secorvo
security consulting

Secorvo Security News

Januar 2014

Skurrile Welt

Es ist schon eine eigenartige Entwicklung, an die wir uns in den vergangenen Jahrzehnten gewöhnt haben.

Inzwischen erfahren wir fast täglich in den Nachrichten von erfolgreichen Angriffen auf IT-Systeme. Der ebenso vorhersehbare (wie wirkungslose) politische Reflex: ein Sicherheitsgesetz, das Unternehmen verpflichten soll, Vorfälle zu melden. Dabei dürfte in den weitaus meisten Fällen mindestens ein sicherheitsrelevanter Fehler in einer genutzten Software mitursächlich gewesen sein. Die Adressaten der Vorwürfe und politischen Maßnahmen sowie die Leidtragenden der wirtschaftlichen Folgen sind jedoch in der Regel die Opfer: nicht der Hersteller der fehlerhaften Software steht am Pranger, sondern der Anwender – und sei es, weil er ein Update nicht eingespielt hat.

In anderen Branchen wäre so etwas unvorstellbar: Würde man den Fahrer eines Autos nach einem Achsbruch verurteilen, weil er nicht umgehend auf eine fehlerärmere Achse des Herstellers „upgedatet" hat? Ihm zum direkten Schaden auch noch den des Reputationsverlusts auferlegen, anstatt den Achshersteller beim Namen zu nennen – und ihn mit Schadensersatzforderungen zu konfrontieren?

Während Verbraucherrechte ständig ausgeweitet werden stiehlt sich die Software-Branche bei Sicherheitsmängeln ihrer Produkte seit Jahren aus der Verantwortung.

Die Wurzel des Übels liegt allerdings tiefer. Dem Berufsstand des Software- und Webanwendungsentwicklers liegt bis heute keine einheitliche Berufsqualifikation zu Grunde. In der Praxis dominieren nicht selten branchenfremde Quereinsteiger, und in den existierenden Berufsausbildungen spielen Sicherheitsaspekte bei der Software-Architektur und der Kodierung nicht einmal eine Nebenrolle. Wenn wir sichere Software wollen, brauchen wir entsprechend qualifizierte Entwickler – und Zertifikate. Damit könnte sich „Software made in Germany" sogar zu einem Qualitätssiegel entwickeln. Bis dahin ist es allerdings noch ein steiniger Weg.

Inhalt

secorvo
security consulting

Security News

Europäisches Aufständchen

Bereits im Oktober 2012 (SSN 10/2012) hatte die Art. 29 Gruppe der Europäischen Datenschutzaufsichtsbehörden Google aufgefordert, die einheitliche Datenschutzerklärung vom März 2012 an das europäische Datenschutzrecht anzupassen. Nun zeitigen die anschließend in Frankreich, Spanien, Großbritannien, den Niederlanden, Italien und Deutschland eingeleiteten Verfahren erste Ergebnisse: In Spanien wurden Google Inc. 900 TEuro Bußgeld auferlegt, in Frankreich 150 TEuro. Die französische CNIL (*Commission nationale de l'informatique et des libertés*) hat Google außerdem verpflichtet, auf www.google.fr eine Pressemitteilung zu ihrer Entscheidung für 48 Stunden zu veröffentlichen. Google plant Rechtsmittel einzulegen.

CNIL und die spanische AEPD (*Agencia Espaniola de Protecciòn de Datos*) begründen die Bußgeldbescheide mit der Unklarheit der vorliegenden Datenschutzerklärung: Zweck, Löschfristen und Umfang der Verarbeitung der Daten seien nicht erkennbar, viele Aussagen enthielten ein „möglicherweise" oder stünden im Konjunktiv. Darüber hinaus behalte sich Google ohne Rechtsgrundlage vor, Daten der verschiedenen Dienste zusammenzuführen.

Bei den übrigen Datenschutzaufsichtsbehörden stockt das Verwaltungsverfahren. Daher ist Frau Reding zuzustimmen, dass die Verfahren weder durch die Höhe der Sanktionen noch mit ihrem schleppenden Verlauf geeignet sind, Google zu beeindrucken. Der Fall zeigt: Zur Durchsetzung europäischer Datenschutzvorstellungen bedarf es sowohl einer stärkeren europäischen Zusammenarbeit als auch wirksamerer Druckmittel.

Drum prüfe...

Am 29.12.2013 wurde die Website des OpenSSL-Projekts Opfer eines Angriffs. Medien in aller Welt berichteten über den Angriff und nannten eine Schwachstelle im eingesetzten Hypervisor als Ursache. Im Kontext zahlreicher anderer Attacken nicht einmal eine Randnotiz der Geschichte – hätte sich nicht im Laufe der Untersuchungen herausgestellt, dass unsichere Passwörter beim Hosting-Provider das Einfallstor waren.

So wurde der Vorfall zu einem lehrbuchmäßigen Beispiel für den verbreiteten Mangel an systematischer Ursachenanalyse: Anstatt zunächst die wahrscheinlichsten Fehlerquellen auszuschließen und Belege für den Ablauf des Angriffs zu suchen, mutierten Spekulationen zu Erkenntnissen. Dabei würde kein seriöser Handwerker einen Toaster als defekt deklarieren, ohne zuvor zu prüfen, ob beim Funktionstest auch der Netzstecker steckte.

000507607999

Auf dem 30. Chaos Communication Congress 30C3 in Hamburg stellten am 27.12.2013 zwei Forscher ihre Analyse einer neuartigen Bankautomaten-Malware vor. Die Angriffsmethode: Man bohre ein Loch in die Gehäusefront des Geldautomaten, um den USB-Port des dahinter montierten Windows-XP-Systems zu erreichen, und übertrage die Malware per USB-Stick. Mit der PIN „000507607999" ließ sich die Benutzeroberfläche der Malware aktivieren; darüber konnte nach Eingabe einer temporären PIN, die ein Automatenräuber telefonisch erfragen musste, der Bargeldbestand des Automaten gezielt dezimiert werden.

Bankautomaten-Malware ist nicht neu; erste Exemplare wurden bereits 2009 analysiert. Sie wird jedoch, wie die Malware Ploutus aus Mexiko, systematisch weiterentwickelt, begünstigt durch fortschreitende Standardisierung: So lassen sich Bankautomaten inzwischen über die CEN XFS API von Microsoft steuern.

Dennoch fällt es schwer zu glauben, dass ein solcher Angriff überhaupt möglich war. So ist die USB-Schnittstelle schon länger als wunder Punkt von Bankautomaten bekannt. Und bereits seit Jahren ist es nicht nur in Banken übliche Praxis, kritische Systeme zu härten – und dabei nicht benötigte Schnittstellen zu deaktivieren. Ein solcher Klick im BIOS hätte den betroffenen Instituten erhebliche Summen erspart.

Belästigende Empfehlungen

Bereits am 12.09.2013 erklärte der Bundesgerichtshof die Praxis, Webseitenbesuchern ein Formular zum Versenden einer Empfehlungs-E-Mail zur Verfügung zu stellen, für wettbewerbswidrig. Maßgeblich für die Einordnung solcher E-Mails als Werbung sei nicht, dass die Versendung durch unbekannte Nutzer veranlasst werde, sondern dass der Versand das Ziel habe, auf die Webseiten aufmerksam zu machen. Die Versandfunktion hierzu würde vom Seitenbetreiber zur Verfügung gestellt, und dieser träte als Absender in Erscheinung. Damit greife § 7 Abs. 2 Nr. 3 UWG, der E-Mail-Werbung ohne Einwilligung des Empfängers als unzumutbare Belästigung einstuft.

Eine rechtskonforme Gestaltung einer solchen Empfehlungsfunktion erfordert also mindestens, dass sie eine Nachricht im E-Mail-Programm des Seitennutzers erzeugt und dieser als Absender erscheint. Doch selbst dies könnte – je nach Intensität der werbenden Inhalte (z. B. Zusatztext zum Link, Logos) – als belästigende und damit unzulässige E-

Mail-Werbung gewertet werden. Webseitenbetreibern ist daher zu raten, die Empfehlungsfunktion ersatzlos zu streichen, um Abmahnungen zu vermeiden.

Offensicher

Wie sicher ist *Open Source*-Software? Der naive Glaube, dass die Veröffentlichung des *Source Codes* mehr oder weniger automatisch die Sicherheit eines Programms garantiere (keine Hintertüren, keine sicherheitskritischen Bugs, keine sicherheitsrelevanten Design-Fehler), hat sich wiederholt als Irrglaube entpuppt. Denn die prinzipielle Möglichkeit zur Code-Prüfung sagt wenig über die tatsächliche Durchführung. Auch muss der zum Download angebotene Binärcode nicht mit dem publizierten Quell-Code übereinstimmen – ein beliebtes Einfallstor für Angreifer (und Nachrichtendienste).

Dagegen hilft nur eine unabhängige Prüfung durch eine kompetente und vertrauenswürdige Instanz. Eine solche Initiative hat jetzt Matthew Green mit seinem *Open Crypto Audit Project* (OCAP) ergriffen. Am 20.12.2013 konnte er in seinem Blog den Start der öffentlichen Analyse von TrueCrypt verkünden – nachdem sein Sponsoring-Aufruf gut 64.000 US$ erbracht hatte. Sollte das Beispiel Schule machen, hätte die eine oder andere *Open Source*-Software bald die besten Argumente auf ihrer Seite.

Zickzack-Kurs

Nachdem die große Koalition sich darauf geeinigt hatte, ein neues Gesetz zur Vorratsdatenspeicherung zu entwickeln, legte am 12.12.2013 der Generalanwalt Pedro Cruz Villalòn am Gerichtshof der Europäischen Union seine Schlussanträge in der Vorabentscheidungsvorlage zur Vorratsdatenspeicherung vor. Prompt verkündete der neue Bundesjustizminister, erst das Urteil des EU-Gerichtshofs abwarten zu wollen. Auch das Innenministerium hat inzwischen die möglichen Auswirkungen des Urteils erkannt und sich zum Abwarten bekannt.

Die Schlussanträge zur Richtlinie 2006/24/EG kommen zu einem ähnlichen Ergebnis wie bereits 2010 das Bundesverfassungsgericht: Für die Beurteilung der Verhältnismäßigkeitsabwägung sei relevant, wie der Zugang zu den Daten geregelt wird. Da solche Regelungen fast völlig fehlten, sei die Richtlinie im Ganzen unverhältnismäßig. Verhältnismäßig sei höchstens eine Speicherdauer von einem Jahr. Zudem müsse der europäische Gesetzgeber zur Wahrung der Verhältnismäßigkeit Regeln erlassen, die möglicherweise außerhalb seiner Kompetenz lägen. Angesichts dieser Umstände wird es bis zu einem neuen Anlauf zur Vorratsdatenspeicherung sicherlich etwas dauern. Die Bundesregierung möchte sich auf EU-Ebene immerhin für eine zeitliche Beschränkung der Speicherung auf drei Monate einsetzen.

Secorvo News

IT-Sicherheit 2014

Mit dem Seminar „IT-Sicherheit heute“ bieten wir seit Jahrzehnt Jahr für Jahr einen vertieften Einblick in aktuelle Themen und Entwicklungen der IT-Sicherheit. Auch 2014 wurde das Programm thematisch ergänzt und aktualisiert. Nächster Seminartermin: 08.-10.04.2014.

Immer mehr Unternehmen – darunter Bertelsmann, VW und die Bundesdruckerei – erwarten von Mitarbeitern im Bereich Informationssicherheit ein T.I.S.P.-Zertifikat als Qualifikationsnachweis. Die nächste Gelegenheit, Ihre Qualifikation als Security-Spezialist zertifizieren zu lassen, bieten wir Ihnen vom 24.-28.03.2014 – mit den Autoren des T.I.S.P.-Begleitbuchs als Referenten.

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

Foto: Sandra Jacques

Karlsruhe schützt sich selbst

Mit über 650 Teilnehmern wurde die von der Karlsruher IT-Sicherheitsinitiative organisierte Anti-Prism-Party im September 2013 zur größten Verschlüsselungsparty Deutschlands. Am **12.02.2014** folgt nun die zweite Staffel: Neben weiteren Tipps und Empfehlungen zum „Selbstdatenschutz“ zeigt das Kryptologikum des Karlsruher Instituts für Technologie (KIT) historische und zeitgenössische Verschlüsselungstechnik zum „Be-Greifen“. Ein „Security Kino“ und eine Live-Hacking-Demo im Foyer des ZKM veranschaulichen die Erforderlichkeit von Schutzmaßnahmen.

Die wahrscheinlich größte Verschlüsselungsparty Europas beginnt um 18 Uhr. Der Eintritt ist frei; eine Anmeldung ist nicht erforderlich.

Veranstaltungshinweise

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

Februar 2014	
05.-06.02.	24. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
12.02.	Anti-Prism-Party 2. Staffel (KA-IT-Si, Karlsruhe)
17.-21.02.	Audit Challenge 2014 (Frankfurt School of Finance & Management, Frankfurt)
18.-19.02.	21. DFN-Workshop "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2014	
24.-29.03.	T.I.S.P.-Schulung und Prüfung (Secorvo College, Karlsruhe)
April 2014	
08.-10.04.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo College, Karlsruhe)
08.-09.04.	Datenschutztage 2014 (FFD Forum für Datenschutz, Wiesbaden)
09.-10.04.	Security Forum 2014 (Hagenberger Kreis, Hagenberg/A)

Fundsache

Am 15.01.2014 hat das NIST eine überarbeitete Fassung der *Special Publication* SP 800-53 (Rev. 4) veröffentlicht. Die inzwischen 460 Seiten umfassenden *Security and Privacy Controls for Federal Information Systems* sind die amerikanische Version des IT-Grundschutzes – allerdings für drei Schutzbedarfsklassen: *low*, *moderate* und *high*. In Appendix H findet sich eine Abbildung auf die Controls des ISO/IEC 27001.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Sven Köhler, Jochen Schlichting

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