secorvo
security consulting

Secorvo Security News

Oktober 2016

Freiwillige Cyberwehr

Es ist kein guter Stil, Salz in offene Wunden zu streuen. DIE ZEIT und netzpolitik.org haben sich bereits ausführlich über die freiwillige Cyberwehr ausgelassen, und via Twitter wurde das BSI mit Spott übergossen. Doch das Thema ist zu wichtig, um es unkommentiert zu lassen. Worum also geht es?

Bereits Anfang Juni 2016 wurde bekannt, dass das BSI ein 20-köpfiges „Mobile Incident Response Team" aufbauen will, das ab 2017 Betreiber kritischer Infrastrukturen bei einem IT-Sicherheitsvorfall unterstützen soll. So weit, so gut. Offenbar bekam das BSI nun jedoch Respekt vor der eigenen Courage und entwarf rasch eine Kooperationsvereinbarung für eine „freiwillige Cyberwehr", die Anfang Oktober publik wurde. Das Konzept: Kooperierende Unternehmen stellen eigene Fachkräfte für IT-Sicherheit ab, die bei einem IT-Sicherheitsvorfall der „Cyberwehr" des BSI unterstellt werden und bis zu drei Tage Soforthilfe leisten. Die Unternehmen sichern ein vom BSI abrufbares Einsatzkontingent von jeweils bis zu 20 Personentagen jährlich (zuzüglich Reisekosten, Übungen und Fortbildungen) zu – unentgeltlich, versteht sich – und besetzen eine rund um die Uhr erreichbare Kontaktstelle für die Alarmierung.

Eine wenig beruhigende Vorstellung: IT-Sicherheitsvorfälle in kritischen Infrastrukturen werden zukünftig von einer bunten, auf Zuruf zusammengetrommelten Truppe freiwilliger Cybercops unter BSI-Leitung bekämpft. Sieht man einmal von der Frage ab, ob Unternehmen bereit sein werden, ihre hoch bezahlten Fachkräfte für solche Einsätze abzustellen – professionell klingt das nicht.

Wollte man Schäden wirksam begrenzen und den Umgang mit Vorfällen professionalisieren, müsste den immer ausgefeilteren Angriffsmethoden eine intensiv trainierte, hoch kompetente und eingespielte schnelle Eingreiftruppe gegenüberstehen. Wer schon einmal eine IT-Notfallübung durchgeführt hat, weiß, dass es dabei mit drei Tagen „Schlauch draufhalten" nicht getan ist. SEKs sind schließlich auch keine spontan einberufenen Grisu-Teams.

Inhalt

secorvo
security consulting

Security News

Risikomanagement erneuert

Am 19.10.2016 hat das BSI die "Community Draft"-Version des neuen Risikomanagement-Standards 200-3 veröffentlicht. Die reichlich formale und in der Praxis selten hilfreiche Vorgehensweise des Vorgängers 100-3 wurde erheblich überarbeitet.

Zum einen wurden die noch als Ergänzung zum 100-3 definierten ‚Elementaren Gefährdungen' nun als wesentliche Komponente für Risikoanalysen integriert, ein für die Praxis durchaus sinnvoller Schritt. Zum anderen ist nun ein kompletter Prozess für das Risikomanagement von Informationssicherheitsrisiken beschrieben. Und der rockt. Praxistauglich, pragmatisch und, wenn man noch die Beispiele kürzt und den nicht wirklich belastbaren Begriff der Eintrittswahrscheinlichkeit durch eine (subjektive) Wahrscheinlichkeitseinschätzung ersetzt, ein wirklich brauchbares Grundlagenwerk. Ein kleiner Schritt in der Versionsnummer, aber ein großer Schritt in Richtung praktikablen IT-Grundschutzes.

Datenübermittlung auf der Kippe

Wer glaubt, mit dem EU-U.S. Privacy Shield (SSN 07/2016, 08/2016) sei der Datentransfer außerhalb der EU wieder in trockenen Tüchern, der wiegt sich in trügerischer Sicherheit. Nach dem erfolgreichen Vorgehen gegen Facebooks Datenübermittlung auf Basis von Safe Harbor hat Max Schrems im Mai 2016 auch die Prüfung EU-Standardvertragsklauseln bei der zuständigen irischen Datenschutzbeauftragten (DPC) initiiert. Diese Klauseln dienen als Rechtsgrundlage einer Datenübermittlung in jedes Drittland (nicht nur den USA) und werden vielerorts als „bessere Alternative" zu Safe Harbor verstanden. Am 28.09.2016 informierte die DPC über den Verfahrensstand: Nach ihrer Überzeugung verstoßen die Klauseln gegen europäisches Recht, denn EU-Bürgern stehen in den USA keine wirksamen Rechtsbehelfe zur Verfügung. Die Argumentation stützt sich auf die Entscheidungsgründe im Safe-Harbor-Urteil des EuGH.

Anfang 2017 wird der Austausch mit dem High Court abgeschlossen sein – und dieser kann kaum etwas anderes tun, als die Frage nach der Rechtmäßigkeit der Klauseln dem EuGH vorzulegen. Folgt dieser seinen eigenen Argumenten, wird er die Standardvertragsklauseln für unwirksam erklären. Damit bliebe für die Datenübermittlung in die USA nur noch der Privacy Shield, den die europäischen Datenschutz-Aufsichtsbehörden zunächst auf ein Jahr befristet beobachten wollen, um dann zu entscheiden, ob sie ihn als rechtmäßig ansehen.

Unendliche Geschichte

Mit seinem Urteil in Sachen Breyer ./. BRD hat der EuGH dem alten Streit um den Personenbezug der IP-Adresse am 19.10.2016 ein neues Kapitel hinzugefügt. Einerseits wird der Personenbezug dynamischer IP-Adressen erneut bejaht, wenn auch nicht uneingeschränkt. Daneben wurde die Frage, ob die Protokollierung von Webseitenzugriffen zu Sicherheitszwecken zulässig ist, gegen die in Deutschland herrschende Meinung entschieden: Nach Auffassung des EuGH ist sie regelmäßig erlaubt.

An der IP-Adresse entzündet sich immer wieder der Streit um ein objektives oder relatives Verständnis der Personenbeziehbarkeit: Reicht es, dass ein Dritter den Betroffenen ermitteln kann oder muss dies dem Dateninhaber selbst möglich sein?

Der EuGH sieht die Personenbeziehbarkeit auch gegeben, wenn der Dateninhaber die Zuordnung nicht allein vornehmen kann, aber die rechtliche Möglichkeit hat, die Zuordnungsdaten zu erlangen. Das ist im Umkehrschluss ein Brückenschlag zur „relativen Theorie". Außerdem stünde die RL 95/46/EG einer Regelung entgegen, die eine Datenverarbeitung ohne jegliche Abwägungsmöglichkeit kategorisch verbiete. Beide Aussagen gehen deutlich über das Telemediengesetz hinaus. Mit der Öffnung zur relativen Theorie sind beispielsweise Pseudonyme rechtlich neu zu bewerten. Die neue Entscheidungslage hat jedoch ein Verfallsdatum, denn mit der Datenschutz-Grundverordnung entfallen ab Mai 2018 wesentliche Teile der Wortlautargumente des EuGH – und der Streit wird wohl von vorne beginnen.

6. Deutscher IT-Sicherheitspreis

Der „Deutsche IT-Sicherheitspreis", gestiftet von Dr. Horst Görtz, dem Gründer des ersten großen deutschen IT-Sicherheitsunternehmens, zeichnet seit 2006 alle zwei Jahre drei herausragende Entwicklungen im Gebiet der IT-Sicherheit aus. Mit einem Preisgeld von insgesamt 200.000 € ist dies einer der höchsten privat gestifteten Preise in Deutschland. Am 06.10.2016 wurden in Darmstadt die diesjährigen Gewinner ausgezeichnet. Den ersten Preis erhielt die Analysesoftware Harvester der Forschungsgruppe um Professor Eric Bodden, die eine Schadsoftwareerkennung auch in obfuskierten Android-Apps erlaubt. Preis zwei ging an die Plattform Octopus zur Schwachstellensuche der Forschungsgruppe um Professor Konrad Rieck, die mit Methoden des Pattern Matching und des maschinellen Lernens beeindruckende Analyseerfolge mit einer Minimalzahl an „False Positives" vorweisen kann. Ein deutliches Signal, welcher Stellenwert der

Bekämpfung von Schadsoftware und Schwachstellen inzwischen eingeräumt wird – und welche überraschende Fortschritte in diesem Bereich noch möglich sind.

Microsoft Edge-VM

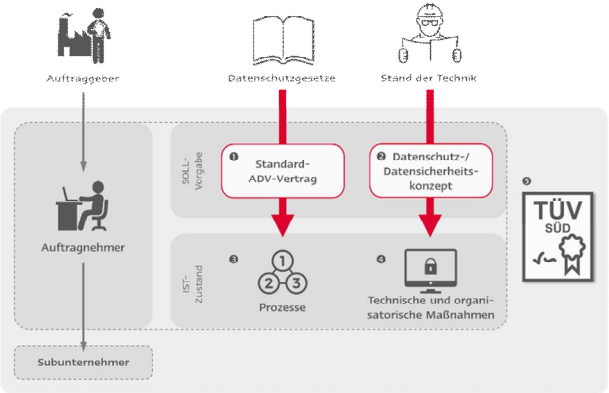
Microsoft plant, den Microsoft-Internetbrowser Edge in der nächsten Version von Windows 10 in eine virtuelle Umgebung zu verfrachten. Die *Windows Defender Application Guard* genannte Technologie startet beim Aufruf von nicht vertrauenswürdigen Seiten eine schlanke virtuelle Windows-Instanz, in welcher der Browser selbst bei infizierten Webseiten Angriffsmöglichkeiten auf das eigentliche Betriebssystem und die Benutzerdaten unterbindet. Im Intranet wird Edge „ganz normal" gestartet und kann auch auf die internen Daten zugreifen. Ein viel versprechender Ansatz, den Zugriff auf Webseiten sicherer zu machen.

Secorvo News

Das Standard-ADV-Modell

Wie lassen sich Auftragsdatenverarbeiter systematisch und kontinuierlich, zugleich aber effizient und effektiv auf die wirksame Umsetzung geeigneter technischer und organisatorischer Maßnahmen (TOM) zum Schutz der verarbeiteten personenbezogenen Daten prüfen? Die Verantwortung für die Verarbeitung liegt beim Auftraggeber: Er muss regelmäßig prüfen, ob geeignete Maßnahmen zu deren Schutz getroffen wurden und die gesetzlichen Anforderungen erfüllt sind.

Eine Zertifizierung kann aufwändige Einzelprüfungen durch ein standardisiertes Verfahren ersetzen. Doch warum hat sich bisher kein Standard etabliert? Genau mit dieser Frage haben sich Secorvo und der TÜV SÜD beschäftigt. Daraus ist das Standard-ADV-Modell mit Zertifizierung entstanden, das Auftragnehmer von Auftragsdatenverarbeitungen beim Nachweis der Eignung und Angemessenheit der getroffenen Maßnahmen gegenüber ihren Auftraggebern mit dem Prüfzeichen und Zertifikat „Zertifizierte Auftragsdatenverarbeitung" unterstützt. Mit einer nach wenigen Monaten bereits zweistelligen Zahl erfolgreicher Zertifizierungen könnte das Konzept ein Erfolgsmodell werden.



Eine ausführliche Darstellung des Modells und des Zertifizierungsverfahrens haben Christoph Schäfer und Dirk Fox in Ausgabe 11/2016 der Fachzeitschrift DuD veröffentlicht.

T.I.S.P.-Zertifikat

Eine letzte Möglichkeit, Ihre Kenntnisse und Qualifikation in der Informationssicherheit noch in diesem Jahr zu zertifizieren, bieten wir mit unserem T.I.S.P.-Seminar im November (**21.–25.11.2016**). Das Begleitbuch erhalten Sie zur Vorbereitung auf das Seminar unmittelbar nach Eingang Ihrer Anmeldung. Programm und Online-Anmeldung sowie die Termine und Seminarangebote für 2017 finden Sie unter www.secorvo.de/seminare.

Mit Brief und Siegel

Zertifizierung eines großen Rechenzentrums – nach IT-Grundschutz? Kann das mit vertretbarem Aufwand und in überschaubarer Zeit funktionieren?

Der Globalways AG ist das mit einem pragmatischen Ansatz bei der Vorbereitung und Umsetzung der IT-Grundschutzmaßnahmen auf effiziente Weise gelungen. Die Erfahrungen, Herausforderungen und „Lessons Learned" im Zertifizierungsprozess, von der Vorbereitung bis zum Zertifikat, stellt der CISO Sascha Grund bei unserer nächsten KA-IT-Si Veranstaltung am **10.11.2016, 18 Uhr** vor. Dabei wird vor allem auf das Zusammenspiel der eingesetzten Werkzeuge und deren Verwendung im Informationsverbund eingegangen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Die Möglichkeit zur Anmeldung finden Sie unter www.ka-it-si.de.

Krypto im Advent 2016

Nach dem großen Erfolg im Advent 2015 bietet die KA-IT-Si gemeinsam mit der Pädagogischen Hochschule Karlsruhe im Dezember 2016 wieder den interaktiven Online-Adventskalender „Krypto im Advent" an, bei dem Schülerinnen und Schüler die Welt der Verschlüsselung und Geheimsprachen kennenlernen und tolle Preise gewinnen können. Auch ältere, an Ver- und Entschlüsselungsverfahren Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

November 2016	
01.-04.11.	Black Hat Europe 2016 (Blackhat, London/UK)
08.-11.11.	DeepSec In-Depth Security Conference 2016 Europe (DeepSec, Wien/AT)
10.11.	Mit Brief und Siegel (KA-IT-Si, Karlsruhe)
10.-11.11.	T.I.S.P. Community Meeting (TeleTrusT, Frankfurt am Main)
17.-18.11.	40. DAFTA (GDD, Köln)
21.-25.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.11.	6. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
29.-30.11.	5. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
Januar 2017	
13.-15.01.	ShmooCon 2017 (Shmoo Group, Washington/US)
16.-18.01.	OmniSecure 2017 (inTime, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, CA/US)

Fundsache

Valerie Tischbein hat am 22.08.2016 auf Netzpolitik.org eine Übersicht der von Facebook erhobenen 98 Datentypen zur Schaltung zielgenauer Werbung und den korrespondieren Datenschutzeinstellungen veröffentlicht, basierend auf einer Analyse der Washington Post.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), 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