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