

Newsletter

In diesem Newsletter erwarten Sie folgende Inhalte:

- **Grußwort**
- **Events und Schulungen**
- **„Incident Response - Wie die Möglichkeit v. Hackerangriffen eingedämmt werden kann“**



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,

heute Morgen erhalte ich eine E-Mail vom 14-jährigen Fabian. Der Junge hat meine Auftritte im Fernsehen und auf Messen verfolgt und bezeichnet sich als Fan von mir. Fabian weist mich auf seine Homepage hin, auf der er insgesamt fünfundzwanzig Video-Tutorials veröffentlicht wie z. B. „Theorie der DDoS-Attacken“, Virenschanner überlisten, „Theorie des Luhn-Algorithmus“, „PDF-Exploits“, „Windows-Accounts knacken – Teil-2“, etc. Insgesamt sind die Inhalte der Videos gut strukturiert und gut aufgearbeitet. Fabian will Penetrationstester werden und fragt mich, was er dafür tun und wie er sich noch weiterbilden kann. Folgendes gebe ich ihm mit auf den Weg:

- Viele Programmiersprachen lernen
- Fremden Code lesen
- Gutes Abitur – danach Hochschulstudium
- Auslandssemester oder Auslandspraktikum
- Sauberes Verhalten, d. h. keinen Kontakt zu kriminellen Hackern

Ich habe den Eindruck, dass Fabian auf dem richtigen Weg ist; er hat Interesse an der Thematik IT-Sicherheit und macht für einen Vierzehnjährigen eine außerordentliche Arbeit. Auch seine Einstellung und sein Verhältnis zum Gegenstand seiner Arbeit gefällt mir: Er distanziert sich in jedem Video von illegalem Hacking.

Aber wie sieht es mit den anderen Teenagern aus? Ist es nicht völlig gewöhnlich, dass man in dem Alter auch mal Dummheiten macht? Einen Fußball in die Fensterscheibe des Nachbarn donnert – oder an Sylvester einen Böller im Briefkasten zündet? Ich weiß genau, dass sich gerade Jugendliche zur illegalen oder halblegalen Hackerszene hingezogen fühlen, hier neue Angriffstechniken lernen und erarbeiten. Gerade im Hinblick auf die vielen Hacker-Einbrüche, über die wir fast täglich aus den Medien erfahren, bin ich in Sorge darüber, dass Angriffe äußerst einfach durchzuführen sind: Neulich trat ich wieder bei Stern-TV auf und hatte dort die Gelegenheit, mich mit DJ Stolen – dem Hacker von Lady Gaga und Justin Timberlake – auszutauschen. DJ Stolen war zum Tatzeitpunkt drei Jahre älter als Fabian – also siebzehn. Zu meinem Erstaunen beherrscht DJ Stolen – ganz im Gegensatz zu Fabian - nicht einmal eine einzige Programmiersprache und war dennoch in der Lage, mp3-Musikstücke von den Servern der großen Musikkonzerne zu kopieren.

Über einen Punkt jedoch bin ich nicht in Sorge: die Thematik IT-Security, die Hacking und Penetrationstests umfasst, bleibt spannend – dass meinem Team und mir die Arbeit ausgeht, ist ausgeschlossen.

Herzliche Grüße,
 Ihr Sebastian Schreiber



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 3/2011

Events:

- **14.09.:** LH¹ Cybersecurity, Berlin
- **22.09.:** LH Messe IT-Business, Stuttgart
- **23.09.:** PD² Sicherheit Soziale Netzwerke, München
- **28.09.:** Vortrag Secure Summit, Darmstadt
- **04.10.:** PD Sicherheit Soziale Netzwerke, Wien
- **11.-13.10.** LH auf IT-SA, Nürnberg

¹LH=Live Hacking

²PD=Podiumsdiskussion

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

Schulungen:

- IT-Security I: **12.-13.09./10.-11.10./28.-29.11.**
- IT-Security II: **14.-15.09./12.-13.10./30.11.-01.12.**
- Exploit: **26.-27.09./23.-24.11.**
- Sicherheit Web-Apps: **17.-18.10.**
- IPv6: **28.10.**
- Durchführung PenTests: **11.11.**
- IT-Forensik: **14.-16.11.**
- IT-Recht: **02.12.**
- WLAN: **12.-13.12.**

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

Incident Response

Wie die Möglichkeit von Hackerangriffen eingedämmt werden kann

von Stefan Arbeiter

Zurzeit vergeht praktisch kein Tag ohne die Meldung von Datendiebstählen. Die letzten Opfer dieser Angriffe sind zum einen prominente Dienstleister des US Militärs (Booze Allen Hamilton und IRC Federal) und zum anderen auch eher bodenständige Unternehmen wie die REWE-Kette, die von unbekanntem Dritten auf Sicherheitslücken hingewiesen wurde. Die technischen Hintergründe der Angriffe sind jedoch nicht bekannt, es sei denn, die Angreifer stellen diese selbst zur Verfügung.

In der Regel liegt jedoch bei solchen Angriffen stets die bekannte „Verkettung unglücklicher Umstände“ vor – und nicht etwa „geheime Hacker-Tools“, gegen die es „keine Verteidigung“ gibt.

Barracuda Networks stellt dankenswerterweise die verschiedenen Schritte eines erfolgreichen Angriffs in Form einer „Post Mortem“-Analyse zur Verfügung¹ und zeigt, wie einzelne – scheinbar banale – Fehler zum Schadensfall führten. Die Beobachtungen sämtlicher Sicherheitsfirmen und nicht einzig der SySS GmbH münden in dem Ergebnis, dass die Angriffe meist einem einfachen Muster folgen:

- (1) Automatische Suche nach Sicherheitslücken oder häufigen Fehlkonfigurationen.
- (2) Manuelle Ausnutzung mit dem Ziel, permanenten Zugang zu dem betroffenen System zu erhalten.
- (3) Ausweitung dieses Zugangs durch Installation von Schadsoftware oder Kompromittierung legitimer Nutzerkonten.
- (4) Sammeln von Daten und Abzug derselben.

Die Logfiles von fast allen Webservern legen von (1) ein beredtes Zeugnis ab. Die Aktivität findet praktisch permanent statt, ohne dass ein Mensch mehr tun muss, als große Adressbereiche vorzugeben – falls sich die Werkzeuge mittlerweile nicht sogar selbst diese Daten zusammenstellen. Doch wie kommt es dann im Schadensfall dazu, dass viele, scheinbar nicht zusammenhängende Informationen den Angreifern in die Hände fallen? Bei IRC Federal wurde das folgende Verzeichnis-Listing eines kompromittierten Servers durch die Angreifer veröffentlicht² (siehe Abbildung 2).

In diesem Fall lagen Datenbanken eines internen Forums auf einem direkt aus dem Internet erreichbaren Webserver und dies sogar in gepackter Form, was den Angreifern im Zweifelsfall das Herunterladen erleichterte. Ein grundlegendes technisches Problem lag an dieser Stelle nicht vor, allerdings ein organisatorisches. Das Kompromittieren eines einzelnen Systems über das Internet sollte nicht die Möglichkeit nach sich ziehen, auch Daten abzugeben, die ausschließlich intern benötigt werden.



Abb.1: Hacker bei der Arbeit

Abb.2: Erfolgreiches Directory Listing

Directory of downloads/webdatabases/intranet

```
07/02/2011 02:58 AM <DIR> .
07/02/2011 02:58 AM <DIR> ..
07/02/2011 03:04 AM 1,044,480 Intranet_Forum.mdb
07/02/2011 02:58 AM 69 intra.7z
07/02/2011 03:04 AM 0 intra.mdb
07/02/2011 03:04 AM 1,155,892 Intra.zip
07/02/2011 03:06 AM 11,272,192 intra_4-17.mdb
07/02/2011 03:11 AM 18,403,328 test_intra.mdb
07/04/2011 08:00 PM 64 Intranet_Forum.ldb
```

Neben technischen Schutzmaßnahmen wie beispielsweise der Validierung aller Client-Eingaben in Webapplikationen sind daher weitere Maßnahmen von Bedeutung, um sowohl den Schaden im Falle eines erfolgreichen Angriffes als auch die Angriffsfläche selbst zu minimieren. Dies schließt ein, alle unnötigen und eventuell überflüssigen Informationen von Systemen in der DMZ und auch anderswo zu entfernen.

Die Spanne der zu entfernenden Informationen bzw. Daten reicht von alten Skripten mit Zugangsdaten bis zu Sicherungen von produktiven Datenbanken und umfasst Elemente nicht aktiver Webauftritte, vollständige Testumgebungen, Spuren derselben, archivierte E-Mails, etc. Oft finden sich vollständige Anwendungen und einzelne Server, die keinen produktiven Zweck mehr erfüllen. Noch im Jahre 2000 führten solche Informationen zu ungläubigen Reaktionen und zu der Frage: „Wie kann man denn einen Server im Internet vergessen?“ Und die Antwort ist einfach und lautet: „Wenn er keinen Ärger macht, sofort!“

Derartige Systeme sind für Angreifer besonders interessant, weil sie hier recht unmerkelt arbeiten können. Schließlich gibt es selten etwas zu kontrollieren und die Systeme sind nicht im unmittelbaren Blickfeld der Betreuer. Die Zeiträume, in denen solche Systeme sich selbst überlassen sind, können oft mehrere Monate betragen. Das Alter der einzelnen Systeme spielt ebenfalls eine Rolle: Sicherheitsmaßnahmen in Webapplikationen waren in den Zeiten der ersten DotCom-Blase noch wenig verbreitet. Am bekanntesten ist das Problem im Fall der Verbreitung von Malware: Immer wieder fallen hier Systeme auf, die gar nicht als vollwertige „Fat Clients“ betrachtet werden. Sie werden ausschließlich für bestimmte Aufgaben genutzt oder gar nur sporadisch eingeschaltet und erweisen sich als Einfallstor, weil sie nicht der üblichen Pflege unterliegen.

¹<http://blog.barracuda.com/pmblog/index.php/2011/04/26/anatomy-of-a-sql-injection-attack/>

²<http://pastebin.com/nHMTSnKF>

Im Falle von Verzeichnissen auf Webservern ergibt sich zudem das Problem, dass deren Betreuung in den wenigsten Fällen in den Händen einer organisatorisch homogenen Einheit liegt. Oft sind es mehrere Gruppen, die Systemverwalter auf der einen Seite und Webmaster und Entwickler auf der anderen. Erstere pflegen dabei Hardware und die Serversoftware an sich, die weiteren Gruppen die Anwendungen.

Bei routinemäßigen Kontrollen kann es geschehen, dass der Administrator schlichtweg nicht entscheiden kann, ob Informationen unnötig sind, da ihm nicht bekannt ist, ob diese eine Funktion haben oder nicht; das Risiko, die Anwendung zu gefährden, möchte er an dieser Stelle nur ungern eingehen. Aus dieser Situation lassen sich verschiedene organisatorische Maßnahmen ableiten:

- (1) Systembetreuer sollten stets wissen, welche Informationen sie gefahrlos entfernen können und sie sollten für das Entfernen auch autorisiert sein.
- (2) Temporär erzeugte Dateien oder Skripte, die nicht zu dem produktiven Teil des Webauftretens gehören, sollten stets so schnell wie möglich wieder entfernt werden.
- (3) Das Ablagesystem von Daten (insbesondere personenbezogenen) sollte dahingehend organisiert sein, dass keine aufwendigen Recherchen nötig sind, um zu erkennen, ob diese an eine bestimmte Stelle gehören oder nicht.

In einfachen Fällen bedarf es schlichtweg eines Datenhausmeisterservices. Systembetreuer sollten prüfen, welche Informationen entfernt werden können und dies anschließend auch tun. Aufgrund der heutzutage teilweise enormen Anforderungen an Systembetreuer ist es sinnvoll, den Personen, die dies durchführen, Rückendeckung zu geben, weil im Vergleich zu anderen Aufgaben diese Arbeit teilweise nicht als „richtige Arbeit“, sondern maximal als Übung für einen Praktikanten angesehen wird. Dies ist aber nicht der Fall. Die bereinigende Instanz sollte genügend Kompetenzen haben, um nicht absichtlich abgewimmelt oder versehentlich in die Irre geführt zu werden - schließlich arbeitet sie scheinbar bequem, (jedoch mit enormen Risiken behafteten) traditionellen Arbeitsweisen entgegen. Es bietet sich daher an, Lösungen in einer normalen und nicht vom Druck eines Sicherheitsvorfalles belasteten Situation zu finden. Zudem ist eine gewisse Kenntnis der IT-Umgebung die bessere Voraussetzung für Entscheidungen, welche Daten entfernt werden können, und wie mit deren Erzeugern verfahren werden soll. Die organisatorische Regelung kann beispielweise umfassen, welche Informationen im Webroot eines Servers zu liegen haben und welche nicht, welche Verzeichnisse Administratoren ohne Rückfragen bereinigen können und welche nicht. Auch Webagenturen sind eher dankbar, derartige Fragen im Vorfeld zu klären anstatt im Schadensfall – berechtigt oder unberechtigt – als verantwortlich dazustehen.

Schließlich und endlich sollte es auch möglich sein, ganze Anwendungen und Systeme zu entfernen. Der Wert eines Systems, welches eventuell nicht mehr produktiv genutzt wird, sollte immer aus der Perspektive eines Angreifers betrachtet werden – denn was für das Unternehmen einen Gefallen für einen einzelnen Kunden ist, der einen Umstieg scheut, kann sich für den Angreifer als bequemes Einfallstor erweisen. Der scheinbare Gefallen erweist sich dann als Waterloo der IT-Sicherheit.

So platt es klingt: Angreifer kennen keine Gnade – sie werden ältere Systeme und Anwendungen nicht aus Mitleid ignorieren, sondern sie eher gleich attackieren. Angreifer arbeiten meist auf ein konkretes Ziel (Datensammeln) hin und alles was den Vorgang beschleunigt, ist positiv.

Ebenso wie man selbst, so hoffen auch Angreifer, dieselben Werkzeuge so lange wie möglich zu nutzen und mit ihnen hohen Gewinn zu erwirtschaften. Schlichtes "Aufräumen" kann hingegen dafür sorgen, dass zumindest der Gewinn mager ausfällt – oder ein verwundbares System erst gar nicht zur Verfügung steht.

In diesem Sinne wünscht ihnen die SySS GmbH viel Erfolg beim Umsetzen dieser Maßnahmen und einen geruhsamen Betrieb ihrer Systeme.