THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden,
liebe Geschäftspartner,
Freunde und Bekannte,

die großen Internetunternehmen wie Google, Apple, Amazon und Facebook sind allesamt fest in amerikanischer Hand. Im Zuge der Enthüllungen rund um Edward Snowden wird zu Recht häufig diskutiert, ob unsere Daten dort, im Ausland, wirklich sicher aufbewahrt werden. Doch sind Daten im Bundesgebiet überhaupt sicherer und besser geschützt? Die Geokoordinaten des Speicherorts spielen keinerlei Rolle. Entscheidend ist, wer Zugriff auf sie hat. So sind auch Server in Deutschland durch Ausspähung aus dem Ausland bedroht.

Außenpolitisch ist Deutschland ein vollständig souveräner Staat und zwar seit dem 15. März 1991, als der am 12. September 1990 in Moskau unterzeichnete Zwei-Plus-Vier-Vertrag in Kraft trat. Damit endete die Besatzungszeit nach dem Zweiten Weltkrieg und Deutschland erreichte den gleichen Rang und Status wie seine Nachbarstaaten. Während traditionell die eigene Armee und die Präsenz in Bündnissen und weltweiten Gremien die Souveränität unterstreichen, prägen Verkehrsknoten, Brücken, Bahnhöfe sowie ein Gleisnetz und Autobahnen die Infrastruktur eines Staates. In gleicher Weise gehören auch Router und Server zu dieser Infrastruktur – sie sind ja quasi die Brücken und Straßen der modernen Kommunikation und gehören seit einiger Zeit zum Zuständigkeitsbereich des Bundesverkehrsministeriums[1].

Die Hauptbestandteile des Fundaments unserer IT-Infrastruktur jedoch sind fest in der Hand ausländischer Staaten. Millionen von Routern in deutschen Unternehmen und Haushalten stammen aus Amerika oder China. Auf ihnen läuft oft Software, deren exakte Funktion uns vorenthalten wird. Zum Beispiel verlassen die Quelltexte chinesischer Router China nicht und manche Router-Modelle initiieren grundlos Verbindungen nach China – ein Schelm, wer Böses dabei denkt!

Amerikanische Hersteller haben zwar keinen direkten Zugriff auf die hinter Firewalls geschützten Server, aber die meisten großen Softwareprodukte führen halbautomatisch Software-Updates durch. Server verbinden sich dadurch also nach Amerika und werden von dort aus mit Software-Komponenten versorgt, die auf dem lokalen Rechner ausgetauscht und ausgeführt werden. Ähnlich wie bei den chinesischen Routern kennen wir weder die genaue Funktion noch die Quelltexte dieser sogenannten Patches.

Wer daher die Kontrolle über die Router hat, beherrscht die digitalen Autobahnen in Deutschland und Europa. Das wissen auch ausländische Geheimdienste, die in der jüngsten Vergangenheit immer wieder einige Server deutscher Großunternehmen in ihre Gewalt gebracht haben.

Natürlich ist Deutschland ein souveräner Staat, jedoch sollten wir darüber nachdenken, ob wir auf Dauer nicht eine vollständig selbst kontrollierbare IT-Infrastruktur benötigen.

Herzliche Grüße,
Ihr Sebastian Schreiber

Aktuelle Events

03.07.14	LH[1] Karrieremesse iteratec, Offenbach
08.07.14	LH[1] Gigatrends, Köln
10.07.14	LH[1] levigo Systemhaus-Event IT-Spionage, Ludwigsburg
18.07.14	LH[1] AdVertum Tag der offenen Tür, Stuttgart
18.07.14	LH[1] Bitfire, Bad Kissingen

[1] Live Hacking

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

Aktuelle Schulungen

Mobile Device:
24. - 25.06.14
11. - 12.11.14

VoIP
16. - 17.09.14

PenTests:
19.09.14
07.11.14

IT-Security I:
22. - 23.09.14
20. - 21.10.14
24. - 25.11.14

IT-Security II:
24. - 25.09.14
22. - 23.10.14
26. - 27.11.14

Exploits:
30.09. - 01.10.14

Incident Response:
14. - 16.10.14

Web-App
04. - 05.11.14

IT-Recht:
14.11.14

IT-Forensik:
18. - 20.11.14

WLAN:
02. - 03.12.14

IPv6:
05.12.14

Windows-Angriffe:
09. - 10.12.14

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] Bundesministerium für Verkehr und digitale Infrastruktur, siehe http://www.bmvi.de

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

THE PENTEST EXPERTS.

Proxy im Baukastenprinzip – Wie Open-Source die Arbeit von Penetrationstestern und Sicherheitsanalysten erleichtert

Von Matthias Dettling und Frederik Hauser

Open-Source ist eine gute Sache. Ihr Kennzeichen ist eine nicht selten große Anzahl an Softwareentwicklern, die freiwillig und weitgehend unentgeltlich die Resultate ihrer Arbeit Dritten zur Verfügung stellen. Dabei fließen oft zahlreiche Stunden unbezahlter Freizeitbeschäftigung und langjährige Erfahrung als Softwareentwickler aus den verschiedensten Branchen mit in die Entwicklung ihrer Software ein. Open-Source ermöglicht einerseits einen Austausch und bietet andererseits Anwendern den großen Vorteil, aktiv an der Entwicklung mitzuwirken und somit Einfluss auf die Fortentwicklung von Software zu nehmen.

Leider überschattet der aus Sicht von Forschungsgrößen im Bereich der IT-Sicherheit sehr schwerwiegende Implementierungsfehler Heartbleed in der SSL/TLS-Implementierung OpenSSL die Arbeit von Open-Source-Projekten. Wenige, aber in ihrem Effekt schwerwiegend fehlerträchtige Zeilen von Programmcode schafften es, die üblichen Qualitätssicherungsmaßnahmen unbemerkt zu durchlaufen und somit in den von vielen Internet-Diensteanbietern eingesetzten Produktivversionen zu landen. Stellvertretend für andere Open-Source-Projekte wurden die internen Organisationsabläufe des OpenSSL-Projektes kritisiert, vielmehr aber allgemeine organisatorische Vorgehensweisen bemängelt. Als Folge wurde dennoch nie die Abschaffung des Open-Source-Modells, sondern vielmehr eine bessere Organisation und eine stärker ausgeprägte Unterstützung aus dem kommerziellen Umfeld gefordert.

Auch bei der täglichen Arbeit im Bereich der Penetrationstests wird nicht selten auf Open-Source-Tools zurückgegriffen. Im Kontext der IT-Sicherheit ist es verglichen mit anderen Bereichen der Informationstechnologie eine durchaus gängige Praxis, die aus der täglichen Arbeit entstandenen Tools selbst unter einer Open-Source-Lizenz zu veröffentlichen und somit auch anderen bereitzustellen. Ein wesentlicher Vorteil im Einsatz quelloffener Software besteht in der Möglichkeit, die Funktionsweise eines Werkzeuges zu jedem Zeitpunkt im Detail überprüfen zu können: Penetrationstests berühren üblicherweise hochsensible Bereiche firmeninterner Netzwerke. Durch die Möglichkeit der Einsichtnahme in die Quellcodes der verwendeten Werkzeuge kann bereits vor einem möglichen Einsatz im Detail nachvollzogen werden, wie Angriffe oder Analysen von den jeweiligen Tools vollzogen werden. Die SySS GmbH möchte im Rahmen der Ende 2013 eingerichteten Research & Development-Abteilung (wir berichteten in unserem Newsletter 2013/Q4) dazu übergehen, wieder mehr Zeit dafür aufzuwenden, eigene Softwareprojekte voranzutreiben. Mit ihren internen Forschungsprojekten ist sie bestrebt, mit den aktuellen Entwicklungen im Bereich der IT-Sicherheit nicht nur Schritt zu halten, sondern vielmehr wegweisend neue Technologien und Vorgehensweisen zu finden, um die Qualität ihrer durchgeführten Penetrationstests durch stetige Optimierung zu verbessern. Schon in der Vergangenheit förderte die SySS GmbH aktiv Open-Source-Modelle und auch künftig sollen ausgewählte Softwareprojekte unter einer Open-Source-Lizenz veröffentlicht und einer breiteren Öffentlichkeit zur Verfügung gestellt werden.

Den Beginn dieser Entwicklung stellt ein im Rahmen einer Abschlussarbeit entstandenes modulares Netzwerk-Proxy-Framework dar. Netzwerk-Proxies sind unverzichtbare Werkzeuge für die Analyse bestehender Protokolle und Anwendungen. Durch die Platzierung eines Proxy in der Verbindung zwischen zwei kommunizierenden Entitäten kann ein als Man-in-the-Middle agierender Sicherheitsanalyst sämtliche ausgetauschte Kommunikationsdaten einsehen und gegebenenfalls modifizieren. Es existiert eine Vielzahl kommerzieller und freier Netzwerk-Proxies, die für den Einsatz in Penetrationstests geeignet sind. Meist sind diese jedoch auf ein spezielles Anwendungsfeld beschränkt. Um den vielfältigen Anforderungen, die an einen Proxy im Umfeld des Penetration-Testings gestellt werden, gerecht zu werden, musste nicht ein neuer Proxy entwickelt werden, sondern vielmehr eine neue Proxy-Architektur. Entstanden ist ein Framework, das es ermöglicht, eine auf den jeweiligen Testfall maßgeschneiderte Proxy-Konfiguration gemäß einem Baukastenprinzip zu erstellen. Im Unterschied zu den meisten existierenden Lösungen ist das neue Framework dabei nicht auf ein spezielles Anwendungsfeld beschränkt. Stattdessen können Daten auf allen Ebenen des TCP/IP-Protokoll-Stack mitgelesen und verändert werden.

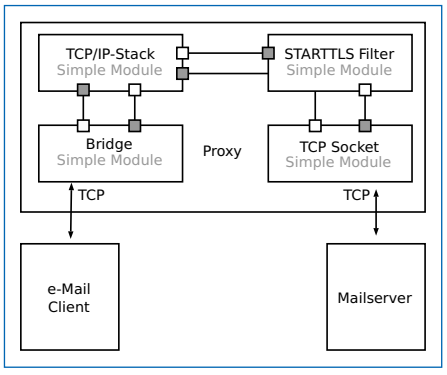

Abb.: Baukastenprinzip d. Proxy-Konfiguration

In einem konkreten Szenario kann ein solcher Proxy beispielsweise in die E-Mail-Kommunikation eines Clients mit einem Mailserver eingefügt werden,

wobei der Proxy den STARTTLS-Befehl zur Initiierung einer verschlüsselten Sitzung ausfiltert. Sofern die vorhandene Konfiguration sowohl auf Server- als auch Clientseite nicht explizit eine verschlüsselte Sitzung verlangt, kann der Einsatz der spezifischen Proxy-Konfiguration die Gefährdung mehrerer Schutzziele belegen: Eine Verschlüsselung der SMTP-Protokollsitzung kann verhindert werden, sodass E-Mail-Nachrichten abgefangen, verändert oder aber gänzlich verworfen werden können. Die Abbildung auf voriger Seite zeigt die entsprechende Proxy-Konfiguration. Anstatt diesen komplett neu zu entwickeln, konnte auf die Module „Bridge“, „TCP/IP-Stack“ sowie „TCP-Socket“ aus einem Repository zurückgegriffen werden, die in Proxies häufig verwendete Funktionalitäten kapseln. Lediglich das Modul „STARTTLS Filter“ zur Filterung des STARTTLS-Kommandos musste neu entwickelt werden und kann somit künftig aber auch als Teil völlig anderer Proxy-Konfigurationen verwendet werden. Das durch ein Modulkonzept hervorgebrachte Baukastenprinzip erlaubt daher nicht nur die flexible Verwend- und Erweiterbarkeit des Proxy-Frameworks, sondern führt darüber hinaus zu einer Steigerung der Arbeitseffizienz, die sich im Rahmen eines Penetrationstests in einer höheren Testtiefe niederschlägt.

Die auf Github unter der GPLv2 veröffentlichte Implementierung[1] des Proxy-Frameworks bietet zwar noch Raum für Erweiterungen und Verbesserungen, soll aber bereits jetzt als Open-Source-Software veröffentlicht werden. Die Autoren der Software erhoffen sich hierdurch Anregungen und Verbesserungsvorschläge aus der Community. Nicht zuletzt wäre es wünschenswert, andere Sicherheitsanalysten davon überzeugen zu können, ihre bereits existierenden Werkzeuge für die Verwendung mit dem Netzwerk-Proxy-Framework zu portieren oder sich an der Entwicklung des Frameworks zu beteiligen.

[1] https://github.com/fhauser/python-proxy-framework