secorvo
security consulting

Secorvo Security News

August 2016

Digitalisierung 5.0

Die Welt wird digital. Das ist nicht neu – auch wenn es einige Menschen erst jetzt zu bemerken scheinen. Rechner bestimmen schon seit Jahrzehnten unser Leben, und vieles bekämen wir ohne sie nicht mehr hin. Vielleicht bewundern wir deshalb Michelangelos David oder Leonardos Mona Lisa, obwohl jeder mit 3D-Drucker und Smartphone selbst perfekte Abbilder der Wirklichkeit erzeugen kann.

Vor einigen Jahren hat jedoch eine neue Phase begonnen, die weit über das „Internet der Dinge“ und „Industrie 4.0“ hinausweist. Ich will sie „Digitalisierung 5.0“ nennen. Es ist eine Phase der Selbstbezüglichkeit: Computer beginnen, sich selbst zu gestalten. Und es ist die IT-Sicherheit, die diese Entwicklung befeuert. So akzeptieren wir (wenn auch nicht immer klaglos), dass unsere Rechner sich via Virenscanner ständig selbst untersuchen, eigenständig die Signaturdatenbank aktualisieren und unsere E-Mails von Spam befreien. Programm- und Betriebssystem-Updates erfolgen inzwischen ohne Freigabe der Benutzer, die Suche nach Programmfehlern übernehmen automatisierte Prozesse und Tools – nicht nur bei Softwareentwicklern, sondern auch als Cloud-Service. Längst arbeiten Angreifer mit Systemen, die systematisch Exploits durchprobieren, kombinieren – und die Zielsysteme sogar auf noch unbekannte Schwachstellen abklopfen. Die Antwort heißt IDS oder SIEM: die automatische Analyse von Netzverkehr und Log-Dateien auf Angriffsspuren.

Nicht mehr lange, und unsere Rechner nehmen sich in Quarantäne, säubern sich gegenseitig von Schadsoftware und setzen sich neu auf. Sie werden ihre Erfahrungen anderen Rechnern über Wissensdatenbanken zugänglich machen, ihre Leistungen womöglich in selbst „geschürften“ Bitcoin bezahlen und die robustesten Kollegen zu Entscheidern wählen. Nutzen könnte man sie wahrscheinlich nicht mehr – wozu aber auch: Schließlich brauchen die Rechner uns, damit wir gelegentlich defekte Festplatten ersetzen oder das RAM erweitern.

Inhalt

secorvo
security consulting

Security News

Abgehörte Tastaturen

In ihrer Veröffentlichung zum KeySniffer-Hack vom 27.07.2016 zeigen die Forscher von Bastille, was sich mit Angriffen wie MouseJack und Keysweeper bereits abzeichnete: Zahlreiche kabellose Tastaturen und Mäuse bekannter Hersteller wie HP oder Toshiba aber auch Logitech und Microsoft sind für das Abhören oder die Injektion von Tastatureingaben anfällig. Angreifer können so an Passwörter oder Kreditkartennummern gelangen oder sogar das Zielsystem übernehmen.

Die Schwachstelle liegt bei den Herstellern der betroffenen Geräte, die eigene Übertragungsprotokolle und Sicherheitsmechanismen entwickelten anstatt auf bewährte Standards zu setzen. Mit einer Behebung der Schwachstelle ist eher nicht zu rechnen, da ein Einspielen neuer Firmware in die Dongles und Eingabegeräte nicht möglich ist oder der Aufwand von den Herstellern als zu hoch eingeschätzt wird.

Grundsätzlich sind kabelgebundene Tastaturen und Mäuse kabellosen Geräten vorzuziehen. Muss es dennoch eine kabellose Variante sein, so sollte man auf den Bluetooth-Standard setzen, der ein sicheres Kommunikationsprotokoll verwendet, das Authentifikation und Verschlüsselung umfasst.

Leitfaden zum EU-U.S. Privacy Shield

Seit dem 01.08.2016 liegt der EU-U.S. Privacy Shield als Garantie angemessenen Datenschutzes für U.S.-Unternehmen vor. Begleitend hat die EU-Kommission einen Leitfaden für Betroffene zu den Rechten aus den Privacy Shield Principles veröffentlicht.

Darin werden die Verpflichtungen von Privacy-Shield-Unternehmen, die diesbezüglichen Betroffenenrechte, die Beschwerderechte, die möglichen Adressaten sowie der für den gesamten EU-U.S.-Datenverkehr anwendbare Ombudsmann-Mechanismus ausführlich erläutert.

Eine Beschwerde kann an die verarbeitende U.S.-Gesellschaft, an eine von dieser einzusetzenden unabhängigen Beschwerdestelle und an die nationale Aufsichtsbehörde beim Department of Commerce oder der Federal Trade Commission gerichtet werden. Arbeitnehmer können sich stets an die nationale Aufsichtsbehörde wenden.

Scheitert eine Beschwerde, kann ein Schiedsverfahren verlangt werden. Dieses findet in den USA statt. Es besteht aber ein Recht auf Hilfestellung durch die nationale Aufsichtsbehörde, die Möglichkeit, per Videokonferenz teilzunehmen und ein Recht auf kostenlose Übersetzungen. Die Kosten werden von einem Fonds getragen.

Der vorerst nur in englischer Sprache verfügbare Leitfaden bietet datenschutzkundigen Betroffenen eine gelungene Übersicht über die grundsätzlichen Möglichkeiten. Er dokumentiert aber auch, dass der praktische Nutzen des Privacy Shields für einen einzelnen Betroffenen nur sehr schwer realisierbar sein dürfte.

IT-Grundschutz-Modernisierung

Am 08.08.2016 hat das BSI den Entwurf für einen modernisierten Baustein der IT-Grundschutzkataloge veröffentlicht. Ein weiterer Baustein folgte am 09.08.2016. Die wesentliche Neuerung ist, dass bei den modernisierten Bausteinen deutlich zwischen einem Anforderungsteil und sogenannten Umsetzungshinweisen unterschieden wird. Letztere weisen einen höheren Detaillierungsgrad auf als die eigentlichen Bausteine und ähneln den bisherigen Katalogen, stellen jedoch nur noch eine Möglichkeit zur Umsetzung dar.

Die neuen Bausteine stellen nun in kompakter Form die Vorgaben zusammen. Auf eine umfassende Gefährdungsdarstellung wurde verzichtet; die wesentlichen Maßnahmen, die aus Grundschutz-Sicht umgesetzt werden müssen, sind übersichtlich auf wenigen Seiten aufgeführt. Aus unserer Sicht eine deutliche Flexibilisierung und der richtige Weg, um die Umsetzung von IT-Grundschutz in der Praxis handhabbarer zu machen.

Vorratsdatenspeicherung revisited

Der Generalanwalt am Europäischen Gerichtshof hat am 19.07.2016 seine Schlussanträge in zwei verbundenen Rechtssachen zu nationalen Vorratsdatenspeicherungsregelungen gestellt.

Bereits 2014 hat der EuGH im Verfahren Digital Rights Ireland Ltd die Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt. Die deutsche Umsetzung in § 113a ff. TKG a.F. war zuvor schon vom Bundesverfassungsgericht für verfassungswidrig erklärt worden (seit Dezember 2015 ist eine bis 2017 umzusetzende Nachfolgeregelung in Kraft).

In seinen Schlussanträgen leitet der Generalanwalt aus der Grundrechtscharta der Europäischen Union strenge Anforderungen an nationale Pflichten zur Vorratsdatenspeicherung ab. Sie dürfe nur der Bekämpfung schwerer Kriminalität dienen und müsse hierfür absolut notwendig sein. Die Anforderungen an den Schutz der Daten des vorausgegangenen Urteils müssten erfüllt und die mit der Vorratsdatenspeicherung verbundenen Gefahren dürften nicht unverhältnismäßig zu ihrem Nutzen sein.

Sollte der EuGH dem Antrag folgen, bleibt eine verfassungsgemäße Vorratsdatenspeicherung möglich. Der Nachweis der Verhältnismäßigkeit vor nationalen Gerichten wird aber angesichts vorliegender Studien schwierig. Den Vorschlägen des deutschen Innenministeriums, die Vorratsdatenspeicherung zu reanimieren und auf Telemedien auszudehnen, dürfte das Urteil jedoch einen Dämpfer setzen.

BSI-Zertifizierung nach TR

Mit der ISO 27001-Zertifizierung auf Basis von IT-Grundschutz darf man die am 12.08.2016 vorgestellte Zertifizierung nach TR in Verbindung mit ISO 27001 nicht verwechseln: Hier geht es, aufbauend auf einer ISMS-Zertifizierung nach ISO 27001, um die Zertifizierung konkreter, in den Technischen Richtlinien (TR) des BSI definierten Maßnahmen für ganz bestimmte Einsatzzwecke. In Vorbereitung ist derzeit eine Zertifizierung nach TR-03108 Secure E-Mail Transport für E-Mail-Provider.

Wir haben Ihren PC aktualisiert

Seit dem 02.08.2016 verteilt Microsoft das drei Gigabyte große Anniversary Update, mit dem die Strategie des „Windows as a Service" fortgesetzt wird: Jeder Windows-Nutzer soll stets die aktuellste Version des Betriebssystems verwenden – Apple lässt grüßen. Home-User können diesen „Service" nicht verweigern.

Neben einigen optischen und funktionalen Anpassungen sowie dem nachhaltigen Aushebeln von Secure Boot, holt das Thema Datenschutz mal wieder Microsoft ein (vgl. SSN 8/2015). Die US-Bürgerrechtsorganisation EFF sowie die französische Datenschutzaufsicht CNIL kritisieren Microsoft deutlich. Im Zentrum steht das Windows-Assistenzsystem Cortana, das nun zur Standardsuche in Windows 10 wird – bislang konnte man es deaktivieren. Cortana ist sehr kommunikativ: Es überträgt zahlreiche persönliche Informationen an Microsoft, darunter den Standort, Text-, Sprach- und Touch-Eingaben, Webseitenbesuche sowie Nutzungsstatistiken. Details zu den übertragenen Telemetriedaten sind bisher nicht bekannt. Firmenkunden können Cortana immerhin per GPO abschalten, Home-User müssen dafür zu regedit greifen. Da wünscht man sich glatt Karl Klammer zurück – der war zwar nervig, aber wenigstens verschwiegen.

Nach erfolgreichem Update wird man von seinem aufgefrischten Windows mit „Hallo. Wir haben Ihren PC aktualisiert." begrüßt. Besser lässt sich der Hoheitsverlust über den eigenen Rechner nicht zusammenfassen - Realsatire as a Service.

Secorvo News

PKI Check-up

In den vergangenen Jahren haben viele Unternehmen und Organisationen interne Public-Key-Infrastrukturen (PKI) aufgebaut. Viele Betreiber fragen sich jedoch, ob ihre PKI noch angemessen sicher, praxistauglich und für künftige Herausforderungen gerüstet ist. Als Abhilfe hat Secorvo daher einen PKI Check-up entwickelt, der PKI-Prozesse, -Architektur und -Dokumentation an bewährten Best Practices und Standards misst, bewertet und Optimierungspotenzial aufzeigt.

Fast ausgebucht

Noch drei letzte freie Plätze gibt es auf unserem rundum erneuerten Seminar „IT-Sicherheit heute" (**27.–29.09.2016**). Das Programm reicht von aktuellen Rechtsthemen wie dem IT-Sicherheitsgesetz und der Datenschutz-Grundverordnung bis zu einem „Hacking Day" mit WebGoat-Workshop – und ist als Weiterbildung zur T.I.S.P.-Re-Zertifizierung anerkannt. Schnell Entschlossene erwischen noch einen Platz (Programm und Online-Anmeldung).

Zertifikate

Im November (**21.–25.11.2016**) bieten wir die nächste Möglichkeit zur T.I.S.P.-Zertifizierung. Nach Ihrer Anmeldung erhalten Sie, frühzeitig vor Seminarbeginn, unser T.I.S.P.-Buch zur Vorbereitung: ein systematischer Zugang zur Informationssicherheit in 26 Kapiteln auf 700 Seiten, verfasst von Experten für Experten.

Software-Architekten und -Entwickler bereiten wir im Oktober (**24.–27.10.2016**) auf die Zertifizierung zum *Certified Professional for Secure Software Engineering* (CPSSE) vor. Auch hier empfehlen wir eine frühzeitige Anmeldung.

Cloud Encryption

Wie real ist die Gefahr, sich mit einer „Ransomware" zu infizieren? Welche Infektionswege verwenden die Angreifer? Wie arbeitet ein solcher Verschlüsselungstrojaner? Und welche technischen und organisatorischen Schutzmaßnahmen wirken dagegen? Auf diese Fragen gibt am **22.09.2016** ab 18 Uhr Tobias Häcker (Leitwerk AG) im Rahmen des nächsten KA-IT-Si-Events im Panoramasaal der IHK Karlsruhe Antworten und wirft einen Blick hinter die Kulissen aktueller Erpressungstrojaner. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – mit Blick über die Dächer von Karlsruhe.

Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

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

September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, mobile business, Frankfurt)
19.09.	Sommerakademie des ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
22.09.	EaaS – Encryption as a Service (KA-IT-Si, Karlsruhe)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt/AT)
26.-30.09.	Informatik 2016 (Gesellschaft für Informatik, Klagenfurt/AT)
27.-29.09.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Oktober 2016	
04.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)
19.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association, Luzern/CH)
24.-27.10.	CPSSE – Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-28.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Wien/AT)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Michael Knopp, 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