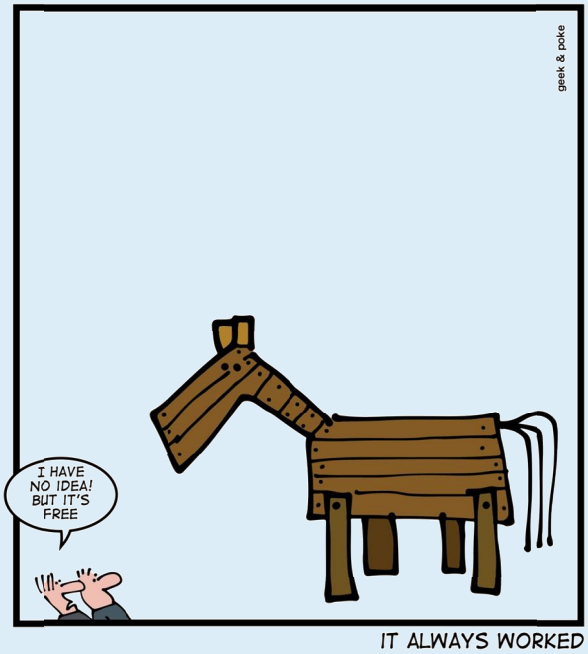
Secorvo Security News

Dezember 2013

Auf den Punkt

Robert Musils „Der Mann ohne Eigenschaften" ist ein Meilenstein der deutschsprachigen Literatur des 20. Jahrhunderts. Allerdings dürfte selbst der eine oder andere Literaturbegeisterte vor den über 1.000 Seiten des unvollendeten Werks zurückschrecken. Nun hat am 11.11.2013 der begnadete Zeichner Nicolas Mahler eine auf 150 Seiten verdichtete Fassung von Musils Hauptwerk publiziert: als Comic.

„Manche Menschen nutzen ihre Intelligenz zum Vereinfachen, manche zum Komplizieren", wusste schon Erich Kästner. Ersteres ist mir sympathischer – denn oft legt eine kompromisslose Verkürzung eine Kernaussage in aller Klarheit bloß. Daher habe ich für diese News das bereits verfasste Editorial durch einen Cartoon von „Geek & Poke" ersetzt, den wir mit freundlicher Genehmigung des ebenfalls begnadeten, aber (zu Unrecht) weniger bekannten Hamburger Zeichners Oliver Widder hier wiedergeben. Schöne Weihnachten.



Inhalt

Auf den Punkt

Security News

PCI DSS 3.0

Mangel an Beweisen

Bundesrat bremst EU-Verordnung

Sicherheit für ICS

Volatility goes CybOX

GroKo und die Sicherheit

GroKo und der Datenschutz

Secorvo News

Zertifikate helfen

Anti-Prism-Party 2. Staffel

Veranstaltungshinweise

Fundsache

secorvo
security consulting

Security News

PCI DSS 3.0

Das PCI *Security Standards Council* hat am 07.11.2013 die Version 3.0 des in der Finanzwelt verbreiteten Zertifizierungs-Standards zum Schutz von Konto- und Kreditkartendaten PCI DSS veröffentlicht. Der neue Standard tritt am 01.01.2014 in Kraft, während der Version 2.0 noch eine Übergangsfrist bis zum 31.12.2014 eingeräumt wird. Einige Anforderungsänderungen, die bei betroffenen Unternehmen ggf. hohe Aufwände erzeugen, bleiben bis zum 01.07.2015 erst einmal *Best Practices* und werden erst danach verbindlich. Unterstützende Arbeitshilfen werden Anfang 2014 bereitgestellt.

Eine Übersicht über die Änderungen von der Version 2.0 auf 3.0 findet sich in den Dokumenten des PCI SSC „Summary of Changes" und „Version 3.0 Change Highlights". Viele der Änderungen in den 112 Seiten des Standards betreffen Klarstellungen und Anpassungen von Anforderungen an den Stand der Technik. Bahnbrechende neue Anforderungen sind nicht enthalten – allerdings werden einige *Best Practices* wie Requirement 8.5.1 „... *use unique authentication credentials for each customer*" festgeschrieben. Für alle, die mit Version 2.0 des PCI DSS vertraut sind, bietet es sich an, die Änderungsdokumente durchzuarbeiten; Neueinsteiger sollten sich gleich mit der Version 3.0 auseinandersetzen.

Mangel an Beweisen

Vor dem Landesarbeitsgericht Hamm ist das Land Nordrhein-Westfalen mit der fristlosen Kündigung zweier IT-Mitarbeiter wegen urheberrechtswidrigen Filesharings auf dienstlichen Rechnern gescheitert. Kern der Begründung des Gerichts im Urteil vom 06.12.2013 sind Mängel in der Beweisführung. So wurden die Rechner, auf denen (nach einer Abmahnung an die Adresse einer Kreispolizeibehörde wegen des illegalen Downloads eines Musikstücks) verschiedene Musiktitel und Filme gefunden worden waren, nicht zügig sichergestellt. Schlimmer noch: Auf den von den beiden gekündigten Mitarbeitern überwiegend genutzten Rechnern gab es keine personalisierten Nutzer-Accounts.

Das Urteil unterstreicht einmal mehr die Notwendigkeit, ausschließlich mit personalisierten Nutzer-Accounts zu arbeiten und feste Prozesse für Störungen oder Richtlinienverstöße festzulegen, damit im Falle eines Vorfalls eine forensische Beweisführung möglich wird.

Bundesrat bremst EU-Verordnung

Der Bundesrat hat in einer Stellungnahme vom 29.11.2013 erhebliche Bedenken gegen den Entwurf einer europäischen Verordnung über Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation geltend gemacht. Die Bedenken richten sich zunächst grundsätzlich gegen den Erlass einer weiteren direkt geltenden Verordnung, die Teile des Telekommunikationsgesetzes ersetzen und hinter dem Schutz- und Regelungsniveau des deutschen Rechts zurückbleiben würde. Kritisiert wird auch die Vielzahl unbestimmter Rechtsbegriffe und fehlender Definitionen. Davon betroffen sind insbesondere die telekommunikationsspezifischen Regelungen zum Datenschutz.

Insgesamt hat der Bundesrat eine Reihe von begründeten Bedenken zusammengetragen, die hoffentlich bei der weiteren Entwicklung der europäischen Gesetzgebungsvorhaben berücksichtigt werden.

Sicherheit für ICS

In der Welt der industriellen Steuerungen (ICS) bewegt sich etwas, wie das BSI ICS-Security Kompendium (vgl. Fundsache SSN 11/2013) und der von der Enisa am 04.12.2013 veröffentlichte Good Practice Guide zur Etablierung von CERT-Strukturen im ICS-Umfeld zeigen. Der Paradigmenwechsel, dass industrielle Steuerungen keine eigene Welt mit eigenen Gesetzmäßigkeiten bilden, sondern als Teil der gesamten IT-Infrastruktur betrachtet werden müssen, kann – Stuxnet sei dank – offenbar als vollzogen betrachtet werden.

Auch bei den Herstellern werden inzwischen Schwachstellen bei früher als „Non-IT" betrachteten Komponenten via Patch geschlossen, wie das am 04.12.2013 veröffentlichte Beispiel von Siemens' Servoantrieben zeigt: Die offenen netzwerkseitigen Zugangswege wurden durch ein Firmware-Update beseitigt. Schwachstellen werden inzwischen durchaus ernst genommen – und zügig abgestellt.

Zu beachten ist allerdings, dass bei der Planung des Betriebs von Steuerungen zukünftig auch die Aufwände für die Beobachtung von Schwachstellen, die Beurteilung der Relevanz von Updates und die Aktualisierung von Komponenten eingeplant werden.

Volatility goes CybOX

Für das freie Forensic-Tool Volatility ist seit dem 05.09.2013 das Plugin CybOXer verfügbar, das die Spezifikation Cyber Observable eXpression (CybOX) (eine Hersteller unabhängige Beschreibungssprache für Hinweise auf Schadsoftware-Muster) von MITRE unterstützt. Damit kann während der Analyse automatisiert auf einzelne oder ganze Gruppen von Indicators of Compromise (IoC) geprüft werden.

Ca. 110 öffentliche IoCs kann man u. a. von IOC Bucket beziehen; allerdings gehen bei der Script-Konvertierung in das CybOX-XML-Format ca. 10 % der IoCs aufgrund der Verwendung von nicht standardisierten Elementen verloren. So ist eine händische Nachbearbeitung unvermeidlich; anschließend aber läuft die Massenanalyse komfortabel, stabil und flott.

GroKo und die Sicherheit

Der Koalitionsvertrag von Union und SPD vom 27.11.2013 sieht die Einführung eines IT-Sicherheitsgesetzes mit verbindlichen Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen vor. Unter anderem soll eine Meldepflicht für erhebliche IT-Sicherheitsvorfälle eingeführt werden.

Zum Schutz vor Spionage soll ein rechtlich verbindliches Abkommen verhandelt werden, um Bürger, Regierung und Wirtschaft vor schrankenloser Ausspähung zu schützen – keine ganz überraschende Forderung in einem demokratischen Rechtsstaat. Die europäischen Telekommunikationsanbieter sollen verpflichtet werden, ihre Kommunikationsverbindungen mindestens innerhalb der EU zu verschlüsseln und keine Daten direkt an ausländische Nachrichtendienste weiterzuleiten. Immerhin.

GroKo und der Datenschutz

Der Begriff „Datenschutz“ findet sich an 35 Stellen im Koalitionsvertrag – das Thema hat Konjunktur. Allerdings bleiben die Vereinbarungen der Großen Koalition vage: Die EU-Datenschutzgrundverordnung soll zügig verabschiedet werden; dabei soll das deutsche Datenschutzniveau im Zweifel höher bleiben – wie das bei einer vereinheitlichenden Rechtsetzung einer EU-Verordnung funktionieren kann, wird nicht erläutert.

Sollte die Verordnung nicht rechtzeitig kommen, ist geplant, das Beschäftigtendatenschutzgesetz wieder auszugraben. Zum Ausgleich – da nun Sabine Leutheusser-Schnarrenberger als Justizministerin nicht mehr im Weg steht – soll, allen NSA-Affären zum Trotz, die Vorratsdatenspeicherung nach den Vorgaben der EG-Richtlinie kommen. Die ungeliebte ‚Stiftung Datenschutz' soll in die Stiftung Warentest integriert werden – wie (und zu welchem Zweck) auch immer. Schließlich soll in der EU auf Nachverhandlungen der Swift- und Safe-Harbour-Abkommen gedrängt werden – eine Idee, auf die die EU unlängst selbst gekommen ist. Bleibt zu hoffen, dass dem Datenschutz in den kommenden vier Jahren eine ebenso große Aufmerksamkeit zuteil wird wie im Koalitionsvertrag.

Secorvo News

Zertifikate helfen

Im Jahr 2013 Jahr wurde das 600ste T.I.S.P.-Zertifikat ausgestellt. Damit ist der T.I.S.P. auf dem besten Weg, zum bedeutendsten berufsqualifizierenden Nachweis für IT-Sicherheitsexperten in Deutschland zu werden. Die einwöchige T.I.S.P.-Schulung vermittelt einen vertieften Einblick in alle Gebiete der Informationssicherheit und hilft, verbliebene Wissenslücken zu schließen. Die nächsten Möglichkeiten, bei Secorvo ein T.I.S.P.-Zertifikat zu erhalten, bietem sich am 24.-28.03.2014 und am 19.-23.05.2015. Auf dem Seminar erleben Sie die Autoren des T.I.S.P.-Lehrbuchs „Zentrale Bausteine der Informationssicherheit“ live.

Für den Fall, dass Sie sich „nur“ beim Thema Informationssicherheit auf den aktuellen Stand bringen wollen, ist das Seminar IT-Sicherheit heute am 08.-10.04.2014 das Richtige für Sie. Alle Termine und Seminarangebote sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college

Anti-Prism-Party 2. Staffel

Die Vorbereitungen zur 2. Staffel der erfolgreichen Anti-Prism-Party am **12.02.2014** im Karlsruher ZKM ist in vollem Gange. Für Schüler und Auszubildende führen wir zwischen 10 und 16 Uhr zweistündige Sonderveranstaltungen durch, die sich aus einer Führung durch das Kryptologikum, einem ‚Security Kino' und Live-Demonstrationen zu verschiedenen Themen zusammensetzen. Aktuelle Informationen zur Anti-Prism-Party gibt es in einem eigenen Newsletter und auf Twitter.

Veranstaltungshinweise

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

Dezember 2013	
27.-30.12.	30th Chaos Communication Congress (30C3) (Chaos Computer Club, Hamburg)
Januar 2014	
17.-19.01.	ShmooCon 2014 (The Shmoo Group, Washington/US)
21.-23.01.	Omnicard 2014 (in TIME berlin, Berlin)
Februar 2014	
04.-06.02.	Cloudzone 2014 (Karlsruher Messe- und Kongress-GmbH, Karlsruhe)
05.-06.02.	24. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
12.02.	Anti-Prism-Party 2. Staffel (KA-IT-Si, Karlsruhe)
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 (Secorvo College, Karlsruhe)

Fundsache

Matthew Green von der Johns Hopkins University (Baltimore/US) publizierte am 02.12.2013 in seinem Blog zu *Cryptography Engineering* eine lesenswerte Analyse der wahrscheinlichen Möglichkeiten der NSA, auf SSL/TLS-geschützte Kommunikation zuzugreifen. Als sicher darf gelten: dank der Stärke des kryptographischen Protokolls muss sie sich verschiedener Tricks bedienen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, 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