secorvo
security consulting

Secorvo Security News

Juni 2013

Überraschung?

Die Aufregung irritiert – als hätte das Editorial der SSN 5/2013 noch einer Bestätigung bedurft. Denn auch vor der Offenlegung von Prism waren die weit gehenden Berechtigungen der amerikanischen Sicherheitsbehörden bekannt; auch die Aufgaben der NSA sind lange kein Geheimnis mehr. Selbst die Mitwirkung der großen „Datensammler" kann man längst öffentlich nachlesen: So dokumentiert Google in seinem Transparenzbericht staatliche Auskunftsersuchen – auch die von US-Behörden.

Mehr noch: Die staatlichen Zugriffe sind vielleicht nicht nett, aber legitim. Denn selbstverständlich ist es eine der wichtigsten Aufgaben einer gesellschaftlichen Ordnung, deren Mitglieder vor inneren und äußeren Bedrohungen zu schützen – dem wird auch kaum jemand widersprechen. Sogar Zweifel an der Verhältnismäßigkeit der Zugriffe verlieren an Gewicht, wenn man auf die Zahlen sieht: 19.000 betroffene Facebook-Profile in sechs Monaten – das sind 0,0018 % der weltweit 1.060.627.980 Nutzerprofile (Stand Juni 2013).

Und wer einwendet, dass die amerikanischen doch weit von unseren deutschen Verhältnissen abweichen, der beweist Realitätsferne. Denn auch hierzulande haben Strafverfolgungsbehörden im Rahmen der Beweiserhebung Zugriff auf Daten – dank §§ 70, 95 StPO ganz ohne richterlichen Beschluss. Googles Transparenzbericht belegt, dass deutsche Behörden ein Fünftel der amerikanischen Anfragezahl beisteuern – fast im Verhältnis der Einwohnerzahlen.

Wer freimütig seine persönlichen Daten oder die seines Unternehmens auf ausländische Server kopiert, darf sich zumindest nicht wundern, wenn sie damit dem unkontrollierten Zugriff staatlicher Stellen preisgegeben sind. Dabei ist diese Preisgabe meist nicht zwingend: Manchmal spart sie Geld (wenigstens temporär oder theoretisch), und manchmal liefert sie einen (wenigstens gefühlten) Bequemlichkeitsgewinn. Und fast immer gibt es Alternativen – andere Anbieter oder auch technische Lösungen, die unerwünschte Zugriffe z. B. durch Verschlüsselung wirksam verhindern.

Inhalt

Security News

Der Vergangenheit verpflichtet

Schon seit einiger Zeit hat Microsoft Mechanismen wie DEP und ASLR in Windows integriert, die dafür sorgen sollen, dass Schadcode, der über eine nicht gepatchte oder unbekannte Schwachstelle in eine Anwendung eingeschleust wurde, nicht ausgeführt wird. Leider werden diese Mechanismen eher selten genutzt, weil sie nicht nur Schadcode, sondern auch manche krude implementierte, aber legitime (Alt-) Software am Ablauf hindern.

Das *Enhanced Mitigation Experience Toolkit* (EMET) von Microsoft, dessen Version 4.0 am 17.06.2013 erschien, hilft aus dieser Zwickmühle, indem es erlaubt, diese Mechanismen nur für diejenigen Anwendungen zu aktivieren, die sie problemlos vertragen. Zusätzlich schlägt die neue Version Alarm, wenn populäre Webseiten wie Google unvermutet TLS-Zertifikate „unüblicher" Trustcenter, bspw. aus den Niederlanden oder der Türkei nutzen.

GSTOOL 4.8

Ein kleiner Schritt für das GSTOOL, aber ein gewaltiger Sprung in der Funktionalität für die Erstellung von IT-Sicherheitskonzepten nach IT-Grundschutz: Das am 07.06.2013 veröffentlichte Servicepack 3 zur Aktualisierung auf die Version 4.8 enthält neben Fehlerkorrekturen und der nun offiziell unterstützten Anbindung aktuellerer SQL-Server-Versionen die Möglichkeit, selbst definierte Bausteine inklusive ihrer Gefährdungen und Maßnahmen in eine andere GSTOOL-Datenbank zu importieren. Bausteine, die für einen IT-Verbund entwickelt wurden, können so weiter verwendet werden.

Das funktioniert an sich recht gut, allerdings wird man auf Konflikte beim Import nicht direkt hingewiesen, beispielsweise wenn eine benutzerdefinierte Maßnahmen-Nummer vor dem Import bereits vergeben war. In unseren Tests wurde dem Titel eine Tilde (~) vorangestellt, so dass man die Kollision zumindest entdecken kann.

Der Umstieg auf Version 4.8 und die Export-/Importfunktionen sollten gründlich getestet werden, zumal eine Rückportierung in Version 4.7 nicht einfach möglich ist. In Anbetracht des Duke Nukem-haften Entwicklungszyklus für Version 5.0 gehen wir davon aus, dass die mit dem aktuellen Servicepack um sehr nützliche Funktionen erweiterte Version 4.8 noch einige Zeit Bestand haben wird.

Auto-Ripper

Mit dem am 14.05.2013 veröffentlichten Wrapper-Skript auto_rip von Corey Harrell für den RegRipper 2.8 ist es nun sehr komfortabel möglich, die seit dem 29.04.2013 verfügbaren 285 RegRipper-Plugins entweder vollständig oder spezifisch nach Kategorien auszuführen. Die dabei verwendete Methodik leitet Kategorien aus einem Untersuchungsschritt (z. B. „Examine User Profiles") und zugehörigen forensischen Artefakten (z. B. extrahiert aus 18 zugeordneten Plugins) ab. Damit können z. B. zielgerichtet für ein Windows-Benutzerkonto alle Aktivitäten der Kategorie „*User Account File/Folder Access Activity*" untersucht werden.

Das Skript liefert unter Windows und Linux zuverlässige Ergebnisse (auch mit eigenen Plugins) und kann insbesondere für solche forensischen Analysen empfohlen werden, bei denen der Untersuchungsgegenstand konkret benannt und sehr eng eingegrenzt ist, da es die Erhebung nicht relevanter Informationen vermeidet.

10 Jahre Top 10

Happy Birthday OWASP Top 10! Am 12.06.2013 wurde pünktlich zum 10. Geburtstag Version 2013 der weithin anerkannten Übersicht über wesentliche Risiken für (Web-)Anwendungen veröffentlicht. Die Übersicht ist auch nach zehn Jahren noch ein wichtiges und aktuelles Awareness-Dokument, das eindrücklich relevante Gefährdungen dokumentiert. So sind auch diesmal die Änderungen zur Vorversion leider nicht gravierend, und es lohnt, die Hitliste an betroffene Führungskräfte und Entwickler weiterzugeben.

Wer aus erster Hand mehr über die Top 10 erfahren möchte, hat im August die Möglichkeit dazu: Auf der OWASP AppSec EU in Hamburg wird – neben vielen anderen spannenden Vorträgen – auch einer der Top 10-Autoren sprechen.

Der Zukunft zugewandt

Falls es noch eines weiteren Beweises bedarf, dass die Malware-„Industrie" stets mit der Zeit geht, dann belegen dies zwei Meldungen aus dem Juni: Am 03.06.2013 thematisierte das Blog der New York Times, dass der berüchtigte Online-Banking-Trojaner Zeus vermehrt über infektiöse URLs verbreitet wird, die auf populären Fan-Seiten in Facebook & Co. hinterlassen werden – E-Mails stoßen offenbar heutzutage entweder auf zu viel Misstrauen oder sind schlicht unpopulär geworden.

Und am 06.06.2013 wies ein Malware-Analytiker bei Kaspersky auf den bisher (mutmaßlich) ausgefeiltesten Trjoaner unter Android hin. Zwar muss der Anwender noch eine Spam-SMS – bald schon einen Facebook-Beitrag? – anklicken, damit sich die Malware installiert. Danach nutzt sie jedoch eine Lücke im Betriebssystem, um sich zu verbergen und vor

Entfernung zu schützen. Die Zeit, in der SMS bedenkenlos als „sicherer Kanal“ für TANs genutzt werden konnte, scheint sich rapide ihrem Ende zu nähern.

LobbyPlag

Transparenz in die Diskussion der europäischen Datenschutz-Grundverordnung bringt das am 06.06.2013 veröffentlichte Online-Projekt LobbyPlag 2.0 der Initiative europe-v-facebook.org: Über 3.100 systematisierte Änderungsvorschläge und eine Hitliste der zehn Datenschutz freundlichsten und unfreundlichsten Vorschläge mit einer Zuordnung zu den verantwortlichen Mitgliedern des EU-Parlaments finden sich darin.

Ernüchternd: In beiden „Top-10“-Listen steht ein deutscher Parlamentarier auf Platz eins, in der Negativ-Liste finden sich insgesamt zwei Deutsche. Nun ja, die nächste Europawahl kommt bestimmt.

Nachlese IPv6-Kongress

Am 06. und 07.06.2013 – genau ein Jahr nach dem IPv6 World Flag Day – fand bereits der fünfte IPv6-Kongress statt. Unter den zahlreichen Beiträgen rund um IPv6 gab es auch mehrere Vorträge zum Thema IPv6-Sicherheit. Herausragend war der gemeinsame Vortrag von Marc Heuse und Fernando Gont zum Thema Security Assessment von IPv6-Netzen. Dabei wurden ausgewählte Beispiele anhand der von den jeweiligen Autoren entwickelten Toolkits THC-IPv6 bzw. IPv6 Toolkit teilweise live vorgestellt. Es wurde nicht nur deutlich, dass die IPv6-Sicherheitseigenschaften gängiger Betriebssysteme und Firewalls namhafter Hersteller noch Verbesserungsbedarf aufweisen, sondern auch, wie nützlich der Einsatz der Toolkits ist, um sich dem Thema IPv6 (in Testnetzen!) ‚spielerisch' zu nähern.

Auch bei den Beiträgen zur Planung, Migration und betrieblichen Praxis war das Thema Sicherheit unterschwellig präsent. Neben der Gelegenheit, die eigenen Netze im Rahmen der Umstellung gründlich „aufzuräumen“, wurde mehrfach darauf hingewiesen, dass Unternehmen, die sich nicht ernsthaft mit IPv6 auseinandersetzen, eine bedeutende Entwicklung des Internets zu verschlafen drohen. Aufgrund des wachsenden Angebots durch Provider (auch an Endkunden) dürften die ersten Anfragen nach einer Erreichbarkeit über IPv6 nur noch eine Frage der Zeit sein.

Wer auch zukünftig (sicher) über das Internet erreichbar sein möchte, sollte sich bald mit IPv6 und den (sicherheits-) technischen Implikationen für die eigene Infrastruktur auseinandersetzen.

Secorvo News

IPv6-Whitepaper

Am 10.06.2013 ist das Secorvo White Paper „IPv6 - Die grundlegenden Funktionen, Bedrohungen und Maßnahmen“ (pdf, 65 Seiten) von Dr. Safuat Hamdy erschienen. Nach einer Einführung in die grundlegenden Eigenschaften von IPv6 werden protokollspezifische Bedrohungen, weitere Sicherheitsaspekte und mögliche Gegenmaßnahmen erläutert.

5. Tag der IT-Sicherheit

Bereits zum fünften Mal findet am **04.07.2013** der "Tag der IT-Sicherheit" statt, den die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) jährlich gemeinsam mit dem CyberForum e.V., der IHK Karlsruhe und KASTEL veranstaltet. Beginn ist um 14.00 Uhr im Haus der Wirtschaft (Saal Baden) der IHK Karlsruhe.

Im Rahmen der diesjährigen Keynote „Smartphone-Sicherheit“ nimmt Prof. Dr. Rainer Gerling, Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, eine vergleichende Sicherheitsanalyse gängiger Handy-Betriebssysteme vor. Es folgen weitere praxisnahe Fachvorträge zu den Themen Cybersicherheit und Grundschutz (BSI), Umgang mit Sozialen Netwerken (Deutsche Bahn) und IT-Security Management Strategie (SAP).

Gelegenheit zum fachlichen und persönlichen Erfahrungsaustausch bietet die Networking-Pause mit kleiner Ausstellung. Detaillierte Informationen zum Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter
www.tag-der-it-sicherheit.de

Wir freuen uns auf Ihre Anmeldung!

T.I.S.P.-Zertifizierung

Das T.I.S.P.-Zertifikat für Information Security Professionals entwickelt sich derzeit zu einer Standard-Qualifikation von IT-Sicherheitsexperten: erste Unternehmen erwarten von ihren Sicherheitsbeauftragten eine T.I.S.P.-Zertifizierung; allein im ersten Halbjahr 2013 wurden 60 Zertifikate erteilt.

In diesem Jahr bietet Secorvo noch zweimal die Möglichkeit zur Zertifizierung: vom **16.–20.09.2013** und vom **21.–25.10.2013**. Angemeldete Teilnehmer erhalten vorab das von Secorvo verfasste Begleitbuch zum T.I.S.P. – über 500 Seiten konzentriertes und aktuelles Wissen zur Informationssicherheit.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Veranstaltungshinweise

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

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)
27.07.-01.08.	Blackhat USA 2013 (Blackhat, Las Vegas/US)
August 2013	
01.-04.08.	DEF CON 21 (DEFCON, Las Vegas/US)
04.-07.08.	13th Annual DFRWS Conference 2013 (DFRWS, Monterey/US)
14.-16.08.	22nd USENIX Security Symposium (USENIX, Washington/US)
18.-22.08.	Crypto 2013 (IACR, Santa Barbara/US)
20.-23.08.	OWASP AppSec Europe Research 2013 (OWASP Foundation, Hamburg)
26.08.	Sommerakademie 2013 (ULD Hamburg, Kiel)
September 2013	
16.-20.09.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
23.-26.09.	Security Engineering (Secorvo College, Karlsruhe)

Fundsache

Am 19.06.2013 publizierte das BSI eine vergleichende 163seitige Studie zur Sicherheit von fünf verbreiteten Content Management Systemen (CMS). Die Ergebnisse sind ernüchternd – und sollten bei betroffenen Unternehmen zu Maßnahmen führen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Dr. Safuat Hamdy, 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