In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

Wer in den letzten Wochen und Monaten die Presse verfolgt hat, sieht, dass Hacker-Angriffe schon lange nicht mehr nur vereinzelte Ausnahmefälle sind (Twitter wurde gehackt, NY-Times trojanisiert, Facebook). Hieraus folgt, dass viele Unternehmen die Sicherheit ihrer eigenen IT nicht vollumfänglich gewährleisten können.

Um auf die persistierende Gefahr zu reagieren, wird nun sowohl auf internationaler als auch nationaler Ebene eine Meldepflicht für Hacker-Attacken gefordert.[1] Dieser Vorstoß betrifft zunächst nur die Unternehmen, die für das öffentliche Leben notwendige Infrastrukturen (Telekommunikation, Energie, Notfallversorgung, etc.) betreuen.

Oft wird der Wunsch nach Sicherheit missbraucht, um mehr staatliche Überwachung durchzusetzen: Bürgerrechtler klagen oftmals zu Recht, dass die Freiheit dann dem Wunsch nach Sicherheit zum Opfer fällt. Im konkreten Fall jedoch sehe ich es nicht so. Wenn ein Energieversorger von chinesischen Hackern angegriffen wird und dies daher einer Behörde zu melden ist, dann bleiben Bürgerrechte davon unangetastet.

Ich stehe Initiativen von staatlicher Seite auch oft skeptisch gegenüber. Meiner Auffassung nach müssen Unternehmen eigenverantwortlich handeln und sich selbst schützen, denn der Staat kann in einem „entgrenzten“ Internet keinen Schutz bieten. Dennoch begrüße ich eine solche Meldepflicht, weil die Gefahrenlage trotz der vielen Medienberichte völlig unterschätzt wird. Auf jeden Hacker-Vorfall, der in den Medien Erwähnung findet, kennen wir mindestens zehn weitere Vorfälle, die unveröffentlicht bleiben.

Eine solche Meldepflicht an sich wird keine konkreten Verbesserungen bringen. Allerdings schärft das Wissen um das Ausmaß unser Bewusstsein und kann uns helfen, auf akute Fälle angemessen zu reagieren.

Auf die ersten amtlichen Statistiken zu IT-Sicherheitsvorfällen bin ich gespannt. Ich erwarte, dass eine enorme Anzahl von Vorfällen dokumentiert werden wird. Noch mehr bin ich auf die Reaktionen der IT-Welt gespannt, wenn die Tatsache ins öffentliche Bewusstsein dringt, dass es gang und gäbe ist, professionelle Hacker im eigenen Unternehmensnetzwerk als blinde Dauerpassagiere zu beherbergen.

Herzliche Grüße,

Ihr Sebastian Schreiber

Bitte beachten Sie die Hinweise zu den aktuellen Events und Schulungen auf der nächsten Seite

Aktuelle Events

27.02.13	LH[1] Finn Steglich, Bechtle IT-Forum Cisco, Bonn
05.-09.03.13	CeBIT 2013, SySS in Halle 5 an Stand F18 (Heise-Stand) LH[1] jeden Tag um 14.00 Uhr
13.03.13	LH[1] Sebastian Schreiber, IDC IT-Security Roadshow, Moskau
09.-10.04.13	Sebastian Schreiber Referent bei Kongressmesse World of Cloud, Frankfurt/Main

[1] Live Hacking

Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage www.syss.de.

Aktuelle Schulungen

Web-App: 12. - 13.03.13 14. - 15.05.13	**IT-Forensik:** 23. - 25.04.13
PenTests: 15.03.13	**IPv6:** 03.06.13
WLAN: 20. - 21.03.13	**Windows-Angriffe:** 05. - 06.06.13
Exploits: 10. - 11.04.13	**Incident Response:** 11. - 13.06.13
IT-Security I: 15. - 16.04.13 17. - 18.06.13	**IT-Recht:** 21.06.13
IT-Security II: 17. - 18.04.13 19. - 20.06.13	**Zusatztermin! Mobile Device:** 25. - 26.06.13

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an info@syss.de.

Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit, wir werden Sie dann umgehend aus dem Verteiler entfernen.

[1] siehe beispielsweise: http://www1.wdr.de/themen/digital/cyberattacken100.html

Impressum:
SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 407856-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Diplom-Inform. Sebastian Schreiber
Verantwortlich für Inhalt: Marcus Bauer

Sebastian Schreiber auf der CeBIT:

Vom 05. - 09.03.13 ist Sebastian Schreiber auf der CeBIT. Wenn Sie ihn unverbindlich treffen möchten, vereinbaren Sie einfach einen Termin über seine Persönliche Assistentin Hanna Zimmermann!
hanna.zimmermann@syss.de

Zusatztermin Mobile Device Hacking:

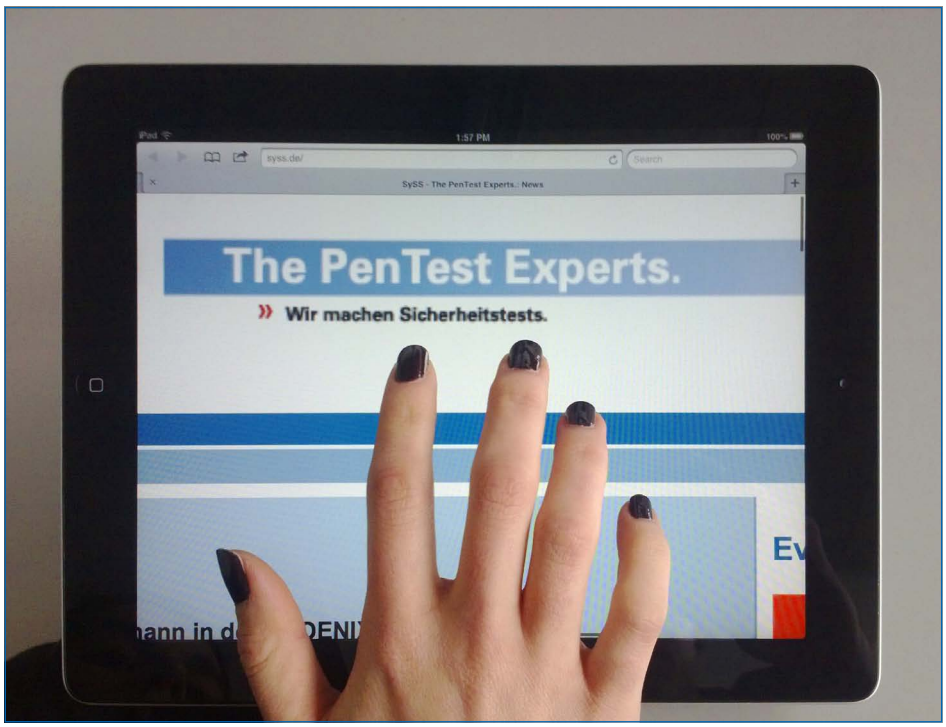
Seit diesem Jahr bieten wir den SySS-Workshop „Mobile Device Hacking“ an.
Wegen der überwältigenden Nachfrage bei der Durchführung des ersten Workshops Anfang Februar bieten wir diese Schulung zusätzlich am 25./26. Juni 2013 an.

Mobile Devices – wie sicher sind die mobilen Alleskönner im Geschäftsleben?

von Philipp Buchegger

Apple brachte letztes Jahr das iPhone 5 heraus und auch der Absatz von günstigen Android-Geräten hat im Quartal 3 des Jahres 2012 einen Marktanteil von 75% erfahren. 1,3 Mio Android-Geräte werden pro Tag aktiviert. Mobile Devices erfreuen sich regen Zuspruchs. Immer mehr Menschen nutzen iPhones und andere Smartphones.

Kein Wunder, dass die Geräte beliebt sind: Schließlich kann ein Nutzer von überall aus ins Internet. Die Geräte sind zudem klein und handlich, passen in Jacken-, Hosen- und Handtaschen und können in vielen Bereichen ein Notebook ersetzen. Doch nicht nur im Privaten erleben diese Mobilgeräte einen kometenhaften Aufschwung. Sie werden auch zunehmend für Geschäftsleute interessant. In Zeiten der Globalisierung und der zunehmenden Flexibilität verschwimmen bei vielen Menschen die Grenzen zwischen Privatem und Geschäftlichem. Sie arbeiten abends und am Wochenende oder müssen ständig erreichbar sein. Mobile Devices erweisen sich hierbei als geschickt, die universell einsetzbaren Geräte sparen Zeit und Aufwand. Geschäftsprozesse und vor allem unternehmenskritische Daten werden infolgedessen auf diesen Devices gespeichert, E-Mails empfangen, gelesen und beantwortet, Kalender gepflegt, etc.



Quelle: SySS

Es ergeben sich Fragen von sicherheitstechnischer und rechtlicher Natur: Wie sicher sind Mobilgeräte überhaupt? Wie leicht können Daten extrahiert werden bei physikalischem Zugriff auf das Gerät? Wie verläuft die Kommunikation, verschlüsselt oder unverschlüsselt? Wo werden die mobilen Devices genutzt? Können die Geräte ausschließlich in sicheren Netzwerken betrieben werden? Dürfen vertrauliche, unternehmenskritische Daten überhaupt auf Mobile Devices gespeichert werden?

Die IT-Sicherheitsbeauftragten eines Unternehmens werden sich daher fragen, wie sie unternehmenskritische Daten besser schützen können und feststellen, dass ihre Aufgabe in der Evaluation besteht, wo eine Separierung zwischen Privat- und Geschäftsbereich nötig und möglich ist.

Neben der Möglichkeit des physikalischen Zugriffs liegt ein Grundproblem in der Tatsache begründet, dass unternehmenskritische Daten aufgrund der mobilen Natur der Geräte durch diverse und unterschiedlich sichere Netzwerke transportiert werden. Ein Nutzer kann daher nie wissen, ob es jemanden gibt, der im für alle zugänglichen freien WLAN am Flughafen oder am Hauptbahnhof als Man-in-the-Middle fungiert. Ebenso stellt sich die Frage, ob Cloud- oder sonstige Internetdienste wirklich sicher sind und ob ein Nutzer diesen Diensten sensible Daten anvertrauen will.

Um vertrauliche Daten schützen und gegen Missbrauch vorbeugen zu können, muss das Mobile Device Management die Nutzerrechte jedes Einzelnen zu einem gewissen Grad beschränken. Dies sorgt natürlich dafür, dass auch die private Nutzung beschnitten werden kann. Somit nehmen Nutzer IT-Sicherheit als negativ wahr, da der Spaß am Gerät deutlich gebremst wird.

Auch die mittlerweile gängige Praxis des „Bring Your Own Device“ erfreut sich hoher Beliebtheit. Aber wenn das Gerät nicht der Firma, sondern dem Nutzer gehört, so kann das Mobile Device Management den Nutzer auch nur bedingt einschränken beziehungsweise die Nutzungsbedingungen des Geräts festlegen, um den Geschäftsdaten möglichst viel Sicherheit zu gewähren. Eine Erhöhung der Sicherheit in diesem Fall kann durch sogenannte Container-Lösungen erreicht werden.

Um IT-Sicherheit Raum zu geben, müssen Unternehmen einen Kompromiss zwischen Bedienkomfort und dem hohen Schutzbedarf der Daten finden. Um abwägen zu können, wie ein solcher Kompromiss gestaltet werden kann, empfiehlt es sich, dass sowohl IT-Zuständige in Unternehmen als auch Einzelnutzer sich klarmachen, wie iOS- und Android-Geräte aufgebaut sind und welche Angriffsszenarien generell möglich sind. Dieses Wissen wird Unternehmen helfen, ihr Mobile Device Management zu steuern und auch notwendige Investitionen in Relation zu aus einem Angriff entstehenden finanziellen Einbußen und dem resultierenden Image-Schaden zu setzen. In gleicher Weise sensibilisiert dieses Wissen End-User in ihrem eigenen Umgang mit vertraulichen, schützenswerten Daten.