

# Newsletter

In diesem Newsletter erwarten Sie folgende Inhalte:

- **Grußwort**  
„Wie bei Sony: So nie!“
- **Events und Schulungen**
- **Zwei neue Schulungen**
- **„Das iPhone erobert die Geschäftswelt“**



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

Sehr geehrte Kunden, liebe Geschäftspartner, Freunde und Bekannte,

von der Tagesschau bis hin zum Provinz-Blatt berichteten absolut alle Medien über den Datenskandal bei Sony. Während bis vor ein paar Tagen nur die Server der Sony Playstation betroffen waren, von denen weit über 70 Millionen Kundendaten ausgelesen werden konnten, berichtet die Presse nun, dass Hacker auch in das Netzwerk der Konzerntochter Sony Online Entertainment eingedrungen seien. SPIEGEL-Online berichtet am 03. Mai 2011, dass dort vertrauliche Daten von 24,6 Millionen Kundenprofilen ausgelesen werden konnten. Zusammen mit den Daten der Kunden von Sony Playstation ist dies ein Skandal mit enormer Auswirkung.

Spektakulär ist insbesondere, dass Sony keine grundlegenden Sicherheitsvorkehrungen getroffen hat! Dass man Passwörter gar nicht unverschlüsselt abspeichern, sondern stattdessen einen Hash-Wert nutzen sollte, war bereits 20 Jahre vor dem Verkauf der ersten Sony Playstation bekannt und Usus. Wie es zu diesem Fehler gekommen ist, kann ich mir sehr gut vorstellen. Zunächst wurde ein Prototyp der Applikation erstellt. Doch da die Zeit bis zum Release-Termin drängte, musste Sony die Prioritäten anders setzen, man brauchte schnell eine funktionierende Lösung. Also verzichtete man auf die Verschlüsselung, da der Produktionsstart unter keinen Umständen gefährdet werden durfte. Vielleicht hatte Sony ursprünglich vor, die Verschlüsselung später nachzurüsten, was dann allerdings (vielleicht im Hinblick auf den Einbau neuer Features) niemals stattfand.

Was zeigt uns diese Geschichte? Wir lernen vor allem eines über die Abspeicherung von Passwörtern im Klartext: „Wie bei Sony: So nie!“.

Die Medien zeigen sich besonders überrascht darüber, dass ein großer internationaler Konzern wie Sony überhaupt „hackbar“ ist. Dies verwundert mich jedoch ganz und gar nicht: Seit dreizehn Jahren bin ich mittlerweile Geschäftsführer der SySS GmbH – und praktisch vergeht keine Woche, in der wir nicht im Rahmen unserer Penetrationstests in die Server unserer Kunden eindringen und Zugriff auf vertrauliche Daten wie Versicherungspolice, Bankkonten, Personaldaten, aber eben auch Klartextkennwörter oder gehashte Passwörter nehmen können.

Ich bin stolz auf mein tolles Team und freue mich, dass wir unseren Kunden einen echten Nutzen bringen, indem wir sie mehrfach pro Woche dabei unterstützen, kleine und größere Sony-Skandale zu verhindern.

Herzliche Grüße,  
 Ihr Sebastian Schreiber



## Zwei neue Schulungen bei der SySS GmbH

Die SySS GmbH hat ihr Schulungsangebot um zwei **SySS-Workshops** erweitert: „Sicherheit bei Web-Applikationen“ (Termine: 08.-09.06. und 17.-18.10.) und „Exploit Development“ (26.-27.09. und 23.-24.11.)

**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.**

## Quartal 2/2011

### Events:

- **11.05.:** Vortrag auf 12. Dt. IT-Sicherheitskongress, Bonn
  - **16.05.:** LH\* 11.Management Circle Jahreskonferenz
  - **20.05.:** LH Informationstag „Cyber Crime“, Berlin
  - **24.05.:** LH „Sicheres Netz hilft“, Bad Nauheim
  - **28.05.:** LH Alumni-Tag, Hochschule Esslingen
  - **30.05.:** LH Dt. Präventionstag, Oldenburg
- \*LH=Live Hacking

**Detaillierte Informationen zu diesen Veranstaltungen finden Sie auf unserer Homepage [www.syss.de](http://www.syss.de).**

### Schulungen:

- WLAN: 26.-27.05.
- Durchführung PenTests: 06.06.
- Sicherheit Web-Apps: 08.-09.06.
- IT-Security I: 27.-28.06.
- IT-Security II: 29.-30.06.
- IPv6: 08.07.
- IT-Recht: 15.07.

### Bei Teilnahmewunsch

**oder Fragen wenden Sie sich bitte an [info@syss.de](mailto:info@syss.de).**

## Das iPhone erobert die Geschäftswelt

Doch ganz gefahrlos ist die Einführung von neuen mobilen Geräten nicht!

Menschen zeigen gerne ihr Mobiltelefon. Wenn sie in Cafés oder Restaurants sitzen, liegt das Gerät griffbereit auf dem Tisch vor ihnen, sie nutzen es an öffentlichen Plätzen oder in Verkehrsmitteln, telefonieren, schreiben Kurznachrichten oder organisieren ihr Leben damit. Seit einiger Zeit fällt auf, dass immer mehr Menschen iPhones oder vergleichbare Smartphones nutzen. Solche Telefone sind kleine Computer, die dem Nutzer eine Menge an Anwendungsmöglichkeiten bieten. Neben den schon seit längerem im Einsatz befindlichen Funktionen wie Kamera oder MP3-Player, können Nutzer mobil ins Internet gelangen, ihre E-Mails abrufen, Nachrichtenseiten lesen oder sonstige Annehmlichkeiten des Internetzugangs nutzen. Das iPhone ist leicht zu bedienen und erfreut sich einer starken Nachfrage.

Was im Privaten geschickt ist, fasziniert auch die Geschäftswelt. Die leichte Bedienweise macht das Gerät für Geschäftsführer interessant, da es ihren Arbeitsalltag immens erleichtert. Daher sorgen sie verstärkt dafür, dass iPhones auch im Geschäftlichen Einzug halten. Da es jeder hat, will niemand darauf verzichten, das iPhone hat schon den Charakter eines Statussymbols. Ungewöhnlich ist, dass hier ein gesellschaftlicher und beruflicher Druck aus mehreren Schichten auf die IT stattfindet, denn sowohl die Geschäftsführungsebene als auch die normalen Mitarbeiter fordern, ein solches Gerät nutzen zu können, ohne jedoch auf Sicherheitsaspekte zu achten.

Doch was im Privaten problemlos verwendet werden kann, birgt im Businessbereich einige Gefahren. SySS-Mitarbeiter, IT-Security Consultant Karsten Kinder, warnt vor einer sorglosen Nutzung im Geschäftsbereich, ohne zumindest organisatorische Richtlinien einzuführen, die Missbrauch und eine Gefährdung des Gerätes samt des Datenbestandes verhindern sollen. So sollte laut Kinder nicht gestattet sein, dass Mitarbeiter ihr geschäftlich genutztes iPhone/iPad an ihren Privat-PC anschließen dürfen. Ein Privat-PC sei in der Regel nicht so gut geschützt wie ein Firmen-PC und aus diesem Grund leichter anfällig für Schadsoftware, die Angreifern die Möglichkeit des Ausspähens erleichtert. Wenn ein Nutzer das iPhone an seinen Computer anschließt, erstellt iTunes nach kurzer oder keiner Nutzerinteraktion ein Backup des mobilen Gerätes. Somit befinden sich alle Daten des iPhones/iPads (Geschäftskontakte als auch SMS sowie E-Mails) auf dem Privatsystem des Nutzers. Und somit ist ihr Speicherort oftmals weitaus weniger geschützt als auf einem System des Unternehmens. Mittlerweile gibt es Programme, mit welchen es relativ einfach ist, die Backups auszulesen. Diese sind unter anderem der iPhone Backup Extractor (Windows)<sup>1</sup> oder das Programm Juicephone (Mac OS)<sup>2</sup>. Um dem unautorisierten Auslesen durch Dritte zu begegnen, können die Backups verschlüsselt werden.

<sup>1</sup> <http://www.iphonebackupextractor.com/>

<sup>2</sup> <http://www.addpod.de/juicephone>



Abb.1: Herkömmliches iPhone

Doch auch hier gibt es mittlerweile Software, wie den Elcom Soft Phone Password Breaker<sup>3</sup>, welcher in der Lage ist, verschlüsselte Backups zu entschlüsseln. Nach der Entschlüsselung ist es für einen Angreifer sehr einfach, die verschiedenen Datenbanken (SQLite) auszulesen. Somit können vertrauliche Daten wie SMS, Adressbücher (siehe Abbildung auf Seite 3), Fotos, Anruflisten und vieles mehr durch einen Angreifer in Erfahrung gebracht werden. Das iPhone verfügt über ein paar Schutzmechanismen, die jedoch unter gewissen Umständen umgangen werden können. Bei Verlust des Gerätes existiert die Möglichkeit, die Daten per Remote Wipe-Modus unkenntlich zu machen. Dies ist jedoch nur dann sinnvoll, wenn der Modus möglichst rasch nach Feststellung des Verlusts aktiviert wird. Liegt ein längerer Zeitraum dazwischen, wird dieser Modus allerdings obsolet.

Zu den organisatorischen sollte auch die Forcierung technischer Richtlinien mit Hilfe des iPhone Configuration Utility in Erwägung gezogen werden. Beispielsweise kann durch eine geeignete Konfiguration das Verschlüsseln von Backups forciert, eine gewisse Passwortkomplexität erzwungen und zusätzlich auch die Installation beliebiger Applikationen verhindert werden - was allerdings dem Gerät seinen Reiz nimmt und damit bei den Nutzern auf Ablehnung stößt.

<sup>3</sup> <http://www.elcomsoft.de/eppb.html>

Eine weitere Sicherheitsmaßnahme ist die Tatsache, dass auf iPhones eine Festplattenverschlüsselung implementiert ist, diese jedoch nur dann aktiviert wird, wenn das Gerät ausgeschaltet ist, was in der Praxis selten vorkommt, da die iPhones meistens einsatzbereit und eingeschaltet sind.

Auch die Möglichkeit eines Jailbreak sollte aus organisatorischen Gründen ausgeschlossen werden und nie passieren, da ein Angreifer somit besonders einfache Möglichkeiten hätte, auf das Gerät zuzugreifen. Ebenso besteht bei eigenmächtiger Installation von Apps ein nicht zu unterschätzendes Risiko von Schadsoftware, da sie nicht unbedingt entdeckt wird.

Gegenwärtig sind noch keine ausreichenden Schutzmechanismen für Mobile Devices auf dem Markt, obwohl hier durchaus Bestrebungen im Gange sind, Smartphones wie das iPhone oder iPad sicherer zu machen. Der Grund besteht hier in der Softwarearchitektur des iPhones bzw. iPads. So besteht das Gerät aus zwei Ebenen, nämlich der Nutzerebene, des sogenannten User- und dem Kernel-Space als ihr Fundament. Zurzeit erlaubt Apple nur die Installation von Software im User-Space. Schutzmechanismen, wie eine Firewall oder eine Antivirensoftware, müssen allerdings nach Ansicht des SySS-Mitarbeiters Karsten Kinder in der darunterliegenden Ebene implementiert sein, um einen sinnvollen Schutz zu gewährleisten.

Aus diesen Gründen rät Kinder, drei organisatorische Tipps für den Umgang mit geschäftlich genutzten iPhones umzusetzen:

1. Ein dienstliches Gerät darf nicht an einen Privat-PC angeschlossen werden
2. Grundsätzlich müssen alle Backups verschlüsselt abgelegt werden
3. Das iDevice darf auf keinen Fall „gejailbreakt“ werden.

Das iPhone/iPad ist aus sicherheitstechnischer Hinsicht als externes Gerät wie beispielsweise ein Notebook für einen Außendienstmitarbeiter zu betrachten.

Eben dieses Notebook wird von der IT mit einer Antiviren-Lösung, einer Firewall sowie einer Festplattenverschlüsselung versehen. Des Weiteren wird dem Mitarbeiter äußerst selten bis nie gestattet, zusätzliche Software auf dem Gerät zu installieren. Dieser Standard ist bei iPhones, iPads, Smartphones, etc. nicht gegeben. Daher sollte die Nutzung von iPhones in der Geschäftswelt gut vorbereitet und die Sicherheitsaspekte sorgfältig abgewägt werden.

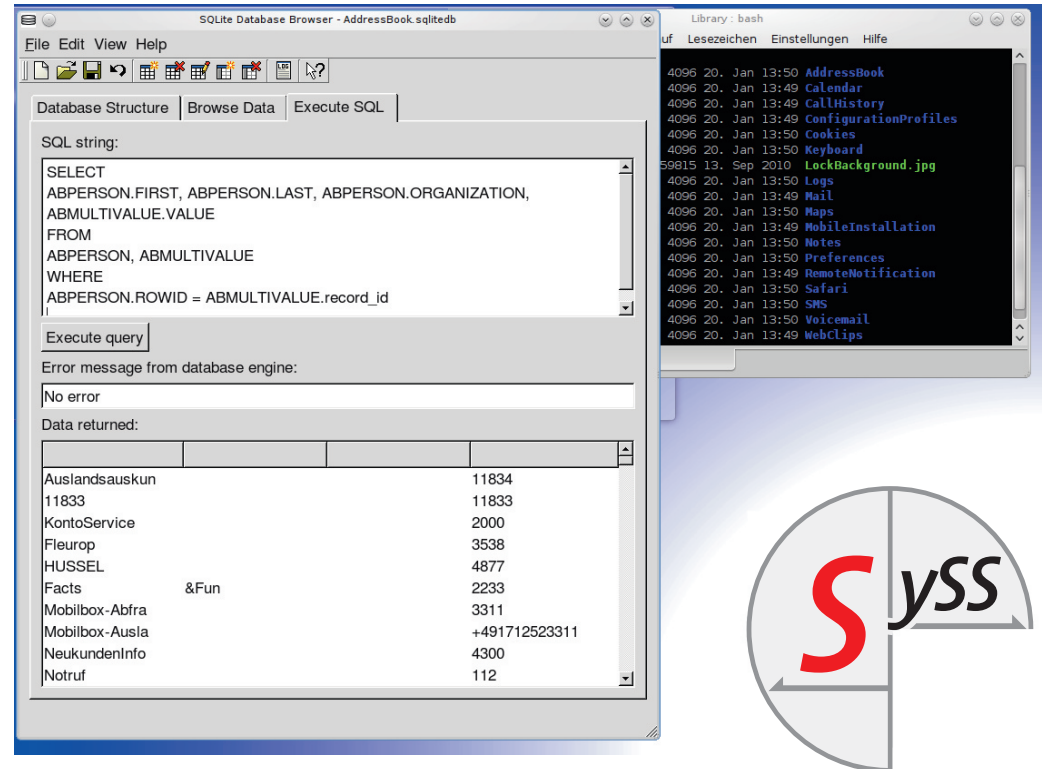


Abb.2: Auslesen des Adressbuches