Avast veröffentlicht 2015er Kollektion

Vereinfachte Nutzeroberflächen sind bei Antiviren-Software im Trend. Auch Avast steht dem nicht nach und hat mit den jetzt erschienenen 2015er Versionen seiner Software die Oberfläche angepasst – große Schaltflächen dominieren das Erscheinungsbild. Auch die Geschwindigkeit der Updates wurde laut Hersteller verbessert. So sollen Kunden viele Mini-Updates sehr zeitnah geliefert bekommen, im Durchschnitt alle sechs Minuten.

Die kostenlose Version Avast Free Antivirus 2015 enthält weiterhin die grundlegenden Funktionen eines Virenscanners. Wer weitere Funktionen wie Firewall, automatische Updates für Drittsoftware und Schutz vor DNS-Hijacking nutzen will, muss auf eine der Bezahlvarianten Avast Pro, Internet Security oder Premier ausweichen. Möglichkeiten, diese Funktionen einzeln hinzuzufügen, bietet der eingebaute Shop. (fab)

Die kostenlose Version von Avast 2015 gibt dem Nutzer ausreichend Gelegenheit, zusätzliche Funktionen zuzukaufen.

Sicherheits-Notizen

Die Entwickler des Content Management Systems **Drupal** haben eine kritische Sicherheitslücke geschlossen, die es einem Angreifer ermöglicht, eine betroffene Seite mit einem POST-Request zu übernehmen. Drupal ist eins der bekanntesten quelloffenen CMS-Projekte und wird unter anderem für die Webseite des Weißen Hauses verwendet.

Version 4.0 des **Tor-Browser-Bundles** nutzt jetzt Firefox 31 und schaltet SSLv3 ab, um den Poodle-Angriff zu verhindern. Die Einführung des Meek-Protokolls erleichtert es außerdem, lokale Web-Zensur zu umgehen.

Durch einen Einbruch auf den Servern des Web-Dienstes **SnapSaved** sind über 13 GByte privater Fotos von Nutzern der Webseite in Umlauf gelangt. Der mittlerweile abgeschaltete Dienst SnapSaved hatte es seinen Nutzern ermöglicht, über Snapchat versendete Bilder zu speichern.

Blackberry hat eine neue Version des App-Stores Blackberry World ausgeliefert, damit dieser ab sofort App-Updates verschlüsselt ausliefert. Bis jetzt gingen diese im Klartext durchs Netz und konnten so missbraucht werden, um Nutzern Schadcode unterzuschieben.

Das Update auf **PHP** 5.6.2 schließt vier Lücken; unter anderem einen Integer Overflow in der Funktion unserialize(). Die drei übrigen klaffen in den Modulen cURL, EXIF und XMLRPC. Auch für die Versionszweige 5.5 und 5.4 stehen Updates bereits, die Versionsnummern lauten 5.5.18 und 5.4.34.

Zero-Day-Lücke in Windows

In fast allen Windows-Versionen klafft eine Sicherheitslücke, die Angreifer bereits für gezielte Cyber-Angriffe missbrauchen. Zwar hatte Microsoft an seinem Oktober-Patchday eine Variante der Lücke geschlossen, die Sicherheitsfirma McAfee fand jedoch heraus, dass es einen Angriffsweg gibt, den der Patch nicht abdeckt. Die Lücke wird über präparierte Office-Dokumente ausgenutzt. Öffnet man ein solches Dokument, wird der darin enthaltene Schadcode ausgeführt.

Wer sich schützen will, musste bei Redaktionsschluss noch selbst aktiv werden. Microsoft hat für die neue Variante eine Reihe von Workarounds zusammengestellt; unter anderem ein FixIt-Tool und eine Konfiguration für das kostenlose Härtungstool EMET. Darüber hinaus soll man sicherstellen, dass die Benutzerkontensteuerung aktiv ist, da sie bei einem Angriff anschlägt. (rei)

c't Schutzmaßnahmen: ct.de/yyec

Strafe wegen Krypto-Export

Das Sicherheitsbüro des US-Handelsministeriums hat gegen die Intel-Tochter Wind River Systems eine Konventionalstrafe von 750 000 US-Dollar verhängt, da diese Verschlüsselungssoftware exportiert hatte, die unter Export-Beschränkungen steht. Wind River exportierte nach China, Hongkong, Russland, Israel, Südafrika und Südkorea. Laut einer auf solche Fälle spezialisierten Anwaltsfirma ist das der erste Fall, in dem eine solche Strafe verhängt wurde, ohne dass dabei der Terroristen-Unterstützung beschuldigte Länder involviert waren, die von der US-Regierung mit umfassenden Sanktionen belegt sind.

Die Kanzlei Goodwin Procter sieht darin einen fundamentalen Wandel und eine Botschaft an die IT-Wirtschaft. (fab)

Der Todesstoß für SSLv3

Forscher von Google haben einen Angriff namens Poodle (Padding Oracle On Downgraded Legacy Encryption) vorgestellt, mit dem sich im Prinzip nahezu alle verschlüsselten Verbindungen im Internet knacken lassen. Die Wurzel des Übels ist das längst veraltete Protokoll SSLv3. Es ist über 15 Jahre alt, wird jedoch als Fallback immer noch von nahezu allen Servern und Browsern unterstützt. Ein Angreifer kann den Einsatz von SSLv3 erzwingen, indem er in den SSL/TLS-Verbindungsaufbau eingreift. Haben sich dann Server und Client auf eine SSLv3-Verbindung geeinigt, gibt es einen Angriff auf die Verschlüsselung, mit dessen Hilfe sich wichtige Daten der Verbindung dechiffrieren lassen. So könnte der Angreifer etwa das Sitzungs-Cookie klauen und damit dann den Account des Anwenders kapern.

Der Schutz vor Poodle ist im Prinzip einfach: Das veraltete SSLv3 muss endlich abgeschaltet werden; es wird so gut wie nicht mehr gebraucht. Es gibt mit dem Internet Explorer 6 nur noch einen nennenswerten Browser, der das nachfolgende TLS 1.0 noch nicht unterstützt. IE 6 wurde ursprünglich mit Windows XP ausgeliefert, doch selbst XP-Nutzer verwenden in aller Regel bereits eine neuere IE-Version. Die bereits erfolgte Abschaltung von SSLv3 auf dem Heise-Server führte zu keinen Problemen oder Beschwerden. Web-Server sollten eigentlich alle mindestens TLS 1.0 unterstützen. Bietet ein Server das nicht an, sollte man auch keine vertraulichen Inhalte, die Verschlüsselung zwingend erfordern, mit ihm teilen.

Browser-Nutzer können SSLv3 entweder manuell abschalten (siehe c't-Link für eine detaillierte Anleitung) oder warten, bis die Browser-Hersteller das für sie erledigen. Mozilla plant das für Firefox 34, Microsoft hat noch keine genauen Angaben für seinen Browser gemacht und Chrome ist laut Google schon jetzt gegen Poodle gefeit. (ju)

c't Poodle-Angriffe verhindern: ct.de/yyec

© Copyright by Heise Zeitschriften Verlag
Persönliches PDF für alle Leser der c't aus 30625 Hannover