secorvo
security consulting

Secorvo Security News

März 2013

Cyber-Hype

Die IT-Sicherheit – pardon: Cyber-Sicherheit – ist *en vogue*. Kein Tag ohne spektakuläre Nachricht, keine Woche ohne Sicherheitsupdate. Sei es aus Überzeugung oder aus dem unverdrängbaren Bedürfnis, dem medialen Dauerbeschuss sichtbare Maßnahmen entgegenzusetzen, hat sich auch die Politik des Themas angenommen.

Wie bei vielen Hypes gehört es ab einem gewissen Punkt der unermüdlichen Wiederholung (siehe Catos „Ceterum censeo Carthaginem esse delendam!“) zum guten Ton, bei diesem Thema etwas vorweisen zu können. Mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen vom Juni 2005 richtete das BMI unter anderem ein Nationales IT-Lagezentrum im BSI ein – eine begrüßenswerte Einrichtung, sorgte sie doch dafür, dass die mit IT-Sicherheitsfragen befassten Behörden ihre Erkenntnisse austauschten und Aktivitäten koordinierten. Eine größere Schlagkraft bei reduziertem Aufwand wäre zu erwarten gewesen – aber der Hype nahm gerade erst Anlauf. Mit der Cyber-Sicherheitsstrategie des BMI vom Februar 2011 wurde die Zuständigkeit des BSI auf kritische Infrastrukturen ausgedehnt. Nun legt das BMI nach: Der Referentenentwurf zu einem „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ vom 05.03.2013 sieht neben einer Pflicht von Betreibern kritischer Infrastrukturen zur Auditierung und Meldung von Vorfällen die Schaffung von 100 Cyber-Sicherheits-Planstellen beim BSI vor. Da will der Bundesnachrichtendienst nicht zurückstehen: am 24.03.2013 wurde bekannt, dass der Aufbau einer Abteilung zur „Abwehr von Cyberangriffen“ mit bis zu 130 IT-Sicherheitsspezialisten geplant ist.

Bei allem Respekt vor der Wichtigkeit des Themas und dem Engagement der Beteiligten: Ab einem gewissen Punkt erzeugt die behördliche Beschäftigung mit Cyber-Sicherheit mehr Kosten als Nutzen. Denn jeder der knappen Spezialisten fehlt in den Unternehmen, und die Planstellen wollen erst verdient sein. Wirtschaftsminister Günter Rexrodt brachte es Mitte der 90er Jahre auf den Punkt: „Die Wirtschaft findet in der Wirtschaft statt.“ Und da gehört sie auch hin.

Inhalt

secorvo
security consulting

Security News

TLS Workarounds

Eine häufig empfohlene Übergangslösung zum Schutz gegen die in den SSN 02/2013 erwähnten BEAST- und Lucky 13-Angriffe gegen SSL/TLS ist, ältere Cipher Suites auf Basis der RC4-Chiffre zu nutzen – stets mit etwas schlechtem Gewissen, da RC4 in der Vergangenheit bereits Schwächen, bspw. in WEP, gezeigt hatte.

Wie berechtigt solche Skepsis war, erwies sich am 13.03.2013, als das „Lucky 13"-Forscherteam, verstärkt um Dan Bernstein, seine neuesten Erkenntnisse zu RC4 in TLS publizierte und nunmehr von dessen Gebrauch abrät. Damit gehen langsam die Übergangslösungen aus – der Umstieg auf TLS 1.2 mit AES-GCM-basierten Cipher Suites ist damit noch dringlicher als in den letzten SSN dargestellt.

Aus bester Quelle

Dass Code-Signaturen nicht die Abwesenheit von Schadcode sicher stellen, sondern – bestenfalls – die Herkunft der betreffenden Software, sollte mittlerweile Allgemeinwissen sein.

Und nicht immer müssen Malware-Autoren fremde Code-Signing-Schlüssel kompromittieren, um auch noch diese Spuren zu verwischen: Am 04.02.2013 wurde gemeldet, dass Malware-Autoren eine brasilianische Briefkastenfirma nutzten, um ein offizielles Code-Signing-Zertifikat zu kaufen, und am 21.02.2013 wurde bekannt, dass dazu auch die Daten einer nicht mehr existierenden französischen Autohandelsfirma reichen. Freiwillige haben im Netz inzwischen Informationen über mehr als Hundert zum Signieren von Malware genutzter Code-Signing-Zertifikate zusammengetragen. Und am 06.03.2013 berichtete Brian Krebs über den schwunghaften Handel mit Android-Entwickler-Accounts, unter deren Registrierung Malware-Apps im Google Play Store eingestellt werden können.

Es scheint leider so, als ob Mechanismen zur Sicherstellung der Herkunft von Software nur gegen Malware-Autoren helfen, die zu klamm sind, um sich bei Bedarf ein offizielles Zertifikat oder eine Registrierung zu kaufen – und nicht wissen, wie man mit fremden Kreditkartendaten bezahlt.

Hacker leben gefährlich

Am 15.03.2013 wurde das vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallin (Estland) bei einer internationalen Expertengruppe in Auftrag gegebene Tallin Manual on the International Law Applicable To Cyber Warfare in London der Öffentlichkeit vorgestellt. Das 270 Seiten starke Dokument ist das Ergebnis einer dreijährigen Untersuchung der Anwendbarkeit internationalen Rechts im Falle eines „Cyberkriegs".

Die 20 Autoren stellen 95 Regeln (*black letter rules*) auf, an denen sich die NATO-Staaten im Falle eines Cyberkriegs halten sollen. So sind grundsätzlich – wie auch in einem konventionellen Krieg – die Auswirkungen auf die Zivilbevölkerung zu begrenzen. Das gilt allerdings nicht für „Hacktivisten", die im Rahmen der Auseinandersetzung zu Angriffszielen werden können: "*Individuals who directly participate in hostilities lose their protection from attack*" (Rule 35). Dabei werden unter ‚Mitwirkung' auch vorbereitende Tätigkeiten verstanden, wie „*identifying vulnerabilities in a targeted system or designing malware in order to take advantage of particular vulnerabilities*" (S. 120).

Das sind keine besonders ermutigenden Aussichten für Schwachstellenfinder. Und man muss kein Hellseher sein, um zu erraten, gegen wen sich wohl ein „Cyber-Präventivschlag" richten dürfte.

Harmlose Bestandsdaten

Der Gesetzentwurf der Bundesregierung zur Änderung des Telekommunikationsgesetzes (TKG) und zur Neuregelung der Bestandsdatenauskunft vom 09.01.2013 hat am 21.03.2013 den Bundestag passiert. Eine Neufassung war notwendig geworden, da das Bundesverfassungsgericht mit Beschluss vom 24.01.2012 die entsprechende Regelung im TKG aufgrund einer Verfassungsbeschwerde von Patrick Breyer (auch bekannt durch sein Engagement im Arbeitskreis Vorratsdatenspeicherung) für verfassungswidrig erklärt hatte.

Tatsächlich bewegt sich die Neuregelung auf dünnem Eis, auch wenn im Bundesrat wenig Widerstand zu erwarten ist. Denn die Bestandsdatenauskunft unterliegt weit geringeren Hürden als eine Verkehrsdatenauskunft, welche ein Ermittlungsverfahren wegen einer schweren Straftat (§ 100a StPO) voraussetzt: bei Bestandsdaten genügt eine Ordnungswidrigkeit.

Mit der Neufassung werden jedoch einige bislang allgemein als Verkehrsdaten verstandene Daten – wie bspw. die dynamische IP-Adresse – zum Bestandsdatum umdefiniert und damit der hohen Zugangshürde entzogen.

Passiert das Gesetz den Bundesrat, will Patrick Breyer erneut vor das Bundesverfassungsgericht ziehen. Bleibt zu hoffen, dass die Verfassungsrichter sich vom TKG-Neusprech nicht blenden lassen.

Datenschutzzertifikat

Nach längerer Pause wird dem De-Mail-Projekt der Bundesregierung neue Aufmerksamkeit zuteil. So hat der Bundesbeauftragte für den Datenschutz am 04.03.2013 die De-Mail-Datenschutz-Zertifizierung von 1&1 bekannt gegeben, drei Tage nach Herausgabe einer Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten mittels De-Mail. Und seit dem 05.03.2013 liegt ein neuer Referentenentwurf zu einem E-Government-Gesetz vor, das De-Mail als Kommunikationsmittel der Verwaltung in einer prominenten Rolle sieht.

Da die gesetzliche Regelung eines Datenschutzaudits nach § 9a BDSG seit nunmehr 12 Jahren vergeblich auf Umsetzung wartet, wurde die Datenschutzzertifizierung der De-Mail-Diensteanbieter in § 18 Abs. 3 Nr. 4 De-Mail-Gesetz direkt dem Bundesbeauftragten für den Datenschutz zugewiesen. Der Kriterienkatalog der Zertifizierung geht erstaunlich weit in die Prüfung der datenschutzunabhängigen Anforderungen des De-Mail-Gesetzes. Von besonderem Interesse sind die Festlegung einer Löschfrist von sieben Tagen für die Speicherung der IP-Adressen der Nutzer zu Sicherheitszwecken, die Ausführungen zur datenschutzgerechten Helpdesk-Gestaltung und die Forderung nach Negativfeststellungen in der Datenschutzerklärung der Diensteanbieter.

Die Handreichung zum Gebrauch von De-Mail enthält wertvolle Hinweise zur Durchführung einer Schutzbedarfsanalyse für personenbezogene Daten, während die Frage, wann zusätzlich zur De-Mail-Verwendung eine Ende-zu-Ende-Verschlüsselung erforderlich ist, mangels De-Mail-Nutzer wohl vorerst eher akademischer Natur bleibt.

Das E-Government-Gesetz will zudem ermöglichen, die De-Mail neben der qualifizierten elektronischen Signatur zur Ersetzung der Schriftform einzusetzen. Ob dies der De-Mail zum erhofften Durchbruch verhelfen kann, darf bezweifelt werden. Schließlich ist De-Mail ein Übermittlungs- und Zustellungsverfahren – zur Ersetzung der Schriftform wurde De-Mail nicht konzipiert.

AppSec News

Das deutsche OWASP Chapter richtet in diesem Jahr in Hamburg vom 20.-23.08.2013 die Sicherheitskonferenz AppSec Research 2013 aus. Die ersten zwei Tage sind Trainingseinheiten zur Sicherheit von (Web-)Anwendungen gewidmet, die beiden folgenden Konferenztage in einen akademischen und einen industriellen Track strukturiert.

Für beide Tracks sind Einreichungen (Industry bis 14.04. und Research bis 15.05.2013) willkommen. Ein zusätzliches Bon-Bon ist die Vergabe freier Tickets für die Konferenz im Rahmen einer monatlichen Ticket-Challenge – in der eine versteckte Schwachstelle zu finden und ein Exploit einzureichen ist.

Secorvo News

Internet bleibt zertifiziert

In den SSN 04/2010 berichteten wir über die erfolgreiche Erstzertifizierung des DE-CIX nach ISO 27001 auf der Basis von IT-Grundschutz.

Drei Jahre später zahlte sich das kontinuierliche und konsequente Management der Informationssicherheit beim DE-CIX aus: Die Re-Zertifizierung wurde erfolgreich bestanden und das Zertifikat mit der Nummer BSI-IGZ-0139-2103 ausgestellt – damit wird Internet-Traffic mit Peaks von 2,5 TBit/s weiterhin zertifiziert sicher übertragen.

Alle Beteiligten konnten bestätigen, dass sich die Qualität des ISMS in den vergangenen drei Jahren noch einmal deutlich verbessert hat, während die Aufwände spürbar reduziert werden konnten. Der Security Officer des DE-CIX dazu: „Viele reden von integraler Sicherheit. Die Zertifizierung hat beim DE-CIX dafür gesorgt, dass wir sie konsequent leben."

Frühjahrsbildung

Noch sind einige wenige Plätze unserer drei April-Seminare zu haben: IT-Sicherheit heute vom 09.-11.04.2013, der T.I.S.P. vom 15.-19.04.2013 und PKI vom 23.-26.04.2013.

Zertifikate, die erworbene Fachkenntnisse und Berufserfahrung in der IT-Sicherheit nachweisen, gewinnen immer mehr an Bedeutung. Daher bieten wir inzwischen drei Zertifizierungen an, von deren Qualität wir überzeugt sind:

Der T.I.S.P. steht für mehrjährige Berufserfahrung und fundiertes Grundlagen- und Expertenwissen in den wichtigsten Themengebieten der Informationssicherheit. Der CPSSE belegt vertiefte Kenntnisse in der Entwicklung von Softwarelösungen mit definierten Sicherheitseigenschaften – durch eine geeignete Gestaltung des gesamten Softwareentwicklungsprozesses. Der T.E.S.S. weist Kenntnisse in „Security by Design" nach – der Integration von Sicherheit in den gesamten Produktentwicklungsprozess, von der Idee über die Konzeption bis zur Realisierung in Hard- oder Software.

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

Veranstaltungshinweise

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

April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
16.-17.04.	Datenschutztage 2013 (FFD, Wiesbaden)
17.-18.04.	a-i3/BSI Symposium 2013 (a-i3/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	BvD Verbandstag 2013 (BvD e.V., Berlin)
Mai 2013	
14.-16.05	13. Deutscher IT-Sicherheitskongress (BSI, Bonn)
15.05.	Cloud – aber sicher! (KA-IT-Si, Karlsruhe)
15.-16.05.	14. Datenschutzkongress (EUROFORUM, Berlin)
26.-30.05.	Eurocrypt 2013 (IACR, Athen/GR)
Juni 2013	
03.-07.06.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
05.-07.06.	Entwicklertag 2013 (VKSI & ObjektForum, Karlsruhe)
10.-11.06.	Cybersecurity 2013 (Handelsblatt & EUROFORUM, Berlin)

Fundsache

Die NSA, deren Akronym lange mit „No Such Agency“ übersetzt wurde, hat die interne Zeitschrift „Cryptolog“ („*a new vehicle for the interchange of ideas on technical subjects in Operations*“) deklassifiziert und am 24.03.2013 die Ausgaben 1/1974 bis 4/1997 als pdf veröffentlicht. Auch wenn einige Stellen geschwärzt wurden: der Schülerzeitungscharme vor allem der frühen Ausgaben ließ sich nicht wegretuschieren.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, 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