secorvo
security consulting

Secorvo Security News

April 2016

Time is money

Die ungebremste Beschleunigung unserer Arbeitswelt, die inzwischen sogar unser Privatleben vereinnahmt, beklagen wir nicht erst seit der Verbreitung des Smartphones (nanu, da ist ja ein „Aus"-Knopf?!). Sie erfasst nun auch die dunkle Seite des Internet: Cyber-Angriffe werden zum stressigen Unterfangen. Die internationale Kooperation und die Nachrüstung von Strafverfolgungsbehörden, Richtern und Staatsanwälten in Sachen IT-Know-How beginnen offenbar Früchte zu tragen. Wer eine Attacke startet, muss heute mit koordinierter und energischer Gegenwehr rechnen: Maliziöse Systeme werden vom Netz getrennt, kriminelle Gruppen ausgehoben.

Zwar lässt sich mit *flux networks*, in denen durch schnelle Änderungen der IP-Konfigurationen das Abkoppeln der Angriffssysteme erschwert wird, etwas Zeit gewinnen – doch wie im echten Leben gilt es nun auch im virtuellen Raum, den kriminellen Zugriff möglichst kurz zu halten. Oft bleibt nur ein Zeitfenster von wenigen Stunden, manchmal sogar Minuten, um von einem Phishing-, Verschlüsselungs- oder DoS-Angriff zu profitieren. Während der Vorbereitungsaufwand für einen erfolgreichen Angriff steigt, sinkt mit der Verkleinerung des Zeitfensters dessen Profitabilität.

Sicherlich darf man trotzdem in naher Zukunft nicht darauf hoffen, dass blanke Not die Cracker zu Gutmenschen mutieren lässt. Denn noch finden sie ausreichend Nahrung: Lange nicht jedes Unternehmen hat seine Hausaufgaben ordentlich gemacht. Und ist erst der gesamte Fileserver verschlüsselt, steigt die Zahlungsbereitschaft meist mit Lichtgeschwindigkeit.

Sollte die Entwicklung so weitergehen, könnte sich dennoch am Horizont ein wenig Licht abzeichnen. Vielleicht genügt es ja eines Tages, nicht jede ankommende E-Mail sofort zu öffnen.

Das wäre zugleich ein kleiner Beitrag zur Entschleunigung – der vielleicht auch einfach mal so gut tun würde.

Inhalt

secorvo
security consulting

Security News

Anti-Ransomware

Fast täglich tauchen neue, immer ausgeklügeltere Varianten von Verschlüsselungstrojanern (*Ransomware*) auf – auch in kritischen Infrastrukturen, wie heise.de am 18.02.2016 berichtete. Anti-Viren-Programme helfen nicht dagegen: Die Schadsoftware wird oft erst Tage später erkannt.

Was lässt sich dagegen tun? Neben einem Backup, das im Katastrophenfall die Wiederherstellung unzugänglich verschlüsselter Daten erlaubt, erreicht man nachhaltigen Schutz nur durch einen zurückhaltenden Umgang mit Schreib- und Ausführungsrechten. Will man den Schaden für Dateien auf Fileservern begrenzen, benötigt man ein differenziertes und restriktives Rechte- und Rollenkonzept, das Benutzern nur die Schreibzugriffe einräumt, die sie tatsächlich benötigen. Auch sollten Anwender nie mit administrativen Rechten auf externe Daten (Webseiten, E-Mail-Anhänge, USB-Stick-Inhalte) zugreifen.

Zusätzlich ist zu empfehlen, via AppLocker über Gruppenrichtlinien einzuschränken, welche Dateien ausgeführt werden dürfen, und das Aktivieren von Ransomware auf allen Systemen zu unterbinden. Auch eine Einschränkung von Skriptsprachen wie Powershell oder CScript sollte in Betracht gezogen werden. Zum Schutz vor Office-Makros bietet sich auch die Verwendung vertrauenswürdiger Speicherorte an. Nicht zuletzt sollten die Anwender mit geeigneten Security Awareness-Maßnahmen für die Risiken sensibilisiert werden, damit sie in Zweifelsfällen fragen, bevor sie eine Schadsoftware aktivieren.

Volksverschlüsselung über Nacht

Am 05.04.2016 poppte in WhatsApp-Chats auf Millionen Smartphones die Nachricht auf: Ab sofort seien alle Nachrichten und Anrufe mit dem Gesprächspartner Ende-zu-Ende verschlüsselt.

Bei aller berechtigter Kritik an WhatsApp muss man vor dieser Maßnahme den Hut ziehen. Unter der Annahme, dass die Implementierung der Verschlüsselung ordentlich erfolgt ist (derzeit gibt es keinen Grund etwas Anderes anzunehmen – sie basiert auf dem anerkannten TextSecure-Protokoll), wurde über Nacht ein immenser Gewinn für die Privatsphäre von Millionen Menschen geschaffen. Die Umsetzung ist unkompliziert: Schlüsselerstellung und -austausch erfolgen automatisch. Zusätzlich kann eine Sicherheitsnummer (QR-Code) abgeglichen werden, um den Gegenüber zu authentifizieren. Diese Funktion ist allerdings stiefmütterlich platziert – offenbar sind die Entwickler zu der (realistischen?) Einschätzung gelangt, dass die Authentifizierung die User ohnehin nicht interessiert.

Allerdings fallen nach wie vor Metadaten zuhauf an (wer kommuniziert wann mit wem?). Und weiterhin synchronisiert WhatsApp automatisch das Adressbuch – im Unternehmensumfeld in der Regel ohne Rechtsgrundlage. Daher sollten Unternehmen nicht dem Irrglauben verfallen, die geschäftliche Nutzung von WhatsApp sei durch die Verschlüsselung unbedenklich geworden.

Paranoia als Sorgfaltspflicht?

Geht es nach der Rechtsprechung steigt die Awareness der Durchschnittsnutzer offenbar stetig. Das Amtsgericht Frankfurt a. M. hat mit Urteil vom 24.03.2016 das Hereinfallen auf eine Phishing-Mail, die zur Mitteilung der Telefon-Banking-PIN verleitete, als grobe Fahrlässigkeit gewertet. Verschiedene Instanzgerichte und 2012 auch der Bundesgerichtshof haben die Herausgabe von TANs und PINs bereits als vom Nutzer zu verantworten qualifiziert, wenn die Bank zuvor auf die Gefahren durch Phishing hingewiesen und klargestellt hat, dass sie zu bestimmten Verhaltensweisen nicht auffordern wird. Bis Oktober 2009 haftete der Bankkunde bereits bei einfacher Fahrlässigkeit, danach wurde § 675v Abs. 2 BGB auf grobe Fahrlässigkeit beschränkt. Sie liegt vor, wenn die erforderliche Sorgfalt in besonders schwerem Maß verletzt wird und selbst naheliegende Überlegungen nicht angestellt werden. Angesichts der steigenden Qualität der Angriffe darf man jedoch bezweifeln, dass vom Durchschnittsnutzer generell erwartet werden kann, eine Phishing-Mail zu erkennen.

Forensische Jagd

Das Google Rapid Response Framework (GRR) ist ein bewährtes forensisches Werkzeug für die Analyse von Apple-, Windows- und Linux-Systemen. Im aktuellen Release 3.1 vom 16.04.2016 wurde die Möglichkeit ausgebaut, eine umfassende Jagd (*hunt*) über eine Gruppe von Zielsystemen durchzuführen, um die Existenz eines spezifischen Artefakts zu prüfen und optional auch Gegenmaßnahmen einzuleiten. Unter der Haube des GRR wurde die forensische Echtzeitanalyse in das am 05.04.2016 fertig gestellte Rekall V1.5 integriert, das jetzt auf den Capstone Disassembler umgestellt hat und dadurch ein sehr viel weiter gehendes Bild über die Ablaufstrukturen von Programmfunktionen liefert als das, was man bisher von einem forensischen *Incident Tool Framework* erwarten durfte. Wer GRR testen möchte, dem seien der aktuelle Docker Build oder die pre-build Binaries empfohlen. *Happy Hunting*!

Standardisiertes Löschen

Die „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ ist am 08.04.2016 als DIN 66398 erschienen und kann nun beim Beuth Verlag bezogen werden. Die Weiterentwicklung der Leitlinie Löschkonzept zu einer DIN-Norm wurde seit Ende 2013 von den Unternehmen Deutsche Bahn, Blancco, DATEV, Secorvo und Toll Collect gefördert (SSN 2/2014, SSN 1/2015 und SSN 9/2015). Ein großer Schritt für den Datenschutz: Nun gibt es einen Standard für die Festlegung von Löschfristen.

Durch Wiederholung richtig?

Das Landesarbeitsgericht Berlin-Brandenburg hat anlässlich eines Falls exzessiver Internetnutzung eines Arbeitnehmers sein Urteil von 2011 bekräftigt und die Stellung des Arbeitgebers als Telekommunikationsanbieter verneint. So sei der Arbeitnehmer bei erlaubter Privatnutzung kein Dritter, und es läge keine Erbringung von Telekommunikationsdiensten vor (§ 3 Nr. 10 TKG). Die Zulässigkeit der Auswertung des Browserverlaufsprotokolls stützt das Gericht auf § 32 BDSG. Die Speicherung sei zur Missbrauchskontrolle zulässig. Da der Arbeitnehmer das Protokoll beliebig löschen kann, ist allerdings bereits die Eignung fraglich.

Insgesamt überzeugt die Begründung des Gerichts auch bei dieser neuen Entscheidung nicht, da sich das Urteil weder argumentativ mit der Dritteigenschaft von Arbeitnehmern noch vollständig mit der datenschutzrechtlichen Qualifizierung von Browserverlaufsdaten auseinandersetzt. Unternehmen sollten daher auch weiterhin bei erlaubter Privatnutzung die Pflichten eines Telekommunikationsdiensteanbieters erfüllen.

Datenschutzgrundverordnung

Am 14.04.2016 hat als letzte Instanz auch das Europäische Parlament die Datenschutzgrundverordnung verabschiedet, die damit nach Veröffentlichung im Europäischen Amtsblatt in Kraft tritt und ab Mitte 2018 europaweit gelten wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich bereits am 07.04.2016 mit der Anpassung der deutschen Datenschutzgesetze auseinandergesetzt. Die Datenschutzbeauftragten fordern u. a. die Einführung eines Beschäftigtendatenschutzgesetzes (oder die Beibehaltung von § 32 BDSG), Beschränkungen für Gesundheitsdaten, die Normierung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit und die Beibehaltung des § 4f Abs. 1 BDSG zur Bestellpflicht eines bDSB.

Die Erklärung macht deutlich, dass auch mit der Grundverordnung noch lange keine Klarheit über die 2018 eintretende Rechtslage und die zu erwartenden Auswirkungen für Unternehmen besteht.

Secorvo News

Zertifikat für Experten

Wir können Ihnen noch einige wenige freie Plätze auf dem kommenden T.I.S.P.-Seminar vom **06. bis 10.06.2016** anbieten. Mit Ihrer Anmeldung erhalten Sie das T.I.S.P.-Begleitbuch zur Vorbereitung. Die nächste Gelegenheit zur Zertifizierung bieten wir dann erst wieder im November – der frühe Vogel bekommt den Platz …

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Auslaufmodell Datenschutz?

Zum Abschluss der Ausstellung "Global Control and Censorship“ lädt die KA-IT-Si zusammen mit dem ZKM | Karlsruhe, KASTEL und dem CyberForum e.V. am **Freitag, 29. April 2016 ab 16 Uhr** zur größten Anti-Prism-Party Europas (4. Staffel) ins ZKM (Eintritt frei). Experten zeigen in Live-Vorführungen und an Beratungsständen, wie Sie sich vor Ausspähungen im Internet schützen können; begleitet von Führungen durch die Ausstellung. Derweil können sich Ihre Kinder in der Spion-Schule der Pädagogischen Hochschule Karlsruhe zum Verschlüsselungsexperten ausbilden lassen.

Gibt es überhaupt Chancen, der allgegenwärtigen Überwachung zu entgehen? Ist das Konzept „Datenschutz“ gar ein Auslaufmodell? Diese Fragen möchten wir um **18:30 Uhr** im Medientheater des ZKM mit Ihnen und dem Datenschutz-Aktivisten Malte Spitz in einer Publikumsdiskussion erörtern.

Programm: https://www.anti-prism-party.de

Save the date - 8. Tag der IT-Sicherheit

Auf dem „Tag der IT-Sicherheit“, einer Veranstaltung von KA-IT-Si, IHK Karlsruhe und CyberForum, zeigen wir einmal jährlich aktuelle IT-Sicherheitsbedrohungen für Unternehmen auf und informieren über Präventionsmöglichkeiten. Unser diesjähriger *Keynote Speaker* ist Tobias Schrödel, IT-Sicherheitsexperte und erster Comedyhacker. Das Programm finden Sie auf unserer Webseite. Merken Sie sich den **22.06.2016, 14 Uhr** schon jetzt in Ihrem Terminkalender vor.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

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

Mai 2016	
08.-12.05.	Eurocrypt 2016 (IACR, Sofia/BG)
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)
Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.06.	IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten (Fachgruppe SECMGT der GI, Frankfurt)
10.-11.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
13.-14.06.	DuD 2016 (Computas, Berlin)
15.-17.06.	Entwicklertag 2016 (VKSI, GI, ObjektForum, Karlsruhe)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)
27.06.-01.07.	OWASP AppSec EU 2016 (OWASP Foundation, Rom/I)
Juli 2016	
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Dr. Volker Hammer, Kai Jendrian, Michael Knopp, Christoph Schäfer, 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