secorvo
security consulting

Secorvo Security News

März 2012

Wer hat Angst vorm Murmeltier?

Wir schreiben das Jahr 1990. Vor wenigen Jahren hat Apple den Macintosh vorgestellt und damit die IT-Landschaft nachhaltig geprägt. Da stellt Microsoft ein ähnliches Betriebssystem für die Geräte anderer Hersteller vor – und rollt damit den Markt auf. Kurz darauf breitet sich Schadsoftware für diese Systeme aus.

Zurück im Jahr 2012. Vor wenigen Jahren hat Apple das iPhone vorgestellt und damit die IT-Landschaft nachhaltig geprägt. Da stellt Google ein ähnliches Betriebssystem für die Geräte anderer Hersteller vor – und rollt damit den Markt auf. Kurz darauf breitet sich Schadsoftware für diese Systeme aus.

Einmal mehr scheint das Murmeltier zu grüßen. Allerdings dieses Mal ein Murmeltier mit Reißzähnen und auf Steroiden: Wir sind „always on" und per Netz angreifbar, Angreifer bewegen sich nicht mehr nur neugierig in fremden Gefilden, sondern haben sich längst ziel- und profitorientiert organisiert und können auf bewährte Angriffsmuster wie Drive-by-Infektionen, Phishing und Trojaner zurück greifen.

Auf Seiten der Verteidiger scheint die Zeit allerdings stehen geblieben zu sein: Anwender nutzen nur selten und widerstrebend ausreichend sichere Passcodes, Hersteller setzen auf die Stabilität ausgelieferter Software und haben die Notwendigkeit eines adäquaten Patch-Managements nicht erkannt, Sicherheitssoftware wird als Komforthindernis und unnützer Kostenfaktor wahrgenommen und nicht selten werden private Geräte an der Unternehmens-IT vorbei genutzt.

Höchste Zeit also, uns klar zu machen, dass das Smartphone von heute eben nicht der Computer von 1990 im Hosentaschenformat ist, auch wenn der Marktinnovator wie vor 28 Jahren noch immer Apple heißt. Sondern genau so sorgfältig geschützt werden muss, wie ein PC (oder Mac) anno 2012. Ehe das Murmeltier schmerzhaft zubeißt.

Inhalt

secorvo
security consulting

Security News

97 % vermeidbare Angriffe

Am 22.03.2012 hat Verizon mit dem 2012 Data Breach Investigations Report eine spannende Analyse publiziert. Auf 80 Seiten werden die Untersuchungsergebnisse von 855 Sicherheitsvorfällen des Jahres 2011 vorgestellt. Die Erkenntnisse sind erschreckend: So werden 96 % aller Angriffe als „nicht schwierig" eingestuft, und 97 % aller Vorfälle wären durch einfache Schutzmaßnahmen vermeidbar gewesen. Erkannt wurden die meisten der Vorfälle (85 %) erst nach Wochen, und in den seltensten Fällen von den Unternehmen selbst (8 %). In größeren Unternehmen konnte der Einfallsweg häufig nicht mehr rekonstruiert werden (31 %).

In den meisten Fällen gelang es einem Angreifer, Schadsoftware remote zu installieren (95 %). In größeren Unternehmen trugen in signifikantem Umfang *SQL-Injections* (12 %), Malware-Downloads (12 %), angeklickte E-Mail-Attachments (18 %) und *Drive-by-Infections* (18 %) zum Angriffserfolg bei: ein Beleg für unzureichende „Security Awareness" in den betroffenen Unternehmen.

Die Erkenntnisse der Studie erlauben den Schluss, dass isolierte Schutzmaßnahmen heute in der Regel zu kurz greifen und Unternehmen verstärkt auf ein umfassendes Schutzkonzept setzen und dabei vor allem ihre im Internet präsenten Anwendungen im Blick behalten müssen.

Dabei können offenbar Zertifizierungen – oder zumindest externe Auditierungen – helfen: Denn 96 % der von den analysierten Sicherheitsvorfällen betroffenen Unternehmen erfüllten nicht die Anforderungen von PCI DSS.

Smartphone-Security-Software

Android ist eines der Sicherheitsthemen, bei denen momentan viel Bewegung zu beobachten ist – im Guten wie im Schlechten. So präsentierte einerseits die NSA im Februar 2012 ein auf SELinux zurück gehendes, um zusätzliche Sicherheitsfunktionen erweitertes SE Android; in Deutschland wurden auf der CeBIT 2012 abhörsichere Handys auf Android-Basis vorgestellt.

Andererseits belegt eine am 07.02.2012 veröffentlichte Untersuchung der Universität North Carolina, dass ca. 0,02 % der Apps in Googles Market und etwa zehn bis 25mal so viele in unabhängigen Märkten Malware enthalten. Dabei behauptete Google am 02.02.2012, nach der Einführung eines automatisierten „Türstehers" bereits einen vierzigprozentigen Rückgang bösartiger Software im Market beobachtet zu haben.

Eine bösartige App zu laden ist jedoch nicht der einzige Weg, über den Schadsoftware auf ein Smartphone gelangen kann: Bei der RSA Konferenz präsentierten Forscher am 29.02.2012 eine funktionsfähige Drive-by-Infektion für Android-Geräte, deren „Marktwert" sie auf 15.000 US$ schätzten. Derweil berichtete die Intel-Tochter McAfee am 14.03.2012 von einem in Spanien gesichteten Android-Trojaner, der sich als vorgeblicher Generator von Sicherheitscodes tarnt, Online-Banking-PINs abphisht und auch gleich die zugehörigen mTANs umleitet – Online-Diebstahl ganz ohne Infektion des heimischen PC.

Dem am 15.03.2012 veröffentlichten Testbericht des unabhängigen Magdeburger Labors AV-Test zufolge erreichen hingegen nur zehn von 41 getesteten Virenscannern für Android eine Schadsoftware-Erkennungsrate von mehr als 90 %. Und auch für verlorene Geräte sieht die Statistik nicht gut aus: Am 09.03.2012 berichtete Symantec von den Resultaten eines Feldtests, bei dem nur etwa die Hälfte der als Köder „vergessenen" Smartphones zurückgegeben, aber die Daten fast aller Geräte vom Finder eingehend durchsucht wurden.

Derzeit sollten daher die Erwartungen an das bei Smartphones erreichbare Sicherheitsniveau generell nicht zu hoch angesetzt werden.

Neues iPad – neuer Crack...

Am 07.03.2012 hat Apple „The New iPad" samt iOS 5.1 vorgestellt. Es kommt mit neuem Prozessor und überarbeiteter Firmware daher und weckte bei Sicherheitsverantwortlichen in Unternehmen die Hoffnung, bestehende Sicherheitslücken, ob durch die Hard- oder die Software der iDevices bedingt, zu beheben. Doch dieser Traum währte nur kurz: Nach kaum einer Woche wurden erste Hinweise auf einen neuen Jailbreak publiziert und auch an älteren iDevices (iPhone 4S und iPad2) demonstriert.

Nicht nur die Geschwindigkeit war überraschend, mit der die Jailbreak Community agierte, sie stellte darüber hinaus auch noch gleich drei Ansätze vor, wie ein solcher Jailbreak in die Tat umgesetzt werden kann. Erstaunlich ist auch, dass einer dieser Ansätze auf einer bereits seit vier Monaten bekannten Schwachstelle beruht. Hier hat wohl die Qualitätssicherung für iOS 5.1 geschwächelt.

Den Sicherheitsverantwortlichen in den Unternehmen bleibt also auch weiterhin nur zu empfehlen, genau zu prüfen, welche Anwendungen und Informationen auf iDevices verwendet und gespeichert werden dürfen, und gegebenenfalls eine Sicherheitsüberprüfung der dienstlich eingesetzten iDevices durchzuführen.

Apple goes Datenschutz

Jedes iOS-Gerät verfügt über eine 40 Stellen lange Zeichenkette, mit der sich iPhone, iPad und iPod touch eindeutig identifizieren lassen: die so genannte UDID (*Unique Device Identifier*). Viele Apps benutzen diese UDID zur Erstellung detaillierter Nutzerprofile und zur Weitergabe an Werbetreibende. Datenschützern war dies schon lange ein Dorn im Auge und führte dazu, dass Apple bereits Mitte August 2011 ankündigte, dies zu ändern.

Nun ist es offenbar soweit: Apple verweigert zur Zulassung eingereichten Apps die Freigabe, wenn sie von der UDID Gebrauch machen. Entwickler, so Apple, sollen sich in ihren Apps zukünftig eigene Kennnummern erstellen und diese unabhängig voneinander verwalten. Eine Umstellung, die vor allem das Tracking individueller Geräte und ihrer Nutzer über mehrere Apps hinweg verhindern soll.

App-Entwickler müssen sich daher umstellen – für sie gibt es zukünftig keine zuverlässige Möglichkeit mehr, anhand der Hardware-ID festzustellen, dass eine App auf einem bestimmten, registrierten und zugelassenen Gerät läuft.

Schwachstellen-Hitliste

Das Forbes-Magazin hat nach eigenen Recherchen eine „Preisliste" für Schwachstellen einzelner Systeme und Anwendungen veröffentlicht. Sie wird derzeit von Apple angeführt: Für iOS-Schwachstellen werden angeblich bis zu 250.000 US$ bezahlt. Die Nachfrage scheint primär von „regierungsnahen Institutionen" zu kommen. Forbes nennt auch einige Kriterien, die erfüllt sein müssen, damit Höchstpreise bezahlt werden: Die Schwachstelle muss neuartig sein, muss dem Käufer exklusiv überlassen werden und darf auch dem Hersteller nicht mitgeteilt werden.

Dieses Interesse könnte aus den Strafverfolgungsbehörden stammen, die im Falle einer Beschlagnahme auch ohne Mitwirkung des Eigners auf die gespeicherten Daten zugreifen möchten, Oder aber es gibt noch Sicherheitsbehörden, deren Glaube an einen funktionierenden behördlichen „Online Trojaner", der sich in der Szene verbergen lässt, nach wie vor ungebrochen ist. Vielleicht arbeiten die Kollegen vom Nachrichtendienst aber auch schon an Stuxnet Mobile.

Secorvo News

Smartphones. Smartpads. Smartlecks.

Steve Jobs hat eine enorme Flutwelle ausgelöst, die Massen an Smartphones und Tablettcomputern in die Unternehmen schwemmt. Zwar können sich IT-Abteilungen eine Zeit lang „schützen", aber früher oder später muss sich auch der letzte standhafte CIO der Kraft der Mobile Device Welle ergeben – der Druck ist einfach zu hoch.

Doch was treibt die Anwender zum verstärkten Einsatz von Smartphones und Tablettcomputern? Was bedeutet der Einsatz solcher Geräte für die IT-Abteilungen, für die IT-Sicherheit und für das Unternehmen? Und welches Mobile Device Management System ist das Beste?

Diese Fragestellungen erörtert Christian Rückert (Netlution GmbH) in seinem Vortrag „Sicheres Mobile Device Management" auf dem nächsten KA-IT-Si Event am **26.04.2012.** Dabei werden neben den führenden Mobile Device Management Lösungen auch organisatorische Themen diskutiert. Beginn ist um 18 Uhr im Schlosshotel Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Seminare in Q2

Das zweite Quartal 2012 startet bei Secorvo College mit dem Seminar PKI – Grundlagen, Vertiefung, Realisierung vom 23.-26.04.2012. Erfahren Sie mehr zu Konzeption, Implementierung und Nutzung von PKIs und sichern Sie sich kurzfristig noch Ihren Seminarplatz. Wir freuen uns auf Ihre Teilnahme.

Wenige freie Plätze gibt es auch noch für die nächste Schulung zum TeleTrusT Information Security Professional (T.I.S.P.) vom 07.-11.05.2012 mit anschließender Zertifikatsprüfung. Als Seminarteilnehmer bekommen Sie Ihr Exemplar des T.I.S.P.-Buchs zur Vorbereitung automatisch vorab zugesandt – Sie können das Buch natürlich auch unabhängig von einer Seminaranmeldung bestellen (ISBN: 978-3-942594-08-0).

Ebenfalls im Mai, vom 23.-24.05.2012, bieten wir mit dem zweitägigen Seminar Aktuelle Herausforderungen der Informationssicherheit einen kompakten Überblick zu wesentlichen Themen rund um die Weiterentwicklung der Informationssicherheit.

Die Programme aller Seminare sowie die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college/.

Veranstaltungshinweise

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

April 2012	
15.-19.04.	Eurocrypt 2012 (IACR, Cambridge/UK)
16.-17.04.	a-i3/BSI-Symposium 2012 (Arbeitsgruppe Identitätsschutz im Internet/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)
Mai 2012	
07.-12.05.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
09.-10.05.	BvD Verbandstag 2012 (BvD e.V., Berlin)
23.-24.05.	Aktuelle Herausforderungen der Informations-sicherheit (Secorvo College, Karlsruhe)
Juni 2012	
11.-13.06.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
14.-15.06.	Datenschutzaudit (Secorvo College, Karlsruhe)
18.-19.06.	DuD 2012 (Computas, Berlin)

Fundsache

Wer hat nicht schon mal von den Sicherheitsprinzipien „Least privilege“ oder „Fail safe defaults“ gehört. Entgegen weit verbreiteter Annahmen handelt es sich hierbei um lang bekannte Prinzipien, die vor 37 Jahren von Saltzer und Schroeder in ihrem Aufsatz „The Protection of Information in Computer Systems“ vorgestellt wurden. Wem das Originalpapier zu trocken ist, dem könnte die Erklärung der Prinzipien anhand von Szenen aus Star Wars gefallen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Jörg Völker

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