secorvo
security consulting

Secorvo Security News

Februar 2017

Die Awareness-Falle

Wie haben wir uns das doch vor 20 Jahren herbeigesehnt: Kaum ein Tag ohne Schlagzeile über einen Security-Vorfall und nur noch wenige Unternehmensleitungen, die dem Thema Informationssicherheit mit Ignoranz begegnen.

Allerdings drohen wir inzwischen diesem Awareness-Erfolg selbst zum Opfer zu fallen. Immer häufiger lotst er Sensibilisierte in eine Fatalismus-Sackgasse: Wenn jedes Kryptoverfahren früher oder später gebrochen und jede Webanwendung geknackt wird – was nützen da noch Schutzmaßnahmen? Warum nicht die Ausgaben sparen und das Beste hoffen?

Nachlässig recherchierte oder mit Halbwissen verfasste Meldungen geben dieser Haltung immer wieder neue Nahrung. Nicht genug damit: Die jüngste Salonfähigkeit von „Fake News" gibt uralten Verschwörungstheorien neuen Aufwind („Tolles Geschäftsmodell: erst Viren(warnungen) verbreiten und dann Virenschutz verkaufen").

Aber die Komplexität der Wirklichkeit ist bekanntlich schwer zu vermitteln. Dabei gleicht die Arbeit eines Sicherheitsbeauftragten der eines Lotsen, der bekannte Untiefen umschifft und für alle unbekannten einen Notfallplan bereithält. Natürlich senkt er mit seiner Expertise Wahrscheinlichkeit und Schadensausmaß einer Havarie – wenn auch er sie nie gänzlich ausschließen kann.

Geht der Lotse seiner Arbeit still und sorgfältig nach, werden mangels Wertschätzung womöglich seine Einflussmöglichkeiten beschnitten oder sein Budget gekürzt. Buhlt er (oder die Öffentlichkeit) umgekehrt zu viel um Aufmerksamkeit für sein Thema, kann ihm dasselbe drohen: Denn wenn wenig passiert, kann das sein Verdienst sein – oder aber der Wirbel um das Thema erscheint übertrieben.

Das richtige Maß zu finden ist im Leben häufiger eine Herausforderung. Helfen kann die Orientierung an Standards und Best Practices: Ruhige Professionalität statt aufregungsgetriebener operativer Hektik wird auch hier auf mittlere Sicht den größeren Nutzen stiften.

Inhalt

secorvo
security consulting

Security News

SHA-1-Kollision

Schon lange war das näher rückende Unwetter am Horizont zu sehen, nun hat der erste Blitz eingeschlagen: Am 23.02.2017 präsentierte eine Gruppe von Forschern des CWI Amsterdam und Google die erste SHA-1-Kollision – zwei PDF Dateien mit gleichem Hashwert. Mit 6.500 CPU-Jahren (oder 110 GPU-Jahren) ist der Aufwand zwar unrealistisch für Massenangriffe, aber immerhin um den Faktor 10^5 schneller als ein „Brute-Force"-Angriff.

Damit ist der SHA-1 nicht komplett gebrochen: Anwendungen, bei denen nur die Einweg-Eigenschaft gefordert ist, sind von dem Angriff nicht betroffen; auch Fingerprints und Signaturen, die nachweislich schon vor längerer Zeit erstellt wurden, sind nicht akut gefährdet. Die Autoren des Angriffs bieten sogar einen File-Tester an, der typische Muster ihres Angriffs erkennt.

Die Normung des SHA-2 und die ersten Angriffe auf den SHA-1 liegen 15 bzw. 12 Jahre zurück. Einen zügigen Wechsel hat behindert, dass der SHA-1 in Standards festgeschrieben war und Systeme in Umlauf gebracht wurden, deren Kryptofunktionen nicht per (Firmware-)Update ausgetauscht werden konnten. Vorausschauende Hersteller sollten gleich zusätzlich den SHA-3 implementieren, damit der nächste Wechsel weniger holperig verläuft.

DSAnpUG-EU

Das Bundeskabinett hat am 01.02.2017 nach einem neuen Anlauf des Bundesministeriums des Inneren ein Datenschutz-Anpassungs- und Umsetzungsgesetz EU beschlossen. Kernstück ist ein an die DS-GVO angepasstes Bundesdatenschutzgesetz (BDSG-E). Nachdem der vorausgegangene Gesetzentwurf sehr unübersichtlich und wiederholungslastig war (SSN 12/2016) hat sich nun Einiges getan: Er wurde unterteilt in die Umsetzung der Datenschutz-Grundverordnung und der Datenschutzrichtlinie für Polizei und Justiz. Ein wichtiger Regelungsgegenstand ist die künftige Aufsichtsstruktur: Die Vertretung im Europäischen Ausschuss übernimmt die Bundesdatenschutzbeauftragte mit einem gewählten Vertreter aus den Bundesländern.

Die §§ 32 ff. BDSG-E enthalten Einschränkungen der Informationspflichten und Betroffenenrechte. Dabei bleibt fraglich, ob diese ausreichend durch Öffnungsklauseln der DS-GVO gedeckt sind. Der Beschäftigtendatenschutz wurde um eine Freiwilligkeitsdefinition zur Einwilligung ergänzt, ansonsten entspricht er im Wesentlichen dem (ursprünglich provisorischen) bisherigen § 32 BDSG. Die Zulässigkeit der Videoüberwachung wird in § 4 BDSG-E massiv ausgedehnt. Daran haben die Aufsichtsbehörden bereits deutliche Kritik geübt.

Immerhin handelt es sich um einen Stand, an dem sich Unternehmen bei der Umsetzung der DS-GVO bereits vorsichtig orientieren können. Als Stärkung des Datenschutzes kann der Gesetzentwurf allerdings kaum gewertet werden.

VPN-Apps im Playstore

Seit Edward Snowdens Veröffentlichungen haben zahlreiche Apps mit VPN-Funktionalität den Weg in Googles Playstore gefunden. Ernüchternd allerdings die Ergebnisse einer Untersuchung von 238 VPN-Apps, die am 15.11.2016 auf der ACM-Konferenz IMC vorgestellt wurde: Danach weisen die meisten der von den Forschern analysierten Apps schwere Mängel auf. So verschlüsseln ganze 18 % den Datenverkehr gar nicht, nur 16 % verschlüsseln IPv6-Pakete und 66 % tunneln keine DNS-Anfragen. Einige verwenden Proxys, um den HTTP-Verkehr zu manipulieren und JavaScript-Code für Werbung oder Tracking in HTTP-Antworten unterzubringen. Andere haben keinen definierten Tunnelendpunkt, sondern leiten die Daten über andere Nutzer in Peer-to-Peer-Netzwerken weiter. Vier der untersuchten Apps brechen sogar den TLS-Verkehr auf.

Beim Einsatz von VPN-Apps muss man sich darüber im Klaren sein, dass das virtuelle Netzwerkinterface vollständig in der Hand des App-Herstellers liegt. Der Betrieb einer VPN-Infrastruktur ist nicht gratis, und dies kompensieren die Betreiber kostenfreier VPNs auch durch den Handel mit Nutzerdaten. Wem es mit dem Schutz der Privatsphäre ernst ist, der sollte nur Apps von Herstellern verwenden, die eine gute Reputation genießen – auch wenn dies mit Kosten verbunden sein sollte.

DIY-Umkopierstation

Am 02.02.2017 veröffentlichte das Computer Incident Response Center Luxembourg Version 2.1 des Projekts CIRCLean, einer Open Source-Lösung zum sicheren Umkopieren von Dokumenten von einem potentiell mit Malware infizierten auf einen vertrauenswürdigen USB-Stick. Die auf einem Raspberry Pi zu installierende Software unterstützt zahlreiche Datei- und Dateisystemformate, die auf der Projektseite aufgelistet sind.

Zur Installation der Umkopierstation genügt es, das Image auf eine SD-Karte zu schreiben, die SD-Karte und den zu kopierenden USB-Stick in den Raspberry Pi einzustecken und die Stromversorgung herzustellen. Auf dem Zielsystem werden die Dateien nach Datenarten (Text, Video, Audio etc.) sortiert abgelegt. Gefährliche Formate erhalten im Dateinamen

die Ergänzung "Dangerous"; dabei werden u. a. komprimierte Dateien auf Zip-Bomben überprüft. Der Abschluss des Kopiervorgangs wird akustisch signalisiert – solange der Raspberry Pi beschäftigt ist, spielt er einen Song aus der mitgelieferten Musiksammlung. Zumindest für das gelegentliche Kopieren von Dateien ist das ein praktikabler Ansatz – sicherlich verträglicher als das generelle Aussperren von USB-Speichermedien und womöglich wirksamer als ein Virenscanner.

Zulässige Videoüberwachung

Der Bayerische Landesbeauftragte für den Datenschutz, Prof. Dr. Petri, hat sich in seinem jüngsten, am 31.01.2017 veröffentlichten 27. Tätigkeitsbericht mit der Videoüberwachung vor allem in problematischen Umgebungen auseinandergesetzt. So fordert er z. B. für den Krankenhausbereich u. a. die Umsetzung einer maximalen Speicherfrist von zehn Tagen; im medizinischen Bereich habe die Aufzeichnung gänzlich zu unterbleiben.

Die umstrittene Frage, ob auf Kameraattrappen auch die datenschutzrechtlichen Bestimmungen anzuwenden sind, befürwortet der Landesbeauftragte unter Verweis auf das Bundesverfassungsgericht. Zudem fordert er als Nachweis für bestehende Gefahren als Überwachungsgrund eine längerfristige Vorfallsdokumentation.

Kameras, die sich selbst nur bei bestimmten Aktionen wie bspw. dem Betätigen eines Öffnungsschalters aktivieren, werden dagegen als regelmäßig unbedenklich eingeschätzt. Allerdings seien Kameras nach Wegfall der Gefährdungslage (z. B. dem Ausbleiben abzuwehrender Schadensfälle) auch wieder abzubauen. Insgesamt belegt der Bericht zahlreiche Fehler bei der Einrichtung von Videoüberwachungen, stellt allerdings – unter Verweis auf die bereit gestellten Schemata und Hilfestellungen des Landesbeauftragten – hohe Anforderungen an die Ausgestaltung.

Metasploit-Erweiterung

Mit der Veröffentlichung der Metasploit Hardware Bridge wurde das bekannte Exploitation Framework am 02.02.2017 um Schnittstellen erweitert, mit denen auch Systeme angegriffen werden können, die nicht über TCP/IP erreichbar sind. Ursprünglich lag der Fokus darauf, eine Schnittstelle zum CAN-Bus zu schaffen, um darüber beispielsweise Abläufe beim Car-Hacking denen „klassischer" Exploits anzunähern. Entstanden ist daraus jedoch eine generische Schnittstelle, die es zukünftig sehr erleichtert, Metasploit um neue Schnittstellen zu erweitern. ZigBee und JTAG werden bereits getestet. Da heute kaum mehr ein Gerät ohne eingebauten Computer und komplexe Software auskommt, ergeben sich so zahlreiche neue Angriffsszenarien, zumal Schnittstellen abseits von TCP/IP vielfach als Angriffsvektor vernachlässigt werden. Aus der Sammlung von Exploits ist mittlerweile ein für Pentester unverzichtbarer Werkzeugkasten mit mächtigen Tools zur Entwicklung von Exploits und Ausnutzung von Schwachstellen geworden.

Secorvo News

Seminare

Für Kurzentschlossene: Vom **14. bis 16.03.2017** geben wir Ihnen auf dem Seminar „IT-Sicherheit heute" einen Überblick über aktuelle Themen der IT-Sicherheit. Ein besonderes Highlight: der „Live Hacking Day" mit der Vorführung verschiedener Angriffsmethoden (Programm und Anmeldung).

Wie sichere Software-Entwicklung professionell funktioniert, zeigt das Seminar „T.P.S.S.E." am **27.-30.03.2017** mit der anschließenden Möglichkeit zur Zertifizierung (Agenda und Anmeldung).

SECORVENTION 2017

Compliance-Erwartungen und staatliche Regulierung wie das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung fordern immer umfassendere Nachweise und belegbare Dokumentation. Damit rücken IT-Sicherheitszertifizierungen verstärkt in den Mittelpunkt des Interesses. Was aber bedeutet beispielsweise eine ISO-27001-Zertifizierung in der Praxis? Welcher Aufwand ist damit verbunden – und lohnt sich das? Was lässt sich aus den Erfahrungen zertifizierter Unternehmen lernen? Diesen Fragen geht die diesjährige SECORVENTION am **30. und 31.05.2017** auf den Grund. Sie findet statt in den stilvollen Räumlichkeiten der Buhlschen Mühle in Ettlingen. Das vollständige Programm und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.secorvention.de.

Lass den Bauch entscheiden ...

... oder warum klassische Risikoanalysen in der Informationssicherheit nicht funktionieren: Bei unserem kommenden KA-IT-Si-Event am **23.03.2017** wirft Kai Jendrian (Secorvo) in seinem Vortrag einen tieferen Blick auf die Herausforderungen bei der praktischen Durchführung von Risikoanalysen in der Informationssicherheit. Dabei wird er verbreitete Ansätze gegenüberstellen und Anregungen für eine praxisorientierte Umsetzung gegeben.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

März 2017	
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
23.03.	No risk, no fun. (KA-IT-Si, Karlsruhe)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
April 2017	
05.-06.04.	Security Forum 2016 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-25.04.	a-i3/BSI-Symposium 2017 (Arbeitsgruppe Identitätsschutz im Internet, Bochum)
25.-26.04.	Datenschutztage 2017 (Forum für Datenschutz, Mainz)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-28.04.	2nd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Paris/FRA)
30.04.-04.05.	Eurocrypt 2017 (IACR, Paris/FRA)

Fundsache

Ein Team von Sicherheitsforschern (u. a. von Mozilla und Google) hat die HTTPS-Verbindungen von Security-Software und -Appliances untersucht. Dabei stellten sie fest, dass bei einigen Lösungen Angriffe auf die gesicherten Verbindungen möglich sind.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Dr. Safuat Hamdy, 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