THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden, liebe Geschäftspartner, Freunde und Bekannte,

ein ereignisreiches Jahr 2015 geht seinem Ende zu. Kaum ein Monat, in dem die Medien nicht über spektakuläre und weniger spektakuläre Angriffe auf die IT-Sicherheit von Unternehmen und Institutionen berichteten. Der weitreichende Sicherheitsvorfall im Deutschen Bundestag im Frühjahr sowie der gezielte und massenhafte Diebstahl von mobileTANs im Herbst seien hier stellvertretend genannt.

Nun sind die kommenden Feiertage und der Jahreswechsel für viele Menschen eine Zeit zurückzuschauen und nachzudenken – vielleicht auch über den Stand der eigenen IT-Sicherheit.

Wäre es vielleicht an der Zeit, Sicherheitsprüfungen auch in regelmäßige Prüfpläne zu integrieren? Solchen Prüfungen kommt im Rahmen der Internen Revision eine noch immer kleine, aber aus gutem Grund ständig wachsende Bedeutung zu. Schon lange setzen Unternehmen zahlreiche Maßnahmen ein, um IT-Sicherheit zu gewährleisten, von ISO- und BSI-Zertifizierungen bis hin zu Audits. Doch diese sind häufig genug nicht ausreichend, wie die eingangs angeführten Beispiele illustrieren.

Verbreitete Maßnahmen der IT-Qualitätssicherung – wie Code-Reviews, Security Development Lifecycle oder Grundschutz- und ISO-Zertifizierungen – reichen möglicherweise aus, um 99 % der Systeme sicher zu gestalten. Entscheidend ist jedoch: Es fehlt genau 1%, und aus diesem ergibt sich eine Verwundbarkeit, die digitale Angreifer gezielt auffinden und ausnutzen können. Sei die Lücke auch noch so klein, sie genügt meist, um über diese „Hintertür“ eine ganze, ansonsten gut abgesicherte IT-Infrastruktur zu kompromittieren.

Genau an dieser Stelle – oder besser gesagt davor – setzt ein Penetrationstest an: Der Penetrationstester simuliert eine Hackerattacke und nimmt dabei die Perspektive derjenigen ein, die versuchen, ein Unternehmen anzugreifen. So werden Sicherheitslücken aufgedeckt, noch bevor böswillige Angreifer sie missbrauchen können.

Ist eine solche Verwundbarkeit nun entdeckt und glücklicherweise sogleich behoben worden, bleibt jedoch keine Zeit, sich zurückzulehnen. Täglich tauchen neue Softwarelücken und damit auch neue potenzielle Angriffspunkte für Hacker auf. Penetrationstests sollten deshalb fest in Revisionspläne integriert und entsprechend regelmäßig durchgeführt werden – und das möglichst nicht von der hauseigenen IT, die vor einer gewissen „Betriebsblindheit“ nie gefeit ist. Der Blick von außen durch einen externen Penetrationstester als Berater des Revisors hilft, „Blinde Flecken“ aufzudecken und Lücken zu schließen – bevor es zum Vorfall kommt.

Soweit mein kleiner vorweihnachtlicher Gedankenanstoß zur IT-Security. Wenn Sie beim Lesen aufgehorcht haben, sich gar in der Rolle wiedergefunden haben, für IT-Sicherheit in Ihrem Unternehmen zu sorgen, dann nutzen Sie den Jahreswechsel doch vielleicht für eine tiefergehende Lektüre. „IT-Revision, IT-Audit und IT-Compliance“ heißt eine neu erschienene Fachpublikation, zu der ich das Kapitel „Penetrationstest als Instrument der Internen Revision“ verfassen durfte. Werfen Sie doch einmal einen Blick hinein. Oder legen Sie das Buch Ihrem IT-Security-Verantwortlichen am besten gleich noch unter den Weihnachtsbaum.

Herzliche Grüße und bereits jetzt frohe Festtage und ein gutes Neues Jahr 2016,

Ihr Sebastian Schreiber

Aktuelle Events

18.02.2016
Seminar „Hackerangriffe auf Stadtwerke und EVUs“, München

7.-9.6.2016
Messeauftritt und Live-Hack, „Infosecurity Europe“, London

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

Aktuelle Schulungen

Hack1:
02. - 03.02.16
19. - 20.04.16

Hack2:
04. - 05.02.16
21. - 22.04.16

VoIP
10. - 11.02.16

Incident Response:
16. - 18.02.16

Mobile Device:
24. - 25.02.16

Forensik:
01. - 03.03.16

Pentests:
08.03.16

Webapp:
16. - 17.03.16

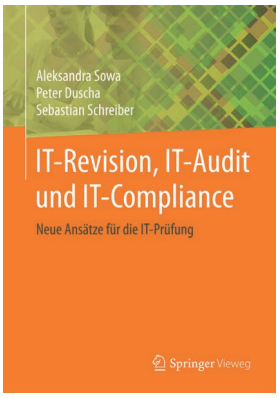
IPv6:
22.03.16

Windows:
05. - 07.04.16

IT-Recht:
26.04.16

Exploit:
10. - 11.05.16

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



Aleksandra Sowa, Peter Duscha, Sebastian Schreiber: IT-Revision, IT-Audit und IT-Compliance. Neue Ansätze für die IT-Prüfung (Springer Vieweg 2015)

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

Verantwortungsvoller Umgang mit Sicherheitsschwachstellen

von Matthias Deeg

Im Rahmen unserer alltäglichen Arbeit bei der SySS GmbH – sei es im Bereich Pentesting, im Bereich Digital Forensics/Incident Response oder auch im Bereich Forschung und Entwicklung – haben wir ständig mit Schwachstellen in informationstechnischen Systemen zu tun. Bei der Durchführung von Penetrationstests beispielsweise besteht unsere primäre Aufgabe schließlich darin, Sicherheitslücken in IT-Systemen unserer Kunden zu finden, Angriffswege aufzuzeigen, wie diese ausgenutzt werden können, und Empfehlungen zu geben, wie die gefundenen Schwachstellen behoben oder zumindest deren negative Auswirkungen verringert werden können.

Der Großteil der Schwachstellen, die wir bei unseren Sicherheitsanalysen finden, ist nicht neu, sondern bereits öffentlich bekannt. Informationen zu bekannten Schwachstellen können beispielsweise in diversen Schwachstellendatenbanken (u. a. SecurityFocus [1], NIST National Vulnerability Database [2], Offensive Security Exploits Database [3], Packet Storm [4]), in Archiven von E-Mail-Verteilern (z. B. BugTraq Mailing List [5], Full Disclosure Mailing List [6]) oder direkt auf der Internetpräsenz verschiedener Hersteller von Soft-, Firm- oder Hardwareprodukten (z. B. Microsoft Security TechCenter [7], Apple Security Updates [8]) gefunden werden. Der Umfang wie auch die Qualität der Schwachstellendokumentation variiert dabei von Schwachstelle zu Schwachstelle sehr stark, sodass der Erkenntnisgewinn bei so mancher dokumentierter Sicherheitslücke lediglich darin besteht, dass diese existiert.

Wie auch in anderen Wissensbereichen wächst im Bereich Informationssicherheit die Menge an Informationen stetig – bezüglich IT-Sicherheitsschwachstellen zuweilen sogar mit einer rasanten Geschwindigkeit. Täglich werden neue Sicherheitslücken in zahlreichen IT-Produkten veröffentlicht und das Wissen um alte, bereits bekannte Sicherheitslücken bleibt natürlich bestehen.

In unserer täglichen Arbeit stellt der Umgang mit bereits öffentlich bekannten Schwachstellen keine besondere Herausforderung dar. Im Gegensatz dazu steht jedoch der Umgang mit Schwachstellen, auf die wir im Zuge unserer Tätigkeit stoßen und die Recherchen zufolge noch nicht in öffentlich zugänglichen Quellen dokumentiert sind. Denn in dieser Situation stellt sich für uns die Frage, wie wir verantwortungsvoll mit Informationen zu solchen Schwachstellen umgehen.

Seit dem Jahr 2013 gibt unser „Responsible Disclosure-Prozess“, mit dem wir nun seit fast zwei Jahren bei der SySS GmbH den verantwortungsvollen Umgang mit Sicherheitsproblemen auf einheitliche Weise verfolgen, Antwort auf diese Frage. Die grundlegende Idee und Verfahrensweise unseres Responsible Disclosure-Prozesses werden in unserer Richtlinie für die verantwortungsvolle Offenlegung von Sicherheitsschwachstellen (Responsible Disclosure Policy [9]) beschrieben:

„Schwachstellen in Produkten, die nicht von Kunden der SySS GmbH hergestellt wurden oder allgemein durch vertragliche Vereinbarungen von einer Veröffentlichung ausgeschlossen sind, werden im Rahmen unseres Prozesses zur verantwortungsvollen Offenlegung von Sicherheitsschwachstellen schriftlich in Form eines Security Advisory an betroffene Hersteller gemeldet.

Tabelle: Übersicht gemeldeter Schwachstellentypen

Schwachstellentyp	Anzahl
Authentication Bypass Using an Alternate Path or Channel (CWE-288)	13
Cross-Site Scripting (CWE-79)	13
SQL Injection (CWE-89)	7
Use of a One-Way Hash without a Salt (CWE-759)	7
Insecure Direct Object Reference (CWE-932)	4
Cryptographic Issues (CWE-310)	3
Insufficiently Protected Credentials (CWE-522)	3
Uncontrolled Resource Consumption (CWE-400)	3
Use of Hard-Coded Cryptographic Key (CWE-321)	3
Violation of Secure Design Principles (CWE-657)	3
Denial of Service (CWE-730)	2
Broken Authentication and Session Management (CWE-930)	1
Credentials Management (CWE-255)	1
Cross-Site Request Forgery (CWE-352)	1
Exposure of Backup File to an Unauthorized Control Sphere (CWE-530)	1
Improper Handling of Insufficient Privileges (CWE-274)	1
Improper Neutralization of CRLF Sequences (‚CRLF Injection‘) (CWE-93)	1
Improper Validation of Integrity Check Value (CWE-354)	1
Improperly Implemented Security Check for Standard (CWE-358)	1
Information Exposure Through Directory Listing (CWE-548)	1
Insufficient Entropy (CWE-331)	1
Insufficient Verification of Data Authenticity (CWE-345)	1
Missing Function Level Access Control (CWE-935)	1
Overly Restrictive Account Lockout Mechanism (CWE-645)	1
Session Fixation (CWE-384)	1
URL Redirection to Untrusted Site (‚Open Redirect‘) (CWE-601)	1
Use of a One-Way Hash with a Predictable Salt (CWE-760)	1

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

Das Security Advisory gibt detaillierte Informationen zu der gefundenen Schwachstelle, sodass der Hersteller das Sicherheitsproblem nachvollziehen und weiter untersuchen kann. Schwachstellen werden, nachdem der Hersteller eine Lösung bereitgestellt hat oder 45 Tage nachdem sie von der SySS GmbH vertraulich an den Hersteller gemeldet wurden, veröffentlicht. Das ist unabhängig davon, ob die Schwachstelle zu diesem Zeitpunkt durch einen Patch oder Workaround vom Hersteller behoben worden ist.

In begründeten Ausnahmefällen sind wir bereit, von diesem Standardvorgehen abzuweichen und gemeinsam mit dem Hersteller einen alternativen Zeitplan für die koordinierte Veröffentlichung der Schwachstelle zu vereinbaren. Ziel der SySS Responsible Disclosure Policy ist es, überlegt das Interesse der Öffentlichkeit, über Sicherheitsschwachstellen informiert zu sein, gegen die Zeit für eine wirksame Behebung durch den Hersteller abzuwägen. Der endgültige Zeitplan für die Veröffentlichung einer Schwachstelle wird nach bestem Wissen unter Berücksichtigung dieser beiden Positionen gewählt. Die SySS GmbH bietet Herstellern die Möglichkeit, vor der Veröffentlichung einer Schwachstelle das Sicherheitsproblem zu analysieren, dieses zu beheben und durch ausführliche Tests die Lösung zu überprüfen."

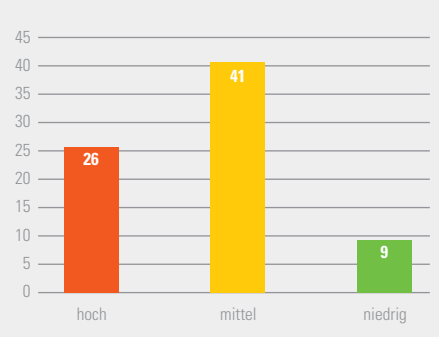
Durch die verantwortungsvolle Offenlegung neuer, bisher nicht öffentlich bekannter Sicherheitsschwachstellen erhoffen wir uns eine Win-Win-Win-Win-Situation, in der

1. der Hersteller des betroffenen Produkts profitiert, indem er die Sicherheit und damit verbunden die Qualität seines Produkts auf Grundlage unserer detaillierten Beschreibung (Security Advisory) verbessern kann,
2. die Kunden des betroffenen Produkts profitieren, indem sie auf vorhandene Schwachstellen aufmerksam gemacht werden und zukünftig ein sichereres Produkt nutzen können, sofern der Hersteller entsprechend handelt (siehe 1), oder sie den Einsatz einer anderen Lösung in Betracht ziehen können,
3. die Öffentlichkeit profitiert, indem Informationen zu Schwachstellen kostenlos und frei zur Verfügung gestellt und somit prinzipiell von allen genutzt werden können, etwa bei der Durchführung von Sicherheitsanalysen, und beispielsweise nicht in dunklen Ecken des Internets für teilweise recht hohe Geldbeträge ausschließlich an zahlungskräftige Kunden mit den unterschiedlichsten Absichten verkauft werden,
4. die SySS GmbH profitiert, indem sie durch die Veröffentlichung von Sicherheitsschwachstellen das Wissen und die Fähigkeiten ihrer Mitarbeiter in verschiedenen Bereichen der Informationssicherheit demonstrieren und dadurch auf ihre Dienstleistungen aufmerksam machen kann.

Die Bilanz hinsichtlich unseres Responsible Disclosure-Prozesses fällt nach knapp zwei Jahren positiv aus. Seit Dezember 2013 wurden insgesamt 76 Security Advisories an Hersteller versandt, 61 davon alleine im Jahr 2015. Zu manchen Schwachstellen wurden zudem ausführlichere Artikel veröffentlicht, wie beispielsweise die Publikation mit dem Titel „Rechteausweitung mittels Client-Management-Software" [10], und es wurden Vorträge auf IT-Sicherheitskonferenzen wie etwa der DeepSec [11] und der BSidesVienna [12] in Wien 2015 gehalten.

Die Tabelle auf der vorigen Seite zeigt eine Übersicht der gemeldeten Schwachstellentypen in Security Advisories der SySS GmbH *(Zuordnung nach Common Weakness Enumeration* [13]).

Die folgende Abbildung gibt eine Übersicht der Risikoeinstufungen von gemeldeten Schwachstellen in Security Advisories der SySS GmbH.



Informationen zu allen unseren veröffentlichten Schwachstellen finden sie im Pentest Blog auf unserer Internetpräsenz [14].

Für das kommende Jahr 2016 erwarten wir weiterhin, neue Sicherheitsschwachstellen in unterschiedlichen IT-Produkten auf verantwortungsvolle Weise veröffentlichen zu können – in der Hoffnung, dadurch die Welt ein kleines bisschen sicherer zu machen.

Referenzen

[1] SecurityFocus,
http://www.securityfocus.com/vulnerabilities

[2] NIST National Vulnerability Database,
https://nvd.nist.gov/

[3] Offensive Security Exploits Database,
https://www.exploit-db.com/

[4] Packet Storm, https://packetstormsecurity.com/files/

[5] BugTraq Mailing List,
http://www.securityfocus.com/archive/1

[6] Full Disclosure Mailing List,
http://seclists.org/fulldisclosure/

[7] Microsoft Security TechCenter,
https://technet.microsoft.com/security/bulletin

[8] Apple Security Updates,
https://support.apple.com/en-us/HT201222

[9] SySS Responsible Disclosure Policy

[10] Rechteausweitung mittels Client-Management-Software,
https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Rechteausweitung_mittels_Client-Management-Software.pdf

[11] Deactivating Endpoint Protection in an Unauthorized Manner,
https://deepsec.net/speaker.html#PSLOT205

[12] Privilege Escalation via Client Management Software,
http://bsidesvienna.at/talks/#5

[13] MITRE Common Weakness Enumeration (CWE),
https://cwe.mitre.org/index.html

[14] SySS Security Advisories,
https://www.syss.de/pentest-blog/advisories/

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