secorvo
security consulting

Secorvo Security News

April 2013

XP Forever

Der Support von Windows XP wird von Microsoft am 08.04.2014 eingestellt: Ab diesem Zeitpunkt werden keine neuen Sicherheitspatches mehr veröffentlicht. Bedeutet dies, dass damit ein Umstieg auf eine neuere Windows-Version unvermeidlich ist? Insbesondere im industriellen Umfeld findet man zahlreiche Anwendungen, die nicht einmal für neuere Windows-Systeme freigegeben sind – da kann ein Betriebssystemwechsel aufwändig und riskant sein.

Die Antwort ist ein entschiedenes „kommt darauf an". Unter bestimmten Voraussetzungen und durch geeignete Maßnahmen kann Windows XP mit ruhigem Gewissen weiter betrieben werden. Eine der wesentlichen Vorraussetzungen ist, dass seitens der Anwendungen kein Änderungsbedarf vorliegt. Schließlich kann nicht ausgeschlossen werden, dass bei einem Anwendungsupdate unbekannte Fehler oder Betriebssystemfeatures Probleme verursachen.

Die geeigneten Schutzmaßnahmen leiten sich aus den möglichen Angriffsflächen ab, die man abhängig von Risiko und Einsatzzweck betrachten sollte. Um Angriffe am System selbst zu erschweren, die etwaige lokale Schwachstellen ausnutzen, sollte der Zugang zum System geschützt werden. Schwieriger ist der Schutz vor netzbasierten Angriffen: Hier kann die Ausnutzung von möglichen Schwachstellen nur durch eine netzseitige Einschränkung der Kommunikation erschwert oder unterbunden werden. Konkret könnte dies durch die Bildung von isolierten Netzsegmenten realisiert werden oder durch die Vorschaltung von „Industrial Firewalls" zur Abschottung des Systems.

Restrisiken verbleiben, wenn Anwendungen erfordern, dass Dienste auf dem XP-System erreichbar sein müssen – bei Client-Betriebssystemen ist das aber nicht die Regel. Vor einem Wechsel lohnt jedenfalls eine kritische Analyse – denn nicht für jeden Einsatzzweck ist „neu" = „besser".

Inhalt

secorvo
security consulting

Security News

Orkan im Schnapsglas

Am 12.04.2013 hat die Deutsche Post per Presse-interview nach einjähriger Vorbereitungszeit ihren Ausstieg aus der De-Mail-Akkreditierung verkündet. Grund für den Ausstieg ist § 4 Abs. 2 Nr. 1, 3 De-Mail-Gesetz. Dieser legt fest, dass von dem Nutzer bei Eröffnung eines De-Mail-Kontos Name, Geburtsort, Geburtsdatum und Anschrift zu erheben sind, nachgewiesen u. a durch den amtlichen Ausweis. Die Post plante, hierfür ihr Postident-Verfahren einzusetzen, in dessen Rahmen – wohl mit Rücksicht auf die Aufzeichnungspflicht in § 8 Geldwäschegesetz – zusätzlich die Personalausweisnummer erhoben wird. Der Bundesdatenschutzbeauftragte versagte hierfür die Akkreditierung, da die Erhebung der Personalausweisnummer nach dem Gesetz für De-Mail – wie im übrigen, bisher unbeanstandet, auch nach Signaturgesetz und -verordnung sowie nach § 111 Abs. 1 TKG beim SIM-Karten Versand – nicht erforderlich und damit unzulässig ist.

Zeitgleich hat sie Beschwerde bei der EU-Kommission gegen das am 19.04.2013 vom Deutschen Bundestag verabschiedete (und noch nicht vom Bundesrat bestätigte) E-Government-Gesetz eingelegt, das die De-Mail als weiteren die Schriftform ersetzenden Kommunikationsweg zur öffentlichen Verwaltung vorsieht. Die Beschwerde sieht einen Verstoß gegen die Notifizierungspflicht und richtet sich gegen den indirekten Ausschluss des E-Postbriefs als Schriftformersatz gegenüber Behörden, der nur durch qualifizierte elektronische Signatur, De-Mail mit sicherer Anmeldung oder per Formular und eID des Personalausweises möglich ist.

Angesichts der geringen Verbreitung aller betroffenen Verfahren dürfte der reale Nachteil sich in Grenzen halten, zumal das E-Government-Gesetz eine Hintertür für sonstige sichere Verfahren lässt. Bemerkenswert ist allerdings die Kompromisslosigkeit, mit der die Deutsche Post erhebliche Investitionen an einer vergleichsweise leicht zu berücksichtigenden Datenschutz-Beanstandung scheitern lässt – da liegt der Verdacht nahe, dass es sich hier um einen Vorwand zum Gesichtsverlust freien Rückzug aus einem drohenden Kostengrab handelt.

Software ohne Sicherheitszertifikat

... ist die Überschrift eines am 16.04.2013 veröffentlichten Prüfungsergebnisses des Bundesrechnungshofes zum neuen Personalausweis und der zugehörigen AusweisApp. Darin wird besonders kritisiert, dass die verbindliche Zertifizierung der Software – mit 4,2 Mio. Euro Entwicklungskosten nicht gerade ein Schnäppchen – durch das BSI nicht bis Ende 2012 erfolgt ist. Seit zwei Jahren findet sich der „Bürgerclient“ auf der Liste laufender Zertifizierungen des BSI. Der Bundesrechnungshof verweist auf mögliche Haftungsrisiken für den Bürger aufgrund der fehlenden Bewertung der Gesamtsicherheit des nPA-Systems. Denkwürdig wird es im Abschnitt 1.3, in dem eine Stellungnahme des BMI paraphrasiert wird: „Es ergebe keinen Sinn, wenn der Hersteller, in diesem Fall das Bundesamt, sein selbst erstelltes Produkt anschließend zertifiziere. Da das Bundesamt die Software verteile, bekräftige es damit die ausreichende Sicherheit des Produkts.“

Offensichtlich hat das BMI die peinliche Panne beim Start der AusweisApp am 09.11.2010 (SSN 11/2010) erfolgreich verdrängt – keine 24 Stunden dauerte es bis zur Kompromittierung. Fehler passieren – aber man sollte doch wenigstens etwas daraus lernen.

„Nicht kritisch“ ...

... ist die Einstufung der Sicherheitslücke, die am 12.03.2013 im Microsoft Security Bulletin MS13-027 adressiert wurde. Damit kann es einem Angreifer durch Einstecken eines präparierten USB-Sticks gelingen, einen Rechner vollständig zu kompromittieren und administrative Rechte zu erlangen – auch wenn an dem Rechner kein Benutzer angemeldet ist. Daher empfehlen wir abweichend von der Einstufung von Microsoft dringend die Installation der entsprechenden Patches – auch an nicht vernetzten IT-Systemen. Betroffen von der Sicherheitslücke sind fast alle Microsoft-Betriebssysteme.

Neue Auskunftsregeln

Am 21.03.2013 hat der Bundestag das Gesetz zur Änderung des Telekommunikationsgesetztes (TKG) und zur Neuregelung der Bestandsdatenauskunft verabschiedet. Die Neuregelung war erforderlich geworden, nachdem das Bundesverfassungsgericht wesentliche Teile der Bestandsdatenauskunft nach § 113 TKG nur mit Auflagen und bis zum 30.06.2013 fortgelten ließ. Das Gesetz folgt den Vorgaben des Urteils, indem es die Auskunft vom Vorliegen weiterer Rechtsgrundlagen abhängig macht, die die anfragenden Behörden mitzuteilen haben.

Eine deutliche Festlegung der in Betracht kommenden Rechtsgrundlagen oder eine Eingrenzung der Voraussetzungen findet jedoch kaum statt. Der neu eingeführte § 100j StPO setzt lediglich die Erforderlichkeit zur Sachverhaltsklärung oder zur Bestimmung des Aufenthaltsortes eines Beschuldigten voraus. Bezüglich der Abfrage von Daten wie PINs oder Login-Informationen wird lediglich vorausgesetzt, dass eine Rechtsgrundlage zu deren Nutzung vorhanden sein muss, da ihre Abfrage sonst nicht erforderlich wäre.

Aussagen zu eben diesen Rechtsgrundlagen fehlen. Den Maßgaben des Bundesverfassungsgerichts mag durch die teilweise Abschrift der Urteilsbegründung Rechnung getragen worden sein. Eine Stärkung der Grundrechte der Betroffenen stellt diese Gesetzesreparatur sicher nicht dar.

Verzweifelt ...

... ist der Ton des „State of Software Security Report“ mit dem bezeichnenden Untertitel „*The Intractable Problem of Insecure Software*“, den das amerikanische Unternehmen Veracode am 08.04.2013 im fünften Jahr in Folge veröffentlicht hat. In der Einleitung werden klare Worte über den inakzeptablen Zustand der Sicherheit vieler Software-Produkte ausgesprochen. Die aktuellen Probleme werden auf 44 Seiten ausführlich dargestellt und bewertet.

Mancherorts ist die Nachricht bereits angekommen: In Zusammenarbeit mit der KA-IT-Si widmet der diesjährige Entwicklertag 2013 am 05.06.2013 diesem Thema einen eigenen Track.

REMnux IV.

Mit der Ubuntu-basierten Distribution REMnux V4 steht seit dem 09.04.2013 nach fast 15 Monaten eine gründlich aktualisierte und erweiterte Toolsammlung für die Malwareanalyse zur Verfügung.

Die kompakte Zusammenstellung und Konzentration auf das Wesentliche wurde beibehalten. Nun gibt es REMnux neben der bekannten Live CD auch als direkt einsatzfähige, virtuelle Appliance. Darin wurden die bisherigen Malwareanalysebereiche für Hauptspeicher, Netzwerk, Web und insbesondere PDF aktualisiert. Da die Analysetätigkeiten hauptsächlich auf der Terminalkommandozeile durchgeführt werden, wurde die Bash-Alias-Vorbelegung deutlich verbessert, so dass man nun sehr komfortabel und schnell mit dem Werkzeugkasten arbeiten kann. Für die Analyse von unbekannten Binärdateien wurden die Unterstützung für XOR (NoMoreXOR, brutexor, XORBruteForcer) und PE (pev, dism-this, ExeScan, udis86) deutlich ausgeweitet.

Eine besonders sinnvolle Ergänzung ist das am 19.03.2013 erschiene Werkzeug ProcDot von CERT.at, mit dem auf der Basis von Sysinternals ProcMon- und PCAP-Logdateien automatisiert eine graphische Zeitlinie erstellt werden kann. Das überarbeitete Cheat-Sheet ermöglicht am Reverse Engineering von Malware Interessierten einen Schnelleinstieg.

Secorvo News

Sommerbildung

So sicher, wie der Sommer kommt, steigen auch die Anforderungen im Bereich Informationssicherheit. Die Antwort darauf heißt kontinuierliche Weiterbildung. Zum Beispiel beim Schlagwort „Security by Design“: In unserem Seminar "Security Engineering" zeigen wir Ihnen Ende September, wie Sicherheit von Beginn an in Entwicklungsprozesse einbezogen werden kann, anstatt das Thema erst zum Schluss ‚aus der Schublade zu kramen'. Die Qualität steigt, ohne die Entwicklungskosten nach oben zu treiben. Schließlich können Sie Ihre Kenntnisse durch die Zertifikatsprüfung T.E.S.S. zertifizieren lassen.

Ihre Berufserfahrung und Ihr Know-How im Bereich Informationssicherheit können Sie in diesem Sommer gleich zu zwei Gelegenheiten bei Secorvo mit dem T.I.S.P.-Zertifikat krönen: Im Juni und im September bieten wir eine T.I.S.P.-Schulung mit nachfolgender unabhängiger T.I.S.P.-Prüfung an.

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

Cloud, aber sicher!

Die Vorbehalte gegenüber der Nutzung von Clouddiensten sind insbesondere in Deutschland hoch. Dabei werden vor allem Sicherheitsbedenken als große Hürde genannt. Das vom Bundesministerium für Wirtschaft und Technologie geförderte Projekt ‚MimoSecco' (Middleware for Mobile and Secure Cloud Computing) will hier Abhilfe schaffen: Die Karlsruher Unternehmen CAS und WIBU-SYSTEMS entwickeln in Zusammenarbeit mit dem KIT (EISS, AIFB) eine Lösung, bei dem Nutzer von mobilem Cloud Computing die Kontrolle über ihre Daten behalten.

Das im Projekt entworfene und bisher umgesetzte Lösungskonzept stellt Daniel Eichhorn (WIBU-SYSTEMS AG) in seinem Vortrag beim nächsten KA-IT-Si-Event "Cloud, aber sicher!" am **15.05.2013** anlässlich der Cloudzone in der Messe Karlsruhe vor.

Das Event findet ausnahmsweise an einem *Mittwoch* statt und beginnt bereits um *17 Uhr*. Als KA-IT-Si-Teilnehmer haben Sie außerdem die Möglichkeit, die Messe vorab kostenfrei zu besuchen. Ein zusätzliches Schmankerl ist die Ausstellung mehrerer Exponate des Kryptologikum – spannend für alle, die an der Eröffnungsveranstaltung im Januar nicht teilnehmen konnten. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

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

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)
13.06.	Swiss Cyber Storm 4 (Swiss Cyber Storm Association, Luzern/CH)
17.-18.06.	DuD 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Juli 2013	
04.07.	5. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
08.-10.07.	IFIP Sec 2013 (IFIP, Auckland/NZ)

Fundsache

Knackige Fakten über den täglichen Gebrauch von Mobilgeräten präsentieren die am 04.04.2013 erschienenen „European Mobile Insights“, die anlässlich des Norton Cybercrime Reports 2012 ermittelt wurden. Dass zwei Drittel aller Nutzer von Smartphones oder Tablets ihr Gerät mit PIN oder Passwort schützen, klingt etwas optimistisch – dass einem Drittel schon einmal ein Gerät abhanden kam, eher beunruhigend.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, 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