Technische Hochschule Ingolstadt

Dokumentation

Security Workbench

angefertigt von

Name:	TBD
Matrikelnummer:	TBD

Betreuer:

Technische Hochschule Ingolstadt:	TBD

Ingolstadt, 19. Oktober 2015

Inhaltsverzeichnis

1. Einleitung

In Zeiten von *Heartbleed*[2] und *Shellshock*[6], der *Snowden-Leaks* und der *NSA-Affäre*[7] und der fortlaufenden Digitalisierung der Industrie und Gesellschaft wird das Thema Informationssicherheit immer wichtiger. Daten werden, unabhängig davon, ob diese Privatpersonen oder Unternehmen zugeordnet sind, immer wertvoller. So ergeben sich beispielsweise aus einem gehackten Smartphone einer Privatperson Informationen wie E-Mail-Adressen, Kontakte und Chat-Verläufe bis hin zu Passwörtern für Online-Banking oder persönlichen Bildern. Wenn diese Informationen auf dem Schwarzmarkt verkauft oder online veröffentlicht werden, kann dies für die Personen oft Reputations- wie auch finanzielle Schäden nach sich ziehen. Diese Tätigkeiten werden unter anderem oft unter dem Schlagwort „Cybercrime“ zusammengefasst. Betrachtet man Unternehmen, so ist der mögliche finanzielle Schaden wesentlich höher als für Privatpersonen. Durch die Entwendung von Kreditkartendaten erlitten zum Beispiel mehrere Supermärkte in den USA beträchtliche Reputationsschäden [1][3]. Eventuell noch höhere Schäden könnte es nach sich ziehen, wenn streng vertrauliche Dokumente von Unternehmen, wie z.B. Konstruktionsskizzen für ein neues Automodell, Quellcode oder vorläufige Geschäftsberichte durch Hacker erbeutet und an ein Konkurrenzunternehmen verkauft würden. Dies hört sich irreal an, aber die Firma McAffee schätzt den Verlust für die Wirtschaft durch „Cybercrime“ im Jahr 2014 auf bis zu 575 Milliarden USD[4]. Um diesem Trend entgegen zu wirken, müssen Unternehmen Maßnahmen ergreifen, welche das Schutzniveau erhöhen. Oft werden hier aufgrund der technischen Sicht nur im Internet erreichbare Komponenten beachtet, wie das schnelle Patching von Servern. Dies ist in Hinsicht auf *Poodle*[5] und *Shellshock*[6] sicherlich auch notwendig, jedoch sollte man alle Wege, über welche Daten von Dritten in das Unternehmen gelangen, Daten an Dritte weitergegeben werden könnten, und alle internen Bedrohungen wahrnehmen, einschätzen und eindämmen. Eine solche Prüfung war die Grundlage für dieses Dokument.

A. Appendix

A.1. Quellcode

A.2. Ergänzende Grafiken

A.3. Quellcode Grafiken

Literatur

[1] *AB Acquisition LLC Confirms Incident Involving Payment Card Data Processing*. URL: http://www.jewelosco.com/2014/08/ab-acquisition-llc-confirms-incident-involving-payment-card-data-processing/ (besucht am 01. 11. 2014).

[2] *Heartbleed*. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160 (besucht am 29. 10. 2014).

[3] *Home Depot probes possible hack, could be larger than Target breach*. URL: http://www.denverpost.com/business/ci_26453916/data-stolen-from-11-colorado-goodwill-stores-home (besucht am 01. 11. 2014).

[4] *McAffee*. URL: http://csis.org/files/attachments/140609_McAfee_PDF.pdf (besucht am 29. 10. 2014).

[5] *Poodle*. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 (besucht am 08. 11. 2014).

[6] *Shellshock*. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271 (besucht am 29. 10. 2014).

[7] *Snowden*. URL: https://www.theguardian.com/us-news/edward-snowden (besucht am 29. 10. 2014).