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

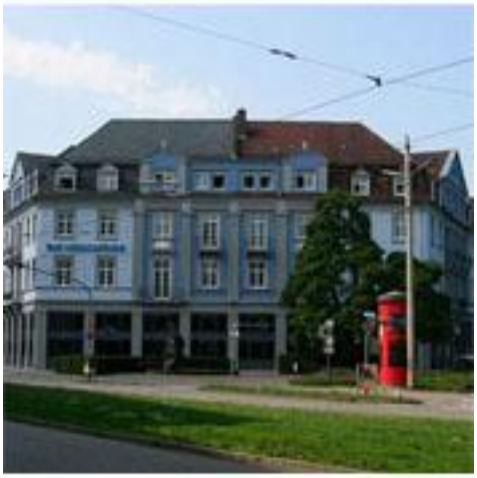
ISSN 1613-4311

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



secorvo
security consulting

Secorvo Security News

Februar 2014

Zwischenbilanz

Neun Monate nach den ersten Enthüllungen Edward Snowdens über die Überwachungstätigkeit der NSA zeichnet sich die zukünftige Entwicklung ab. In seiner Rede vom 17.01.2014 machte Präsident Obama deutlich, dass sich allein bei der Überwachung amerikanischer Bürger und ausgewählter Staatsoberhäupter etwas ändern wird. Und RSA-CEO Art Coviello erklärte in seiner Keynote am 25.02.2014 unzweideutig: Auch amerikanische Sicherheitsunternehmen arbeiteten mit der NSA zusammen – und werden es auch künftig tun, wenn es um die (Sicherheits-) Interessen der USA geht. Selbst die Kritik namhafter Kryptologen vom 24.01.2014 zielt in erster Linie auf die Überwachung amerikanischer Bürger und die Schwächung von Sicherheitstechnologie ab. Vor diesem Hintergrund und den dank Snowden bekannten Fakten können wir daher dreierlei festhalten:

1. **Trust the Math**: Wie Bruce Schneier bereits am 06.09.2013 schrieb, gibt es keine Hinweise darauf, dass die NSA in der Lage ist, kryptografische Verfahren zu brechen, die von Kryptologen als ausreichend sicher angesehen werden. Wer „ausgemusterte" Verfahren und kurze Schlüssellängen meidet, liegt daher mit kryptografischem Ende-zu-Ende-Schutz immer richtig.
2. **Misstraue der Implementierung**: Auch gute kryptografische Verfahren lassen sich so implementieren, dass ein Angreifer leichtes Spiel hat – dank einer schwachen Schlüsselerzeugung (Pseudo-Zufall), einer Hintertür (Backdoor) oder einem Programmierfehler. Deutschen Herstellern und überprüfter oder zertifizierter Software gebührt diesbezüglich ein Vertrauensbonus.
3. **Misstraue den Vertrauensankern**: Sicherheit gibt es nicht aus dem Nichts – so wie man sich nicht am eigenen Schopf aus dem Sumpf ziehen kann, benötigt auch Sicherheit einen Vertrauensanker wie z. B. den Aussteller eines SSL-Zertifikats. Statt blindem Vertrauen ist hier eine kritische Prüfung Pflicht.

Inhalt

secorvo
security consulting

Security News

Zeit zum Wechsel

Die Ankündigung von Facebook, den Instant-Messaging-Dienst WhatsApp für 19 Mrd. US$ zu übernehmen, hat am 19.02.2013 für viel Wirbel gesorgt. Dieser Deal hat bei zahlreichen Nutzern das Interesse an sicheren Alternativen zu WhatsApp geweckt; auch die Stiftung Warentest stufte WhatsApp in einem am 26.02.2014 veröffentlichten Vergleichstest als „sehr kritisch" ein. Die stolze Nutzerzahl von ca. 450 Mio. könnte daher schon bald erodieren.

Bereits auf der ersten Karlsruher Anti-Prism-Party am 05.09.2013 stellten wir die aus der Schweiz stammende Alternative Threema vor. Zu einer weiteren Alternative könnte sich der Open-Source Messenger Surespot entwickeln. Die Offenheit des Quellcodes ist ein Plus für Surespot – Threema kann hingegen bei der Implementierung des Schlüsselaustausches punkten. Neben den Instant-Messengern mit Zwischenspeicherung von Daten bleibt die Nutzung von OTR über Jabber-basierte Chat-Dienste eine sichere Alternative – hierbei müssen allerdings beide Gesprächspartner online sein.

Die Downloads zur Anti-Prism-Party umfassen eine Installations- und Konfigurationsanleitung sowie weitere Informationen zur sicheren Nutzung von Internet-Diensten.

Facebook rechtswidrig

Die Berufungsentscheidung des Kammergerichts Berlin vom 24.02.2014 bestätigte Facebook, dass an Nicht-Mitglieder versandte Einladungen zur Registrierung wettbewerbswidrig und die AGB sowie die Datenschutzbestimmungen u. a. hinsichtlich der Gewinnung der Adressen rechtswidrig sind. Auch die unbestimmte, vergütungsfreie und vollständige Rechteübertragung der Inhalte an Facebook verstößt gegen geltendes AGB-Recht. Dasselbe gilt für die einschränkungslosen Änderungs- und die einseitigen Beendigungsklauseln. Die Entscheidung zum *Friend Finder* folgt der Rechtsprechung zu Empfehlungs-E-Mails (SSN 1/2014) und stellt fest, dass die Beteiligung des Nutzers bei der Versendung von Registrierungseinladungen an Dritte für die Einstufung als belästigende Werbung unmaßgeblich und die diesbezügliche Nutzereinwilligung in die Datenverwendung unwirksam ist.

Besonders brisant – und im Widerspruch zum Schleswig-Holsteinischen Verwaltungsgericht (SSN 2/2013) – wird die Anwendbarkeit deutschen Rechts bejaht: Als 100%ige Gesellschafterin habe ungeachtet aller Verträge Facebook Inc., USA, die Entscheidungsmacht. Eine Auftragsdatenverarbeitung käme in dieser gesellschaftsrechtlichen Konstellation nie in Betracht. Dieser Satz dürfte die meisten Konzerngesellschaften mit zentralen Verarbeitungsprozessen und ausländischer Muttergesellschaft mit Entsetzen erfüllen.

Kleiner Bug – große Wirkung

Die Zeilen 631 und 632 der Datei sslKeyExchange.c sehen eher harmlos aus – wird dort doch nur das eingerückte Statement „goto fail" wiederholt. Allerdings hat diese Einrückung weitreichende Wirkung – wie Apple am 21.02.2014 in einem Security Update mitteilen musste. Die offenbar bei der Entwicklung von OS X 10.9 eingeführte Änderung öffnet Man in the Middle-Angriffen auf Apple-Betriebssysteme Tür und Tor. Nach 46 Jahren werden damit Dijkstras Befürchtungen zur bitteren Realität – ein unverzügliches Update von OS X 10.9, iOS 7.0 und iOS 6.1 wird daher dringend empfohlen.

Durchsuchungsverbot

Mit einem nun ausführlich veröffentlichten Urteil vom 20.06.2013 hat das Bundesarbeitsgericht die Anforderungen an das Vorgehen bei Verdachtsmomenten gegen Beschäftigte weiter konkretisiert und den besonderen Rechtfertigungsbedarf für heimliche Überwachungsmaßnahmen verdeutlicht.

In dem entschiedenen Fall war ein Spind aufgrund eines Diebstahlsverdachts unter Einbeziehung des Betriebsrats, aber ohne Beteiligung des Betroffenen durchsucht worden. Dies führte im anschließenden Kündigungsschutzprozess wegen der Unverhältnismäßigkeit der Maßnahme zu einem Beweisverwertungsverbot.

Diese Entscheidung unterstreicht einmal mehr, dass das Vorgehen bei derartigen Untersuchungen klar geregelt und der Betroffenenbeteiligung und -information ein hoher Stellenwert eingeräumt werden sollte, um am Ende belastbare Feststellungen zu erhalten.

Gefahr aus dem IoT

Zunehmend werden Alltagsgegenstände mit eingebetteten Computern ausgestattet und über das Internet vernetzt, wie Babyphones, Videoüberwachungsanlagen oder Heimnetzwerksteuerungen. Das „Internet der Dinge" (*Internet of Things* – IoT), Mark Weisers Vision einer vernetzten Welt aus dem Jahr 1991, wird langsam Realität. Leider sind auch die damit verbundenen Gefahren inzwischen real. Symantec berichtete am 21.01.2014 über einen Linux-Wurm, der auf das IoT zielt. Der Wurm existiert für typische Chiparchitekturen des IoT.

Darauf ist das IoT jedoch nicht vorbereitet. Dort stehen wir bei der Sicherheit da, wo wir vor zwanzig Jahren bei PCs standen: Sicherheitsschwachstellen wurden nicht veröffentlicht, und falls Hersteller Patches bereitstellten, wussten die Benutzer nicht, wie diese zu installieren waren. Schlimmer noch: Soft- oder Firmware der Geräte sind im IoT oft älter als diese. Ist der Quellcode nicht vollständig verfügbar, kann nicht einmal ein Patch erzeugt werden.

Zudem sind die Geräte des IoT ständig mit dem Internet verbunden. Sie lassen sich mit der Suchmaschine Shodan sogar gezielt suchen. Dennoch werden auch solche Geräte mit einem Default-Passwort ausgeliefert. Da die Geräte meist keinen automatischen Update-Mechanismus besitzen, besteht die Gefahr, dass mit vermeintlichen Updates aus nicht autorisierter Quelle Firmware mit Hintertüren eingeschleust wird – wie bei dem am 18.02.2014 bekannt gewordenen Fall der intelligenten Haushaltsgeräte von Belkin Wemo.

Erweiterter Process Explorer

Am 29.01.2014 wurde der Process Explorer von Microsoft um eine hilfreiche Funktion ergänzt: Version 16 unterstützt nun VirusTotal-Abfragen für laufende Prozesse und die von diesen bei jedem Programmstart zahlreich hinzugeladenen Dynamic Link Librarieres. Ist die Funktion aktiviert, werden MD5-Summen gebildet und mit den Erkenntnissen von 50 verschiedenen Virenscannern bei VirusTotal abgeglichen. Ein blauer (‚gut') oder roter (‚böse') Zahlenwert weist dann auf „kritische Erkenntnisse" hin. Ein blaues Ergebnis ist allerdings eher eine „Tendenzaussage", schließlich gibt es Schadsoftware, die von diesem Werkzeug und vielen Antivirusprogrammen in einer Live-Umgebung nicht gefunden wird.

Bei der Aktivierung wird man um die Zustimmung zur Nutzungsvereinbarung von VirusTotal gebeten – in der man alle Verwertungsrechte für hochgeladene Daten an VirusTotal abtritt. Ach ja: Seit 2012 gehört VirusTotal zu Google.

DIN-Norm Datenlöschung

Im Dezember 2012 stellte Secorvo die DIN-Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten vor, die auf großes Interesse stieß. Ende 2013 startete daher ein von den Unternehmen Blancco, DATEV, Deutsche Bahn, Secorvo und Toll Collect gefördertes Projekt, in der die Leitlinie nun zu einer DIN-Norm weiterentwickelt wird. Am 12.02.2014 beschloss der DIN-Arbeitskreis für Identitätsmanagement und Datenschutz-Technologien (AK 05 im NIA 27) die Aufnahme eines Normungsprojekts.

Die Norm für Löschkonzepte soll bis zum Herbst 2015 verabschiedet werden. Die veröffentlichte Leitlinie gibt bereits heute wesentliche Hilfestellung für die Entwicklung eigener Löschkonzepte.

Secorvo News

System Security

Security Engineering – die Entwicklung inhärent sicherer Systeme – ist eine vergleichsweise junge Disziplin. In den vergangenen Jahren ist jedoch aus zahlreichen Erfahrungen und *Best Practices* ein sinnvolles Vorgehensmodell entstanden. Dabei wird die Sicherheit eines Systems aus unterschiedlichen Blickwinkeln betrachtet, um die vielfältigen Abhängigkeiten und externen Einflüsse bereits beim Systemdesign zu berücksichtigen.

In dem Seminar Security Engineering – Sichere Systeme durch Security by Design legen wir dar, wie Sicherheit in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie haben die Möglichkeit, Ihre erworbenen Kenntnisse anschließend mit dem T.E.S.S. zertifizieren zu lassen (**12.–15.05.2014**). Und falls Sie – schnell entschlossen – zuvor noch ein T.I.S.P.-Zertifikat erwerben wollen: vom **24. bis 28.03.2014** haben Sie die Gelegenheit dazu, es gibt noch einige wenige freie Plätze. Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Herkunft verpflichtet.

In modernen Informationssystemen (Stichwort *Data Warehouse* oder *Big Data*) erreicht die Verarbeitung von personenbezogenen Daten eine Komplexität, die die Umsetzung datenschutzrechtlicher Transparenzanforderungen erheblich erschwert. *Data Provenance* (Bestimmung der Datenherkunft) kann dabei unterstützen, die Herkunft und die Bearbeitung von personenbezogenen Daten sowie den Zugriff auf diese nachvollziehbar zu gestalten. Beim nächsten KA-IT-Si Event am **03.04.2014** um 18 Uhr in den Räumen des Fraunhofer IOSB in Karlsruhe zeigt Christoph Bier (Fraunhofer IOSB) in seinem Vortrag „Data Provenance. Auch Daten haben ihre Geschichte", wie die Datenschutzauskunft der Zukunft aussehen könnte.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wir freuen uns auf Ihre Anmeldung!

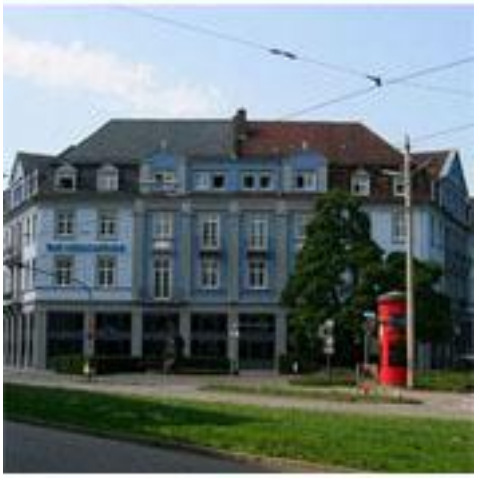
Veranstaltungshinweise

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

März 2014	
24.-29.03.	T.I.S.P.-Schulung und -Prüfung (Secorvo College, Karlsruhe)
April 2014	
03.04.	Herkunft verpflichtet. (Karlsruher IT-Sicherheitsinitiative, Karlsruhe)
08.-10.04.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen, Schutzmechanismen (Secorvo College, Karlsruhe)
Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-16.05.	Security Engineering – Schulung & T.E.S.S.-Prüfung (Secorvo College, Karlsruhe)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)

Fundsache

Das Portal Netzpolitik.orG verschenkt seit dem 19.02.2014 das im November 2013 erschienene Buch „Überwachtes Netz“ mit spannenden Beiträgen von Autoren wie Constanze Kurz, Frank Rieger, Markus Beckedahl, Peter Schaar, Bruce Schneier und Richard Stallman. Das Buch ist erhältlich als ePub, AZW3 oder PDF.



Impressum

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

ISSN 1613-4311

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

secorvo
security consulting

Secorvo Security News

März 2014

Im Netz der Spinne

Die Raumsonde Deep Space 1 wurde am 24.10.1998 zur Erforschung des Asteroiden (9969) Braille gestartet. Am 22.09.2001 nahm sie spektakuläre Bilder des Kometen 19P/Borrelly auf; am 18.12.2011 wurde sie schließlich deaktiviert.

Auch der israelische Gesichtserkennungsdienst face.com machte schon spektakulär auf sich aufmerksam. Im Juli 2011 gelang die Aufsehen erregende Erkennung von Emotionen, und im März 2012 die automatische Alterserkennung. Nach langer Freundschaft war die am 18.06.2012 von face.com bekannt gegebene Übernahme durch Facebook ein logischer Schritt. Euphorisch jubelte die Pressemitteilung: „By working with Facebook directly, and joining their team, we'll have more opportunities to build amazing products that will be employed by consumers – that's all we've ever wanted to do." Inzwischen erreicht die DeepFace getaufte Software mit Hilfe eines neuronalen Netzwerkes eine Treffergenauigkeit von 97,25 % bei der Identifikation von Personen auf einem Bild. Das menschliche Gehirn ist nur unwesentlich erfolgreicher – sofern es ebenso viele Personen kennt wie DeepFace...

Zwar wehrten sich die europäischen Datenschützer zuletzt erfolgreich gegen Facebooks Gesichtserkennung – frei nach Ovids Empfehlung in seiner Remedia amoris, die Liebe im Keim zu ersticken („Wehret den Anfängen"). Allerdings könnte es dafür bereits zu spät sein.

Denn anders als die Raumsonde Deep Space 1 macht DeepFace seine Analysen nicht im Orbit, sondern auf der Erde. Und es wäre sicherlich naiv zu hoffen, dass die Mission von DeepFace nach dreizehn Jahren durch Deaktivieren beendet wird. Denn DeepFace ist kein Forschungsprojekt, sondern eine Einnahmequelle, die perfekt in Mark Zuckerbergs selbst erklärter Mission passt, die Welt zu vernetzen.

Ein Schelm, wer dabei an eine Spinne denkt.

Inhalt

secorvo
security consulting

Security News

Das NIST und das Vertrauen

NSA-Enthüllungen und der Verdacht einer Backdoor im NIST-Standard SP 800-90A für Zufallszahlengeneratoren (siehe SSN 11/2013) haben die Integrität des NIST-Entwicklungsprozesses für kryptographische Standards in Frage gestellt.

In einem öffentlichen Schreiben vom 17.02.2014 betont das NIST nun die Bedeutung der Unterstützung durch die weltweite Krypto-Gemeinde für die Akzeptanz von kryptographischen Algorithmen und bittet im Rahmen der bereits im November 2013 initiierten Überprüfung des Standardentwicklungsprozesses um Kommentare.

Die Prinzipien und Prozeduren sind als Draft NIST Interagency Report 7977 öffentlich verfügbar. Dazu zählen insbesondere die Transparenz, die Offenheit und der Ausgleich der Interessen unterschiedlicher Gruppen. Als Prozeduren kommen beispielsweise internationale kryptographische Wettbewerbe und die Veröffentlichung von Standardentwürfen zum Einsatz.

Allerdings betont das NIST, auch weiterhin eng mit der NSA (einer der Interessensgruppen) zusammen zu arbeiten, da Mitarbeiter der NSA über immense Erfahrung in der Kryptographie verfügen und das NIST per Gesetz verpflichtet ist, bei der Standardentwicklung die NSA zu befragen.

Bis zum 18.04.2014 können Kommentare eingereicht werden. Eine 90 Seiten umfassende Kommentarsammlung zum NIST SP 800-90A ist bereits verfügbar.

Widerspruchsrecht bei Piwik

Auch wenn die IP-Adressen von Seitenbesuchern mit dem Webanalyse-Tool Piwik nur anonymisiert erfasst werden, muss der Seitenbesucher eine Möglichkeit zum Widerspruch haben. Das entschied das LG Frankfurt am 18.02.2014 (Az. 3-10 O 86-12). Ein entsprechender Hinweis ist in die Datenschutzerklärung der Webseite aufzunehmen.

Damit liegt ein weiteres Urteil vor, welches die Möglichkeit einer wettbewerbsrechtlichen Abmahnung für Verstöße gegen das Telemediengesetz bejaht. Bereits das OLG Hamburg hatte mit seinem Urteil vom 27.06.2013 einen Verstoß gegen datenschutzrechtliche Informationspflichten ähnlich bewertet.

Folgt man dem Frankfurter Urteil, so muss jeder Webseiten-Betreiber „zu Beginn des Nutzungsvorgangs“ auf den Einsatz eines Webanalyse-Tools hinweisen, was bei enger Auslegung wohl bedeutet, dass sich vor dem Öffnen einer Webseite ein Pop-up-Fenster öffnen muss, welches den Besucher informiert. So etwas sieht kaum eine Webseite vor.

Dies ist eine ähnliche Forderung, wie sie die in Deutschland noch nicht umgesetzte „Cookie-Richtlinie“ (2009/136/EG) der EU enthält, die eine Einwilligung (Opt-in) für Cookies verlangt. Webseitenbetreiber sollten diese Entwicklungen im Auge behalten und in jedem Fall ihre Datenschutzerklärung aktuell und gut erreichbar halten.

Full Disclosure ist tot – es lebe...

Am 19.03.2014 hat John Cartwright, Gründer der im Jahr 2002 ins Leben gerufenen Mailing-Liste Full Disclosure, per E-Mail an die Mailing-Liste bekannt gegeben, dass er den Dienst einstellen wird. In der Liste wurden in den letzten zwölf Jahren viele wichtige Hinweise auf Sicherheitsschwachstellen anonym veröffentlicht. Die Security-Community wird diese wichtige Informationsquelle vermissen.

Das dachte sich auch Gordon Lyon – und kündigte am 25.03.2014 an, die Liste fortzuführen. Allerdings ist dafür eine Neuanmeldung erforderlich.

Datenschutzaufsicht zu BYOD

Bereits am 06.02.2014 hat der Hamburgische Landesdatenschutzbeauftragte seinen Jahresbericht für die Amtsjahre 2012/2013 vorgelegt und anhand der berichteten Vorkommnisse zu einer Vielzahl praktischer Datenschutzfragen Stellung genommen. Ein längerer Abschnitt ist dem Thema „Bring your own device“ (BYOD) gewidmet.

Die warnende Analyse des Berichts basiert auf der Prüfung der Container-Lösung DME-Extractor für iPhone und Android-Geräte in der hamburgischen Verwaltung. Grundsätzlich wird BYOD danach als sehr risikoreich eingeschätzt; der Bericht warnt vor einer Unterschätzung des Schutzbedarfs. Gefordert wird als Stand der Technik wenigstens ein Mobile Device Management, eine Container-Lösung, eine umfassende Nutzungsregelung für den Geräteeinsatz, vor allem bezüglich der Container-Löschung im Falle einer Wartung durch Dritte.

Vor einer Freigabe des Verfahrens wird ein umfassender Penetrationstest empfohlen. Die zum Bezug der verfahrensnotwendigen App (unter Android) erforderliche Registrierung des Nutzers bei Google wird wegen der verbundenen Datenübertragung von Beschäftigtendaten an Google als inakzeptabel angesehen. Allgemein seien die für die private Freizeitnutzung ausgelegten Geräte für die geschäftliche Verarbeitung von Daten mit möglicherweise hohem Schutzbedarf ungeeignet.

Vor dem Hintergrund der aufgezeigten Bedenken mutet das Résumé, der Einsatz sei sehr ‚risikoreich', inkonsequent an. Wünschenswert wäre eine klare Feststellung gewesen, dass der Einsatz bei Nichterfüllung der aufgestellten Anforderungen schlicht als rechtswidrig angesehen werden muss.

Die Stellungnahme kündigt eine abgestimmte Wertung der Datenschutzbeauftragten des Bundes und der Länder an. Diese wird sich hoffentlich in der Frage der Zulässigkeit eindeutiger festlegen, um Unternehmen eine rechtssichere Orientierung für den Datenschutz konformen Umgang mit BYOD-Bestrebungen zu geben.

Nachweis des Nicht-Ereignisses

Der BGH hat in einem Urteil vom 19.02.2014 seine Rechtsprechung zur Beweisführung bei streitigen Faxzugängen präzisiert. Die Vorinstanz hatte den Zugang – trotz vorgelegter Sendeberichte – ohne weitere Beweisaufnahme verneint, da der OK-Vermerk des Sendeprotokolls lediglich ein Indiz darstelle, aber keinen Anscheinsbeweis begründe.

Der BGH führt nun aus, dass bei vorliegendem Sendeprotokoll ein einfaches Bestreiten des Zugangs nicht ausreicht. Der Empfänger hat im Rahmen der so genannten sekundären Darlegungslast wenigstens darzustellen, welches Gerät er nutzt, ob dieses eine Verbindung verzeichnet hat, und – soweit vorhanden – sein Empfangsjournal vorzulegen. Anhand dieser Angaben hat das Gericht dann eine Beweiswürdigung vorzunehmen.

Einen Zuwachs an Rechtssicherheit bringt das Urteil jedoch weder für den Empfänger noch für den Sender. Sowohl Sendeprotokolle als auch Empfangsjournale sind regelmäßig nicht gegen Manipulationen geschützt, so dass sie nur schwache Anhaltspunkte darstellen. Das Versenden im Beisein eines Zeugen ist ein wirksamerer Beweis – umgekehrt lässt sich aber ein Nicht-Empfang schlechthin nicht bezeugen.

Da Empfangsprotokolle oft nur eine begrenzte Zeit zurückreichen und nicht wirksam gegen Manipulation geschützt werden können, und Faxgeräte zudem meist nicht nur einer Person zugänglich sind, dürfte ein wirksames Abstreiten des Empfangs in der Regel schwierig sein. Vor einer ungerechtfertigten Zurechnung schützt danach wohl nur ein vollständig digitaler Empfang mit ausführlichen und weit zurück reichenden Log-Protokollen – eine datenschutzrechtlich unschöne Lösung.

Geldfund

Die insolvente Bitcoin-Börse Mt. Gox hat am 20.03.2014 bekannt gegeben, ein Wallet mit 200.000 der vermissten 850.000 Bitcoins ‚gefunden' zu haben. Das entspricht – nach dem aktuellen Kurs – immerhin beachtlichen 90 Mio. US$. Offenbar kommen Bitcoins leicht unter die Räder: Zuletzt hatte am 27.11.2013 der britische Guardian über James Howells berichtet, der Bitcoins im Wert von 4,5 Mio. Pfund zusammen mit seiner Festplatte entsorgt hatte. Da war das Leben früher doch viel sicherer: 90 Mio. US$ in Scheinen verliert man nicht – in 50-Dollar-Bündeln wiegen diese 1,8 Tonnen.

Secorvo News

Zertifikat mit Erkenntnisgewinn

Auf rund 190 Jahre summiert sich die Berufserfahrung aus unterschiedlichen Tätigkeitsfeldern der Informationssicherheit der elf Secorvo-Referenten in der fünftägigen T.I.S.P.-Schulung. Die nächste Gelegenheit, von diesem Erfahrungsschatz als Teilnehmer eines Secorvo-T.I.S.P.-Seminars unmittelbar zu profitieren, bietet sich Ihnen **vom 19. bis 23.05.2014**.

Sicherheit ist programmierbar

Wenn grundsätzlich im Software-Entwicklungsprozess Sicherheit als wesentliches Entwurfskriterium von Anfang an berücksichtigt werden würde, dann gäbe es viele heutige Sicherheitsprobleme definitiv nicht. Doch was noch nicht ist, kann ja noch werden: Als Certified Professional for Secure Software Engineering (CPSSE) kennen Sie – oder Ihre Kollegen – die Techniken und Vorgehensweise von „Security by Design". Das nächste Seminar mit noch freien Plätzen findet statt **vom 05. bis 08.05. 2014**. (Online-Anmeldung).

Herkunft verpflichtet

"Data Provenance. Auch Daten haben ihre Geschichte." ist das Thema des nächsten KA-IT-Si-Events am **03.04.2014** um 18 Uhr im Max-Syrbe-Saal des Fraunhofer IOSB in Karlsruhe. Christoph Bier (Fraunhofer IOSB) wird in seinem Vortrag zeigen, wie die Datenschutzauskunft der Zukunft aussehen könnte. Anschließend gibt es – wie gewohnt – Gelegenheit zum „Buffet-Networking". Wir freuen uns auf Ihre Anmeldung.

Teamverstärkung

Wieder konnten wir eine Verstärkung für das Consulting-Team gewinnen: Am 01.03.2014 ist André Domnick zu uns gestoßen. Er bringt viel Erfahrung in den Bereichen sichere Softwareentwicklung und Web Application Security mit – und einen Bachelor in Information Security.

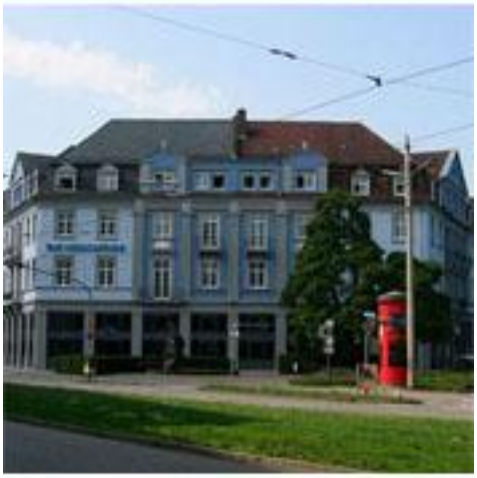
Veranstaltungshinweise

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

April 2014	
03.04.	Herkunft verpflichtet. (Karlsruher IT-Sicherheitsinitiative, Karlsruhe)
08.-09.04.	Datenschutztage 2014 (FFD Forum für Datenschutz, Wiesbaden)
09.-10.04.	Security Forum 2014 (Hagenberger Kreis, Hagenberg/AT)
Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
12.-16.05.	Security Engineering – Schulung & T.E.S.S.-Prüfung (Secorvo College, Karlsruhe)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)
19.-24.05.	T.I.S.P. - Schulung und Prüfung (Secorvo College, Karlsruhe)
21.-23.05.	Entwicklertag 2014 (VKSI, Karlsruhe)

Fundsache

Apple hat am 20.02.2014 eine aktualisierte Version der Dokumentation zur iOS Security veröffentlicht. Darin erläutert Apple viele Sicherheitsfeatures, über die bisher lediglich spekuliert werden konnte. Lesenswert.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Yun Ding, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp, Christoph Schäfer (Editorial), 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

secorvo
security consulting

Secorvo Security News

April 2014

Was jetzt zählt

Nicht jeder IT-Sicherheitsverantwortliche wird dieses Editorial lesen können – denn der eine oder andere wird noch mit den Aufräumarbeiten nach „Heartbleed“ beschäftigt sein. Dennoch sollte in der unvermeidlichen operativen Hektik nicht übersehen werden, was genau dieser JAB (*Just Another Bug*) uns eigentlich lehren müsste.

IT-Sicherheit hat viel mit Vertrauen zu tun. Das ist aber mehr Not als Tugend – denn wünschen würden wir uns, dass wir uns von der Vertrauenswürdigkeit einer Soft-, Hard- oder Cloudwarelösung, der wir unsere Kommunikation oder unsere Daten anvertrauen, zuverlässig überzeugen könnten.

Leider funktioniert das meistens nicht. So steht der Aufwand für die Analyse oft in keinem realistischen Verhältnis zum Schutzbedarf der Daten – oder bedroht gar die Wirtschaftlichkeit des Geschäftsmodells des Nutzers. Zudem ist jede Analyse immer nur eine Momentaufnahme: Jede Änderung am System (Konfiguration, Firmware, Hardware, Software, ...) kann ein zunächst positives Urteil in sein Gegenteil verkehren. Was bleibt ist bestenfalls ein strenger Vertrag mit dem Anbieter, das Einspielen von Patches und die fromme Hoffnung, dass die eigene Infrastruktur verschont bleibt.

Allerdings gibt es Bereiche, in denen wir uns nicht mit solcherart halbblindem Vertrauen begnügen dürfen: den „Herzstücken“ unserer IT-Sicherheitsinfrastrukturen – zu denen angesichts der weiten Verbreitung und zentralen Bedeutung zweifellos OpenSSL gezählt werden muss. Es hilft auch nicht, wie nach dem Bekanntwerden von Prism gebetsmühlenartig nach „Security made in Germany“ zu rufen – denn unglücklicherweise war es gerade ein deutscher Programmierer, dem die Welt nun Heartbleed verdankt.

In den zentralen Organen unserer Infrastrukturen brauchen wir mit Methoden der sicheren Softwareentwicklung erzeugten und nachprüfbar verifizierten Code. Sich dabei lediglich auf die Offenheit des Sourcecodes zu verlassen, ist schlicht unverantwortlich.

Inhalt

secorvo
security consulting

Security News

Persilschein für Office 365

Mit seiner Cloud-Kollaborationslösung Office 365 will Microsoft seine Kunden von komplizierten Lizenzverträgen befreien. Die neuen nutzerbezogenen Lizenzmodelle können dabei zu hohen Einsparungen führen. Um das Angebot datenschutzrechtlich abzusichern, hat Microsoft ein Vertragskonstrukt entworfen, welches eine Vereinbarung zur Auftragsdatenverarbeitung mit Microsoft Irland (Standort des europäischen Rechenzentrums) vorsieht. Da die Lizenzverwaltung und der Support durch Microsoft USA erfolgen, ist außerdem der Abschluss von EU Model Clauses erforderlich. Die Vertragsvorlagen können über das Office 365 Trust Center bezogen werden.

Mit Schreiben vom 29.11.2011 hatte das Bayerische Landesamt für Datenschutzaufsicht bereits die grundsätzliche Eignung der Microsoft-Verträge bestätigt. Nach intensiven Diskussionen liegt nun mit Datum vom 02.04.2014 eine weitere Bestätigung der Artikel-29-Gruppe vor, die Microsoft seit dem 10.04.2014 als Persilschein nutzt. Dabei sollte man allerdings nicht vergessen, dass man für die Übermittlung im Rahmen von EU Model Clauses nach wie vor eine Rechtsgrundlage benötigt. Ob es zudem ratsam ist, einen erheblichen Teil der Unternehmensdaten in die Hand eines (US-) Dienstleisters zu legen, steht auf einem anderen Blatt.

XP ist tot...

Mit dem Sicherheitsupdate MS14-020 veröffentlichte Microsoft am 08.04.2014 die letzten Patches für Windows XP und Microsoft Office 2003. Beide Produkte erfreuen sich jedoch weiterhin großer Beliebtheit. Die britische Regierung, das Land Niedersachsen und weitere Großkunden schlossen daher Verträge über ein weiteres Jahr Support für ihre Systeme ab. Den meisten Nutzern der beiden Softwarepakete werden jedoch weitere Updates verwehrt bleiben.

Voraussichtlich wird die Zahl der Schwachstellen und Exploits ansteigen – auch weil Windows XP und Office 2003 sich mit den neueren Versionen große Teile des Quellcodes teilen. So lassen sich aus zukünftigen Sicherheitsupdates mit einfachen Reverse Engineering-Techniken wie binären Diff-Tools die behobenen Schwachstellen ausfindig machen – von dort ist der Weg zum funktionierenden XP-Exploit nicht mehr weit.

Immerhin: Eingebettete Alt-Systeme wie Bankautomaten sind von dem Problem meist nicht betroffen, da sie überwiegend Windows XP Embedded verwenden – und das wird bis 2016 mit Updates versorgt.

Ende der Verantwortungsabschiebung

In einem mit Spannung erwarteten Urteil hat der Europäische Gerichtshof am 08.04.2014 die Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG) rückwirkend für ungültig erklärt. Die europarechtliche Pflicht zur Einführung einer Vorratsdatenspeicherung ist damit entfallen.

Der EuGH folgt in seinem Urteil weitgehend der Argumentation, die bereits das Bundesverfassungsgericht seinem Urteil zu Grunde gelegt hatte: Der schwerwiegende Eingriff in Art. 7 und 8 der Charta der Grundrechte der Europäischen Union sei nur verhältnismäßig, wenn die Verwendung der Daten anhand klarer Kriterien begrenzt, die Datensicherheit durch strikte Regeln gewährleistet und die Speicherdauer anhand objektiver Kriterien auf das absolut Notwendige beschränkt werde. Auch schreibe die Richtlinie keine Speicherung im Unionsgebiet vor, so dass nicht sichergestellt sei, dass die Umsetzung der Datensicherheitsanforderungen durch eine unabhängige Stelle der EU überwacht werden könne.

Zwar berührt auch nach Auffassung des EuGH die Vorratsdatenspeicherung nicht den Wesensgehalt der Chartagrundrechte. Doch kann sich jetzt keine Regierung eines Mitgliedsstaats mehr bei der Einführung einer Vorratsdatenspeicherung hinter einer europäischen Umsetzungspflicht verstecken.

Schutz durch Big Data

Am 25.03.2014 stellte Mark Hammell auf der Webseite der Facebook-Sicherheitsinitiative „protectthegraph“ vor, wie Facebook Security-Informationen automatisiert verarbeitet – mit hauseigenen Big Data-Techniken.

Die Komponente Feeds sammelt ständig sicherheitsnahe Informationen aus freien und abonnierten externen und eigenen Quellen und reichert diese mit Kontextdaten wie Ort und Zeit an. Dies können Daten von Malware-Diensten sein, Hinweise aus Infoportalen, Security-Blogs oder Informationen der eigenen Security-Teams.

Diese Daten werden jeweils als Thread-Datum im Hieve, dem Hadoop-Datawarehouse von Facebook archiviert. Das für Massendaten entwickelte Analysewerkzeug Scuba untersucht jedes neue Thread-Datum auf Trends oder Muster und startet Reaktionsprozesse – Blacklisting gefährlicher URLs, Benachrichtigung von Nutzern oder Alarmierung des Security-Teams.

In internen Tests habe dieses System die eingesetzten Antiviren-Produkte geschlagen. Dieses Ergebnis steht und fällt jedoch mit aktuellen externen Informationen, wie von Lösungsanbietern kritisiert wurde. Es deutet aber daraufhin, dass das Teilen von Information z. B. über erkannte Angriffsmuster oder eigene Vorfälle für alle Beteiligten – außer dem Angreifer natürlich – Vorteile bietet.

Innerhalb einiger Branchen gibt es dieses kooperative Vorgehen bereits. Was fehlt ist allerdings ein einheitliches Datenformat. Dessen Spezifikation wäre einmal eine sinnvolle Aufgabe für eine der zahlreichen Cybersecurity-Initiativen.

Open Source-Desaster

Gleich mehrere verbreitete Open Source-Lösungen standen in den vergangenen Wochen im Rampenlicht. Zunächst sorgte bekanntlich am 07.04.2014 das Security Announcement von OpenSSL, inzwischen als Heartbleed bekannt, für Furore (siehe Editorial). Die Schwachstelle ermöglicht das (spurlose) Auslesen von 64 kByte großen Speicherbereichen eines SSL-Servers. Der Programmierfehler wurde weder während des Reviews noch in den zwei darauffolgenden Jahren bemerkt, bis Neel Mehta von Google ihn entdeckte und dem OpenSSL-Team meldete.

Mit den Updates für iOS 7.1 vom 23.03.2014 und iOS 7.1.1 sowie die Safari Browser 6.1.3 und 7.0.3 vom 22.04.2014 behob Apple einen weiteren, als „Triple Handshake" bezeichneten Bug in der SSL/TLS-Implementierung sowie zahlreiche Schwachstellen in der Open-Source-HTML-Engine WebKit, die von Safari und vielen weiteren Browsern genutzt wird. Von den 27 Schwachstellen in WebKit wurden 26 durch Programmierfehler verursacht, die den Datenspeicher korrumpieren: Beim Besuch manipulierter Webseiten kann damit Code vom Angreifer auf dem Rechner des Opfers ausgeführt werden.

Das Google Chrome Security Team fand 18 der 26 Schwachstellen, da Chrome die Engine Blink verwendet, die im April 2013 aus dem Sourcecode von WebKit abgespaltet worden war. Dabei konnte Google 8.8 Millionen Codezeilen entfernen. Möglicherweise schlummern noch immer etliche Bugs in WebKit, die Google bereits in Chrome beseitigt hat – bis Apple sie eines Tages findet.

Schließlich erschien am 14.04.2014 der Bericht über den ersten Teil des Source-Code-Audits zu TrueCrypt. Er dokumentiert eine gründliche Prüfung des Bootloaders und des Kernel-Treibers. Zwar wurden keine gravierenden Schwachstellen aufgedeckt; dennoch gibt die Bewertung „*Overall, the source code for both the bootloader and the Windows kernel driver did not meet expected standards for secure code*" zu denken.

Zur Vermeidung von gravierenden Schwachstellen in so grundlegenden Bausteinen der Sicherheit sollte die Offenheit des Codes mit der gebotenen Professionalität beim Entwickeln und prüfen kombiniert werden (siehe SSN 01/2014). Hierzu bedarf es entsprechender Anreize und Ressourcen. Initiativen wie das Open Crypto Audit Project zeigen einen möglichen Weg dafür auf.

Secorvo News

PKI für Profis

Seit den späten 90er Jahren realisiert Secorvo PKI-Projekte. Der dabei entstandene, Produkt unabhängige Erfahrungsschatz in Sachen Konzeption, Aufbau, Betrieb und Weiterentwicklung wurde für das Seminar „PKI – Grundlagen, Vertiefung und Realisierung" in einem viertägigen Programm verdichtet. Die fünf Referenten des Seminars bringen zusammen über 90 Jahre Berufserfahrung in der IT-Sicherheit mit. Für den Einsteiger bietet die Schulung eine grundlegende, Produkt unabhängige Einführung, für den Profi eine vertiefende Auseinandersetzung mit den Möglichkeiten von Public Key Infrastrukturen. Nächster Seminartermin ist der 24. bis 27.06.2014.

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

Live Hacking

Live-Hacking-Demos haben gelegentlich vor allem Show-Charakter – die vorgestellten Angriffe betreffen entweder längst ausgemusterte IT-Systeme oder führen für einen praktischen Angriff eher ungeeignete Spezialschwachstellen vor.

Nach dem großen Erfolg der Live-Vorführung eines äußerst wirkungsvollen WLAN-Angriffs auf der vergangenen Anti-Prism-Party am 12.02.2014 im Karlsruher ZKM werden Kai Jendrian und Jörg Völker von Secorvo den Angriff und einige einfache und elementare Maßnahmen zum Schutz der Privatsphäre auf der kommenden Veranstaltung der KA-IT-Si am **05.06.2014** erneut vorstellen (18 Uhr im Panoramasaal der IHK Karlsruhe).

Nach Vortrag und Diskussion haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – diesmal über den Dächern von Karlsruhe. Weitere Informationen und die Möglichkeit zur Anmeldung auf www.ka-it-si.de.

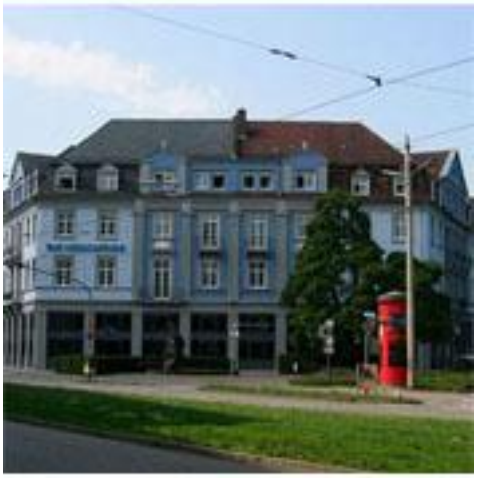
Veranstaltungshinweise

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

Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)
16.05.	Jahrestagung "Datenschutz im digitalen Zeitalter – global, europäisch, national" (Institut für Rundfunkrecht an der Universität zu Köln, Köln)
19.-20.05.	a-i3/BSI-Symposium 2014 (Arbeitsgruppe Identitätenschutz im Internet/BSI, Bochum)
21.-22.05.	BvD Datenschutztage (BvD e. V., Berlin)
21.-23.05.	Entwicklertag 2014 (VKSI, GI, Objekt-Forum, Karlsruhe)
Juni 2014	
23.-24.06.	DuD 2014 (Computas, Berlin)
23.-26.06.	OWASP AppSec EU 2014 (OWASP, Cambridge/UK)

Fundsache

Damn Vulnerable iOS App ist eine App, die alle gängigen Sicherheitslücken von iOS-Anwendungen enthält – sie ist „verdammt verwundbar". Diese App bietet Sicherheitsinteressierten eine Plattform, auf der sie iOS-Penetrationtests legal durchführen können.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, André Domnick, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer.

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

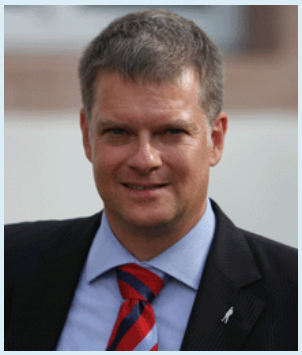
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

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

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

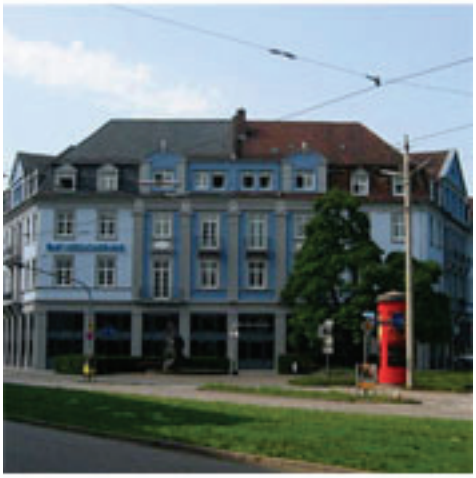
ISSN 1613-4311

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



secorvo
security consulting

Secorvo Security News

Juni 2014

Die Vertrauensattacke

Während das US-amerikanische Repräsentantenhaus am 23.06.2014 mit überwältigender Mehrheit (293:123 Stimmen) der NSA untersagte, Hintertüren in US-amerikanische IT-Produkte einzubauen und die Internet-Aktivität amerikanischer Bürger ohne Gerichtsbeschluss zu überwachen, blieben wichtige Aspekte der Geheimdiensttätigkeit ungeregelt.

Vor dem Hintergrund der amerikanischen Überwachungsaktivitäten der vergangenen 20 Jahre wird ein bedenkliches Gesamtbild erkennbar. In den 90er Jahren versuchte die NSA vergeblich, sich den Zugriff auf verschlüsselte Daten zu sichern: Schwache Verschlüsselungsverfahren, wie der auf Drängen der NSA von 128 auf 56 bit Schlüssellänge verkürzte DES, waren durch öffentlich evaluierte, starke Verfahren wie den AES ersetzt worden. Und das „Law Enforcement Access Field" (LEAF), mit dem sie sich eine Entschlüsselungsmöglichkeit erhalten wollte, scheiterte 1994 an einer blamablen Protokollschwäche.

Danach verlegte sich die NSA auf eine verdeckte Universalstrategie – und attackierte jeden möglichen Angriffspunkt der entstehenden, auf SSL basierenden Vertrauensinfrastruktur:

- SSL-Serverbetreiber, deren geheimer SSL-Schlüssel die Entschlüsselung mitgeschnittener Kommunikation ermöglichte,
- Zertifizierungsinstanzen, die Schlüsselpaare erzeugten (und damit auch Zugang zu geheimen SSL-Schlüsseln besaßen),
- Zertifizierungsinstanzen, die der NSA falsche SSL-Zertifikate für Man-in-the-Middle-Angriffe ausstellten,
- möglicherweise auch (Open)SSL-Implementierungen, um Hintertüren in Soft- oder Firmware zu verankern und
- Standardisierungsgremien, um Zufallszahlengeneratoren mit Vorhersagemöglichkeit für die NSA zu etablieren (SSN 11/2013).

Das Ergebnis ist ein Scherbenhaufen: Vertrauensverlust in SSL, amerikanische Anbieter und die Standardisierung. Wer wird das kitten?

Inhalt

secorvo
security consulting

Security News

Sicherer im Netz mit Tails

Am 10.06.2014 wurde Version 1.0.1 des Live-Betriebssystems Tails veröffentlicht. Tails kann von einem USB-Stick gestartet werden und eröffnet den Internetzugang standardmäßig über das Tor-Netzwerk. Weitere Maßnahmen zum Schutz der Privatsphäre sind die Veränderung der MAC-Adresse sowie die GPG-Unterstützung des E-Mail-Clients. Um Angriffswege zu reduzieren ist zudem in der Grundeinstellung der Root-Account deaktiviert.

Im Test lief Tails auf verschiedenen Laptops einwandfrei, mit ordentlicher Bildschirmauflösung und WLAN-Unterstützung – ohne dass die Grundkonfiguration angepasst werden musste. Will man eine dauerhafte Datenpartition auf dem Stick anlegen, sollte man Tails von einem bereits laufenden Tails – beispielsweise von DVD gestartet – kopieren. Auf der verschlüsselten Partition können dann eigene Dateien abgelegt werden. Tails hinterlässt keine Spuren auf dem genutzten Rechner.

Tails macht einen durchdachten Eindruck und ist ein möglicher Weg, einen „ergrauten" XP-Rechner mit einem aktuellen Betriebssystem auszustatten – das gelingt sogar im „XP-Look", wenn man diese Option beim Starten auswählt.

Dämmer im Dunkel

TK-Unternehmen haben Transparenzberichte als Mittel entdeckt, um ihrer juristischen Machtlosigkeit gegenüber staatlichen Zugriffen zumindest ihren guten Willen zum Schutz der Kundendaten entgegenzusetzen. So bestätigt Vodafone in einem am 06.06.2014 veröffentlichen Bericht, in 29 Staaten Behörden Zugriff auf Telekommunikationsdaten gewähren zu müssen.

Dabei werden deutliche Unterschiede in Art und Umfang der Zugriffe erkennbar. In Deutschland müssen TK-Anbieter auf Grundlage von § 5 des Artikel 10-Gesetzes, § 110 Abs. 1 Nr. 5 TKG und § 27 TKÜV staatlichen Stellen Zugriff auf die bei ihnen gespeicherten Daten gewähren. Dazu speichern sie die relevanten Daten in einer so genannten *interception copy* („Überwachungskopie"), die dem Nachrichtendienst übergeben wird. Vorher werden die Daten nach vorgegebenen Suchbegriffen gefiltert – und nicht relevante Teile gelöscht.

Ein solch umständliches Vorgehen ist in zumindest sechs Staaten, die Vodafone nicht namentlich benennt, nicht erforderlich: Dort müssen TK-Anbieter Direktzugriffe gewähren. In Albanien, Ägypten, Indien, Malta, Katar, Rumänien, Südafrika, Türkei und Ungarn darf zudem nicht darüber berichtet werden, wie und in welchem Umfang Überwachungsmaßnahmen erfolgen. Auch ohne weitere Snowdens wissen wir nun immerhin, wer sich neben den USA noch an unseren TK-Daten bedient.

Cyberabwehr in der Kritik

Das holperige Kürzel ist Programm: Irgendwie ist niemand mit dem seit dem 01.04.2011 tätigen Nationalen Cyberabwehrzentrum (NCAZ) so recht glücklich. Die einen wundern sich, dass Deutschland mit zehn Mitarbeitern im „Cyberwar" bestehen will. Verfassungsrechtler schlagen Alarm, da die vorgeschriebene Trennung zwischen Nachrichtendiensten und Polizei durch das NCAZ ad absurdum geführt werde – immerhin arbeiten ihm das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPol), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) sowie die Bundeswehr zu. Vernichtend äußert sich der Bundesrechnungshof in einem nicht öffentlichen Bericht, aus dem die Süddeutsche am 07.06.2014 zitierte: Danach sei das NCAZ „*nicht geeignet, die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyberraum zu bündeln.*" Der Nutzen der Einrichtung sei fraglich. Der Bundesrechnungshof rät, das „*Abwehrzentrum (...) mit eigenen Aufgaben und Kompetenzen für die Abwehr von Cyberangriffen*" auszustatten.

Allein das BMI sieht das NCAZ als Erfolgsgeschichte: Bis März 2013 habe es 900 nationale und internationale IT-Sicherheitsvorfälle bewertet. Sensationelle 1,2 Vorfälle pro Tag.

Ende der WLAN-Störerhaftung

Endlich hat der Bundesgerichtshof die Urteilsbegründung zu seinem am 08.01.2014 verkündeten Urteil zur Störerhaftung des Anschlussinhabers bei Urheberrechtsverletzungen veröffentlicht. Das Urteil schließt an die Entscheidung „Sommer unseres Lebens" an, in dem die Haftung bejaht worden war (SSN 06/2010). Im aktuellen Fall verwies der Beklagte auf die WLAN-Mitnutzung volljähriger Familienangehöriger, und der BGH verlangte lediglich eine überzeugende Darlegung, dass es weitere (familienangehörige) WLAN-Nutzer gäbe. Auch bei einer unzureichenden Sicherung könne eine Vermutung der Täterschaft des Anschlussinhabers nicht greifen. Schließlich ergebe sich selbst eine Überwachunspflicht von Minderjährigen (SSN 11/2012) erst bei Anzeichen für eine missbräuchliche Nutzung.

In einem ähnlichen Fall wies das AG Hamburg am 10.06.2014 die Haftung des Betreibers eines

Ferienhotels zurück, der seinen Mietern ein WLAN zur Nutzung anbot: Es erkannte ihn als Dienste-anbieter an, womit der Haftungsausschluss des § 8 TMG greift. Nach dieser Rechtsprechung sinkt das Risiko von Abmahnungskosten für Anschluss-inhaber, die Mieter oder Familienangehörige als Mitnutzer zulassen.

E2E-Verschlüsselung in Chrome

Am 03.06.2014 hat Google die Alpha-Version von „End-to-End“ angekündigt, eines Verschlüsselungs-tools für den Chrome-Browser. Überraschender-weise soll es nicht den S/MIME-Standard, sondern OpenPGP unterstützen und damit einen mit PGP und GnuPG kompatiblen, verschlüsselten E-Mail-Austausch ermöglichen.

Die Implementierung erfolgte in JavaScript. Es werden ausschließlich ECC-Schlüssel erzeugt; RSA-Keys können aber aus einem anderen Schlüsselring importiert werden.

Einige wichtige Fragen rund um die Implementie-rung beantwortet Google in einer FAQ. Nach der Testphase soll die End-to-End-Erweiterung im Google Web Store bereitgestellt werden. Jetzt wird es vor allem von der Bedienungsfreundlichkeit der Browser-Erweiterung abhängen, ob sich diese Lösung bei Privatnutzern durchsetzen kann.

Folgen des Suchmaschinenurteils

Als Reaktion auf das Suchmaschinenurteil des EuGH (SSN 05/2014) stellte Google ein Löschantragsfor-mular bereit, von dem bereits rege Gebrauch ge-macht wurde. Inzwischen hat Microsoft angekün-digt, mit seiner Suchmaschine Bing nachzuziehen.

Die Blockierung der Suchergebnisse erfolgt jedoch nur gegenüber europäischen Suchmaschinennut-zern; allen anderen werden die Ergebnisse weiter angezeigt. Da der EuGH in seinem Urteil Google Inc. als verantwortliche Stelle spanischem Datenschutz-recht unterworfen hat, reicht die regional begrenzte Sperrung jedoch nicht aus; sie muss für den gesamten Dienst des Betreibers erfolgen.

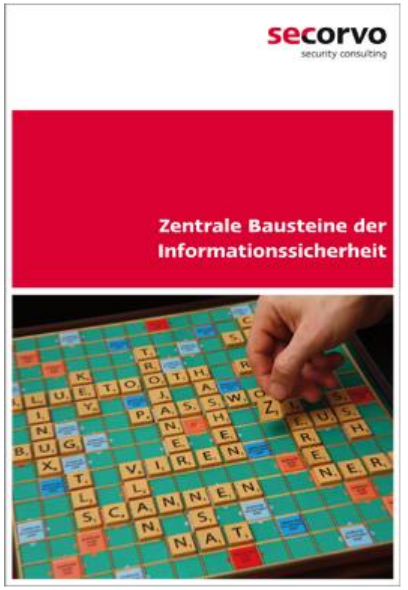
Zudem stellt die Authentifizierung der Antragsteller ein ungelöstes Problem dar. In der ersten Version des Formulars hatte Google rechtswidrig die Vorlage einer Personalausweiskopie verlangt; die aktuelle Version fordert eine Kopie eines „identifizierenden Dokuments“ – keine geeignete, Missbrauch aus-schließende Identifizierungsform. Für die Prüfung behält sich Google die Einschaltung der Aufsichts-behörden vor. Wie Anträge geprüft werden sollen, zu denen eine Begründung verlangt wird, ist derzeit noch offen.

Secorvo News

Das Buch, der T.I.S.P. und das Zertifikat

Mitte Juni haben wir die erweiterte, aktualisierte und überarbeitete Ausgabe unseres Grundlagen-buchs „Zentrale Bausteine der Informationssicher-heit“ fertiggestellt. Das auch für die Vorbereitung auf eine T.I.S.P.-Zertifizierung geeignete, 700 Seiten starke Begleitbuch ist bereits als E-Book (pdf) verfügbar; die gebundene Fassung ist noch im Druck, kann aber schon bestellt werden und wird voraussichtlich in der zweiten Julihälfte geliefert.

Die nächste Gelegenheit zur Vorbereitung auf das T.I.S.P.-Zertifikat bieten wir vom **22.–27.09.2014**., alternativ können Sie sich auf dem Seminar „IT-Sicherheit heute“ (**30.09.–02.10.2014**) auf den aktuellen Stand bringen lassen.



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

6. Tag der IT-Sicherheit

Bereits zum sechsten Mal findet am **09.07.2014** der „Tag der IT-Sicherheit“ statt, den die KA-IT-Si jährlich gemeinsam mit dem CyberForum e.V., der IHK Karlsruhe und KASTEL veranstaltet. Frau Dr. Birte Mössner, Leiterin Corporate Compliance und Daten-schutz der EnBW beleuchtet in ihrer Keynote die Relevanz des Datenschutzes im Compliance-Kon-text. Während TechniData auf das nicht immer einfache Verhältnis von IT-Managern und Sicher-heitsverantwortlichen und Secorvo auf die daten-schutzrechtlichen Fallstricke im Marketing eingeht, steht bei 1&1 die technische Sicherheit im Mittel-punkt. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

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

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)
20.-22.08.	23rd USENIX Security Symposium (Usenix, San Diego/US)
25.-25.08.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
September 2014	
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/US)
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
18.09.	Informationstag "Elektronische Signatur" 2014 (TeleTrust, Berlin)

Fundsache

Die Agentur der Europäischen Union für Grundrechte, der Europarat und die Kanzlei des Europäischen Gerichtshofs für Menschenrechte haben am 05.06.2014 ein gut strukturiertes, 220 Seiten starkes Handbuch zum Europäischen Datenschutzrecht in fünf Sprachen herausgegeben.

Impressum

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

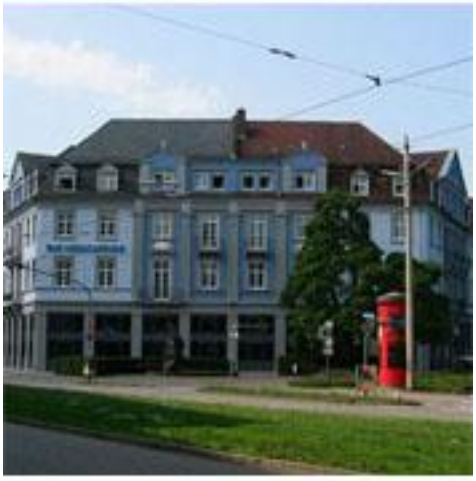
ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Michael Knopp, Christoph Schäfer

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



secorvo
security consulting

Secorvo Security News

Juli 2014

Verdeckte Profilbildung

Mit Erfolg haben sich Datenschützer gegen die Speicherung der IP-Adresse (als ein oft auf eine natürliche Person beziehbares Datum) und von Cookies gewehrt, die eine Verknüpfung von zeitlich auseinanderliegenden Nutzungsvorgängen ermöglichen. Der EU waren letztere sogar die wenig technikneutrale „Cookie-Richtlinie“ (RL 2009/136/EG) wert.

Tatsächlich aber handelt es sich dabei um ein Randthema. Denn das Kernproblem ist nicht Identifikation, sondern Profilbildung: Gelingt es einem Webseitenanbieter, Nachrichtendienst oder – schlimmer noch – Werbungs-Vermittler (wie Google oder Facebook), Seitenzugriffe zu einem eindeutigen Profil zu verdichten, so entwickelt sich daraus ein äußerst aussagekräftiger „Schattenriss“ eines, wenn auch zunächst anonymen, Benutzers.

Dieses Internet-Verhaltensprofil wird dabei mehr und mehr zum Abbild unserer Identität. Für den Anbieter kommt es dabei nur auf die Wiedererkennung an – und die gelingt ihm auch ohne Cookies und IP-Adressen, z. B. durch *Canvas Fingerprinting*. Dabei werden mittels versteckter HTML5-Kommandos Unterschiede im Zeichensatz-Rendering identifiziert, die von Grafikkarte, Treiber-Versionen und installierten Zeichensätzen abhängen. Kombiniert mit anderen Browser-Spezifika wie aktiven PlugIns oder Konfigurationseinstellungen ist heute so eine nahezu eindeutige Rechner-Wiedererkennung möglich – unbemerkt vom Nutzer und nur durch ständigen Rechnerwechsel zu verhindern.

Daher springt das jüngst gefeierte „Recht auf Vergessen“ gegenüber Suchmaschinen (SSN 5/2014) zu kurz. Denn was ist das Wissen aus Veröffentlichtem gegenüber einem vollständigen Profil unserer Internet-Nutzung? Wenn technische Mechanismen eine solche Profilbildung gegen den Willen der Betroffenen nicht verhindern, mutiert das Internet – ganz ohne NSA und BND – unweigerlich von einer Informations- zu einer verdeckten Überwachungsinfrastruktur.

Inhalt

secorvo
security consulting

Security News

Google-Projekt Zero

In der Vergangenheit haben Google-Mitarbeiter zahlreiche Sicherheitslücken in Software gefunden, die im Zusammenhang mit Google-Produkten zum Einsatz kommen. Dazu gehören die OpenSSL Heart-Bleed-Schwachstelle und Schwachstellen in der Open-Source HTML-Engine WebKit (siehe SSN 04/2014). Motiviert durch diese Erfolge kündigte Google am 15.07.2014 an, unter dem Projekt-namen Zero ein Team mit Sicherheitsexperten auf-zubauen, das sich in Vollzeit um Internetsicherheit kümmern soll. Ihr Ziel: Zero-Day-Schwachstellen finden, bevor sie von Kriminellen oder staatlichen Behörden genutzt werden, um Rechner zu infizie-ren, sensible Daten zu stehlen oder Kommunikation zu überwachen. Die Bug-Suche ist dabei nicht auf Google-Produkte beschränkt, da deren Sicherheit oft von der Sicherheit fremder Software abhängt.

Google will die gefundenen Lücken ausschließlich an die betroffenen Hersteller melden und mit ihnen gemeinsam an einem Fix arbeiten. Anschließend werden alle Lücken in einer Datenbank veröffent-licht; dazu existiert bereits eine eigene Blogseite. Eine löbliche Initiative, die der Sicherheit von Soft-ware erneut Auftrieb geben könnte.

Telefonwerbung

Telefonwerbung unterliegt spätestens seit der Ein-führung des § 7 Abs. 2 Nr. 2 UWG im Jahr 2004 erheblichen Beschränkungen. Neben dem wettbe-werbsrechtlichen Einwilligungserfordernis ist auch die Verwendung der Telefonnummer zu Werbe-zwecken ein Fallstrick. Das Verwaltungsgericht Berlin hat in einem Urteil vom 07.05.2014 die anzulegenden Maßstäbe klargestellt.

Das Gericht wies die Klage gegen eine Anordnung des Berliner Beauftragten für Datenschutz und Informationsfreiheit ab, nach der die Klägerin die Praxis ihres Call-Centers beenden sollte, im Rahmen von telefonischen Kundenzufriedenheitsbefragun-gen eine Einwilligung in Werbeanrufe zu erbitten. Das Verwaltungsgericht bestätigt, dass dabei eine Verwendung der Telefonnummer für zwei unter-schiedliche Zwecke vorliegt. Während die Frage nach der Kundenzufriedenheit nach § 28 Abs. 1 Nr. 1 BDSG zulässig sei, habe die Frage nach einem Opt-In für Werbeanrufe bereits Werbecharakter. Hierfür sei § 28 Abs. 3 BDSG eine abschließende Spezialregelung. Erforderlich sei eine Einwilligung des Betroffenen vor dem Anruf.

Das sehr klare, wenn auch noch nicht rechtskräftige Urteil stärkt die Bedeutung der sorgsamen Diffe-renzierung von Einzelzwecken in einem Verfahren und stellt klar, dass Datenschutzrecht nicht durch eine Vermengung mit einem im Vordergrund stehenden Zweck umgangen werden darf.

Mit Licht ins WLAN

Das „Internet der Dinge“ hält noch viele Über-raschungen mit Sicherheitsimplikationen bereit. Eine davon hat Alex Chapman am 04.07.2014 in seinem Blog-Post „Hacking into Internet Connected Light Bulbs“ aufgedeckt: Bei der Analyse des Zu-sammenspiels von über das Internet verbundenen Lampen stellte er fest, dass das Wi-Fi-Passwort des Netzwerks, in dem sich die Lampen befinden, bei der Kommunikation zwar mit AES verschlüsselt wird, der verwendete Schlüssel aber in der Firmware der Lampen fest verdrahtet ist. Damit öffnen die Leuchten die Tür zum heimischen WLAN. Wer über Wi-Fi verbundene Geräte nutzt, sollte stutzig werden, wenn es an einer Eingabemöglichkeit für das WLAN-Passwort mangelt…

Europas großer Wurf

Vor gut zwei Jahren, am 04.06.2012, hatte die Europäische Kommission einen Verordnungsent-wurf zu Diensten der elektronischen Identifizierung und Vertrauensdiensten für elektronische Transak-tionen im Binnenmarkt vorgestellt. Nun wurde die Verordnung am 16.07.2014 vom Europäischen Rat angenommen. Sie tritt nach Veröffentlichung im Amtsblatt in Kraft und gilt ab dem 01.07.2016; zu diesem Zeitpunkt hebt sie die Signaturrichtlinie auf.

Die Verordnung regelt als unmittelbar geltendes Recht den Rechtsrahmen für elektronische Signa-turen, Siegel, Zeitstempel, Dokumente, Zustel-lungs- und Zertifizierungsdienste für die Webseiten-authentifizierung. Außerdem legt sie die Voraussetzungen für die Anerkennung von elektro-nischen Identifizierungssystemen fest und enthält Vorschriften für die Anbieter der genannten Dienste. Ohne Berücksichtigung geltender nationaler Regelungen legt die Verordnung Beweisregeln fest.

Dabei verweist fast jeder Artikel der Verordnung auf von der Kommission noch zu erlassende Rechtsakte zu technischen Spezifikationen, Verfahren, Maßnah-men, Meldeinhalten und intereuropäischen Abstim-mungen, ohne dass es hierfür klare Vorgaben gäbe. Für Deutschland wird nun die Anpassung einer Reihe von Gesetzen anstehen: Signaturgesetz, De-Mail-Gesetz, Personalausweisgesetz, Verwaltungs-verfahrensgesetze und viele weitere Regelungen sind von der Verordnung betroffen. Zu den Vertrau-ensdiensten gehören auch die in Deutschland bislang aus systematischen Gründen ausgeschlos-senen Fremdsignaturen, bei denen die Signaturer-

stellungseinheit Dritten überlassen wird. Umgekehrt entfällt die deutsche Sonderform der qualifizierten Signatur mit Anbieterakkreditierung.

Damit stehen dem elektronischen Rechtsverkehr nicht nur in Deutschland erhebliche Veränderungen bevor – ohne erkennbare Vertrauenssteigerung. Wie dabei die unvermeidliche Rechtsunsicherheit und die in einigen Bereichen erheblichen Umstellungskosten zu einer größeren Akzeptanz elektronischer Signatur- oder Identifikationstechniken führen sollen, bleibt das große Geheimnis des Verordnungsgebers. Offenbar wähnt sich dieses Paralleluniversum frei von der Geltung profaner Marktmechanismen.

Einfallstor Virenschutz

Virenschutz-Software soll vor Viren schützen – und schafft dabei neue Angriffsflächen, denn sie besitzt höchste Berechtigungen, die sie für Angreifer besonders interessant macht. Außerdem öffnet sie jede Schadsoftware – besitzt sie Schwachstellen, lassen diese sich daher besonders leicht ausnutzen.

Und tatsächlich ist es mit der Sicherheit von Anti-Viren-Software bei weitem nicht so gut bestellt, wie man erwarten könnte: Am 23.07.2014 veröffentlichte Joxean Koret die Ergebnisse seiner Analyse von 17 AV-Lösungen, die er eine Woche zuvor auf der SyScan360 in Singapur vorgestellt hatte. Seine Erkenntnisse machen sprachlos: die meisten Produkte laden Updates via HTTP, in 14 fand er klassische Schwachstellen wie *Heap Overflows*, *Remote Command Injection* und Fehler in Entpacker-Routinen – Ansätze wie ASVS sind den Herstellern offenbar unbekannt. Angesichts dieser Schwachstellen gehört der zentrale Virenscanner im Netz auf ein isoliertes System.

Passwords are dead – again...

Online-Passwortdienste füllen Passwortfelder aus, arbeiten plattformübergreifend, verwalten Passwörter von Millionen Nutzern – und stellen daher attraktive Angriffsziele dar. Im August werden Forscher der Universität Berkeley auf dem 23. Usenix Security Symposium eine Untersuchung zur Sicherheit von Online-Passwortmanagern vorstellen, die Schwachstellen in der Implementierung aller fünf untersuchten Produkte aufdeckte. So war das automatische Einloggen auf Webseiten via Bookmarklets angreifbar, drei Lösungen hatten XSS- oder CSRF-Schwachstellen, zwei prüften die Autorisierung beim *credential sharing* nicht, zwei waren über die Benutzeroberfläche angreifbar. Seit August 2013 sind die Hersteller informiert; LastPass und RoboForm haben die beanstandeten Schwachstellen nach eigenen Angaben inzwischen beseitigt.

Grundsätzlich sind Passwörter aber auch im Kopf nicht sicher und verursachen Kosten durch Passwort-Rücksetzungen und -Wechsel. Die Alternative sind lokal speichernde Passwortmanager – bei denen man sich allerdings selbst um die Verfügbarkeit kümmern muss.

Secorvo News

Know-How-Update

Der ständigen Weiterentwicklung des Themas IT-Sicherheit versuchen wir mit unserem Seminar „IT-Sicherheit heute“ Rechnung zu tragen: Das Programm unterziehen wir einer ständigen Aktualisierung und Überarbeitung. Besonders zu empfehlen als Auffrischung Ihres Basiswissens – die nächste Möglichkeit zur Teilnahme bieten wir vom **30.09.–02.10.2014** (anrechenbar mit 21 CPEs).

Wie sich sichere Softwareentwicklung in die Entwicklungsprozesse integrieren lässt, vermittelt unser Zertifikatslehrgang Certified Professional for Secure Software Engineering (CPSSE) vom **20.–24.10.2014**. Für Ihre T.I.S.P.-Zertifizierung bieten wir in diesem Jahr noch zwei Termine: vom **22.–26.09.2014** und vom **10.–14.11.2014** jeweils mit anschließender Prüfung – und der aktualisierten und überarbeiteten Neuauflage des T.I.S.P.-Buchs. Alle Termine und Seminarangebote dazu sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

3. Staffel der Anti-Prism-Party

Zwei Auflagen der größten Cryptoparty Europas mit 650 bzw. 900 Teilnehmern gab es bereits. Doch aller guten Dinge sind drei – daher veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) anlässlich der Uraufführung des Edward-Snowden-Stücks „Ich bereue nichts“ am Badischen Staatstheater am **Samstag, 11.10.2014** eine dritte Staffel der Anti-Prism-Party. Dort erfahren Sie alles, was Sie schon immer über Verschlüsselung wissen wollten, aber bisher nicht zu fragen wagten.

Auf Bühnen und an Stationen in den Foyers des Staatstheaters zeigen Karlsruher IT-Sicherheits- und Datenschutzexperten in Live-Vorführungen, wie man Tracking verhindert, seine Passwörter wählt und geschützt aufbewahrt, E-Mails vor fremdem Zugriff schützt, Chats verschlüsselt und wie File-Sharing in der Cloud sicher wird. Derweil können sich Ihre Kinder zum Verschlüsselungsexperten ausbilden lassen. Krönender Abschluss ist ein **Anti-Prism-Plenum** im Kleinen Haus.

Aktuelle Informationen zum Programm der Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter.

Veranstaltungshinweise

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

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 22 (DEFCON, Las Vegas/US)
17.-21.08.	Crypto 2014 (IACR, Santa Barbara/US)
20.- 22.08.	23rd USENIX Security Symposium (Usenix, San Diego/US)
25.- 25.08.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
September 2014	
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/Colorado)
22.-27.09.	T.I.S.P.-Schulung und Prüfung (Secorvo, Karlsruhe)
30.09.	Anwendertag IT-Forensik (Fraunhofer, Darmstadt)
30.09.-02.10.	IT-Sicherheit heute (Secorvo, Karlsruhe)

Fundsache

Am 30.06.2014 veröffentlichte die KPMG eine Studie zu den Auswirkungen des von der Bundesregierung geplanten IT-Sicherheitsgesetzes. Danach werden im Bereich der kritischen Infrastrukturen knapp 18.500 (Groß-)Unternehmen von den Meldepflichten erfasst, deren Bürokratiekosten sich auf 1,1 Mrd. € summieren werden – ein teures Vergnügen.

Impressum

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

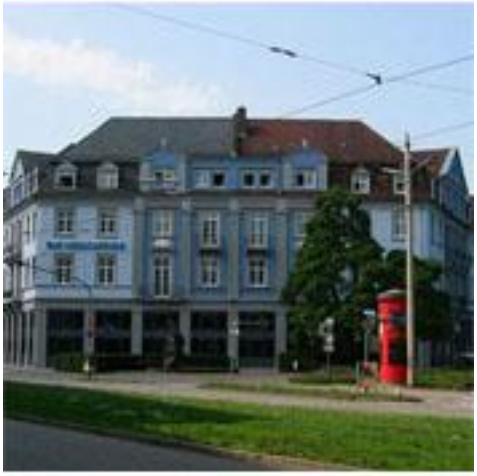
ISSN 1613-4311

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

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



secorvo
security consulting

Secorvo Security News

August 2014

Semantische Authentizität

Eines der elementaren Schutzziele der Informationssicherheit ist die Authentizität. Sie bezeichnet die Echtheit und Vertrauenswürdigkeit einer Information. In der Fachliteratur wird Authentizität praktisch ausschließlich im Zusammenhang mit der technisch überprüfbaren Urheberschaft einer elektronischen Nachricht oder eines Datensatzes verwendet: Mit Schutzmechanismen wie digitalen Signaturen oder anderen, unter realistischen Annahmen praktisch unfälschbaren Authentikatoren stellt man sicher, dass ein Datum eindeutig einem technischen System oder menschlichen Urheber zugeordnet werden kann. Ein vernünftiger Ansatz in der Welt der IT-Sicherheit.

In der Welt der Informationssicherheit hingegen springt ein solches Verständnis zu kurz. Denn Echtheit und Vertrauenswürdigkeit einer *Information* sind mehr als die eines *Datums* – erstere erfordert nämlich nicht nur *syntaktische*, sondern auch *semantische* Authentizität. Zwar ist der Unterschied bei vielen technischen Vorgängen vernachlässigbar: Wer eine Transaktion elektronisch signiert, möchte damit die Echtheit seiner Willenserklärung bestätigen.

Wie steht es aber mit veröffentlichten Informationen? Am 26.02.2014 demonstrierte Bryan Seely, wie sich Angaben in Google Maps fälschen lassen – mit womöglich dramatischen Folgen z. B. für ein betroffenes Unternehmen (falsche Telefonnummer oder E-Mail-Adresse, Hinweis „Seit 01.01.2014 insolvent“ o. ä.). Hier würde ein Berechtigungskonzept mit strikter Identitätsprüfung helfen. Bei Wikipedia ist das schon schwieriger: Tendenziöse Beiträge, verdeckte Werbung oder vorsätzliche Falschaussagen lassen sich weder durch Peer Review noch durch Identitätsprüfungen ausschließen. Und wie kann man die Verbreitung von Fälschungen wie das Youtube-Video eines Adler-Angriffs auf ein Kleinkind wirksam verhindern?

Lösen wir dieses Authentizitätsproblem nicht, werden wir uns womöglich bald in einer Welt wiederfinden, in der sich Wahrheit und Lüge nicht mehr auseinanderhalten lassen.

Inhalt

secorvo
security consulting

Security News

Rechtsrisiko Spam-Filter

Das LG Bonn hat mit einem Ende Juni veröffentlichten Urteil vom 10.01.2014 bestätigt, dass auch eine im Spam-Ordner gelandete E-Mail zugegangen ist – und einen Rechtsanwalt, dem so eine E-Mail mit einem Vergleichsangebot einer gegnerischen Partei entgangen war, zu 90.000 € Schadensersatz verurteilt. Erste Reaktionen auf das Urteil stellten das Konzept der Spam-Filter in Frage. Allerdings räumte der Beklagte in dem abgeurteilten Fall den Empfang der E-Mail ein; der rechtssichere Nachweis eines bestrittenen Zugangs einer E-Mail dürfte hingegen selbst mittels der Serverprotokolle des Absenders schwierig sein. Ein Anscheinsbeweis verbietet sich im Umkehrschluss zu § 5 Abs. 8 De-Mail-G und § 371a Abs. 2 ZPO.

Zweifellos besteht eine Rechtspflicht zur Prüfung von zugegangenen E-Mails; darin enthaltene Willenserklärungen sind wirksam (§ 130 Abs. 1 BGB), ob vom Empfänger wahrgenommen oder nicht. Wird eine E-Mail hingegen wie beim Greylisting vom Server temporär abgewiesen, erreicht sie die Sphäre des Empfängers nicht und gilt daher nicht als zugegangen. Abweisungen aufgrund einer Blacklist könnten allerdings als Nachrichtenunterdrückung gewertet werden – Spam-Filterung bleibt daher ein vermintes Gelände.

Die Yetis kommen

Am 31.07.2014 veröffentlichten die Kaspersky Labs Hintergründe über Crouching Yeti – eine Angriffswelle, der bisher 3.000 Unternehmen zum Opfer gefallen sind, darunter viele Maschinenbauer. Das Vorgehensmuster: Die IT des Ziel-Unternehmens wird über einen von drei Wegen infiziert: über maliziöse XDP-Dokumente, die mit individualisierten E-Mails, so genanntem Spear-phishing versandt werden, über präparierte SCADA-Softwarepakete, die statt der Originale auf Anbieterseiten platziert werden, oder über eine watering hole-Attacke, bei der gezielt branchentypische Webseiten gehackt werden – ein Besuch dieser Seiten infiziert dann das Zielunternehmen. Die Steuerung der Angriffe und der Abgriff von Daten erfolgen über gehackte Webserver.

Lehrreich sind die Details: So werden ausschließlich bekannte Exploits z. B. aus dem Metasploit-Umfeld genutzt; dagegen schützt ein aktueller Virenschutz. Den Austausch von Update-Paketen auf Hersteller-Webseiten kann eine Prüfung der Pakete nach dem Download aufdecken. Und im Netz des Opferunternehmens sucht die Malware gezielt nach SCADA-Systemen; deren Abschottung würde verhindern, dass sie gefunden und infiziert werden. Da die Yeti-Angriffe andauern, ist eine schnelle Maßnahmenumsetzung angeraten.

Klare Fristen

Am 03.07.2014 hat der BGH in seinem zweiten Revisionsurteil zur Speicherung von Verkehrsdaten durch die Deutsche Telekom bestätigt, dass eine Speicherfrist von sieben Tagen zum Zweck der Erkennung, Eingrenzung oder Beseitigung von Störungen (§ 100 Abs. 1 TKG) ausreicht. Damit wird die im Urteil des OLG Frankfurt vom 28.08.2013 festgelegte Frist bestätigt, die fehlende Wochenenddienste und die Bearbeitungsdauer bestimmter Meldungen berücksichtigt.

Die Festlegung von Löschfristen für Log-Daten ist ein ständiges Thema der Datenschutzpraxis. Zwar begründet der BGH die Frist einerseits mit den spezifischen Verhältnissen der Telekom; das Urteil selbst geht aber von deren Vergleichbarkeit aus. Die Sieben-Tage-Frist sollte daher für jegliche Form der Protokollierung zur Abwehr von Störungen und Angriffen als Obergrenze gewählt werden.

USB – eine ignorierte Gefahr

Am 07.08.2014 sorgten Carsten Nohl und Jacob Lell auf der BlackHat in Las Vegas mit ihrem Vortrag BadUSB für Aufsehen: Sie stellten vor, wie sich verbreitete USB-Controller umprogrammieren und in Angriffswerkzeuge verwandeln lassen. Zwar ist mindestens seit 2005 bekannt, dass USB-Geräte für Angriffe missbraucht werden können. Neu ist allerdings, dass ein Angreifer ohne spezielle Hardware handelsübliche USB-Sticks umprogrammieren kann. Zwar ist das Feature seit 1999 in der USB-Spezifikation als Device Firmware Upgrade vorgesehen – ein Einfallstor, über das schon die nPA-App stolperte (SSN 11/2010). Dass dieselbe Gefahr bei USB-Sticks lauert, wurde offenbar erst jetzt wahrgenommen.

Bis alle USB-Hersteller erklärt haben, ob ihre Geräte von BadUSB betroffen sind, sollten Sie daher bei der Nutzung fremder oder der Weitergabe eigener USB-Hardware zurückhaltend sein. Virenschutz oder Device Control helfen gegen diesen Angriff nicht, da das betroffene Device sich dem kontrollierenden Rechner gegenüber beliebig „maskieren“ kann.

Kein privates Auskunftsrecht

Der Bundesgerichtshof erteilte am 01.07.2014 dem Anspruch von Privatpersonen auf Auskunft über die Nutzeridentität bei einer Verletzung von Persönlichkeitsrechten eine klare Absage. In dem entschiedenen Fall wollte ein Arzt gegen Nutzer eines Bewertungsportals vorgehen und verlangte von dem Portalbetreiber Auskunft über deren Identität.

Das Zivilrecht kennt für solche Fälle einen Auskunftsanspruch aus § 242 BGB nach Treu und Glauben. In der Anfang August veröffentlichten Urteilsbegründung stellt der BGH jedoch klar, dass nach § 14 Abs. 1 Telemediengesetz Bestandsdaten von Nutzern nur für Zwecke des Anbieter-Nutzer-Verhältnisses verwendet werden dürfen. Eine anderweitige Erlaubnis muss auf das Telemediengesetz Bezug nehmen (§ 12 Abs. 2 TMG); das ist bei § 242 BGB nicht der Fall. Mangels datenschutzrechtlicher Erlaubnis darf der Portalbetreiber daher keine Auskunft geben.

So hat der BGH mit seinem Urteil zum Schutz von Pseudonymen im Internet beigetragen. Allerdings ist nach § 14 Abs. 2 TMG Ermittlungsbehörden Auskunft zu erteilen, so dass die Nutzeridentität per Strafanzeige aufgedeckt werden kann. Daher könnte nun das Strafrecht zum Vehikel zivilrechtlicher Auseinandersetzungen werden.

Datenschutzfolgenabschätzung

Fast neun Jahre hat die Entwicklung und Verabschiedung einer RFID-Strategie durch die EU-Kommission gedauert: vom Arbeitspapier zum Einsatz von RFID der Artikel-29-Gruppe (Arbeitsgruppe der europäischen Datenschutz-Aufsichtsbehörden) vom 28.09.2005 über die erste Konsultation der EU-Kommission und die öffentliche Konsultation vom 03.07.2006, deren Ergebnisse am 16.10.2006 publiziert wurden, bis zum Vorschlag einer RFID-Strategie vom 15.03.2007, deren Empfehlungen am 12.05.2009 angenommen wurden. Das Rahmenwerk für die dabei eingeführte Datenschutzfolgenabschätzung (PIA) wurde am 12.01.2011 vorgestellt und kurz darauf von der Artikel-29-Gruppe bestätigt.

Seit Juli 2014 gelten nun EU-weit technische Normen zur Nutzung von RFID (EN 16570:2014) und zur Datenschutzfolgenabschätzung (EN 16571:2014), konkretisiert in mehreren Technischen Richtlinien (CEN/TR 16670:2014, 16672:2014-16674:2014).

Damit werden eine einheitliche Informations- und Kennzeichnungspflicht durch ein neues RFID-Zeichen eingeführt und ein verlässlicher Rechtsrahmen geschaffen. Ein Schritt in die richtige Richtung: Mit der Einführung der Datenschutzfolgenabschätzung, die auch in der geplanten EU-Datenschutz-Grundverordnung vorgesehen ist, sollen die Standards für klare Vorgaben und mehr Transparenz sorgen.

Secorvo News

Zertifikate sind Trumpf

Wenn Sie zu den Kurzentschlossenen zählen, können Sie sich noch einen der letzten freien Plätze des Seminars „IT-Sicherheit heute“ (**30.09.-02.10.2014**, 21 CPEs) sichern. Oder im Oktober und November 2014 Ihre Erfahrungen und Kenntnisse auffrischen und mit einem Zertifikat krönen:

Wie integriert man sichere Softwareentwicklung in die Entwicklungsprozesse? Das ist Thema des Zertifikatslehrgangs „ISSECO Certified Professional for Secure Software Engineering (CPSSE)“ vom **20. bis 24.10.2014**. Wie es gelingt, die Sicherheit eines Gesamtsystems zu konzipieren, und wie sich dies in der Praxis umsetzen lässt, erfahren Sie im Zertifikatsseminar „Security Engineering – Sichere Systeme durch Security by Design (T.E.S.S.)“ vom **17. bis 22.11.2014**. Und vom **10. bis 14.11.2014** können Sie Ihr Know-How und Ihre mehrjährige Erfahrung im Bereich Informationssicherheit mit der Zertifizierung zum „TeleTrusT Information Security Professional (T.I.S.P.)“ abrunden.

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

Gretchenfrage

Selber machen oder machen lassen? Cloud-Dienst oder eigenes Rechenzentrum? Wir haben zwei Anbieter gebeten, ihre Argumente mit uns auf der kommenden Veranstaltung der KA-IT-Si am **18.09.2014** (18 Uhr im Schalander, Karlsruhe) zu diskutieren: Herrn Kühne von Rittal, einem Unternehmen mit jahrzehntelanger Erfahrung im Bau von Rechenzentren und RZ-Modulen, und Herrn Kess von befine Solutions, dem jungen Anbieter der sicheren Kommunikationslösung Cryptshare. Wir freuen uns auf eine spannende Diskussion mit Ihnen!

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Lassen Sie den Abend im gemütlichen Biergarten des Schalander der Hoepfner-Burg ausklingen. Anmeldung unter www.ka-it-si.de.

„Das Buch“ auf der it-sa

Das Erscheinen der zweiten, gründlich überarbeiteten und erweiterten Auflage des T.I.S.P.-Buchs nehmen wir zum Anlass, Sie herzlich auf unseren „T.I.S.P.-Buch-Stand“ auf der it-sa am 07.-09.10.2014 einzuladen. Sie finden uns in Halle 12 (Stand 12.0-646). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail an security-news@secorvo.de.

Veranstaltungshinweise

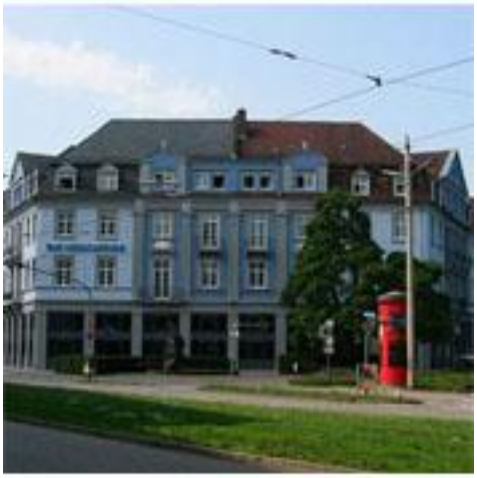
Auszug aus http://www.veranstaltungen-it-sicherheit.de

September 2014	
16.-17.09.	D • A • CH Security (GI, OCG, BITKOM, SI, TeleTrusT, Graz/AT)
16.-19.09.	OWASP AppSec USA 2014 (OWASP Foundation, Denver/Colorado)
18.09.	Informationstag "Elektronische Signatur" 2014 (TeleTrust, Berlin)
18.09.	Gretchenfrage (KA-IT-Si, Karlsruhe)
30.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
30.09.-02.10.	IT-Sicherheit heute (Secorvo, Karlsruhe)
Oktober 2014	
07.-09.10.	it-sa 2014 (NürnbergMesse GmbH, Nürnberg)
11.10.	Anti-Prism-Party 3. Staffel (KA-IT-Si, Karlsruhe)

Fundsache

Für verregnete letzte Urlaubstage ein paar Literaturtipps aus der SSN-Redaktion:

- Dave Eggers: Der Circle
- Marc Elsberg: Blackout – Morgen ist es zu spät, Zero – Sie wissen, was du tust
- Mark E. Russinovich: Zero Day, Trojan Horse, Rogue Code
- Neal Stephenson: Snow Crash, Cryptonomicon
- Daniel Suarez: Daemon: Die Welt ist nur ein Spiel, Darknet



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer

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

secorvo
security consulting

Secorvo Security News

September 2014

Nichts gelernt?

Diskussionen zur Inneren Sicherheit sind vermintes Gelände. Dort treffen – meist kraftvoll – Terroristenjäger auf Liberale und Datenschützer auf Nichts-zu-verbergen-Haber. Allem verbalen Hauen und Stechen zum Trotz ist aber in einem Punkt zumindest die heimliche Einigkeit groß: Auch wer „nichts zu verbergen" hat, mag sich nicht wie ein Staatsfeind behandeln lassen. Die eigenen E-Mails, SMS und Fotosammlungen möchte man als unbescholtener Bürger dann doch nur mit Personen des Vertrauens teilen – und nicht anlasslos mit unbekannten Staatsdienern.

So ist unstreitig, dass Kommunikationsdaten verschlüsselt gehören. Eigentlich keine große Sache – hätte man die Protokolle TCP/IP und DNS im Jahr 1981 gleich als das konzipiert, was sie heute sind: eine systemkritische Infrastruktur moderner Gesellschaften. Dann wären Verschlüsselungsmechanismen ein integraler Bestandteil des Internet und müssten nicht nachträglich aufgesetzt werden.

„Hätte, hätte, Fahradkette", würde Peer Steinbrück wahrscheinlich kommentieren. Denn einen wenigstens elementaren Schutz bei der Nutzung von Internet-Diensten hat nur, wer sich kümmert – zum Beispiel durch die Aktivierung von TLS beim Zugriff auf E-Mail-Konten oder die Verwendung von Chat-Programmen mit starker Verschlüsselung. Das ist, selbst für einen IT-Laien, so schwierig nicht. Angesichts des drastischen Vertrauenseinbruchs nach den Veröffentlichungen von Edward Snowden wäre eine spürbare Verhaltensänderung zu erwarten gewesen. Tatsächlich aber scheint die Wirkung schon wieder zu verblassen: das Vertrauen ins Internet wächst wieder, ohne dass sich substantiell viel geändert hat.

Mit unserer dritten „Anti-Prism-Party" wollen wir am 11.10.2014 erneut ein Zeichen gegen das „Weiter so" setzen, und hoffen, viele Tausend Besucher für eine sicherheitsbewusstere Nutzung des Internet zu gewinnen. Wer nicht kommen kann, dem sei unsere „Download"-Seite ans Herz gelegt.

Inhalt

secorvo
security consulting

Security News

Ende der Kulanz

Durch Online-Banking-Angriffe verursachte Schäden wurden bisher meist von den betroffenen Banken übernommen oder in außergerichtlichen Vergleichen geregelt. Auf die Zunahme von Phishing- und Trojanerangriffen haben die Institute in den vergangenen Jahren mit der Einführung neuer Schutzmechanismen wie SMS-TANs und TAN-Generatoren reagiert – und verweigern inzwischen gelegentlich die Schadensübernahme. Nun hat das LG Darmstadt in einem aktuellen Fall die Schadensersatz-Verweigerung mit Urteil vom 28.08.2014 bestätigt.

Da das von der beklagten Bank zur Verfügung gestellte Verfahren „Sm@rt-TAN-plus" eine Autorisierung der Überweisung mit Kennwort und EC-Karte fordere und die Überweisungsdaten auf dem TAN-Generator angezeigt würden, sei die Prüfung der Daten vor der Bestätigung der Transaktion (durch Eingabe der TAN) die Aufgabe des Kunden. Dieser müsse sich den durch die Verwendung der TAN entstandenen Rechtsschein zurechnen lassen, da die durch den Angreifer manipulierte Überweisung anhand der angezeigten Kontonummer und des Betrags für ihn erkennbar gewesen sei.

Es ist zu erwarten, dass Banken und Gerichte zukünftig die Verantwortung des Kunden bei Verwendung eines sicheren Online-Banking-Verfahrens höher ansetzen werden. Bei Schäden, die erst durch den leichtfertigen Umgang mit den Schutzmechanismen ermöglicht wurden, werden Verbraucher sich in Zukunft nicht mehr auf Kulanz und richterliches Wohlwollen verlassen können.

Meine grüne Welle

Auf der WOOT'14 (*8th USENIX-Workshop on Offensive Technologies*) stellten Forscher der Universität Michigan im August vor, wie verwundbar typische US-Verkehrsleitsysteme sind. Die untersuchten Ampeln kommunizieren über unverschlüsselte W-LAN-Kanäle, Voreinstellungen für Nutzername und Passwort wurden beibehalten, Kommandos des NTCIP-1202-Protokolls zur Verkehrssteuerung ließen sich per UDP an Ampelsteuerungen senden. Damit werden persönliche grüne Wellen und Verkehrsstaus auf Knopfdruck Wirklichkeit.

Eine ähnliche Verwundbarkeit der auch in Europa eingesetzten Verkehrsleittechnik von Sensys Networks zeigte Cesar Cerrudo, ebenfalls im August, auf der diesjährigen DEFCON. Das System erlaubt Code-Downloads ohne Integritätsprüfung und arbeitet ohne Verschlüsselung oder Authentisierung. Inzwischen liegen Software-Updates gegen die veröffentlichten Schwachstellen vor.

Da ausfallende Ampelsteuerungen ein Verkehrschaos auslösen können, werden Verkehrsleitsysteme in Deutschland zu Recht als kritische Infrastruktur angesehen. Dennoch ist auch hierzulande nach wie vor veraltete Technik im Einsatz. Auch hier ist Sicherheit ein Prozess, kein Zustand: Deshalb gehören regelmäßige Audits der Systeme, das Einspielen von Updates und Gespräche mit den Herstellern zu den regelmäßigen Aufgaben eines Sicherheitsmanagements.

Deutsche Post startet SIMSme

Am 13.08.2014 veröffentlichte die Deutsche Post AG ihren kostenfreien Messenger SIMSme. Nach anfänglichen technischen Schwierigkeiten läuft der Dienst inzwischen problemlos: Nutzer können Bilder, Nachrichten, Videos und andere Inhalte verschicken. Den Versand von Nachrichten, die sich wie bei Snapchat nach einer vorgegebenen Zeit selbstständig löschen, erlaubt ein 89-Cent-Upgrade.

Wie bei der oft empfohlenen schweizerischen WhatsApp-Alternative Threema werden die Daten Ende-zu-Ende-verschlüsselt, und das ausschließlich auf deutschen Servern. Der private Schlüssel kann bei einem persönlichen Treffen per QR-Code verifiziert werden. Eine anonyme Nutzung ist nicht möglich – zur Aktivierung benötigt man eine Telefonnummer. Ein Datenschutz-Patzer ist, dass der Sender mitgeteilt bekommt, wenn der Empfänger die Nachricht gelesen hat. Hier sollte die Post nachbessern und eine Deaktivierung dieser Funktion ermöglichen. Positiv sind hingegen die Nutzungsbedingungen hervorzuheben, die kompakt und übersichtlich gehalten sind. Im Gegensatz zu vielen insbesondere amerikanischen Anbietern verzichtet die Post darauf, sich Rechte an den Inhalten der Nutzer zu sichern.

Ein wenig Nacharbeit bei der handwerklichen Implementierungsqualität des aktuellen App-Releases sei der Deutschen Post allerdings angeraten: Vertrauen kann auch an Kleinigkeiten scheitern – zumindest bei Nerds.

OWASP Guides – reloaded

In diesem Sommer wurden zwei wichtige Arbeiten des OWASP zum Test von Anwendungen grundlegend überarbeitet. Am 11.08.2014 veröffentlichte OWASP Version 2.0 des Application Security Verification Standards (ASVS). Der ASVS dient zur Überprüfung der Umsetzung elementarer Sicherheitsmaßnahmen in Anwendungen und ist ein wichtiger Baustein sicherer Software. In die Überarbeitung sind zahlreiche Anmerkungen aus der Praxis einge-

flossen; die Lektüre lohnt sowohl für Anwendungsentwickler als auch für Tester. An Letztere wendet sich Version 4.0 des OWASP Testing Guide, der am 17.09.2014 publiziert wurde. Er enthält Praxistipps für die Durchführung von Sicherheitsüberprüfungen von Anwendungen.

Löschkriterien

Seit der Europäische Gerichtshof (EuGH) Mitte Mai die Suchmaschinenbetreiber als verantwortliche Stellen bestätigt (SSN 05/2014) und Betroffenen das Recht zugesprochen hatte, unter bestimmten Umständen die Löschung von Suchergebnissen zu verlangen, sind allein bei Google binnen vier Monaten 120.000 Anträge eingegangen. Da die Suchmaschinenbetreiber nicht allen Löschbegehren nachgekommen sind, sind zahlreiche Beschwerden bei den europäischen Datenschutzaufsichtsbehörden eingegangen.

Die Art. 29 Gruppe, das gemeinsame Gremium der europäischen Datenschutzaufsichtsbehörden, hat sich am 18.09.2014 nun auf erste Maßnahmen geeinigt. So wollen die Aufsichtsbehörden eine Übersicht über die von ihnen getroffenen Entscheidungen gewinnen und ähnliche, sowie besondere Fallkonstellationen identifizieren. Ziel ist die Entwicklung gemeinsamer Entscheidungskriterien. Auch wenn das kein einfacher Prozess werden dürfte, ist das allemal besser, als die Entscheidung den Suchmaschinenanbietern zu überlassen.

CrypTool 2.0

Das mehrfach preisgekrönte Krypto-Lernprogramm CrypTool erschien am 20.08.2014 in einer von rund 60 Open-Source-Entwicklern in siebenjähriger Entwicklungszeit rundumerneuerter Version 2.0. Die in Deutsch und Englisch verfügbare neue Version wird der Initiator und Gesamtprojektkoordinator, Herr Professor Esslinger, am 11.10.2014 auf der Karlsruher Anti-Prism-Party vorstellen (s. u.).

Secorvo News

Sichere Systeme sind möglich

Die Formulierung und Ausgestaltung angemessener Sicherheitsanforderungen an komplexe Systeme ist nicht trivial – aber möglich. Die Zertifikatsschulung Sichere Systeme dank System Security Engineering (T.E.S.S.) zeigt, wie Sicherheit erfolgreich in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie lernen aktuelle Standards, Vorgehensmodelle und Best Practices kennen und anwenden (17.-20.11.2014). Im Anschluss an die Schulung können Sie an der T.E.S.S. Prüfung teilnehmen, um Ihre erworbenen Kenntnisse mit dem T.E.S.S. Zertifikat bestätigen zu lassen. Speziell für die Entwicklung sicherer Software bieten wir die Zertifikatsschulung ISSECO Certified Professional for Secure Software Engineering (CPSSE) (20.-23.10.2014) an. Auf beiden Seminaren gibt es noch wenige freie Plätze.

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

Anti-Prism-Party, zum Dritten

Die „dritte Staffel“ der Anti-Prism-Party am **11.10.2014** findet anlässlich des Edward-Snowden-Stücks „Ich bereue nichts“ im Foyer des Badischen Staatstheaters Karlsruhe statt (ab 14 Uhr). Neben aktuellen Tipps und Empfehlungen rund um das Thema Selbstschutz im Internet wird das Kryptologikum des Karlsruher Instituts für Technologie (KIT) historische und zeitgenössische Verschlüsselungstechnik zum „Be-Greifen“ vorstellen. Ihre Kinder können Sie derweil in der Spion-Schule, die von der Pädagogischen Hochschule Karlsruhe betreut wird, zum Verschlüsselungsexperten ausbilden lassen oder zur Präsentation der KIT-Kinderuni schicken, die um 15 und 16:30 Uhr stattfindet. Krönender Abschluss ist ein Anti-Prism-Plenum um **19:30 Uhr** im Kleinen Haus des Staatstheaters Karlsruhe (Eintritt frei). Mehr zum Programm im APP-Newsletter.

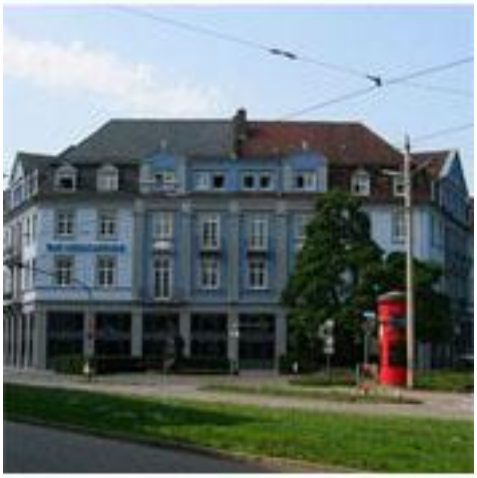
„Das Buch“ auf der it-sa

Anlässlich des Erscheinens der zweiten, aktualisierten und erweiterten Ausgabe des T.I.S.P.-Buchs laden wir Sie am **07.-09.10.2014** herzlich zum Besuch unseres „T.I.S.P.-Buch-Stands“ auf der it-sa in Nürnberg ein. Sie finden uns in Halle 12 (Stand 12.0-646). Gerne lassen wir Ihnen einen Registrierungscode zukommen, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können. Schicken Sie uns bei Interesse bitte eine kurze E-Mail an security-news@secorvo.de.

Veranstaltungshinweise

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

Oktober 2014	
07.-09.10.	it-sa 2014 (NürnbergMesse, Nürnberg)
07.-09.10.	14. IDACON 2014 (WEKA-Akademie, Würzburg)
11.10.	Anti-Prism-Party, 3. Staffel (KA-IT-Si, Karlsruhe)
14.-17.10.	Blackhat Europe 2014 (Blackhat, Amsterdam/NL)
14.-15.10.	ISSE 2014 (TeleTrusT/eema, Brüssel/BE)
20.-24.10.	CPSSE – Schulung und Prüfung (Secorvo, Karlsruhe)
November 2014	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
03.-07.11.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Arizona/US)
10.-15.11.	T.I.S.P. – Schulung und Prüfung (Secorvo, Karlsruhe)
13.11.	Future IT-Kongress 2014 (AppSphere AG, Ettlingen)
17.-21.11.	Security Engineering – Schulung und T.E.S.S.-Prüfung (Secorvo, Karlsruhe)
20.-21.11.	38. Datenschutzfachtagung (DAFTA) (GDD, Köln)
Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Sven Köhler, Christoph Schäfer

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

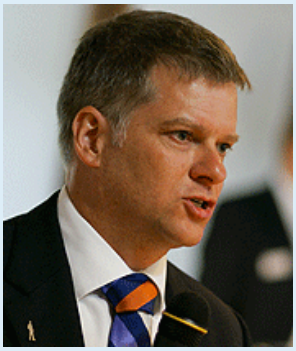
Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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

secorvo
security consulting

Secorvo Security News

Oktober 2014



Der Anforderungs-Zyklus

Es gibt Erkenntnisse, die sich wie Naturgesetze in unserem Weltverständnis eingenistet haben, obwohl sie sich den in den Naturwissenschaften bewährten Beweisverfahren und Modellbildungen entziehen. Dazu zählen das Pareto-Prinzip („80:20-Regel") – und der Hype-Zyklus von Jackie Fenn (Gartner) aus dem Jahr 1995, der den charakteristischen Verlauf der Aufmerksamkeit für ein Thema beschreibt.

Auch in der IT-Sicherheit lässt er sich beobachten. Tatsächlich beschreibt der Zyklus sogar die Entwicklung der Systemanforderungen. Ein Blick auf die fast 40jährige Geschichte der modernen Kryptografie macht das deutlich: Nachdem das RSA-Verfahren von 1978 erste Bekanntheit erlangt hatte, verbreiteten sich Implementierungen wie die Open Source-Software PGP, die viel Wert auf ein vom Anwender kontrolliertes Vertrauensmodell legte (welchen Schlüssel halte ich für authentisch?). Mit der Verabschiedung des ersten deutschen Signaturgesetztes im Jahr 1997, das höchste Sicherheitsvorgaben für Zertifizierungsdiensteanbieter enthielt und von einem zunächst 350 Seiten starken Maßnahmenkatalog des BSI begleitet wurde, erreichte der Anforderungs-Zyklus seinen Höhepunkt.

Es folgte der Absturz. Trotz EU-weit vereinheitlichtem Signaturgesetz konnte keine Anwendung eine nennenswerte Zahl von Anwendern gewinnen; PGP- bzw. S/MIME-Verschlüsselung blieben eine Nerd-Beschäftigung. Sicherheitsexperten, Gesetzgeber und Entwickler hatten übersehen, dass der Aufwand für hohe Sicherheitsanforderungen den Nutzen einer Verschlüsselungslösung reduziert.

Nun haben Edward Snowdens Veröffentlichungen den Ruf nach Verschlüsselung wieder aufleben lassen. Gesucht werden jedoch transparente Lösungen, bei denen die Verschlüsselung automatisch erfolgt – z. B. in einem lokalen „Verschlüsselungs-Proxy", der dem Benutzer Verwaltung und Prüfung öffentlicher Schlüssel abnimmt. Aus Sicherheitssicht vielleicht nicht perfekt. Aber anwendbar.

Inhalt

secorvo
security consulting

Security News

Des Pudels SSL-Kern

Am 14.10.2014 veröffentlichte das Google Security Team eine neu entdeckte Schwachstelle der SSL/TLS-Protokollfamilie und taufte sie auf den Namen POODLE. Sie ermöglicht einem Man in the Middle-Angreifer zunächst ein Downgrade der Verbindung auf die veraltete Version SSLv3 und anschließend einen Angriff auf dessen Block-Cipher-Modus CBC. Da nur stark veraltete Browser die aktuelle TLS-Version nicht unterstützen und inzwischen alle SSLv3-Cipher-Suites angreifbar sind, sollte SSLv3 in allen Clients und Servern deaktiviert werden.

Ein Blick auf die lange Reihe von Schwachstellen der komplexen SSL/TLS-Suite legt nahe, bei Sicherheitssoftware auch deren Komplexität als grundsätzliches Sicherheitsproblem im Auge zu behalten. Das einfache Design der Crypto-Bibliothek NaCl weist einen Ausweg.

ULD gegen Facebook

Nach Auffassung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) sind Fanpage-Betreiber für die Auswertung des Nutzungsverhaltens der Seitenbesucher durch Facebook verantwortlich. Daher hatte es gegenüber der Wirtschaftsakademie Schleswig-Holstein die Deaktivierung der Fanpage angeordnet, die das Verwaltungsgericht daraufhin in erster Instanz aufhob (siehe SSN 11/2013). Nun ist das ULD am 04.09.2014 in der Berufung beim Schleswig-Holsteinischen Oberverwaltungsgericht (OVG) gescheitert.

Bezüglich der Verantwortung der Fanpage-Betreiber kommt das OVG zu demselben Ergebnis wie die Vorinstanz: Fanpage-Betreiber seien zwar eigene Dienste-Anbieter; anders als bei einem Website-Betreiber, der Trackingcode in seine Seite einbettet, bestehe aber keinerlei Kontakt zu der Datenerhebung durch Facebook. Die Grundsätze der Störerhaftung kämen daher nicht zur Anwendung.

Zwar lässt das Urteil die Frage offen, ob das deutsche Datenschutzrecht anwendbar ist und die Datenverarbeitung durch Facebook dagegen verstößt. Entgegen den Verlautbarungen des ULD ist es jedoch überzeugend begründet. Für die Revision wird das ULD sich eine bessere Begründung für die Verantwortlichkeit der Seitenbetreiber einfallen lassen müssen. So einleuchtend und richtig die Forderung auch ist, dass ein Diensteanbieter nicht völlig von der Verantwortung für illegale Datenverarbeitungen seiner Dienstleister entbunden werden darf – sie muss sich auch mit rechtlichen Zurechnungsnormen begründen lassen.

Google-Token

Für die Anmeldung bei Google-Diensten wird schon länger die Zwei-Faktor-Authentisierung „2sv“ angeboten (siehe Editorial SSN 01/2013). Dabei wird ein Einmalpasswort als zweiter Faktor per SMS verschickt. Geklaute Login-Daten können so nicht dauerhaft genutzt werden; Angriffsmöglichkeiten durch Phishing bestehen aber nach wie vor. Und nicht jeder will Google seine Handy-Nummer anvertrauen – auch wenn diese Zurückhaltung in Zeiten von WhatsApp etwas hilflos anmuten mag.

Eine vielversprechende Alternative stellt der von Google am 21.10.2014 vorgestellte USB-Token „Security Key“ dar, der bereits ab sechs Euro erhältlich ist. Er unterstützt das PKI-basierte, von der Fast IDentity Online (FIDO-) Allianz spezifizierte Universal Second Factor Protocol (U2F). Neben Google gehören der Allianz Größen wie MasterCard, Microsoft, Nok Nok, NXP, Visa und Paypal an.

Leider ist das Verfahren eher für PC und Laptop gedacht als für das Anstecken an ein Smartphone. Auch ist zu hoffen, dass die Zahl der Allianz-Mitglieder steigt, damit man gute Authentisierung nicht irgendwann mit einem dicken Token-Schlüsselbund bezahlen muss.

Beweis-Last

Die Frage der Beweislastverteilung bei tatsächlichen oder vorgeblichen Hacking-Angriffen und Phishing-Attacken gewinnt zunehmend an Bedeutung. Das LG Coburg hat am 29.04.2014 den Streit über die Verbindlichkeit eines Ebay-Angebots zugunsten des Käufers entschieden, der einen Porsche Carrera sehr günstig erworben hatte. Der Ebay-Anbieter argumentierte, das Angebot sei nach einer Phishing-Attacke ohne seine Mitwirkung erstellt worden; der Porsche hätte gar nicht zum Verkauf gestanden.

Das LG Coburg sah den Beklagten für die unbefugte Account-Nutzung in der Beweispflicht. Einen Nachweis für die Phishing-Attacke konnte dieser jedoch nicht erbringen und die behauptete Anzeige bei der Polizei nicht belegen.

Das Urteil folgt dem Trend (siehe SSN 09/2014), das Risiko von Angriffen faktisch den System-Nutzern aufzubürden. Allerdings sind Phishing-Attacken und Hacking-Angriffe für Privatnutzer meist nur schwer nachweisbar; daher wäre wenigstens regelmäßig zu hinterfragen, ob das verwendete Authentifizierungssystem überhaupt geeignet ist, ein Handeln des Account-Inhabers hinreichend sicher zu belegen.

Orientierung für Cloud-Nutzer

Am 09.10.2014 veröffentlichten die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Düsseldorfer Kreis die Version 2.0 ihrer „Orientierungshilfe Cloud Computing". Die Broschüre geht darauf ein, dass nicht alles, was technisch möglich, auch rechtlich zulässig ist. Es erläutert ausführlich die rechtlichen Rahmenbedingungen der Cloud-Nutzung, vor allem bei Anbietern mit Sitz außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR).

Vor dem Hintergrund der NSA-Affäre erklären die Datenschutz-Aufsichtsbehörden, dass sie sich vorbehalten, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten zur Nutzung von Cloud-Diensten zu erteilen und zu prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind, solange der Zugriff ausländischer Nachrichtendienste nicht begrenzt wird.

Hunde, die bellen, beißen oft nicht: Die Verträge mit den relevanten Dienstleistern sind in der Regel nicht genehmigungspflichtig. Und die nebulöse Hoffnung auf eine „Begrenzung der Zugriffe ausländischer Geheimdienste" bleibt vage – und wäre, falls sie denn kommen sollte, wohl kaum überprüfbar. Davon abgesehen gibt das Dokument einen guten Überblick über die derzeitige Rechtslage.

Secorvo News

Lesestoff

Im Oktober erschien das Sonderheft 4/2014 iX Kompakt zum Thema „Security" – ein lesenswertes Kompendium mit 27 Beiträgen zu aktuellen Fragen der IT-Sicherheit. Zwei der Beiträge hat Secorvo beigesteuert: Einen Ansatz zur pragmatischen und effektiven Umsetzung von IT-Grundschutz in kleinen und mittleren Unternehmen von Kai Jendrian und Stefan Gora, und die Vorstellung eines strukturierten Vorgehens beim Testen der Sicherheit von Apps mit Hilfe von Threat Modeling von Dr. Yun Ding und Jörg Völker.

Bereits im August erschien ein Aufsatz von Kai Jendrian in Heft 8/2014 der DuD über den neu gefassten Standard ISO/IEC 27001:2013 – verfügbar zum Download auf unseren Webseiten.

Forschen gegen das Ausforschen

Abseits vom Katz-und-Maus-Spiel zwischen Angreifern und IT-Sicherheitsbeauftragten beschäftigt sich die IT-Sicherheits-Forschung mit Fragen von Übermorgen: Können wir Sicherheit beweisen? Wie können wir Vertrauen in der Cloud erzeugen? Welche Sicherheitsgarantien kann uns Technik liefern?

Auf der kommenden KA-IT-Si-Veranstaltung am **27.11.2014** werfen wir in zwei Vorträgen einen Blick in das Karlsruher Zukunftslabor der IT-Sicherheit und werden Lösungsansätze kennenlernen, die den Status des Laborversuchs bereits hinter sich haben. Gastgeber ist diesmal das Karlsruher „House of Living Labs" des Forschungszentrums Informatik. Für die ersten 25 schnell Entschlossenen bieten wir eine Führung durch dieses Zukunftslabor: vom intelligenten Stromzähler über Roboterkonzepte von morgen bis zum selbstfahrenden Auto mit Straßenverkehrszulassung (Führungsbeginn: 17 Uhr, Dauer: ca. 1 Stunde; Anmeldung unter www.ka-it-si.de).

Im Anschluss an die Veranstaltung haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking".

T.I.S.P. und T.E.S.S.

Vom 10. bis 14.11.2014 können Sie sich Ihre Kompetenz im Bereich Informationssicherheit mit dem Zertifikat „TeleTrusT Information Security Professional (T.I.S.P.)" bestätigen lassen (noch zwei freie Plätze). Nächster Termin des Zertifizierungsseminars im kommenden Jahr ist der 09. bis 13.03.2015. Als Teilnehmer des Seminars erhalten Sie die im August 2014 erschienene zweite, erweiterte Auflage des 700 Seiten starken Begleitbuchs „Zentrale Bausteine der Informationssicherheit" vorab zugesandt.

Die Komplexität von informationstechnischen Systemen wird zunehmend zum Sicherheitsrisiko. Dass und wie es dennoch möglich ist, komplexe Systeme sicher zu konzipieren und zu realisieren, ist Thema der viertägigen Zertifikatsschulung „T.E.S.S. – Sichere Systeme dank System Security Engineering" vom 17. bis 20.11.2014, die Sie durch die Teilnahme an der T.E.S.S.-Prüfung mit einem T.E.S.S.-Zertifikat abschließen können. Die Schulung zeigt, wie Sicherheit in die Prozesse und Lebenszyklen der Systementwicklung integriert werden kann. Sie lernen aktuelle Standards, Vorgehensmodelle und Best Practices kennen und anwenden (noch vier freie Plätze).

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

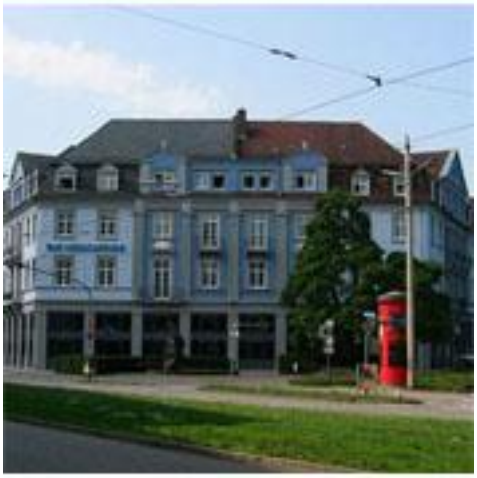
Veranstaltungshinweise

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

November 2014	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
03.-07.11.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Arizona/US)
10.-15.11.	T.I.S.P. – Schulung und Prüfung (Secorvo, Karlsruhe)
17.-21.11.	Security Engineering – Schulung und T.E.S.S.-Prüfung (Secorvo, Karlsruhe)
20.-21.11.	38. Datenschutzfachtagung (DAFTA) (GDD, Köln)
Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.12.	German OWASP Day 2014 (OWASP Germany, Hamburg)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)
Januar 2015	
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)

Fundsache

Wer Videoüberwachung einsetzen will, muss einen Vielzahl gesetzlicher Vorschriften beachten. Wie das nach Auffassung der Aufsichtsbehörden richtig geht, zeigt die aktuelle Broschüre des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.



Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Christoph Schäfer

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

secorvo
security consulting

Secorvo Security News

November 2014

Über den Wolken

Die Berichterstattung über den NSA-Untersuchungsausschuss wird immer mehr zur Realsatire. Schon über die parteipolitischen Zänkereien um die Befragung von Edward Snowden konnte man nur noch den Kopf schütteln. Als der Ausschuss schließlich um ein informelles Treffen in Russland bat, erteilte Snowden dem Vorhaben über seinen Anwalt eine Absage.

Einer der Höhepunkte der Ausschussarbeit war die Befragung der Datenschutzbeauftragten des BND im Oktober. Frau „Dr. F." konnte ihren offenbar reichlich angestauten Frust darüber loswerden, dass die BND-Führung ihre datenschutzrechtlichen Einschätzungen zwar zur Kenntnis nahm, ansonsten aber weitgehend ignorierte. Da wurde selbst die Peinlichkeit eines US-Spions in den Reihen des BND zur Randnotiz.

Möglicherweise ist aber auch nur Reinhard Meys „Über den Wolken" das Lieblingslied von Gerhard Schindler: Nach seiner Überzeugung ist die Freiheit des BND zumindest dort definitiv grenzenlos – und die Verfassung scheint plötzlich nichtig und klein. Denn die BND-Führung vertritt die Meinung, dass bei der Überwachung von Kommunikation über Satelliten per se kein deutsches Recht gelten kann – schließlich befinden sich diese im Weltraum. Die Abhörstation in Bad Aibling sei dabei ohne Bedeutung.

Wie hanebüchen diese Auffassung ist, weiß neben dem gesunden Menschenverstand auch die juristische Fachwelt. Ganz abgesehen davon, dass das Bundesverfassungsgericht dies bereits 1999 ausdrücklich feststellte.

Grundlage für die BND-Arbeit ist das G-10-Gesetz – und dieses ist dringend reformbedürftig. Wir benötigen gesetzliche Regelungen und eine effektive parlamentarische Kontrolle, die die Arbeit der deutschen Geheimdienste aus dem Weltraum zurück auf den Boden demokratischer Tatsachen holen. Und eine Amtsführung, die die verfassungsrechtlichen Grenzen ihrer Tätigkeit respektiert.

Inhalt

secorvo
security consulting

Security News

Grafikkarten als UKW-Sender

Wie bekommt man einen isolierten PC dazu, Daten an ein Smartphone zu übermitteln – auch wenn dieser nicht vernetzt ist? Mit dieser Fragestellung haben sich Forscher der israelischen Ben-Gurion Universität beschäftigt und ihre Erkenntnisse am 29.10.2014 auf der Malcon 2014 präsentiert.

Grundidee ihres kuriosen Seitenkanalangriffes ist es, die Grafikkarte derart zu beeinflussen, dass über das Monitorkabel als Antenne ein Signal im UKW-Frequenzbereich ausgesendet wird. Dieses wird vom Smartphone empfangen und von einer zu diesem Zweck entwickelten App „AirHopper" dekodiert.

Auch wenn die Datenrate sehr niedrig ist und die Übermittlung nur über recht kurze Distanzen funktioniert, könnte ein Trojaner auf diesem Weg ausgespähte Kennworte und Daten auf ein Smartphone weiterleiten. In Umgebungen mit sehr hohen Anforderungen an die Vertraulichkeit sollte man daher auf eine angemessene Abschirmung des Raumes achten – und keine Smartphones hineinlassen. Letzteres verbietet sich ohnehin wegen der in PCs und Smartphones verbauten Bluetooth-Chips.

Placebo-Zertifikate

Die US-amerikanische Federal Trade Commission (FTC) hat am 17.11.2014 die Einigung in einem Verfahren gegen TRUSTe, Inc., bekanntgegeben. Dem Anbieter von Gütesiegeln für Online-Dienste wurde vorgeworfen, seit dem kommerziellen Auftreten (ab 2008) bei seinen Kunden nicht für eine entsprechende Änderung der Siegel gesorgt zu haben.

Außerdem habe TRUSTe zwischen 2006 bis 2013 in etwa 1.000 Fällen entgegen der Angaben zu den Siegeln die jährlich erforderliche Rezertifizierung nicht durchgeführt. TRUSTe wurde zur Zahlung von 200.000 USD und zu genauer Rechenschaftslegung über seine Aktivitäten in Bezug auf den *Children's Online Privacy Protection Act* (COPPA) und die Zertifizierung der Einhaltung der *Safe Harbor*-Anforderungen verpflichtet. In diesem Zusammenhang hat die FTC betont, dass sie nicht zögern will, zum Schutz der Verbraucher einzuschreiten, wenn Marktteilnehmer bei Selbstverpflichtungen ihren Versprechungen nicht nachkommen.

Die damit öffentlich gewordenen TRUSTe-Verfehlungen zeigen deutlich, dass im Bereich der Online-Dienste Gütesiegel derzeit mehr schaden als nutzen. Hinter dem Vertrauen, das Nutzer und Geschäftspartner dem Siegel entgegenbringen, steht häufig wenig oder nicht nachvollziehbare Substanz. Dieses (blinde) Vertrauen hält Nutzer oder Anwender jedoch von eigenen Vorsichtsmaßnahmen und Kontrollen ab. Anstelle eines Sicherheitszuwachses führen derartige „halbseidene" Siegel eher zum Gegenteil.

Kampf der Grundrechte

Nachdem die Lehrerbewertungsportale bereits 2009 „dran" waren, hat der Bundesgerichtshof (BGH) sich nun mit einem Internetportal zur Ärztebewertung beschäftigt. In seiner am 06.11.2014 veröffentlichten Urteilsbegründung bewertet der BGH die Meinungs- und Informationsfreiheit der Portalnutzer und deren Interesse an einem Austausch über ärztliche Leistungen höher als das Recht auf informationelle Selbstbestimmung und die Berufsfreiheit des klagenden Arztes.

Dabei hat der BGH die Beeinträchtigung der Ärzte durch die Auffindbarkeit der Bewertungen mit Suchmaschinen, die Gefahr anonymer Wertungen ohne wahren Sachverhaltsbezug, die aufgezwungene Vergleichssituation mit anderen Ärzten und die Wettbewerbskonsequenzen als durchaus substantiell angesehen. Im Gegensatz zu dem in diesem Punkt ähnlichen EuGH-Urteil zu Suchmaschinen orientiert sich der BGH aber eher an der Dogmatik der Meinungs- und Informationsfreiheit. Danach ist das entscheidende Kriterium, dass die Bewertungen sich auf die Sozialsphäre des Arztes (das Arbeitsleben) beschränken.

Der Konflikt zwischen informationeller Selbstbestimmung und Informationsfreiheit in einem wenig vergessenden und jedermann zugänglichen Internet beginnt sich gerade erst zu entfalten. Für den Informationsaustausch in sozialen Netzwerken steht er im Grunde noch bevor; Suchmaschinen und Bewertungsportale sind da erst der Anfang. In den Argumentationen stoßen unterschiedliche Grundwerte aufeinander (Kontrolle des Einzelnen über die eigenen Daten gegenüber gesellschaftlichem Informationsinteresse). Für die Bedeutung und Grenzen des Datenschutzes ist dies eine wesentliche und wegweisende, aber keineswegs einfache Auseinandersetzung.

Stuxnet

Am 11.11.2014 veröffentlichte das Kaspersky Lab neue Erkenntnisse zum Verlauf der Stuxnet-Angriffe auf Irans Atomprogramm 2009 bis 2010. Einfallstor waren demnach nicht USB-Sticks (SSN 10/2010), sondern Dienstleister. Alle besaßen Expertise in der Automatisierungstechnik (SCADA) im iranischen Energiesektor. Alle wurden mehrfach infiziert oder konnten ihre Systeme nie von Stuxnet

reinigen. Das erste Opfersystem wurde wenige Stunden nach der Kompilation von Stuxnet am 22.06.2009 infiziert. Der zunächst vermutete Infektionsweg USB-Gerät erscheint damit unwahrscheinlich. Das System gehörte der Foolad Technic Engineering Co. Über die Behpajooh Co. Elec & Comp. wurde auch Irans größter Stahlproduzent Mobarakeh Steel Company angesteckt. Von dort breitete sich eine Infektionslawine bis in ferne russische Niederlassungen aus. Infiziert wurden auch die Neda Industrial Group, Teilnehmer der US-Sanktionsliste und die Control-Gostar Jahed Company. Der fünfte Dienstleister, Partner im Iranischen Atomprogramm, wurde von drei Systemen aus gleichzeitig angegriffen, was E-Mail als Infektionsweg unwahrscheinlich macht. Letztlich fand der Schadcode über die dauerinfizierten iranischen Dienstleister seinen Weg zum Ziel.

Was bleibt ist die Erkenntnis, dass Vertrauensbildung mit Dienstleistern nicht zum laxen Umgang bei der (IT-) Sicherheit verleiten sollte. Die strikte Kontrolle von Fernzugriffen und eingebrachten Daten sowie vertragliche Regelungen zur Mindestsicherheit mit Dienstleistern bleiben auch dann sinnvolle Maßnahmen, wenn man sich mit seinem Dienstleister gut versteht.

Blinder Fleck

Am 18.11.2014 veröffentlichte Mark Schloesser Erkenntnisse der Rapid7 Labs über Schwachstellen in digitalen Videorecordern der Firma Hikvision – gleich mit Metasploit-Exploit. Die betroffenen Geräte sind weltweit für die digitale Videoüberwachung im Einsatz – ein Scan fand über 150.000 im Internet erreichbare Geräte. Neben einem Trivialpasswort für den Admin-Zugang zeigt der Bericht drei aktuelle Firmware-Schwachstellen, die durch Pufferüberlauf (das „Cross-Site-Scripting“ der 80er Jahre des vergangenen Jahrhunderts) einem Angreifer die volle Kontrolle über das Gerät ermöglichen. Ähnliche Schwachstellen zeigen die IP-Kameras desselben Herstellers.

Für Angreifer sind dies Einfallstore ins Intranet eines Unternehmens. Fremdgenutzt wird bereits die Rechenpower der Geräte, um Bitcoins zu minen. Und Einbrecher könnten aus der Ferne Beweisfotos ihrer Taten verschwinden lassen. Seit September ist der Hersteller informiert; Patches sind bisher nicht verfügbar.

Überwachungstechnik mit Fernzugriff wird gern genutzt, um Routinearbeit auszulagern. Sobald aber IP-Technik mit dem Intranet verbunden wird, muss sie sicher administriert werden (Standardfehler: Default-Passwort). Sie muss patchfähig sein und sollte daher von einem Hersteller stammen, von dem bekannt ist, dass er Patches liefert. Diese Aspekte müssen Gegenstand der Beschaffungsentscheidung sein. Ein sicherer Internet-Fernzugriff erfordert weitere Maßnahmen wie einen VPN-Zugang oder eine Firewall.

Secorvo News

Weiterbildung 2015

Auch im kommenden Jahr werfen wir mit dem dreitägigen Seminar IT-Sicherheit heute einen vertiefenden Blick auf aktuellen Angriffe, neue Bedrohungen und mögliche Schutzmechanismen. Der erste Termin ist der 03.-05.03.2015.

Mit dem anerkannten Expertenzertifikat TeleTrusT Information Security Professional (T.I.S.P.) können Sie Ihre Erfahrungen und Kenntnisse in der IT-Sicherheit dokumentieren und sichtbar machen. Die nächste Schulung (mit anschließender Zertifikatsprüfung) findet vom 09. bis 13.03.2015 statt.

Sie suchen ein Seminar, das Ihnen das Thema PKI praxisnah und produktunabhängig vermittelt? Seit über 15 Jahren führen wir PKI-Projekte durch – und haben aus unseren Erfahrungen und Einsichten das Seminar PKI – Grundlagen, Vertiefung, Realisierung entwickelt, das inzwischen mehr als 350 Teilnehmer besucht haben (Termin: 21.-24.04.2015).

Sollen Sie in Zukunft Ihren Datenschutzbeauftragten in seinen Aufgaben unterstützen und ihm zuarbeiten? Die Schulung Geprüfter Datenschutzkoordinator im Unternehmen bereitet Sie auf zwei intensiven Seminartagen darauf vor (28.-29.04.2015). Nach bestandener Prüfung erhalten Sie ein Zertifikat vom TÜV Rheinland.

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

Zum Nachlesen

Im Dezemberheft der iX (12/2014, S. 64-71) erschien ein ausführlicher Beitrag der Secorvo-Experten André Domnick, Dr. Safuat Hamdy und Kai Jendrian zur systematischen Überprüfung der Sicherheit von Anwendungen.

Wer mehr von Secorvo lesen möchte, dem sei „das Buch“ empfohlen – „Zentrale Bausteine der Informationssicherheit“, erschienen Mitte 2014 in zweiter, aktualisierter und deutlich erweiterter Auflage, zugleich Begleitbuch des T.I.S.P.-Seminars. Je nach Präferenz als Hardcover oder E-Book (pdf) eine wunderbare, 720seitige Lektüre für den Lesesessel vor dem vorweihnachtlichen Kaminfeuer.

Veranstaltungshinweise

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

Dezember 2014	
01.-02.12.	IsSec/ZertiFA 2014 (Computas, Berlin)
09.12.	German OWASP Day 2014 (OWASP Germany, Hamburg)
09.-10.12.	3. DFN-Konferenz Datenschutz (DFN-CERT Services, Hamburg)
Januar 2015	
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)
Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Der am 21.10.2014 veröffentlichte Melani-Halbjahresbericht 2014/1 zur Informationssicherheitslage in der Schweiz und international stellt unterhaltsam und lesenswert aktuelle Informationen zu bekannt gewordenen Angriffen, Entwicklungen und Hintergründen vor.

Impressum

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

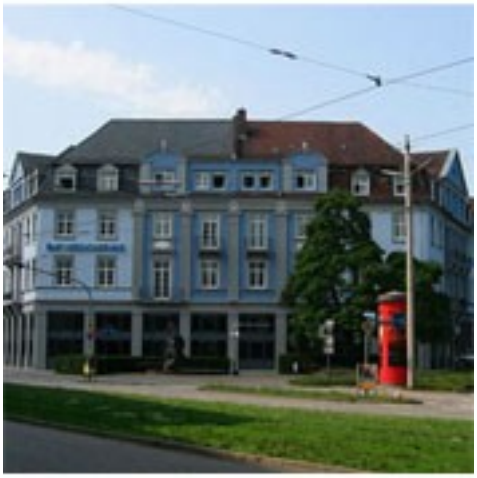
ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer (Editorial)

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



secorvo
security consulting

Secorvo Security News

Dezember 2014

Im Überwachungsstaat

Es war ein Jubiläum, das niemand beging – 30 Jahre nach „1984“, dem Jahr von Orwells Überwachungsstaat. Wirkte der Schreck über Snowdens Veröffentlichungen so nach, dass uns das Feiern verging? Oder ist die Ursache beunruhigender: Sind wir Frösche im Kochtopf, dessen Wasser schleichend erwärmt wird? Fragen wir uns vielleicht: Können wir überhaupt (noch) etwas tun? Oder blenden wir die allgegenwärtige Überwachung aus und reden uns (immer noch) ein, dass wir nichts zu verbergen haben? Es ist ja noch nichts passiert (zumindest haben wir nichts gemerkt), und böse Tyrannen gibt es ohnehin nur in Geschichtsbüchern und Nachrichten aus fernen Ländern.

Wenn wir die Realität nicht zumindest teilweise ausblenden, wird es unangenehm. Wer mag WhatsApp, GMail oder Facebook noch nutzen, wenn er ständig daran denkt, dass jede Nachricht und jeder „Like“-Klick, jeder Chat und jede Internet-Suche mitgeschnitten, beobachtet und zu einem Bild von uns verdichtet wird, das nie mehr gelöscht und jederzeit ausgewertet werden kann? Aber das Smartphone ausschalten? Dann ist man nicht erreichbar! E-Mails verschlüsseln? Dann kann man sie nicht mehr mit jedem Client abrufen! Auf das Navi verzichten? Wer hat denn heute noch einen Autoatlas? („Papi, was ist ein Autoatlas?“)

Derweil schrumpft der Bereich, in dem unser Verhalten nur im Gedächtnis unserer Mitmenschen vergängliche Spuren hinterlässt. „Car-IT“ analysiert Fahrverhalten und Regelverstöße, „SmartHomes“ steuern Heizung und Beleuchtung, und abends erfreut „SmartTV“ mit individualisiertem Programmangebot. Vielleicht war es richtig, sich nicht an „1984“ zu erinnern. Denn was uns wirklich bevorsteht, hat Ray Bradbury („Fahrenheit 451“) 1953 zutreffender vorausgesehen: Wir leben in einem technologischen Wunderland, rundumversorgt und perfekt unterhalten, bei umfassender Kontrolle (zu unserer eigenen Bequemlichkeit) – und haben vor lauter Unterhaltungsglück vergessen, wie Freiheit und Erkenntnis schmecken.

Inhalt

secorvo
security consulting

Security News

Und wieder SSL...

Am 08.12.2014 veröffentlichte der Security Engineer Adam Langley ein weiteres Poodle-Dilemma, von dem diesmal TLS betroffen ist. Das Protokoll füllt beim blockweisen Verschlüsseln den letzten Block per Padding auf. Der Empfänger muss die Gesamtlänge des Paddings prüfen – Load-Balancer von F5 und A10 Networks sowie einige Cisco-Geräte prüfen jedoch nicht und sind daher anfällig für Poodle. Wahrscheinlich ist die Wiederverwendung alter SSL-Funktionen die Ursache. F5 und A10 haben bereits Patches veröffentlicht.

Mit dem SSL Server Test von Ivan Ristić (Qualys) kann man die Verwundbarkeit des eigenen Servers testen. Grundsätzlich empfiehlt sich die Umstellung auf die aktuelle TLS-Version 1.2 mit AEAD-Blockverschlüsselung. Den Entwicklern der anfälligen Implementierungen empfehlen wir vor der Wiederverwendung von Security-Code sorgfältige Funktionstests.

Ein Klick für mehr Datenschutz

Social Plugins, die kleinen Spione der sozialen Netzwerke, die viele Betreiber von Internetseiten allzu freiwillig in ihren Quellcode einbinden, sind seit langem ein Dorn im Auge der Datenschützer. 2011 stellte Heise eine 2-Klick-Lösung für mehr Datenschutz vor (SSN 1/2012): Baute man den Code-Schnipsel in seine Seite ein, konnten die Social Plugins nicht ungefragt Daten übertragen. Stattdessen wurde der Benutzer über einen gesonderten Hinweis (erster Klick) gefragt, ob er z. B. eine „Like"-Meldung an das soziale Netzwerk übermitteln will. Erst nach seiner Bestätigung (zweiter Klick) wurde das Skript des Plugins aktiviert.

Zwei Klicks auf einer Internetseite sind eine Hürde, daher setzte sich die Heise-Lösung nicht flächendeckend durch. Mit Shariff hat Heise am 27.11.2014 nun einen Nachfolger in den Ring geschickt, bei dem nur noch ein Klick nötig ist. Die neuen Buttons sind einfache HTML-Links, die via CSS individuell gestalten werden können; sie müssen nicht mehr umständlich eingebettet werden.

IM Encryption for the Masses

Am 18.11.2014 hat Open Whisper Systems, der Spezialist für Verschlüsselungslösungen für Instant Messaging, seine Zusammenarbeit mit WhatsApp bekannt gegeben. In den letzten sechs Monaten hat man an einer Integration des TextSecure Protokolls gearbeitet. Die neueste Version von WhatsApp auf Android nutzt das Protokoll bereits transparent im Hintergrund. Auch wenn noch wichtige Funktionen wie die Verifikation der Schlüssel von Kommunikationspartnern, die Unterstützung von Gruppenchats und die Unterstützung anderer Plattformen fehlen, ist die Implementierung einer Ende-zu-Ende-Verschlüsselung ein Schritt in die richtige Richtung. Hoffentlich folgt der notwendige Rest...

Türsteuerung gibt Zugang preis

Am 01.12.2014 publizierte das RedTeam ein Advisory zur Schwachstelle in der Türsteuerung EntryPass N5200 – über die Konfigurationsoberfläche konnte die Kennung und das Passwort des Administrators in Erfahrung gebracht werden. Die – insbesondere bei der Timeline recht unterhaltsame – Schwachstellenmeldung zeigt, was man nicht tun sollte: So gibt der auf dem System betriebene simple Webserver recht freizügig Informationen preis. Woraus wir lernen können: Auch bei einem physischen Sicherheitssystem darf man die Sicherheit des IT-Anteils nicht ignorieren. Es muss immer das Gesamtsystem betrachtet werden.

Bei Angriffsmöglichkeiten kann man nicht voraussetzen, dass Systeme in einem separierten Management-Netz betrieben werden. Sofern ein System über einen netzseitigen Zugang verfügt, muss der auch entsprechend abgesichert werden. Debug-Meldungen oder sonstige Informationen, die einem Angreifer helfen können, darf das System im Auslieferungszustand nicht mehr ausgeben.

Strafverfolgungspfründe

Der U. S. District Court, S. D. New York hat am 31.10.2014 eine gerichtliche Weisung gegen einen Mobilfunkbetreiber bestätigt, der die Durchsuchung eines Mobiltelefons durch Hilfestellung bei der Entschlüsselung des Speicherinhalts unterstützen sollte. Die Weisung stützt sich auf ein über 225 Jahre altes Gesetz, nach dem ein US-Gericht Dritte zur Mitwirkung verpflichten kann, wenn diese in einer Position sind, in der sie auch als Unbeteiligte den Erfolg einer gerichtlichen Maßnahme verhindern könnten.

Aus dieser Entscheidung könnte abgeleitet werden, dass Mobilfunkbetreiber nach US-Recht verpflichtet sind, sich die Möglichkeit zur Entschlüsselung bei von ihnen vertriebenen Geräten offen zu halten. Das wäre ein weiterer Rückschlag für US-Anbieter, die gerade dabei sind, verlorenes Vertrauen ausländischer Kunden nach dem NSA-Skandal zurückzugewinnen. Jedenfalls lassen die Strafverfolgungsbehörden keine Gelegenheit aus, um zu verhindern, dass Daten ihrem Zugriff entzogen werden.

Ob Turing das gewollt hätte?

Ohne den Turing-Test durch CAPTCHAs (SSN 2/2008) würden viele Kontakt- und Registrierungsformulare, Foren und Downloadangebote im Internet von Bots überrollt. Allerdings werden CAPTCHAs auch für den Nutzer immer herausfordernder (und nerviger), weil Maschinen die Aufgaben zunehmend besser lösen können als wir (SSN 4/2009).

Wie ein verfrühtes Weihnachtsgeschenk kam am 03.12.2014 eine neue Methode von Google namens No CAPTCHA reCAPTCHA daher. Google berechnet dabei schon vor der Eingabe des CAPTCHA-Codes mithilfe der IP-Adresse, der Verweildauer auf der Seite und der Mausbewegungen im CAPTCHA-Feld, wie wahrscheinlich es ist, dass der Besucher ein Mensch ist. Dieser muss dann keinen Code mehr lösen, sondern nur noch einen Haken setzen. Auf Smartphones funktioniert die Methode mangels Mausbewegungen nicht – hier muss man „lustiges" Tier-Memory spielen.

Doch halt: IP-Adresse übermitteln? Mausbewegungen auswerten? War da nicht etwas mit Datenschutz? Nicht erst „No CAPTCHA", schon der Einsatz des reCAPTCHA-Dienstes bedarf der vorherigen Einwilligung der Seitenbesucher. Schließlich werden dabei personenbezogene Daten an Google übermittelt. reCAPTCHA kann man nicht einmal per Browser-Plugin blockieren. Unterhalb des Radars der meisten Datenschützer hat sich reCAPTCHA massenweise ausgebreitet. Datenschutzkonform und benutzerkompatibel ist einzig eine selbst gehostete CAPTCHA-Lösung.

Internationaler Datenverkehr

Mit ihrem am 26.11.2004 veröffentlichen Arbeitspapier 226 hat die Art. 29-Gruppe ein Verfahren in Kraft gesetzt, das Zuständigkeitskonflikte und bürokratische Hindernisse bei der Verwendung von EU-Standardvertragsklauseln vermeiden soll, wenn bspw. eine internationale Unternehmensgruppe für den konzerninternen Datenverkehr die an sich unveränderlichen Standardvertragsklauseln aufgrund nationalem Recht ergänzt und hierzu eine Genehmigung benötigt. Nun kann die anfragende Stelle eine führende Aufsichtsbehörde vorschlagen, die für alle übrigen Stellen die Rechtskonformität prüft. Alle anderen zuständigen Behörden prüfen nur noch die Voraussetzungen des nationalen Rechts.

Das Papier bekräftigt, dass die Standardvertragsklauseln um weitere Regelungen ergänzt werden können. Auch wenn zunächst nicht viele betroffene Stellen von dem neuen Verfahren Gebrauch machen werden, ist dies eine wichtige Klarstellung.

Secorvo News

Zertifizierter Datenschutzkoordinator

Für Datenschutzbeauftragte gibt es Weiterbildungsangebote wie Sand am Meer. Dünner wird die Luft bei Angeboten für Datenschutzkoordinatoren, die ihrem Datenschutzbeauftragten zuarbeiten. Am 28. bis 29.04.2015 bieten wir die Weiterbildung zum „Geprüften Datenschutzkoordinator im Unternehmen" an. Mit Bestehen der Abschlussprüfung kann der Datenschutzkoordinator anschließend seine Qualifikation mit einem Zertifikat belegen.

Der T.I.S.P. entwickelt sich zu dem am weitest verbreiteten deutschen Personenzertifikat für Informationssicherheit. 700 T.I.S.P.-Absolventen gibt es inzwischen, die sich in einer eigenen Community regelmäßig zum Erfahrungsaustausch treffen. Die nächste Möglichkeit, eine unserer T.I.S.P.-Schulungen zu besuchen, bieten wir Ihnen Mitte März.

Anfang März bringt Sie das Seminar IT-Sicherheit heute in drei Tagen auf den aktuellen Stand – Sie erfahren, was Sie als IT-Sicherheitsverantwortlicher über die aktuelle Sicherheitslage wissen sollten.

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

Krönungsfest

Es ist der höchstdotierte, privat gestiftete Preis Deutschlands: der deutsche IT-Sicherheitspreis, ausgelobt von der Horst Görtz Stiftung und seit 2006 alle zwei Jahre verliehen. Der Preis würdigt mit Preisgeldern in Höhe von insgesamt 200.000 € herausragende deutsche Innovationen in der IT-Sicherheit. Im Jahr 2014 ging der erste Preis über 100.000 € an Herrn Professor Müller-Quade (KASTEL/KIT) und die Karlsruher Firma WIBU-Systems für die Entwicklung der Blurry-Box – einer zukunftsweisenden Lösung für den Softwareschutz, die nicht auf der Geheimhaltung des Verfahrens beruht.

Nicht genug, dass damit Professor Müller-Quade nach seiner Auszeichnung im Jahr 2008 bereits zum zweiten Mal Träger des ersten Preises ist: der KA-IT-Si-Partner WIBU-Systems erhielt die Auszeichnung pünktlich zum 25. Unternehmensjubiläum. Gründe genug für die KA-IT-Si, um Ihnen vorzustellen, was in Karlsruhe möglich ist – und diese Krönung unseres IT-Sicherheitsstandorts bei unserer nächsten KA-IT-Si-Veranstaltung am **15.01.2015** im Informatik-Gebäude des KIT mit Ihnen zu feiern. Anmeldung unter www.ka-it-si.de.

Veranstaltungshinweise

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

Januar 2015	
15.01.	Krönungsfest (KA-IT-Si, Karlsruhe)
16.-18.01.	ShmooCon 2015 (The Shmoo Group, Washington/US)
20.-22.01.	Omnicard 2015 (in TIME berlin, Berlin)
Februar 2015	
04.-05.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
24.-25.02.	22. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2015	
03.-05.03.	IT-Sicherheit heute – aktuelle Angriffe, Bedrohungen & Schutzmechanismen (Secorvo, Karlsruhe)
09.-13.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
23.-26.03.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)

Fundsache

Im November 2014 wurde auf der CCS 2014 eine Studie zur Aussagekraft von Webseiten-Prüfsiegeln vorgestellt (siehe auch Placebo-Zertifikate, SSN 11/2014). Dabei fanden praktisch alle Prüfverfahren bei einer präparierten Webseite nur einen Bruchteil der Schwachstellen. Auch wurden zahlreiche Webseiten im Netz gefunden, die trotz Prüfsiegel Schwachstellen aufwiesen. Hier wird dem Besucher der Website ein Sicherheitsniveau vorgegaukelt, das eher zu einer Sicherheitsgefährdung aufgrund falschen Vertrauens als zu einem Sicherheitsgewinn führt.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Kai Jendrian, Michael Knopp, Sven Köhler, Christoph Schäfer.

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