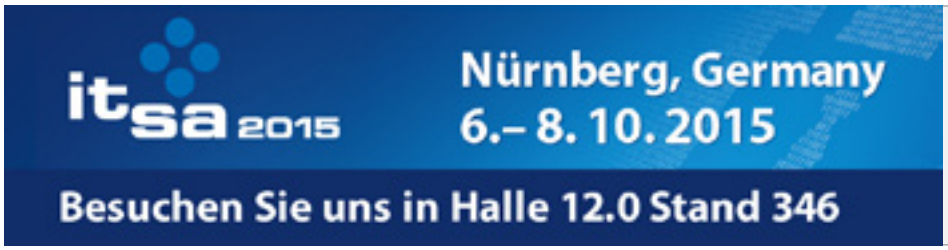
THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:



SySS auf der it-sa vom 06. - 08. Oktober 2015

Auch in diesem Jahr sind wir wieder auf der IT-Security-Messe it-sa in Nürnberg, Messezentrum Nürnberg, **Halle 12, Stand 346**. Sie können uns gerne dort treffen. Vereinbaren Sie einfach einen Termin mit uns via E-Mail an info@syss.de. Oder kommen Sie vorbei, wir haben ein attraktives Vortragsprogramm am Stand.

Sehr geehrte Kunden, liebe Geschäftspartner, Freunde und Bekannte,

Der Ruf nach einer Regulierung von Verschlüsselungstechniken ist fast so alt wie die Kryptografie, also die Kunst der Verschlüsselung selbst. Zwar deklariert die Politik Kryptotechnologien gern als Wettbewerbsvorteil und fordert den Schutz von Daten und Privatsphäre selbstbewusst, doch zugleich soll in Ausnahmesituationen der Zugriff auf diese schützenswerten Daten seitens ermittelnder Behörden möglich sein – ein ambivalenter, nicht zu vereinbarender Anspruch.

Nach dem Anschlag auf Charlie Hebdo zu Beginn des Jahres wurde der Ruf nach staatlicher Kryptoregulierung wieder laut. Bundesinnenminister Thomas de Maizière bekannte sich als Befürworter, ebenso der britische Premierminister David Cameron oder Gilles de Kerchove, Anti-Terror-Koordinator der Europäischen Union. Diese Forderung mag einerseits nachvollziehbar sein, denn sie gibt Politikern Handlungsspielraum. Andererseits weckt sie bei den politisch Verantwortlichen Begehrlichkeiten nach Macht und Kontrolle. Hinzu kommt die Angst des Staates, auch im Fall von „Gefahr im Verzug“ wegen der Verschlüsselung keine Kontrolle über die Kommunikation vermeintlich böswilliger Bürger erlangen zu können.

Ganz gleich wie sinnvoll oder nicht, wäre eine Kryptoregulierung angesichts der heutigen Entwicklung überhaupt umsetzbar? Zunächst müsste ein sogenannter „Key Recovery“ geschaffen werden, der die Rekonstruktion eines verwendeten Schlüssels für bereits verschlüsselte Daten ermöglicht. Klingt simpel, hat jedoch weitreichende Auswirkungen. Eine enorme Anzahl von technischen Geräten müsste ersetzt und erweitert werden, wie beispielsweise der Zugriffsschutz bei BlueRay-DVDs, WLAN/LAN-Routern, Sat-Receivern, iPhone/DECT-Telefonen oder Bluetooth bei Sport-Armbändern. Gleiches gilt für Freisprecheinrichtungen in Kraftfahrzeugen oder Chips in EC- und Kreditkarten und in medizinischen Geräten wie Hörgeräte und Herzschrittmacher. Der Aufwand, betroffene Geräte umzurüsten oder vollständig auszutauschen, wäre unverhältnismäßig hoch und praktisch wohl kaum durchführbar.

Auch die Hinterlegung verwendeter Schlüssel bei einer zentralen staatlichen Stelle wäre nicht nur juristisch heikel, sondern die Komplexität von Systemen würde sich derart erhöhen, dass Implementierungsfehler und Sicherheitslücken praktisch unvermeidbar wären. Eine solche „Zentralstelle für Kryptografie-Schlüssel“ wäre zudem ein kaum zu schützender, idealer Single-Point-of-Attack – ein einziger erfolgreicher Hacker-Angriff ein Sicherheitsdesaster.

Nicht nur die Politiker, die noch vor kurzem Nutzer dazu aufriefen, sich selbst um ihre Datensicherheit zu kümmern, würden ihre Glaubwürdigkeit verspielen. Die Kryptoregulierung wäre für jeden

Aktuelle Events

29.09. - 01.10.15
Täglich Live-Hacks, IT & Business, Messe Stuttgart

09. - 10.10.15
Vortrag, Konferenz Hacktivity, Budapest

10.11.15
Live-Hack, Prosecurity, Fürstenfeldbruck

10.11.15
Live-Hack, tcworld, Stuttgart

19.11.15
Vortrag, Konferenz DeepSec, Wien

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

Aktuelle Schulungen

IT-Forensik:
29.09. - 01.10.15
01.03. - 03.03.16

Exploits:
13. - 14.10.15

Hack I:
19. - 20.10.15
02. - 03.02.16

Hack II:
21. - 22.10.15
04. - 05.02.16

WebApp:
27. - 28.10.15
16. - 17.03.16

PenTests:
30.10.15
08.03.16

VoIP
11. - 12.02.16

Incident Response:
16. - 18.02.16

Mobile Device:
24. - 25.02.16

Windows:
05. - 07.04.16

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

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: Marcus Bauer · 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.

Computernutzer ein neuer zusätzlicher Hemmschuh auf dem Weg zum verantwortlichen Umgang mit den eigenen Daten. Obwohl heute viele technische Geräte Sicherheits-Chips in sich tragen, die automatisch verschlüsseln, nutzen normale Anwender die vorhandenen Techniken zur Ende-zu-Ende-Verschlüsselung kaum. Eine Regulierung würde die Zahl nicht heben. Was hinzukommt: Kryptoregulierung ergäbe nur dann Sinn, wenn sich ein möglicher Verstoß gegen dieselbe auch ahnden ließe. Kriminelle setzen bereits heute die sogenannte „Steganographie" ein, wodurch Daten für Außenstehende nicht nur verschlüsselt, sondern sogar verborgen gespeichert werden (z. B. „Hidden Volumes" bei True Crypt). Den Verstoß gegen eine Kryptoregulierung nachzuweisen, ist bereits heute in diesen Fällen gar nicht möglich.

„Wer seine Daten sichern will, wird sie wohl verschlüsseln müssen und kann nicht mehr auf seinen Nationalstaat hoffen."

So der innenpolitische Sprecher der Unionsfraktion, Hans-Peter Uhl, in einem Interview im Jahre 2013

Wir leben heute in weiten Teilen Europas in „streitbaren Demokratien", deren Bürger sich gegen Feinde der freiheitlich-demokratischen Grundordnung zur Wehr setzen. Doch es ist durchaus denkbar, dass sich heutige Rechtsstaaten in einigen Jahrzehnten in Unrechtsregime verwandeln. Ob ein solcher Wandel aufzuhalten ist, wird nicht jetzt und heute von rechtsstaatlichen und demokratisch gewählten Regierungen entschieden, sehr wohl aber, ob zukünftige, undemokratische Regierungen über Instrumente verfügen werden, die umfassenden Zugriff auf die Daten *aller* Bürger gewähren und in der Folge jegliche politische Opposition verhindern. Der aktuelle Ruf nach Kryptoregulierung bietet nur höchst unwahrscheinlich einen erhöhten Schutz, auf alle Fälle schwächt er jedoch entscheidend unsere streitbaren Demokratien.

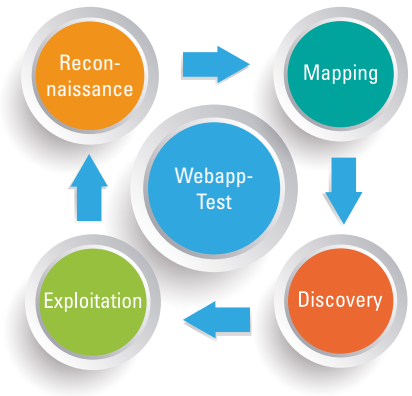
Herzliche Grüße,
Ihr Sebastian Schreiber

Ein Webapplikationstest – Was geschieht denn da? Einführung in die Methodologie eines Penetrationstests

von Dr. Erlijn van Genuchten

In den letzten Jahren spezifizierten in der IT-Sicherheit führende Organisationen – wie beispielsweise das OWASP und der PCI Security Standards Council – immer häufiger, wie erstklassige Penetrationstests und deren Dokumentation aussehen sollten. Da die SySS GmbH bei jedem Projekt ein hohes Maß an Qualität und Vollständigkeit anstrebt, muss ein IT-Security Consultant abwägen, wie er seine Zeit für ein optimales Ergebnis beim Test und bei der Dokumentation einsetzen kann. Ein Aspekt, der dabei meistens nicht so ausführlich dokumentiert werden kann wie gewünscht, ist die Methodologie des Penetrationstests selbst.

Um Kunden und an IT-Sicherheit Interessierten einen Einblick in die Vorgehensweise bei einer Sicherheitsanalyse zu bieten, soll im Folgenden beschrieben werden, wie ein Webapplikationstest durchgeführt wird.



Methodisches Vorgehen bei einem Webapplikationstest
Quelle: antkevyv/Shutterstock.com

Der „Grey-Box"-Test

Der Test einer Webapplikation ist für die SySS GmbH typischerweise ein sogenannter „Grey-Box"-Test. Dies bedeutet, dass der IT-Security Consultant wichtige Informationen – wie beispielsweise Login-Daten der Webapplikation – vor Testbeginn bekommt. Dieser Testtyp steht im Gegensatz zu einer „Black-Box"-Situation, in der sich zum Beispiel ein „Black Hat"-Angreifer befindet. In dieser Situation werden vor einem Angriff keine Informationen explizit bereitgestellt. Da ein Pentester im Gegensatz zu einem Angreifer jedoch anderen zeitlichen Einschränkungen unterliegt, erlaubt es ein „Grey-Box"-Test, die verfügbare Zeit und Ressourcen besser einzusetzen.

Der eigentliche Test kann in verschiedene Phasen unterteilt werden: die Reconnaissance-, die Mapping-, die Discovery- und die Exploitation-Phase. Alle Phasen sind für einen erfolgreichen Test und relevante Ergebnisse wichtig. Bei einem „Grey-Box"-Test liegt jedoch der Schwerpunkt auf den letzten drei der vier Phasen.

Die Reconnaissance-Phase

Das Ziel der ersten Phase ist das Kennenlernen der Webapplikation, der Infrastruktur, die der Webapplikation zugrunde liegt, und der Organisation, die die Webapplikation veröffentlicht hat. In dieser Phase wird nach Informationen gesucht, die im Internet verfügbar sind, ohne direkt mit der Webapplikation zu interagieren. Dazu gehören zum Beispiel DNS-Anfragen, aber auch eine Recherche in Suchmaschinen wie Google. Diese Informationen sind später wichtig, um einen sinnvollen Angriff zu planen und die Erfolgschancen zu erhöhen. Tools, die in dieser Phase verwendet werden, sind unter anderem whois, host oder dig und dnsrecon.

Die Mapping-Phase

Nachdem der Tester einen Überblick über den Kontext der Webapplikation bekommen hat, verlagert er den Fokus auf die Webapplikation selbst. Das Ziel dieser zweiten Phase ist es, die Applikation genau unter die Lupe zu nehmen, indem unter anderem Funktionen, Technologien, die logische Abfolge der Seiten, Parameter und sonstige Einstiegsstellen für einen Angriff aufgelistet werden. Zum Einsatz kommen verschiedene Browser-Plugins, darunter Wappalyzer und Firebug in Firefox sowie die Burp Suite als lokaler Angriffs-Proxy und Tools wie nikto und dirbuster.

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: Marcus Bauer · 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.

Ein zweites Ziel dieser Phase ist es, möglichst detaillierte Kenntnisse über das zugrunde liegende System zu erlangen. Dazu gehören sowohl das Erforschen von offenen Ports als auch die Analyse der eingesetzten Betriebssysteme und Software-Versionen. Das wichtigste Tool für diesen Zweck ist nmap.

Die Discovery-Phase

In der dritten Phase fängt der Consultant an, die Webapplikation und das zugrunde liegende System anzugreifen. Dabei gilt es zu prüfen, ob die vorgefundenen Einstiegsstellen auch tatsächlich eine Schwachstelle aufzeigen. Dazu werden Informationen aus den ersten beiden Phasen verwendet und ausgenutzt. Der dabei verwandte Hybrid-Ansatz beinhaltet, dass sowohl automatisierte als auch manuelle Tests durchgeführt werden. Hier fließen Ergebnisse der automatischen Tests in die manuellen Prüfungen ein und umgekehrt. Zum Beispiel zeigen automatisierte Tests, wo der Consultant noch einmal genauer hinschauen sollte. Manuelle Prüfungen offenbaren, wo ein zusätzlicher automatischer Test sinnvoll ist. Dieser Hybrid-Ansatz erlaubt es dem Penetrationstester, die Vorteile von beiden Methoden zu vereinbaren: mit einem automatisierten Test können innerhalb von kürzester Zeit viele Angriffsszenarien ausprobiert werden; mit einer manuellen Prüfung können die besonderen Eigenschaften der Webapplikation berücksichtigt, logische Fehler und die Ergebnisse der automatisierten Tests geprüft werden.

Tools, die in dieser Phase für automatisierte Tests eingesetzt werden, sind Nessus, ein Schwachstellen-Scanner, und der Scanner in Burp Suite. Für manuelle Tests wird Burp Suite in Kombination mit Browser-Plugins eingesetzt.

Die Exploitation-Phase

Das Ziel der letzten Phase ist das Ausnutzen von Schwachstellen, die in der Discovery-Phase identifiziert worden sind, um neue Informationen zu erhalten, die weitere Angriffe ermöglichen oder Schwachstellen offenlegen, die zuvor noch nicht ersichtlich waren. Jedoch können in der Regel nicht alle Schwachstellen ausgenutzt werden, da für manche Schwachstellen einige Bedingungen zutreffen müssen, deren Simulation den zeitlichen Rahmen des Penetrationstests sprengen würde. Für andere Schwachstellen ist es nicht notwendig, sie auszunutzen, da die Identifikation deren Ausnutzung schon impliziert, beispielsweise bei einem Denial-of-Service von Benutzerkonten, einer Schwachstelle, die durch Passwort-Rate-Angriffe identifiziert wird. Ein wichtiges Tool in dieser Phase ist wiederum Burp Suite. Je nach Schwachstelle können auch weitere Werkzeuge eingesetzt werden, wie beispielsweise Metasploit Framework und SQLmap. Ebenso erstellt der Tester immer wieder eigene Skripte und Exploits, um bei der Ausnutzung von Schwächen erfolgreich zu sein.

Diese Phasen werden bei jedem Penetrationstest durchlaufen, je nach Test und Art der Ergebnisse auch öfter. Zum Beispiel könnte das Feststellen einer SQL-Injection-Schwachstelle in der Discovery-Phase zur Ausnutzung in der Exploitation-Phase führen, indem die Inhalte der Datenbank ausgelesen werden. Für den IT-Security Consultant fängt in diesem Fall der Prozess von vorne an, denn er wird die Inhalte der Datenbank dahingehend erforschen, welche Informationen er für weitere Angriffe finden kann (Reconnaissance-Phase), welche Angriffsflächen es gibt (Mapping-Phase) und wo weitere Schwachstellen vorhanden sind, die er ausnutzen könnte (Discovery- und Exploitation-Phase). Ebenso könnte der Consultant eine Tabelle mit Benutzernamen und Passwörtern entdecken, in der das Klartextpasswort des Administrators abgelegt ist. Mit diesem Passwort kann er versuchen, das zugrunde liegende System zu kompromittieren. Falls dies gelingt, fängt der Prozess dieser vier Phasen erneut von vorne an. Ein „Black Hat"-Angreifer wird in der Schleife dieses „Reconnaissance-Mapping-Discovery-Exploitation"-Prozesses so lange verweilen, bis er sein jeweiliges Ziel erreicht hat. Einem IT-Security Consultant jedoch liegt am Herzen, seine Testzeit optimal auszuschöpfen, zu möglichst vielen Erkenntnissen zu gelangen und seine Funde sowie die erzielten Testergebnisse für den Kunden genau zu dokumentieren, sodass er sein IT-Sicherheitsniveau nachhaltig steigern kann.

Advisories

In diesem Jahr hat die SySS GmbH eine ganze Reihe von Sicherheitsschwachstellen in diverser Software und in diversen Anwendungen gefunden und als Advisories veröffentlicht. Wenn Sie auf unsere Homepage https://www.syss.de/pentest-blog/advisories blicken, sehen Sie, wie aktiv wir beim Aufdecken von Sicherheitslücken sind.

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: Marcus Bauer · 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.