Regeln fest. Die französische Firma Vupen etwa verkauft Exploits laut eigener Aussage an Regierungen von NATO-Staaten und „NATO-Partner". Wer genau zu diesem Kundenkreis zählt, wollte Vupen jedoch nicht kommentieren.

Vor diesem Hintergrund kann man solche Firmen als moderne Waffenschieber, ja sogar als „Händler des Todes" bezeichnen, wie es Chris Soghoian, Sicherheitsforscher und -aktivist getan hat. Denn Angriffe auf Industrieanlagen oder die Infrastruktur eines Staates können verheerende Folgen für die Bevölkerung haben. Genauso kritisch betrachten muss man aber die Rolle der Regierungseinrichtungen. „Regierungen, einige mehr als andere, haben die Forschung nach Sicherheitslücken enorm befeuert", meint Sean Sullivan von F-Secure. Von den USA etwa weiß man seit Stuxnet, dass sie aktiv Cyberwaffen entwickeln, um ferne Ziele zu attackieren – bei Stuxnet die Atomanreicherungsanlage im iranischen Natanz. Aber auch Deutschland forciert seine Cyberwar-Aufrüstung. Ein potenzieller Käufer für Exploits ist auch das Kommando Strategische Aufklärung (KSA) der Bundeswehr und die dazu gehörende Gruppe Computer-Netzwerk-Operationen (CNO). Die 60 Mann starke Truppe ist die Cyberwar-Abteilung der Bundeswehr. Sie soll die Streitkräfte mit Informationen unterstützen, etwa indem sie fremde Systeme infiltriert („Fernmelde- und Elektronische Aufklärung" und „Elektronischer →

ZUSATZINFOS

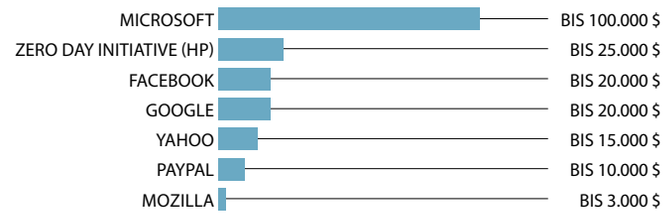
Exploits verkaufen

Wer Sicherheitslücken kennt und Programme besitzt, die diese ausnutzen (Exploits), kann auf dem freien Markt viel Geld verdienen

Das zahlen Softwarehersteller

Bug-Bounty-Programme belohnen Hacker, die den Softwarefirmen unbekannte Fehler in deren Programmen verraten.

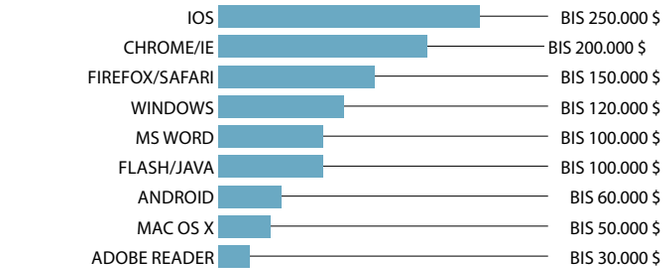
BUG-BOUNTY-PROGRAMME DER HERSTELLER



Das zahlen Geheimdienste und Militär

Für Exploits in beliebten Programmen zahlen Regierungseinrichtungen viel höhere Summen als die meisten Softwarehersteller.

SCHWARZMARKT-PREIS FÜR EXPLOITS



Quelle: Grugq, Exploit-Dealer

Auf dem Hacker-Event Pwn2Own zeigen chinesische Hacker Fotos, die sie über eine iOS-Lücke von einem iPhone klauten

```
    end

    def is_win7_ie9?(agent)
      (agent =~ /MSIE 9/ and agent =~ /Windows NT 6\.1/)
    end

    def get_preq_html(cli, req)
      %Q|
<html>
<script>
  function getDLL() {
    var checka = 0;
    var checkb = 0;

    try {
      checka = new ActiveXObject("SharePoint.OpenDocuments.4")
    } catch (e) {}

    try {
```

Exploits sind meist in JavaScript programmiert, denn sie werden auf Webseiten platziert, von wo aus die Angriffe starten

Kampf“, wie es im Bundeswehrjargon heißt). Offiziell setzt man dazu nur frei verfügbare Tools ein, zum Beispiel den Open-Source-Passwortknacker John the Ripper. Den möglichen Kauf von Exploits kommentiert man jedoch nicht, „aus Geheimhaltungsgründen“, wie ein Sprecher des KSA erklärt. Bislang befindet sich diese Abteilung allerdings noch im Aufbau- und Trainingsstadium, echte Einsätze, etwa in Afghanistan, hat es noch nicht gegeben.

Mehrzweckwaffe Exploit-Kit

Der von den USA und Israel entwickelte Trojaner Stuxnet ist nach wie vor eines der Vorzeigemodelle für die militärische Nutzung von Exploits. Stuxnet attackierte vier bis dato unbekannte Lücken in Windows, um Steuerungssysteme in der Atomanlage Natanz zu manipulieren. Dahinter steckt aber dasselbe Prinzip wie bei Malware-Attacken auf PCs. Die Exploits schauen, welche Betriebssystem- und Softwareversionen auf dem Zielrechner laufen. Ist eine dabei, für die eine Sicherheitslücke bekannt ist, führt das Exploit bestimmte Befehle aus – zum Beispiel einen Pufferüberlauf im Speicher. Einfach gesagt, wird bei dieser Lücke der dem Programm zugewiesene Speicherbereich vollgeschrieben und daraufhin Code in einem angrenzenden Speicherbereich geladen und ausgeführt. Damit kann man Rechner in Industrieanlagen genauso infizieren wie PCs von Usern, die eine manipulierte Website besuchen.

Auf solchen Websites verstecken sich nicht einzelne Exploits, sondern Exploit-Kits, die einen PC auf diverse Lücken in verschiedenen Anwendungen checken. Auch diese Kits werden von Spezialisten entwickelt, gepflegt und im Untergrund gehandelt – mit den Malware-Attacken selbst haben sie nichts zu tun. Einige verkaufen die Exploit-Pakete, andere vermieten sie. Das CritX-Toolkit etwa kann man für 150 US-Dollar pro Tag mieten, fand McAfee heraus. Die Nummer eins ist jedoch seit rund zwei Jahren das Blackhole-Kit. Blackhole nutzt diverse Lücken im Adobe Reader, Flash Player und Java aus, wobei die jeweiligen Exploits und einzelne Codeelemente regelmäßig verändert werden, um sich vor Virenscannern zu verbergen. Um die Browser-Plug-ins potenzieller Opfer zu prüfen, verwendet Blackhole die gratis verfügbare JavaScript-Bibliothek PluginDetect.

Die meisten dieser Exploits zielen auf Lücken ab, die schon lange bekannt und gepatcht sind. Doch da viele Nutzer es mit Software-Updates nicht so genau nehmen, klappen die Angriffe immer noch. „Zero-Day-Exploits sieht man deshalb selten in Kits wie Blackhole, zumal deren Entwickler meist nicht das Wissen haben, um schnell Exploits zu neuen Lücken zu entwickeln“, sagt Candid Wüest von Symantec. „Eine Ausnahme war das Cool-Exploit-Kit. Dessen Entwickler hat das Kit teuer verkauft und von den Einnahmen Zero-Days gekauft. Der Entwickler wurde inzwischen aber gefasst“, sagt Wüest.

Der beste Schutz: regelmäßige Updates

Solange unvorsichtige Nutzer aber auf veraltete Software vertrauen, brauchen Cyberkriminelle die teuren Zero-Day-Exploits allerdings auch nicht. So war zum Beispiel im ersten Halbjahr 2013 die am häufigsten attackierte Schwachstelle eine Windows-Lücke in der Verarbeitung von TrueType-Schriften. Die ist seit 2011 bekannt und wurde damals sogar vom Stuxnet-Nachfolger Duqu ausgenutzt, um in Industriesystemen zu spionieren. Im Schnitt, so das Ergebnis einer Symantec-Studie, wird ein einzelner Exploit 312 Tage verwendet. Erst danach sinkt die Zahl der noch immer ungepatchten Ziele so weit, dass sich Angriffe nicht mehr lohnen.

Der Schutz vor solchen Exploit-Attacken hängt sowohl von den Softwareherstellern als auch den Usern ab. Zunächst müssen die Unternehmen schnell reagieren. „Sobald wir den Fehler identifiziert

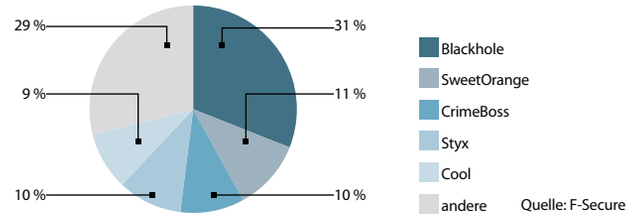
ZUSATZINFOS

Lücken ausnutzen

Cyberkriminelle nutzen Exploits, um Rechner mit Malware zu infizieren. Das klappt, weil viele User ihre Software nur selten aktualisieren

Die beliebtesten Exploit-Kits

Einige wenige Exploit-Sammlungen dominieren den Markt, allen voran das aus Russland stammende Kit Blackhole.



Quelle: F-Secure

Die am häufigsten attackierten Softwarelücken

Diese fünf Lücken, gekennzeichnet nach dem Industriestandard CVE, nutzten Hacker im ersten Halbjahr 2013 am häufigsten aus.

Lücke	Ziel	Betrifft	CVSS Score *
CVE 2011-3402	Windows XP, Vista, 7	Verarbeitung von TrueType-Schriften erlaubt Code-Ausführung	9,3
CVE 2013-1493	Java SE 7.15 und frühere	Fehler im Farbmanagement ermöglicht Code-Ausführung und DoS-Attacken	10
CVE 2011-3544	Java SE 7 und frühere	Gewährt nicht vertrauenswürdigen Webanwendungen Zugriff auf Daten	10
CVE 2011-2423	Java SE 7.17 und frühere	Fehler in der Java VM HotSpot gestattet Angreifern, Berechtigungen auszuhebeln	4,3
CVE 2013-0422	Java SE 7.11 und frühere	Fehlerhafte Sicherheitsabfragen befähigen Angreifer, beliebigen Code auszuführen	10

*COMMON VULNERABILITY SCORING SYSTEM (0–10)

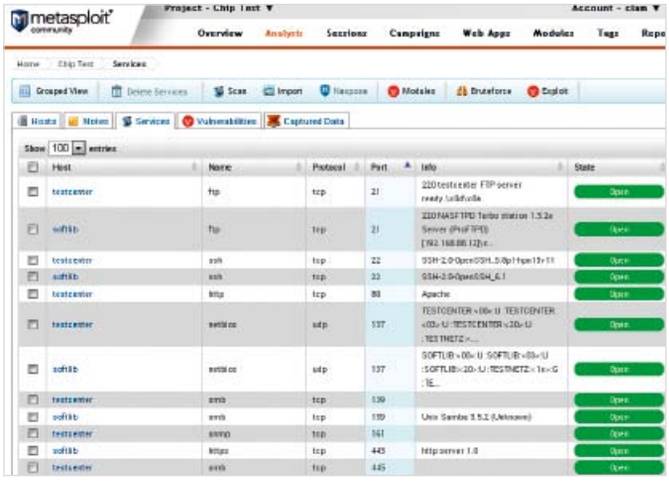
MAXIMALE GEFAHR HOHE GEFAHR MITTLERE GEFAHR Quellen: F-Secure/CVE Details

Alte Software-Versionen im Einsatz

Viele User aktualisieren ihre Software nur unregelmäßig und sind damit angreifbar, obwohl die Sicherheitslücken längst gepatcht sind.

GENUTZTE JAVA-VERSIONEN (AUG. 2013)

*ERSCHEINUNGSDATUM Quelle: Kaspersky



Ein gutartiges Exploit-Kit: Mit dem Tool Metasploit prüfen Sicherheitsexperten Netzwerke auf Sicherheitslücken

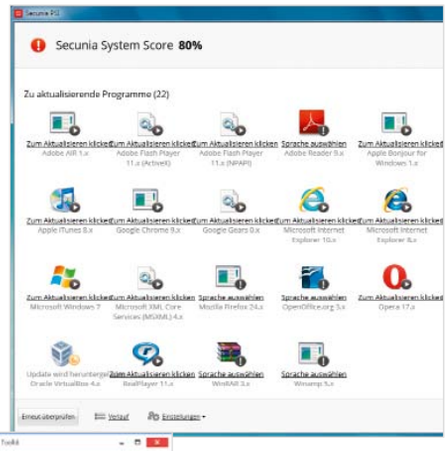
Rechner absichern

Wenn möglich, sollten Sie bei Programmen die automatischen Updates aktivieren. Darüber hinaus helfen die Tools Secunia PSI (auf Heft-DVD) und Microsoft EMET (chip.de), offene Sicherheitslücken abzudichten

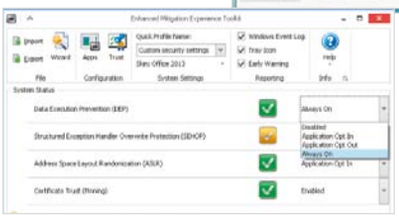
und behoben haben, durchläuft der Patch einen automatischen und manuellen Testprozess, damit keine unerwünschten Nebenwirkungen auftreten“, sagt Johnathan Nightingale von Mozilla. „Auch in Notfällen wie einer Zero-Day-Lücke muss jeder Patch unsere Qualitätschecks bestehen.“ Das dauert, aber die Softwareindustrie wird messbar schneller. Laut Secunia wurden im Jahr 2011 nur 72 Prozent aller Lücken innerhalb eines Tages gepatcht, 2012 waren es bereits 84 Prozent. Und um die Verantwortung für die Installation nicht nur dem Kunden zu überlassen, setzen immer mehr Programme auf automatische Updates, allen voran die Browser Chrome und Firefox.

Ein verbesserter Updateprozess kann den Handel mit Sicherheitslücken aber kaum eindämmen. Die Frage ist, ob man diesen Markt regulieren muss – und regulieren kann. Denn Exploits sind Waffen, die man sowohl gegen Privatpersonen als auch gegen Staaten richten kann. „Aber den Handel mit digitalen Gütern wie Exploits kann man nicht verhindern, denn sie lassen sich nicht verfolgen wie Gegenstände. Daher ist eine Regulierung auch nicht sinnvoll“, sagt Virenforscher Candid Wüest. „Beschränkungen könnten hier einen ähnlichen Effekt haben wie beim Drogenhandel, der in der Illegalität aufgeblüht ist.“ Und damit liegt es an den Herstellern der weit verbreiteten Programme, einen größeren Teil ihrer Milliardenumsätze in die Entwicklung und Prüfung ihrer Software zu stecken. Denn wenn etwa ein einzelner Hacker eine Lücke in Windows findet, sollte das auch einem Weltkonzern wie Microsoft mit knapp 100.000 Mitarbeitern möglich sein.

trend@chip.de



Secunia PSI prüft Software auf verfügbare Updates und installiert sie automatisch



EMET aktiviert Sicherheitsfeatures wie DEP und ASLR, um Angriffe wie Pufferüberläufe zu verhindern (siehe S. 103)