schiedlichster Qualität. Beispielsweise wurden E-Mails, Passwörter, Fotos und Chat-Protokolle erfasst.

Nachdem der Sachverhalt im Jahre 2010 aufgedeckt wurde, eröffnete die Staatsanwaltschaft Hamburg ein Ermittlungsverfahren, das im November 2012 eingestellt wurde. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat daraufhin den Vorgang im Rahmen eines Ordnungswidrigkeitsverfahrens wieder aufgegriffen.

Mit der rechtskräftigen Feststellung, dass Google Inc. fahrlässig unbefugt personenbezogene Daten erhoben und gespeichert hat, wurde dieses Verfahren nunmehr zum Abschluss gebracht. Gleichzeitig mit dem Bußgeldbescheid wurde Google angewiesen, die unzulässig erhobenen Daten vollständig zu löschen. Der Vollzug der Löschung wurde dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegenüber bestätigt.

„Nach meiner Einschätzung handelt es sich bei dem Sachverhalt um einen der größten bislang bekannt gewordenen Datenschutzverstöße überhaupt. Google hat sich bei der Aufklärung kooperativ gezeigt und öffentlich ein Fehlverhalten eingeräumt. Das Speichern personenbezogener Daten sei nie beabsichtigt gewesen. Dass es dennoch über einen solchen Zeitraum und in dem von uns festgestellten Umfang erfolgt ist, lässt dann nur den Schluss zu, dass die firmeninternen Kontrollmechanismen in erheblicher Weise versagt haben", so Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.

Fälle wie dieser zeigen deutlich, dass die Sanktionen, die das Bundesdatenschutzgesetz vorsieht, für die Ahndung derartig schwerwiegender Datenschutzverstöße bei weitem nicht ausreichen. Für multinationale Konzerne dürfte ein Bußgeld bis zu 150.000,- Euro für fahrlässige, bis zu 300.000,- Euro für vorsätzliche Verstöße regelmäßig keine abschreckende Wirkung erzielen. Dazu Caspar: „Solange Datenschutzverstöße nur zu Discount-Preisen geahndet werden können, ist die Durchsetzung des Datenschutzrechts in der digitalen Welt mit ihren hohen Missbrauchspotentialen kaum möglich. Die derzeit im Zuge der künftigen europäischen Datenschutzgrundverordnung diskutierte Regelung, die als maximales Bußgeld 2% des Jahresumsatzes des Unternehmens vorsieht, würde dagegen eine wirtschaftlich spürbare Ahndung von Datenschutzverletzungen ermöglichen."

F-Secure-Studie: 87 Prozent der PC-Systeme in Unternehmen mit Lücken bei sicherheitskritischen Software-Updates

Nur bei 13 Prozent der PC-Systeme in Unternehmen sind alle sicherheitskritischen Updates wirklich installiert. Bei 87 Prozent der Unternehmenscomputer fehlen kritische Software-Updates, wodurch die Sicherheit der Unternehmens-IT massiv gefährdet ist. Dies sind die Ergebnisse einer F-Secure Auswertung der Daten von rund 200.000 überwiegend in Europa installierten Arbeitsplätzen. Die größten Update-Lücken bestehen ausgerechnet bei so wichtigen und für ihr Risiko bekannten Anwendungen wie Java, Adobe Flash Player, Firefox, aber auch bei Microsoft-Technologien oder Open Office. Diese Zahlen belegen, dass Software-Updating nicht mehr länger nur eine Disziplin des Patch Managements ist, sondern auch definitiv eine Aufgabe der IT-Sicherheit. F-Secure Experten gehen nämlich davon aus, dass etwa 83 Prozent der zehn am häufigsten entdeckten Malware-Typen durch upgedatete Software schon im Vorfeld hätten verhindert werden können.

Der Auswertung von F-Secure zufolge fehlen bei 49 Prozent der Firmen-PCs und -Laptops ein bis vier kritische Updates, bei 25 Prozent sind fünf bis neun Updates und bei 13 Prozent sogar zehn oder mehr Updates nicht installiert.

54 Prozent der Rechner haben Lücken bei Java-Updates (Java 6 Update 43 mit 39 Prozent bzw. Java 7 Update 17 mit 15 Prozent). 36 Prozent der Systeme hatten keinen vollständig aktuellen Adobe Flash Player. Bei 23 Prozent bestand eine Verwundbarkeit in Windows Common Controls, was die Remote Ausführung von Schadcodes erlaubt hätte.

Die Zahlen belegen eine immer noch enorme Sorglosigkeit in diesem Bereich. Diese ist umso erstaunlicher angesichts der Schlagzeilen der letzten Monate über Angriffe auf Unternehmen und Institutionen, die sich gegen Schwachstellen im Netzwerk richteten. So hatte sich etwa die Red October-Malware fünf Jahre lang bis zu ihrem Ende im Januar 2013 allein auf Exploits in Microsoft Word, Microsoft Excel und Java verlassen. Sensible Informationen aus Regierungs- und Forschungseinrichtungen sowie Unternehmen wurden gestohlen. Red October nutzte dabei Sicherheitslücken in Software, für die schon längst Patches vorlagen. Alleine durch eine Aktualisierung der Software hätten die Angriffe abgewehrt werden können.

Die gesamte Software in einem Unternehmen auf neuestem Stand zu halten, kann eine aufwändige und komplizierte Aufgabe sein, weshalb sie gerne vernachlässigt wird. Software Updater (z.B. von F-Secure) vereinfacht dies und stellt sicher, dass alle Betriebssysteme sowie 3rd Party-Anwendungen auf den Rechnern im Unternehmensnetz up-to-date sind. Die Lösung scannt proaktiv PC-Systeme nach ihrem Sicherheits-Update und -Patch-Status, führt notwendige Updates automatisch aus und erstattet Bericht. Eine manuelle Option ist auf Wunsch verfügbar, wenn der Anwender das Patching zusätzlich kontrollieren möchte.

Weitere Informationen unter *http://www.f-secure.com/de/web/business_global/software-updater*

Sicherer Austausch von E-Mail-Dateianhängen

E-Mails mit großen Dateianhängen versenden – und das verschlüsselt und ohne lange Übertragungszeiten: Das sind die Stärken der am 11.04.2013 veöffentlichten Appliance fideAS mail LFM der Applied Security GmbH (apsec). Die Lösung schützt große Dateianhänge automatisch gegen Datendiebstahl, und das sowohl unternehmensintern, als auch im Austausch mit Externen.

Jeder kennt das Problem: Wenn große Dateien hin und her verschickt werden müssen und es dabei auf hohe Sicherheit ankommt, wird der Datenaustausch oft kompliziert oder teuer. Dafür bietet apsec jetzt eine schnelle und einfache Lösung: die Appliance fideAS mail LFM (Large File Management). Die Innovation der Großwallstädter IT-Sicherheitsspezialisten sichert Dateianhänge ab einer vordefinierten Größe automatisch und legt sie in ihrem Datenspeicher verschlüsselt ab. Der Clou daran: Empfänger der Nachricht erhalten bei Empfang nicht die Anhänge direkt, sondern lediglich eine Einladung zu deren Download. Wenn sie zum ersten Mal eine Datei aus der Appliance abrufen wollen, müssen sie sich dafür mit einem Passwort authentifizieren, das sie zum Beispiel per SMS erhalten haben. Hat die Appliance ihre Identität bestätigt, wird ihnen die Datei über eine sicher verschlüsselte Verbindung zur Ver-