secorvo
security consulting

Secorvo Security News

Mai 2014

Das Fressen und die Moral

Noch hat sich der von Edward Snowden aufgewirbelte Staub nicht gelegt, da feiern amerikanische Cloud-Anbieter schon wieder erste Siege im Kampf um europäische Kunden. Denn nicht nur Microsoft buhlt mit Office 365 um die Gunst der IT-Kostenreduzierer, auch Google hat den Markt entdeckt und mit Apps for Business eine Unternehmenslösung im Angebot. Die Vorteile einer „Alle-Büroanwendungen-ins-Netz"-Lösung sind offenkundig: Installation, Konfiguration und Wartung (Patches, Pflege) von Client- und Serversystemen entfallen, Lizenzkosten sind besser kalkulierbar und die Software ist ständig auf dem neuesten Stand. Diese Angebote sind eine Herausforderung für die traditionellen Geschäftsmodelle der Anbieter von Standardsoftware: sie sind billiger, aktueller und oft bedienungsfreundlicher als die gewohnten „Software-Boliden".

Microsoft versucht dieser Herausforderung durch die Flucht nach vorne zu begegnen und bemüht sich, die eigenen Kunden von Microsoft 365 zu überzeugen. Und stößt dabei auf Widerstand – denn die Übermittlung personenbezogener Daten in Drittstaaten, die dabei allein durch den Wartungszugriff aus den USA auf das Rechenzentrum in Irland unvermeidlich erfolgt, ist nicht ohne weiteres zulässig. Mit an das EU-Recht angepassten Verträgen und Vereinbarungen mit der Art.-29-Gruppe versucht Microsoft, eine saubere Rechtsgrundlage zu schaffen (siehe SSN 4/2014). Wer sich darauf einlässt, sollte wissen, dass von der rechtlich geforderten „Kontrolle" der Verarbeitung durch den Auftraggeber keine Rede sein kann – wer das nicht glaubt, der versuche einmal, eine Prozessbeschreibung für den Wartungszugriff von Microsoft zu erhalten.

Und noch eines: Wer mit dem Gedanken spielt, sein in Daten geronnenes Know-How auf fremde Server auszulagern, der sollte zumindest voher prüfen, wie schnell er den eigenen Betrieb wieder aufnehmen kann, sollte der Dienst eines Tages plötzlich nicht mehr zur Verfügung stehen.

Inhalt

secorvo
security consulting

Security News

Heartbleed und PKI Basics

Am 09.05.2014 hat Netcraft aktuelle Zahlen zu Reaktionen auf die Heartbleed Schwachstelle veröffentlicht: 57 % der Betreiber betroffener Webseiten haben den Kopf in den Sand gesteckt und akzeptieren das Risiko. Ebenfalls bedenklich: Weitere 16 % ließen sich zwar ein neues Zertifikat ausstellen, nicht aber ein neues Schlüsselpaar. Daran wird deutlich, dass das Vertrauensmodell einer PKI noch nicht von jedem Betreiber verstanden wurde. Für einen korrekten Umgang mit Heartbleed empfehlen wir einen Blick in die Hinweise des DFN-CERT.

Agentenfrühstück

Jérome Nokin stellte am 17.04.2014 auf der Full-Disclosure-Mailingliste sein Angriffswerkzeug ePolicy 0wner vor. Es ermöglicht auf einfache Weise Schwachstellen behaftete Versionen von McAfees zentraler Management-Lösung für Virenschutz (bis v4.6.6) ‚zum Frühstück' zu kapern. Brisant ist, dass damit nicht nur der Management-Server, sondern auch alle darüber verwalteten Clients übernommen werden können. Ursachen dieser verketteten Schwachstelle sind die weltweit einheitliche Anmeldung am Management-Server (zur Aufnahme von zu verwaltenden Clients) und Schwachstellen in den Management-Protokollen, welche typische Angriffe via SQL-Injection (CVE-2013-0140) oder Directory Traversal (CVE-2013-0141) ermöglichen. Über die hoch privilegierten Virenschutz-Agenten können durch Ausnutzung dieser Schwachstellen die Client-Systeme über den Server angegriffen werden.

Dieses Problem hat nicht nur McAfee: auch bei Symantec Endpoint Protection (CVE-2013-1612) und AVG wurden ähnliche Schwachstellen gefunden. Ein Update oder – bei exponierten Systemen – eine Neuinstallation und Aktualisierung der betroffenen Systeme wird dringend empfohlen.

Agenten stellen generell eine Gefährdung dar, wie weitere aktuelle Beispiele z. B. bei Nagios-Agenten zeigen: Überwachte Server mit Schwachstellen im Nagios-Agent wurden gemäß den Recherchen von Link11 für das Mining von virtuellen Währungen genutzt. Die aktuellen Vorfälle machen einmal mehr dreierlei deutlich:

1. Auch Software, die Sicherheit schaffen soll, kann Schwachstellen enthalten: Haben Sie dies in Ihren Bedrohungsanalysen berücksichtigt?

2. Für Sicherheitssoftware braucht man Sicherheitskonzepte, die Angriffsmöglichkeiten der Agenten als Szenario umfassen.

3. Weniger kann mehr sein: Ein System, das keine Agenten hat, ist vielleicht nicht so schön administrierbar – dafür ist es schwieriger anzugreifen, wenn an anderer Stelle etwas schief geht.

Triple Handshakes

Die am 04.03.2014 publizierte TLS-Schwachstelle Triple Handshakes ging zwischen anderen „Bug-Aufregern" der vergangenen Monate unter. Dabei handelt es sich nicht um einen Implementierungs-, sondern um einen Designfehler im TLS-Protokoll, der mehrere gängige Webbrowser betraf und mittlerweise in allen großen Browsern beseitigt wurde (darunter Firefox, Chrome und Safari für iOS 7.1.1).

TLS definiert drei verschiedene Arten von „Begrüßungen": Ein *Standard Handshake* wird beim Aufbau einer TLS-Verbindung durchgeführt. Dabei authentifiziert sich oft nur der Server (z. B. die Webseite einer Bank). Nutzt der Client die gleiche SSL-Verbindung anschließend für den Zugriff auf eine geschützte Ressource, initiiert der Server einen *Renegotiation Handshake* für die nachträgliche Client-Authentifikation. Ein *Resumption Handshake* schließlich dient der Performanceoptimierung. Bei einem Triple-Handshakes-Angriff vermittelt ein Angreifer als Man-in-the-Middle die drei Handshakes und übernimmt schließlich als authentifizierter Client die Verbindung zum Server.

Die Sicherheit der einzelnen Handshake-Protokolle wurde formal nachgewiesen. Der Triple-Handshakes-Angriff nutzt jedoch eine subtile Interaktion zwischen den drei Protokollen. Das TLS-Protokoll wurde in den vergangenen 20 Jahren immer wieder um neue Funktionen erweitert und mit Bug-Fixes geflickt. Vielleicht ist es an der Zeit für einen komplett neuen Entwurf...

Revolution per Urteil

Mit seinem Urteil vom 13.05.2014 gegen Google Spain SL hat der EuGH Betroffenen das Recht zugesprochen, von Suchmaschinen die Streichung von Treffern aus der Ergebnisanzeige zu verlangen. Voraussetzung ist, dass die Treffer einer Suche nach dem Betroffenennamen sich auf personenbezogene Daten des Anspruchstellers beziehen, dieser überwiegende Interessen oder Grundrechtspositionen geltend machen kann und das europäische Datenschutzrecht anwendbar ist.

Damit bejaht der EuGH zugleich die Zuständigkeit der spanischen Datenschutzaufsicht und die Anwendbarkeit des spanischen Datenschutzrechts. Rechtsgrundlage der Suche sei das berechtigte Interesse gemäß Art. 7 f der DS-Richtlinie (RL 95/46/EG). Diese entfalle, sobald der Betroffene widerspreche und entgegenstehende, schutzwür-

dige Interessen geltend mache. Hierfür reiche es bereits, dass die Daten durch Zeitablauf nicht mehr für ihren Zweck erheblich sind. Die Beurteilung sei völlig unabhängig von der Datenquelle, der andere Interessen oder Ausnahmen (journalistische Zwecke z.B., Art. 9 DS-RL) zugrunde liegen können.

Der praktische Nutzen des schlüssigen Urteils ist allerdings begrenzt, da der Betroffene die Suchmaschinen nur einzeln und begrenzt auf den Anwendungsbereich der Datenschutzrichtlinie in Anspruch nehmen kann. Die klare Position zur nationalen Zuständigkeit dürfte allerdings Bewegung in die laufenden Streitigkeiten mit internationalen Internetriesen in Deutschland bringen.

Aktuelle Studien

In den Monaten April und Mai sind vier umfangreiche Reports zur aktuellen Sicherheitslage erschienen. Zunächst veröffentlichte am 15.04.2014 WhiteHat Security ihren „2014 Website Security Statistics Report“. Er dokumentiert die häufigsten Sicherheitsprobleme aus Anwendungssicht. Am 23.04.2014 folgte Verizon mit ihrem „2014 Data Breach Investigations Report“, der die Ergebnisse der Untersuchung von über 100.000 Sicherheitsvorfällen in Unternehmen zusammenfasst. Am 05.05.2014 publizierte das Ponemon Institute mit die „2014 Cost of Data Breach Study“, die sich den finanziellen Schäden von Sicherheitsvorfällen widmet. Am 12.05.2014 schließlich erschien der Bericht „Protecting personal data in online services: learning from the mistakes of others“ des britischen Information Commissioner's Office, in dem Schlussfolgerungen aus bekannt gewordenen Sicherheitsvorfällen gezogen werden („learning from the mistakes of others“).

Zusammen vermitteln die Ergebnisse der Studien einen aktuellen und schonungslosen Eindruck von der weltweiten IT-Sicherheitslage.

Kassierte Datenschutzaufsicht

Das Verwaltungsgericht Berlin hat am 13.01.2014 eine Löschanordnung des Berliner Datenschutzbeauftragten aufgehoben. Der betroffene Hersteller von Stadtkarten speichert bei sämtlichen Bearbeitungen Namen und Bearbeitungszeit der Beschäftigten einer beauftragten Agentur, um seine Urheberrechte nachweisen zu können. Da diese Daten in verschiedenen Urteilen zu Urheberansprüchen in der Beweisführung von Gerichten verlangt wurden, hat das VG Berlin die Erforderlichkeit und das berechtigte Interesse des Herstellers anerkannt.

Die Urteilsbegründung gibt allerdings zu denken. So geht das Gericht von § 28 Abs. 1 Nr. 2 BDSG als Erlaubnistatbestand aus, zitiert im Sachverhalt jedoch eine Einwilligungserklärung, die den Betroffenen abverlangt wurde – und Mängel aufweist. Die zulässige Speicherdauer wird nicht betrachtet; dafür stellt es die Praxis anderer Gerichte bei der Beweisführung im Urheberrechtsstreit pauschal über die Betroffeneninteressen. Offenbar haben auch Richter Nachholbedarf in Sachen Datenschutzrecht.

Secorvo News

Seminare nach der Sommerpause

Die T.I.S.P.-Schulung von Secorvo bereitet nicht nur auf die Zertifikatsprüfung vor, sondern bietet geballtes Erfahrungswissen aus über 200 Jahren Berufserfahrung in der Informationssicherheit. Wenn Sie davon profitieren möchten, merken Sie sich den 22.-26.09.2014 vor. Wollen Sie sich auf den aktuellen Stand beim Thema IT-Sicherheit bringen, empfehlen wir Ihnen die Teilnahme am Seminar IT-Sicherheit heute (30.09.-02.10.2014).

Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Selbstschutz zum Nachlesen

Die auf den erfolgreichen Anti-Prism-Partys im September 2013 und Februar 2014 vorgestellten „Anleitungen zum Selbstschutz“ gibt es nun auch ausführlich: Sie erschienen in Ausgabe 5/2014 der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)“. Die digitalen Fassungen der von Secorvo verfassten Beiträge sind über unsere Webseite abrufbar.

Tag der IT-Sicherheit

Am **09.07.2014** richtet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) gemeinsam mit der IHK Karlsruhe, dem CyberForum e.V. und KASTEL bereits den 6. Tag der IT-Sicherheit aus (ab 14 Uhr im Haus der Wirtschaft der IHK Karlsruhe).

Die diesjährige Veranstaltung beleuchtet IT-Sicherheit und Datenschutz aus der Compliance-Perspektive. Mit einer Keynote von Frau Dr. Birte Mössner, Leiterin Corporate Compliance und Datenschutz der EnBW, einem Beitrag von TechniData über das nicht immer einfache Verhältnis von IT-Managern und Sicherheitsverantwortlichen, einem Vortrag von Secorvo zu den datenschutzrechtlichen Fallstricken im Marketing und der Vorstellung der technischen Sicherheit bei 1&1 bieten vier Karlsruher Unternehmen kompetente Best Practice-Einblicke – flankiert von der Gelegenheit zum fachlichen „Networking“. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2014	
02.-03.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Luzern/CH)
05.06.	Live Hacking (KA-IT-Si, Karlsruhe)
23.-24.06.	DuD 2014 (Computas, Berlin)
23.-26.06.	OWASP AppSec EU 2014 (OWASP Foundation, Cambridge/UK)
24.-27.06.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
Juli 2014	
09.07.	6. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
August 2014	
02.-07.08.	Blackhat USA 2014 (Blackhat, Las Vegas/US)
03.-06.08.	14th Annual DFRWS Conference 2014 (DFRWS, Denver/US)
07.-10.08.	DEF CON 21 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Sanata Barbara/US)

Fundsache

Mitarbeiter von ESET, einem Anbieter von Virenschutzlösungen, haben mit einer am 18.03.2014 veröffentlichten, fast 70seitigen Studie eine umfassende Analyse der Schadsoftware-Kampagne „Windigo“ legt, in deren Verlauf über Jahre systematisch SSH-Credentials gestohlen und Webseitenbesucher auf infizierte Seiten umgeleitet wurden.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Stefan Gora, Kai Jendrian, Michael Knopp

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de