Peter Schartner · Norbert Pohlmann (Hrsg.)

D·A·CH Security 2018

Bestandsaufnahme
Konzepte
Anwendungen
Perspektiven

syssec

IT Security & IT Management

IT Security & IT Management

herausgegeben von Patrick Horster

In der Buchreihe IT Security & IT Management werden ausgewählte Titel aus den Bereichen der IT-Sicherheit und dem Management von IT-Systemen behandelt. Ziel ist es, einen aktuellen Stand über Forschung und Entwicklung zu geben, administrative und rechtliche Probleme aufzuzeigen sowie existierende Lösungen im relevanten Kontext interdisziplinär zu präsentieren.

In der Buchreihe IT Security & IT Management sind bisher folgende Titel erschienen:

Patrick Horster (Hrsg.)
Elektronische Geschäftsprozesse
ISBN 3-936052-00-X

Patrick Horster (Hrsg.)
Sichere Geschäftsprozesse
ISBN 3-936052-07-7

Patrick Horster (Hrsg.)
Enterprise Security
ISBN 3-936052-02-6

Peter Schartner
Security Tokens
ISBN 3-936052-03-4

Petra Wohlmacher
Digitale Signaturen und Sicherheitsinfrastrukturen
ISBN 3-936052-01-8

Die vorstehenden Bände sind beim IT Verlag in Sauerlach erschienen.

Patrick Horster (Hrsg.)
D•A•CH Security
ISBN 3-00-010941-2

Patrick Horster (Hrsg.)
D•A•CH Security 2004
ISBN 3-00-013137-X

Patrick Horster (Hrsg.)
Elektronische Geschäftsprozesse 2004
ISBN 3-00-014186-3

Patrick Horster (Hrsg.)
D•A•CH Security 2005
ISBN 3-00-015548-1

Patrick Horster (Hrsg.)
D•A•CH Security 2006
ISBN 3-00-018166-0

Patrick Horster (Hrsg.)
D•A•CH Mobility 2006
ISBN 3-00-019635-8

Patrick Horster (Hrsg.)
D•A•CH Security 2007
ISBN 978-3-00-021600-8

Patrick Horster (Hrsg.)
D•A•CH Security 2008
ISBN 978-3-00-024632-6

Patrick Horster · Peter Schartner (Hrsg.)
D•A•CH Security 2009
ISBN 978-3-00-027488-6

Peter Schartner · Edgar Weippl (Hrsg.)
D•A•CH Security 2010
ISBN 978-3-00-031441-4

Peter Schartner · Jürgen Taeger (Hrsg.)
D•A•CH Security 2011
ISBN 978-3-00-034960-7

Peter Schartner · Jürgen Taeger (Hrsg.)
D•A•CH Security 2012
ISBN 978-3-00-039221-4

Peter Schartner · Peter Trommler (Hrsg.)
D•A•CH Security 2013
ISBN 978-3-00-042097-9

Peter Schartner · Peter Lipp (Hrsg.)
D•A•CH Security 2014
ISBN 978-3-00-046463-8

Peter Schartner et al. (Hrsg.)
D•A•CH Security 2015
ISBN 978-3-00-049965-4

Peter Schartner (Hrsg.)
D•A•CH Security 2016
ISBN 978-3-00-053829-2

Peter Schartner · Andrea Baumann (Hrsg.)
D•A•CH Security 2017
ISBN 978-3-00-057290-6

Peter Schartner · Norbert Pohlmann (Hrsg.)
D•A•CH Security 2018
ISBN 978-3-00-060424-9

Peter Schartner · Norbert Pohlmann (Hrsg.)

D·A·CH Security 2018

Bestandsaufnahme • Konzepte • Anwendungen • Perspektiven

syssec

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-00-060424-9

Vorwort

Informationstechnik (IT) und das Internet sind Motor und Basis für das Wohlergehen unserer modernen und globalen Informations- und Wissensgesellschaft. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer IT-Systeme, wie Endgeräte, Server, IoT-Geräte und Netzkomponenten nicht sicher genug konzipiert und aufgebaut sind, um den Fähigkeiten von intelligenten Hackern standzuhalten. Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software für erfolgreiche Angriffe zu Nutze machen, Malware installieren, Passwörter sowie Identitäten stehlen, mit Fake News Wahlen beeinflussen, unsere Endgeräte ausspionieren, usw. Wenn wir diese IT-Sicherheitsprobleme in der Zukunft nicht mit wirkungsvolleren IT-Sicherheitslösungen in den Griff bekommen und damit auch Vertrauen aufbauen, wird eine nachhaltige Digitalisierung nicht gelingen. Die Artikel in diesem Buch sollen einen Beitrag für mehr Sicherheit und Vertrauen leisten.

Die Arbeitskonferenz D·A·CH Security ist eine gemeinsame Veranstaltung der Gesellschaft für Informatik (GI), der Österreichischen Computergesellschaft (OCG) und der TeleTrusT – Bundesverband IT-Sicherheit e.V. Die Konferenz behandelt IT-Sicherheit als interdisziplinäre Aufgabe mit dem Ziel, eine fachübergreifende Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft in Deutschland, Österreich und der Schweiz zu geben, administrative, organisatorische, rechtliche und technische Probleme aufzuzeigen, sowie existierende Lösungen zu präsentieren.

Die Beiträge dieses Tagungsbandes decken eine Vielzahl von Aspekten der IT-Sicherheit und des rechtlichen Umfeldes ab. Beginnend bei personellen und organisatorischen Maßnahmen (wie Awareness & Schulung, und Sicherheits- und Risikomanagement) wird der Bogen über Kritische Infrastrukturen bis hin zu Automatisierung, Industrie 4.0 und IoT gespannt. Neben den Themen, welche vorrangig für Betriebe und Organisationen von Interesse sind, werden auch Bereiche betrachtet, die zudem für einzelne Personen relevant sind. Hierzu zählen beispielsweise Beweiswerterhaltung und Identifikation & Authentifikation. Begleitend zur Entwicklung sicherer Systeme (Software & Security-Engineering) werden auch Schwachstellen & Angriffe bestehender Systeme diskutiert. Ergänzt wird die Veranstaltung durch die Workshop KRITIS und ACS und die Präsentation ausgewählter studentischer Abschlussarbeiten.

Die vorliegenden Beiträge zeigen die Vielfalt sicherheitsrelevanter Themen eindrucksvoll auf. Daher bedanken wir uns insbesondere bei den Autoren, die mit ihren hochaktuellen Beiträgen einen für die weitere Diskussion der behandelten Themen wertvollen Tagungsband möglich machten. Außerdem gilt unser Dank denen, die bei der Vorbereitung und bei der Ausrichtung der Konferenz geholfen und so zum Erfolg beigetragen haben, insbesondere den Mitgliedern des Programmkomitees und des Organisationskomitees. Unser Dank gilt zudem der TeleTrusT – Bundesverband IT-Sicherheit e.V. für die Unterstützung der Veranstaltung. Nicht zuletzt danken wir em.Univ.-Prof. Dr. Patrick Horster (Forschungsgruppe Systemsicherheit, Universität Klagenfurt), der wesentlichen Anteil am Gelingen der Konferenz und des Tagungsbandes hatte. Unterstützt wird die Tagung zudem vom Bundesministerium des Innern, für Bau und Heimat, der Deutsche Bahn AG und dem AIT Austrian Institute of Technology.

Wie in den vergangenen Jahren auch, wird die Arbeitskonferenz sicher als Forum für einen regen Ideenaustausch genutzt und somit dazu beitragen, bestehende Probleme im Umfeld der IT-Sicherheit nicht nur aufzuzeigen, sondern auch zu lösen.

Peter Schartner
peter.schartner@aau.at

Norbert Pohlmann
pohlmann@internet-sicherheit.de

Programmkomitee

P. Schartner · Uni Klagenfurt & N. Pohlmann · Westfälische Hochschule (Vorsitz)

A. Alkassar · TeleTrusT
R. Baumgart · Secunet AG
A. Baumann · UniBw München
P. Beenken · Porsche AG
R. Benzmüller · GDATA AG
J. Dittmann · Uni Magdeburg
D. Engel · FH Salzburg
K. Frintrop · AFCEA
J. Fuß · FH Hagenberg
M. Hartmann · SAP
P. Horster · AAU Klagenfurt
G. Jacobson · Secardeo GmbH
S. Janisch · Uni Salzburg
A. Kreth · AFCEA
K. Knorr · HS Trier
U. Korte · BSI
W. Kühnhauser · TU Ilmenau
P. J. Kunz · HiSolutions AG
S. Lechner · JRC
H. Leitold · A-SIT
K. Lemke-Rust · HS Bonn-Rhein-Sieg
M. Meier · Uni Bonn
B. Mester · datenschutz nord
H. Mühlbauer · TeleTrusT
I. Münch · BSI
J. Neuschwander · HTWG Konstanz
A. Philipp · PrimeKey Labs GmbH
R. Posch · TU Graz
W. Rankl · Infineon Technologies AG
S. Rass · AAU Klagenfurt
A. Roßnagel · Uni GH Kassel
S. Rudel · UniBw München
S. Schauer · AIT
H. Storck · Schneider Electric Systems
S. Teufel · Uni Fribourg
P. Trommler · TH Nürnberg
M. Ullmann · BSI
G. Weck · Infodas
C. Wegener · Uni Bochum
E. Weippl · SBA Research
S. Wendzel · HS Worms/FKIE
S. Werth · FH Lübeck
A. Wespi · IBM CH
T. Wich · ecsec GmbH
B. C. Witt · it.sec GmbH
K.-D. Wolfenstetter · DTAG

Organisation

N. Pohlmann · Westfälische Hochschule
M. Möhlmann

Workshop KRITIS

U. Lechner · UniBw München & S. Rudel · UniBw München (Organisatorinnen)

Workshop ACS

T. Kleinert · BSI & S. Becker · BSI (Organisatoren)

Inhaltsverzeichnis

Informationssicheres Verhalten automatisiert messen

Maximilian Janik · Kristin Weber · Andreas E. Schütz · Tobias Fertig

Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt
maximilian@janik.xyz
{kristin.weber | andreas.schuetz | tobias.fertig}@fhws.de

Zusammenfassung

Um Informationen im Unternehmen zu schützen, ist die Sensibilisierung der Beschäftigten eine wichtige Aufgabe im Rahmen des Informationssicherheitsmanagements. Die Effektivität von Security-Awareness-Maßnahmen ist allerdings nur schwer messbar, wodurch die Rechtfertigung ihrer Kosten schwerfällt. Diese Arbeit stellt einen Weg vor, informationssicherheitsrelevantes Verhalten technisch zu messen. Dadurch kann der Erfolg von Security-Awareness-Maßnahmen genauer beurteilt werden. Es werden Kennzahlen vorgestellt, mit denen das Verhalten der Beschäftigten an ihren stationären Computern an sicherheitsrelevanten Stellen in datenschutzkonformer Weise aufgezeichnet und ausgewertet wird. Ein Prototyp demonstriert anhand einer Kennzahl die Machbarkeit des Konzepts.

1 Motivation und Zielsetzung

In der Informationssicherheit nimmt der Mensch eine zentrale Rolle ein. Das Verhalten der Beschäftigten am Arbeitsplatz und außerhalb des Unternehmens beeinflusst die Vertraulichkeit, Integrität und Verfügbarkeit von sensiblen Unternehmensinformationen: Sei es ein verlorenes Smartphone, ein versehentlich auf dem Schreibtisch liegen gelassenes vertrauliches Dokument oder ein fremder USB-Stick, der aus Unwissenheit über mögliche Gefahren verwendet wird. Zudem nutzen Kriminelle den „Faktor Mensch“ gezielt als Schwachstelle mit Techniken wie Phishing, Malware und Social Engineering aus [ISAC17, 11]. Der ehemalige Social Engineer Kevin Mitnick drückt es wie folgt aus: „Es ist oft ein Kinderspiel, die menschliche Firewall zu knacken. Das erfordert außer einem Telefonanruf keine Investitionen und beinhaltet nur ein minimales Risiko.“ [MiSD11, 20] Um der Belegschaft ihre wichtige Rolle bewusst zu machen, muss sie für Informationssicherheit sensibilisiert werden [Heli09; WeSc18]. Ein verbreitetes Mittel zur Sensibilisierung ist die Durchführung von Security-Awareness-Maßnahmen.

Um finanzielle Unterstützung für Security-Awareness-Maßnahmen auf Führungsebene zu erhalten, sollte deren Wirtschaftlichkeit nachgewiesen werden. Während die Kosten für diese präventiven Informationssicherheitsmaßnahmen noch vergleichsweise einfach zu ermitteln sind, ist der Nutzen bzw. Erfolg meist schwer nachweisbar [Lubi06; Heli09, 12f]. Eine hohe Security Awareness führt in der Regel zur Verringerung der Eintrittswahrscheinlichkeit von Informationssicherheitsrisiken und damit idealerweise zur Abwesenheit von Informationssicherheitsvorfällen und deren negativen Auswirkungen auf das Unternehmen. Anders ausgedrückt, Investitionen in Informationssicherheit zeigen ihren Nutzen darin, dass nichts passiert: „… den Nutzen von IT-Sicherheit kann man weder sehen noch spüren.“ [Fede06, 4].

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 1-12.

Diese Arbeit zeigt einen Weg, um das informationssicherheitsrelevante Verhalten der Belegschaft in Unternehmen technisch zu messen. Ein IT-System zeichnet das Verhalten der Beschäftigten an ihren stationären Computern an sicherheitsrelevanten Stellen datenschutzkonform auf und wertet die Messergebnisse aus. Wird vor und nach der Durchführung von Security-Awareness-Maßnahmen gemessen, zeigt sich in der Veränderung der Messergebnisse idealerweise der Erfolg der Maßnahmen.

Im Folgenden wird das Verständnis von Security Awareness und verschiedene Ansätze zur Messung von Security Awareness erklärt. Anschließend betrachtet die Arbeit Vorgaben des Datenschutzes, die beim Messen von Sicherheitsverhalten beachtet werden müssen und beschreibt anschließend exemplarisch messbare Kennzahlen. In Kapitel 5 wird die grundlegende Funktionsweise eines solchen IT-Systems mit Hilfe eines Prototyps demonstriert. Am Ende folgt eine Diskussion über die Auswertung und Interpretation der Messergebnisse und schließlich ein Resümee mit Ausblick.

2 Security Awareness

Im Forschungsbereich Security Awareness steht der „Faktor Mensch“, also die Personen, die Informationssysteme und -technik nutzen, im Fokus. Unternehmen, die ihre Informationen schützen möchten, müssen sich darauf verlassen können, dass ihre Belegschaft die hierfür getroffenen Regelungen und Richtlinien befolgen. Mit der Steigerung der Security Awareness der Beschäftigten wird versucht, dieses informationssicherheitskonforme Verhalten zu fördern. [Heli09, 11] beschreiben Security Awareness als Zusammenspiel von Kognition (Beschäftigte wissen was zu tun ist), Handlungsabsicht (Beschäftigte möchten informationssicherheitskonform handeln) und Organisation (Beschäftigte können sich in ihrem Umfeld informationssicherheitskonform verhalten). Die Erhöhung der Security Awareness ist ein komplexes und andauerndes Vorhaben, das auf die Verhaltensänderung der Zielgruppe hin zu einem informationssicherheitskonformen Verhalten abzielt [BaSN15].

Maßnahmen zur Erhöhung der Security Awareness können das menschliche Verhalten jedoch nicht direkt beeinflussen [ScWe17]. Stattdessen müssen die Einflussfaktoren Wissen und Fähigkeiten, Salienz, Gewohnheit, Verhaltensabsicht und die Einschränkungen aus dem Umfeld adressiert werden (vgl. Abbildung 1, erstellt in Anlehnung an [ScWe17, 5]). Eine Person mag wissen, dass das geschäftliche Smartphone mit einer PIN gesichert werden soll. Wenn sie jedoch nicht von der Wichtigkeit dieser Verhaltensweise überzeugt ist, wird sie vermutlich trotzdem keine PIN nutzen. Hier muss erst die Verhaltensabsicht beeinflusst werden. Andere Verhaltensweisen, wie das Sperren des Bildschirms bei Verlassen des Arbeitsplatzes, können stark über die Etablierung einer Gewohnheit unterstützt werden. Um Beschäftigte dazu zu bringen, sich informationssicherheitskonform zu verhalten, müssen Security-Awareness-Maßnahmen zielgerichtet auf diese Faktoren abgestimmt werden. Für zielgerichtete Maßnahmen ist die Analyse der Ist-Situation, also der aktuellen Ausprägung der Einflussfaktoren bei den Beschäftigten und somit der Security Awareness, unerlässlich [BaSN15, WeSc18].

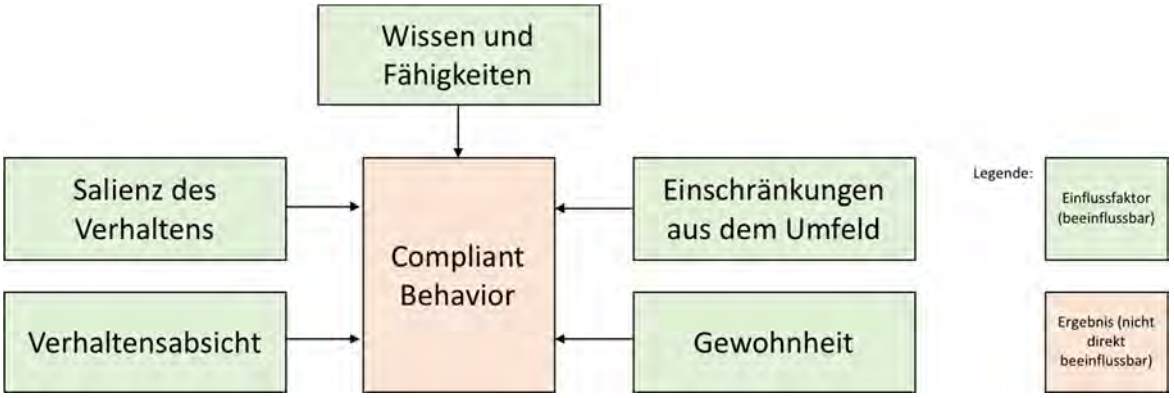

Abb. 1: Einflussfaktoren auf menschliches Verhalten

Sowohl Unternehmen als auch die Wissenschaft beschäftigen sich mit der Frage, wie Security Awareness gemessen werden kann. Eine Liste des „SANS Institute“ [Spit14] zeigt mögliche Metriken, wie die Anzahl infizierter Rechner im Unternehmen sowie Ergebnisse von Umfragen, Brute-Force-Versuchen auf Passwörter, nächtlichen Prüfungen auf nicht gesperrte Computer und Social-Engineering-Angriffen per Telefon oder E-Mail. Die Forschung zeigt Ansätze zur Messung der Security Awareness mittels Befragung [KrKe06, 290ff; HaPo09, 81ff.; WeSc18; FHFP18] und durch das Versenden fingierter Phishing-E-Mails [DoCF07, 74f]. [KANK11] stellen zudem einen Ansatz vor, wie mit Metriken wie Sicherheitsvorfällen, Anrufen beim Help Desk oder der Anzahl der Zugriffe auf unautorisierte Webseiten Security Awareness gemessen werden kann.

Bei der Betrachtung der verschiedenen Methoden aus dem vorhergehenden Absatz zeigt sich, dass es unterschiedliche Auffassungen von Security Awareness gibt. Der Definition von [Heli09] und den Einflussfaktoren von [ScWe17] folgend, wird teilweise mehr das „Compliant Behavior“ (informationssicherheitskonformes Verhalten) und damit das Ergebnis der Security Awareness gemessen, während andere Ansätze sich auf die Security Awareness selbst konzentrieren. Die erste Variante gibt also Auskunft darüber, inwieweit Mitarbeiter die Regelungen des Unternehmens befolgen. Hieraus geht allerdings nicht hervor welche Gründe zu dem jeweiligen Verhalten führen, beispielsweise ob den Mitarbeitern das Wissen oder die Motivation fehlt oder doch eine technische Hürde für unerwünschtes Verhalten verantwortlich ist. Daher sollte bei der Auswahl eines Ansatzes genau geprüft werden, was letztendlich gemessen werden soll.

Eine möglichst standardisierte, wiederholbare und kostengünstige Messmethode ist die automatisierte Erfassung an den stationären Computern der Belegschaft.

3 Datenschutzkonform Messen

Das Erheben von personenbezogenen Daten der Belegschaft, um deren informationssicherheitsrelevantes Verhalten zu analysieren, fällt in den Anwendungsbereich des Datenschutzrechts. Spätestens mit dem Inkrafttreten der DSGVO am 25. Mai 2018 sind Unternehmen für den gesetzeskonformen Umgang mit personenbezogenen Daten stärker sensibilisiert und sind sich der härteren Strafen bewusst. Im Rahmen dieses Papers ist keine umfassende und juristisch einwandfreie Betrachtung dieses Themas möglich. Es werden im Folgenden daher nur einige grundsätzliche Überlegungen zum Datenschutzrecht und anderen Gesetzen aufgeführt, die bei der Entwicklung des Prototyps zu berücksichtigen sind.

Techniken in OpenBSD zur Vermeidung von ROP-Angriffen

Jan Klemkow

genua GmbH
jan_klemkow@genua.de

Zusammenfassung

Dieser Beitrag erläutert neue Sicherheitstechniken im Betriebssystem OpenBSD, welche in den letzten Jahren und Monaten hinzugekommen sind, um sich gegen ROP-Angriffe zu wehren. Zunächst wird noch einmal grundlegend auf die ROP-Thematik eingegangen, um das Problemfeld einzuleiten. Danach werden wechselweise die verschiedene Angriffsmöglichkeiten dargelegt zusammen mit den neuen Sicherheitsfunktionen, die diese Angriffe erschweren oder sogar ganz verhindern. Abschließend wird am Ende des Beitrag erörtert, welchen Einfluss der Einsatz von OpenSource-Software auf die Umsetzung von progressiven Sicherheitstechniken hat.

1 Einleitung

Das Ausnutzen von Buffer-Overflows zum Infiltrieren von fehlerhaften Computer-Systemen ist seit vielen Jahrzehnten ein Problem. Seither hat sich aber die Methodik, wie man diese Schwachstellen ausnutzt, stark verändert. Nachdem sich die Data-Execution-Prevention durchgesetzt hat, verbleibt die Technik des Return-Oriented-Programming [RBSS12] (ROP), um auch heute noch mit klassischen Buffer-Overflows aktuelle Computer-Systeme zu kompromittieren.

Dieser Beitrag zeigt, wie das auf hohe Sicherheit ausgelegte Open-Source-Betriebssystem OpenBSD mit dieser Angriffstechnik umgeht. Es wird dargelegt, welche neuen Speicherschutztechniken in den letzten Jahren implementiert wurden, um solche Angriffe zu vermeiden. Zunächst werden dabei einige Spezialformen von ROP-Angriffen erklärt und danach die Gegenmaßnahmen erläutert.

2 Return-Oriented-Programming

Das Einschleusen von eigenem Programm-Code (auch Shell-Code genannt) durch einen Buffer-Overflow auf dem Stack eines fehlerhaften Programms ist auf modernen Betriebssystemen nicht mehr ohne weiteres möglich. Der Stack-Bereich ist in den Page-Tables durch das Non-Execution-Bit als nicht ausführbar markiert. Dadurch würde das Programm sofort von Prozessor und Betriebssystem beendet werden, sobald versucht würde, innerhalb dieses Speicherbereichs Programm-Code auszuführen.

In der Abbildung 1 ist ein klassischer Buffer-Overflow mit eingeschleustem Shell-Code auf dem Programm-Stack abgebildet. Der Angreifer überschreibt dabei die Rücksprungadresse der fehlerhaften Funktion mit einer eigenen Adresse. Diese Adresse zeigt auf den ebenfalls auf dem

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 59-67.

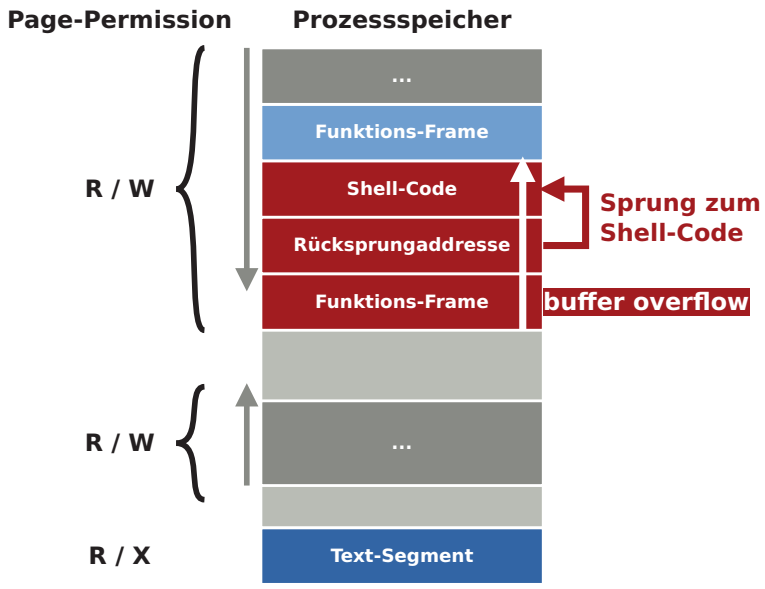

Abb. 1: Schema eines klassischen Buffer-Overflow-Angriffs

Stack eingeschleusten Schadcode (Shell-Code). Sobald der Prozessor versucht, den Programmcode an der Rücksprungadresse zu laden und auszuführen, wird er feststellen, dass dieser in einem Bereich liegt, welcher in den Page-Tables als nicht-ausführbar markiert ist. Daraufhin wird der Prozess unterbrochen und das Betriebssystem über einen Trap informiert. Das Betriebssystem wird dann den Prozess mit einer Fehlermeldung beenden.

Angriffe mittels ROP sind daher in den letzten Jahren zu einer beliebten Methode geworden, um weiterhin die Kontrolle über ein fehlerhaftes Programm zu erlangen.

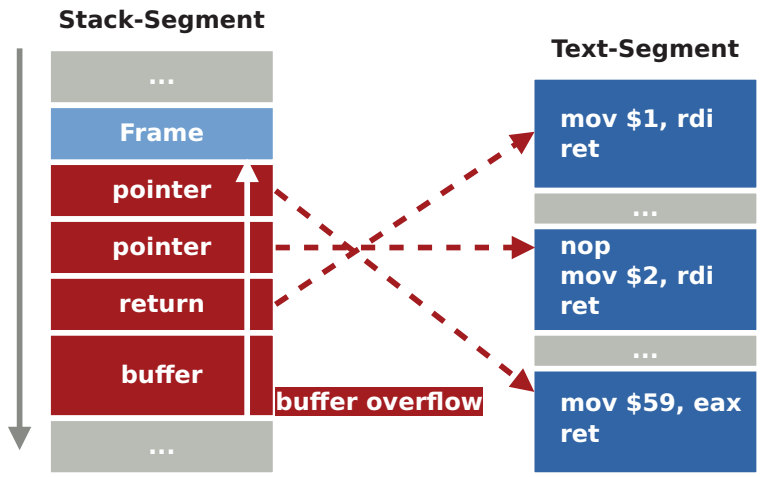

Abb. 2: Schema eines ROP-Angriffs

Da das Einschleusen von eigenem Programm-Code direkt nicht mehr möglich ist, stützen sich ROP-Angriffe darauf, Code-Schnipsel zu verwenden, welche das zu exploitende Programm bereits im eignen Text-Segment enthält (Abbildung 2). Die für einen ROP-Angriff verwendeten Code-Schnipsel werden auch “Gadgets” genannt. Ziel des Angriffs ist es also, den Program-

mablauf zu beeinflussen. Dieses gelingt dem Angreifer, indem er den Stack des Programms mit eigenen Rücksprungadressen überschreibt, welche dann nacheinander abgearbeitet werden. Die Gesamtheit der angesprungenen Code-Stücke bilden dann den Schadcode des Angreifers, ohne, dass dieser explizit eingeschleust werden muss.

3 ASLR

Um es dem Angreifer zu erschweren, die korrekten Adressen von Gadgets anzuspringen, wurde die Address-Space-Layout-Randomization (ASLR) implementiert. Dabei werden verschiedenen Bestandteile eines Prozesses mit zufälligen Offsets in den virtuellen Speicherraum gemapped. Diese Offsets erschweren es dem Angreifer, die gewünschten Gadgets zu treffen.

Die Speichersegmente von Text, Stack und Heap sind nun mit zufälligen Offsets im Speicher angeordnet. Allerdings unterliegen die Offsets der Anforderung, dass die verschiedenen Segmente page-alignt im Speicher liegen müssen. Dadurch kann der Angreifer den Bereich, indem die gewünschten Gadgets liegen stark eingrenzen. Dieses erlaubt es ihm gezielt, sich mit mehreren Angriffen iterativ an die richtigen Speicheradressen heranzutasten, bis sein Angriff funktioniert. Außerdem ist es einem Angreifer möglich, auf die Adressen aller Elemente eines ASLR-Blocks zu schließen, sobald ihm die Adresse eines Objekts innerhalb des Blocks bekannt wird. Dieses kann durch Debug-Ausgaben oder anderen Informations-Leaks geschehen.

4 Zufälliges Re-Linking

Experimente mit dynamischem Linken in zufälliger Reihenfolge hat es auch schon zuvor in der OpenBSD-Entwickler-Gemeinde gegeben [Sha10]. Nur wurden diese erst in den letzten Veröffentlichungen des Projektes produktiv umgesetzt. Dieser Abschnitt erläutert die neuen Sicherheitsmechanismen in diesem Bereich.

4.1 Standard-C-Bibliothek

Return-to-LibC ist ein spezieller ROP-Angriff, welcher sich zueigen macht, dass in fast jedem Programm die Standard-C-Bibliothek eingebunden ist. Diese bietet eine Fülle an ROP-Gadgets, welche für einen Angriff genutzt werden können. Somit kann der Angreifer einen einmal vorhandenen Schadcode-Pfad innerhalb der C-Bibliothek bei Angriffen unterschiedlicher Programme wiederverwenden. Da die C-Bibliothek selbst sehr stabil ist, muss ein Angreifer nur die Position der Bibliothek im Speicher herausfinden. Mit dieser Position kann er dann die genauen Adressen der Gadgets selbst berechnen.

Die Abbildung 3 zeigt, wie dieses im Build- und Release-Prozess realisiert wurde [dR16a]. Zunächst werden die C-Quelldateien zu Shared-Objects kompiliert. Anstatt diese nun direkt in zu dynamischen Bibliothek zu linken, werden diese Dateien in das Archiv “libc.so.a” zusammen gefügt. Dieses Archiv wird in der Binär-Distribution des System ausgeliefert. Bei jedem Start des Systems, wird dieses Archiv entpackt und die enthaltenden Objekt-Dateien in einer zufälligen Reihenfolge zusammen gelinkt. Somit hat jede laufende OpenBSD-Instanz eine eigene Standard-C-Bibliothek, in der die Speicheradressen der ROP-Gadgets individuell verschoben sind.

Ein Angreifer hat dadurch einen enorm höheren Aufwand, die Positionen der benötigen Gadgets zu finden. Es reicht nun nicht mehr, den Offset der Standard-C-Bibliothek zu finden, sondern die Adressen jedes verwendeten Gadgets.

Sei gewarnt! Vorhersage von Angriffen im Online-Banking

Tobias Urban[1] · René Riedel[1] · Christine Paulisch[2]
Norbert Pohlmann[1]

[1]Institut für Internet-Sicherheit – if(is) Westfälische Hochschule
{urban | riedel | pohlmann}@internet-sicherheit.de

[2]Institut für Psychologie und Arbeitswissenschaft
Technische Universität Berlin
christine.paulisch@mms.tu-berlin.de

Zusammenfassung

In diesem Artikel wird ein Alert-System für das Online-Banking vorgestellt, welches das Schutzniveau im Kontext von *Social-Engineering*-Angriffen sowohl clientseitig als auch serverseitig erhöhen soll. Hierfür wird durch das Alert-System ein kontinuierliches Lagebild über die aktuelle Gefahrenlage beim Online-Banking erstellt. Bei konkretem Bedarf wird der Nutzer punktuell vor aktuellen Betrugsmaschen gewarnt und zielgerichtet über Schutzvorkehrungen und Handlungsempfehlungen informiert. Für die Berechnung der aktuellen Gefahrenlage wurden unterschiedliche *off-the-shelf*-Algorithmen des Maschinellen Lernens verwendet und miteinander verglichen. Die Effektivität des Alert-Systems wurde anhand von echten Betrugsfällen evaluiert, die bei einer Bankengruppe in Deutschland aufgetreten sind. Zusätzlich wurde die Usability des Systems in einer Nutzerstudie mit 50 Teilnehmern untersucht. Die ersten Ergebnisse zeigen, dass die verwendeten Verfahren dazu geeignet sind, die Gefahrenlage im Online-Banking zu beurteilen und dass ein solches Alert-System auf hohe Akzeptanz bei Nutzern stößt.

1 Einführung

Online-Banking und Online-Transaktionen sind ein wichtiger Teil der modernen Informationsgesellschaft und werden in Zukunft noch weiter an Bedeutung gewinnen. Allein zwischen 2006 und 2016 stieg die Nutzung von Online-Banking in Europa von 25% auf 49% an [1]. Aufgrund des Wachstums von Anwendungen die Micro-Transaktionen nutzen und der fortschreitenden Digitalisierung der Gesellschaft, wird dieser Bereich auch in Zukunft weiter wachsen [2].

Online-Banking Systeme werden heutzutage erfolgreich von Betrügern angegriffen (siehe z. B. [3]). Laut offiziellen Angaben des Bundeskriminalamtes entstand allein 2016 in Deutschland ein Schaden von insgesamt 8,7 Millionen Euro [4] im Zusammenhang mit Phishing im Online-Banking. Es kann davon ausgegangen werden, dass der tatsächlich entstandene Schaden deutlich höher ist, da die Dunkelziffer bei der Aufklärung von Cyberkriminalität generell hoch ist und Finanzinstitute ihre Kunden meist direkt entschädigen [5], um z. B. negativer Presse und dem damit verbundenen Reputationsschaden vorzubeugen.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 151-163.

Aufgrund der aktuellen Sicherungsverfahren (z. B. smsTAN oder chipTAN [6]) muss der Online-Banking-Nutzer von einem Angreifer initial zu einem Fehlverhalten verleitet werden, damit ein erfolgreicher Angriff überhaupt erst möglich ist. Die Erkennung und Bekämpfung von *Social-Engineering*-Angriffen ist auf technischer Seite nur schwer zu realisieren. Aus diesem Grund muss der Nutzer in das Sicherheitskonzept des Online-Bankings eingebunden werden.

Das Alert-System, das in diesem Dokument vorgestellt wird, soll den Nutzer warnen, wenn eine besonders hohe Gefahr vorliegt, dass dieser im Online-Banking angegriffen wird. So kann dem Nutzer mitgeteilt werden, welche Gefahr vorliegt und er kann über Abwehrmaßnahmen aufgeklärt werden. Dem Nutzer wird so die Möglichkeit gegeben, besser auf *Social-Engineering*-Angriffe zu reagieren und diese leichter zu erkennen. Ein Vorteil ist, dass Nutzer über Gefahren aufgeklärt werden, wenn diese real auftreten. So wird die Wahrscheinlichkeit, dass der Angriff erfolgreich ist, verringert. Des Weiteren können *Fraud-Prevention-Systeme* von Finanzinstituten von einer Übersicht zur aktuellen Gefahrenlage profitieren, um die Aktionen der Nutzer besser bewerten zu können, z. B. sind bei einer hohen Gefahrenlage Überweisungen ins Ausland verdächtiger, als bei einer geringen Gefahrenlage.

Banken gehören in Deutschland zu den kritischen Infrastrukturen [7] und sind somit verpflichtet, Lagebilder zum Zustand der Struktur zu erstellen [8]. Die Gefahrenlage, die von dem vorgestellten Alert-System bestimmt wird, liefert wertvolle Informationen für solche Lagebilder.

Die Hauptaugenmerke dieser Arbeit liegen auf den folgenden Punkten:

- Es wurden wichtige Kennzahlen identifiziert, die für die Bestimmung der aktuellen Gefahrenlage ausschlaggebend sind (Kapitel 2).
- Es wurden die Zeitpunkte, an denen die Gefahrenlage besonders groß ist, bestimmt. Validiert wurden ebenso die identifizierten Zeitpunkte anhand echter Betrugsfälle, die bei einer deutschen Bank aufgetreten sind (Kapitel 3).
- In einer Nutzerstudie ($n = 50$) wurde die Nutzerfreundlichkeit, das Sicherheitsempfinden, das Nutzungsverhalten und die Akzeptanz des Systems untersucht (Kapitel 4).

Verwandte Arbeiten werden in Kapitel 6 vorgestellt.

2 Konzept

Im Folgenden wird der konzeptionelle Aufbau des entwickelten Alert-Systems erläutert. Es werden die ermittelten Kennzahlen (Abschnitt 2.1) sowie die Metrik zur Evaluierung des Alert-Systems beschrieben (Abschnitt 2.2).

2.1 Kennzahlen

Phishing ist im Online-Banking eine weit verbreitete Strategie, um beispielsweise Passwörter, Kreditkartendaten oder TAN-Nummern zu stehlen. Phishing bezeichnet dabei die Technik den Benutzer z. B. durch gefälschte E-Mails und Internetseiten dazu zu bewegen, dem Angreifer seine geheimen Informationen preiszugeben. Daher ist es für das hier vorgestellte Alert-System wichtig, Informationen zum aktuellen Aufkommen von Phishing (Spam) zu erhalten. Aus den verwendeten Quellen werden nur Informationen extrahiert, die im direkten Zusammenhang mit Online-Banking stehen. Innerhalb des entwickelten *Alert-Systems* werden drei Quellen genutzt, die für Phishing-Angriffe relevant sind:

- **E-Mail:** Klassischerweise werden Phishing-Angriffe über E-Mails durchgeführt. Die Angreifer versenden eine E-Mail, die einer echten Nachricht der Bank gleicht, um den Kunden zu täuschen. In dieser Arbeit werden Spam-Nachrichten verwendet, die im „Spam Archive“ [9] zur Verfügung gestellt werden. Im Beobachtungszeitraum (456 Tage) wurden insgesamt 670.622 Spam-Mails im Archive veröffentlicht. Anhand einer Stichwortsuche konnten 5.589 relevante Mails identifiziert werden.
- **Foren / Soziale Netzwerke:** Phishing-Angriffe werden zunehmend auf anderen Plattformen, z. B. in sozialen Netzwerken, Foren, oder Ähnlichem durchgeführt. Hier wird das Phishing z. B. über private Nachrichten oder öffentliche Posts durchgeführt. In dieser Arbeit werden Spam-Nachrichten genutzt, die auf den Webseiten des *Stackoverflow*-Netzwerkes erkannt werden [10]. Basierend auf einer Schlagwort-Suche wurden 1.904 Nachrichten identifiziert.
- **Webseiten:** Zusätzlich wird auf Information zu aktuellen Phishing-Webseiten zurückgegriffen. Als Quelle für Phishing-Seiten werden alle Seiten verwendet, die von der Organisation *PhishTank* [11] veröffentlicht wurden. Insgesamt wurden anhand einer Klassifizierung von *PhishTank* und einer Schlagwortsuche 2.776 Phishing-Seiten für den Testzeitraum gefunden.

Die Kennzahlen mit Bezug zum Phishing wurden zusammengefasst, um die Dimension der entwickelten Ansätze möglichst klein zu halten.

Wichtig für die Einschätzung der aktuellen Gefahrenlage beim Online-Banking ist auch die Aktivität von Banking-Trojanern. Da keine globale Sicht zu den zugehörigen *Botnetzen* verfügbar ist, müssen andere Indizien genutzt werden, um die Gefahr, die von einem *Botnetz* ausgeht, beurteilen zu können. Die Anzahl der Endgeräte, die mit einem Banking-Trojaner infiziert wurden, ist ein starker Indikator dafür, dass sich ein Nutzer mit einem Banking-Trojaner infizieren könnte (z.B., wenn der Angreifer eine ‚Kampagne‘ zum Verteilen des Trojaners durchführt). In dieser Arbeit wurden die erkannten Infektionen (insgesamt 23.184 im Testzeitraum) von Banking-Trojanern durch einen großen Hersteller von Antivirus-Produkten genutzt.

Die Gefahr, dass sich Nutzer mit Schadsoftware infizieren, kann aber auch anhand aktueller Software-Schwachstellen gemessen werden. Die Kennzahlen zu bekannten Schwachstellen werden aus der *National Vulnerability Database* [12] (kurz NVD) extrahiert. Die NVD beinhaltet Informationen zu Software-Schwachstellen, Fehlkonfigurationen und Metriken zu deren Einfluss. Von dem entwickelten Alert-System werden nur Schwachstellen beachtet, die Remote ausgenutzt werden können, gängige Browser und Betriebssysteme betreffen und die es erlauben beliebigen Code auszuführen. In dem Testzeitraum traten 875 solcher Schwachstellen auf.

Für die Kontrolle des Alert-Systems werden Betrugsfälle, die bei einer deutschen Bankgruppe aufgetreten sind, genutzt. Anhand dieser Betrugsfälle kann die Effizienz der entwickelten Verfahren gemessen werden. In dem Testzeitraum lagen 459 Betrugsfälle vor. Abbildung 1 zeigt die genutzten Quellen und deren Verwendung in dem Aufbau des Alert-Systems.

Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain

Tomasz Kusber[1] · Steffen Schwalm[1]
Christian Berghoff[2] · Ulrike Korte[2]

[1]Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS)
{tomasz.kusber | steffen.schwalm}@fokus.fraunhofer.de

[2]Bundesamt für Sicherheit in der Informationstechnik (BSI)
{christian.berghoff | ulrike.korte}@bsi.bund.de

Zusammenfassung

Die Blockchain-Technologie ([Lem16], [WEKJ17]) findet zunehmend branchenübergreifend Beachtung und Verwendung. Dabei sind Blockchains integritätsgeschützte Datenstrukturen, in denen Transaktionen als verteilte elektronische Journale ohne zentrale Instanzen realisiert werden. Zur vertrauenswürdigen Abwicklung und Nachweis elektronischer Geschäftsprozesse sind im Rahmen der Anwendung der Blockchain-Technologie insbesondere Anforderungen hinsichtlich der geltenden gesetzlichen Nachweispflichten, der beweiswerterhaltenden Aufbewahrung gemäß Artikel 34 [eIDAS-VO] und Artikel 15 [VDG] sowie der EU-Datenschutzgrundverordnung (EU-DSGVO) zu erfüllen. Ausgehend von diesen juristischen und technischen Vorgaben werden die vorgenannten Anforderungen erläutert und Lösungen für den Einsatz von Blockchain-Technologien insbesondere im Zusammenhang mit dem Beweiswerterhalt abgeleitet. Dabei werden drei Lösungsvarianten, zusätzliche dedizierte Blöcke in Blockchain, Blockchain und der Einsatz von Evidence Records gemäß [RFC4998] und logische Blockchain auf Basis von [RFC4998], vorgestellt, miteinander vergleichen, und es wird eine Bewertung mit Ausblick gegeben.

1 Einführung

Die Blockchain-Technologie mit ihrem prominentesten Vertreter Bitcoin [Na08] erlebt seit einiger Zeit einen regelrechten Hype. Ihr wird in verschiedenen Branchen, so z.B. der Finanzindustrie, der Energiewirtschaft oder der öffentlichen Verwaltung, großes Potenzial zugeschrieben [WEKJ17]. Blockchains realisieren faktisch eine Technologie für verteilte elektronische Journale. Dabei werden neue Datenblöcke an eine stetig wachsende Kette angehängt und mit ihrem Vorgänger kryptographisch sicher verkettet. Die so entstehende Blockchain wird in einem dezentralen Peer-to-Peer-Netzwerk verteilt. Ein sogenannter Konsensmechanismus sorgt dafür, die Daten auf allen Netzwerkknoten konsistent zu halten. Als wesentliche Neuerung von Blockchains wird ihr Vertrauensmodell angesehen. Im Unterschied zu bestehenden, zentralisierten Technologien wie Datenbanken gibt es in einer Blockchain keine zentrale Instanz, über die die Kommunikation abläuft sowie gesteuert und verwaltet wird und der alle Nutzer vollumfänglich vertrauen müssen. Das Vertrauen in den korrekten Zustand der Blockchain entsteht vielmehr aus der dezentralen Speicherung und Prüfung der Daten durch die übrigen Netzwerkknoten, wobei das Ausmaß der tatsächlichen Dezentralität je nach konkreter Ausgestaltung va-

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 177-191.

riiert. Mittels des Verzichts auf eine zentrale Instanz soll es möglich sein, in Blockchain-Anwendungen Kosten zu sparen, wobei gleichzeitig eine hohe Verfügbarkeit der abgelegten Daten erreicht wird. Nachteile im Vergleich zu Datenbanken ergeben sich wegen der verteilten Speicherung in den Punkten Effizienz und Vertraulichkeit.

Die Aufnahme von Daten (in diesem Kontext meist als Transaktionen bezeichnet[1] [WEKJ17]) in eine Blockchain läuft folgendermaßen ab: Der Netzwerkknoten, der eine Transaktion in die Blockchain integrieren möchte, verteilt diese zunächst an die übrigen Knoten im zugrundeliegenden Peer-to-Peer-Netzwerk. Transaktionen werden gesammelt und in einer festgelegten Frequenz von speziellen Knoten, den Minern, zu Blöcken zusammengefasst. Neben einer Liste von Transaktionen enthält ein Block stets einen Verweis auf seinen Vorgängerblock, der durch eine Hashfunktion realisiert ist und nachträgliche Manipulationen früherer Blöcke verhindert bzw. nachweisbar gestalten soll. Der Anfang der so entstehenden Kette von Blöcken, der „Blockchain“, wird als Genesis-Block bezeichnet. Da es im Allgemeinen mehrere Miner gibt, die Blöcke erzeugen können, wird ein sogenannter Konsensmechanismus verwendet, um unter allen Teilnehmern des Netzwerks Einigkeit über den jeweiligen Zustand der Blockchain herzustellen und die Daten konsistent zu halten [Na08, WEKJ17]. Für die konkrete Ausgestaltung des Konsensmechanismus gibt es verschiedene Möglichkeiten, die von der Art der verwendeten Blockchain abhängen. Am bekanntesten ist das von Bitcoin genutzte Proof-of-Work-Verfahren, bei dem der Konsens mithilfe eines rechenintensiven mathematischen Puzzles hergestellt wird. Ein großer Nachteil dieser Methode besteht in ihrem exorbitanten Energieverbrauch und dem niedrigen Datendurchsatz, den sie erlaubt [Di18]. Weiterhin tritt der Konsens nicht unmittelbar, sondern erst nach einer gewissen Zeitspanne ein. Wesentlich effizientere nachrichtenbasierte Konsensverfahren, die auf langjährigen Forschungsarbeiten im Bereich der Verteilten Systeme basieren, können jedoch auf sogenannten privaten (permissioned) Blockchains eingesetzt werden [CGR11]. Anders als beispielsweise bei Bitcoin ist aufgrund des vernachlässigbaren Energie- und Rechenaufwands für diese Konsensmechanismen auf privaten Blockchains ein sogenanntes Anreizsystem für die Mitarbeit der Miner nicht erforderlich.

Private Blockchains unterscheiden sich von öffentlichen Blockchains wie Bitcoin in ihrem Rechtemanagement. Während öffentliche Blockchains für beliebige Nutzer zugänglich und einsehbar sind, trifft dies bei privaten Blockchains nur für einen autorisierten Kreis zu. Zusätzlich geben die Begriffe „permissionless“ und „permissioned“ an, ob alle Nutzer über die gleichen Berechtigungen verfügen. Bei Bitcoin ist beispielsweise jeder Nutzer a priori ein Miner, wohingegen dies bei permissioned Blockchains nur für eine berechtigte Teilmenge der Fall ist [WEKJ17]. Aus diesem Grund sind private permissioned Blockchains in Bezug auf das Vertrauensmodell klassischen Lösungen ähnlicher, ohne aber die Eigenschaft der Dezentralität völlig aufzugeben. Die Identität der Teilnehmer ist, anders als bei öffentlichen Blockchains, in der Regel bekannt, was die angesprochenen Vorteile durch effizientere Algorithmen ermöglicht.

Die Ideen für den Einsatz von Blockchains in der Wirtschaft sind vielfältig. In Anlehnung an Bitcoin und andere Kryptowährungen können Blockchains eingesetzt werden, um allgemein den Transfer von Gütern, z. B. im Energiehandel, zu dokumentieren. Andere Anwendungen nutzen die Technologie in ausgewählten Fällen, wo dies möglich ist, zur Integritätssicherung von Dokumenten, indem deren Hashwerte in einer Blockchain gespeichert und so vor Manipulationen geschützt werden. Weitere Vorschläge betreffen die Kontrolle von Geschäftsprozessen sowie beispielsweise die Lieferketten- oder Vertragsinhaltsüberwachung durch sog. Smart

[1] Die zuerst auf der Bitcoin-Blockchain (BTC) verwendeten Begriffe haben sich allgemein etabliert.

Contracts [WEKJ17]. In den meisten dieser Fälle ist aus rechtlichen (z.B. Datenschutz, Nachweispflichten (vgl. Kapitel 2) und Effizienzgründen zu erwarten, dass sie mithilfe privater Blockchains realisiert werden. Da die Lebensdauer einer Blockchain potenziell unbegrenzt ist, ist insofern ein umfassendes Konzept zur Archivierung der in Blockchain abgelegten Daten inklusive der Wahl und Aktualisierung geeigneter Kryptoalgorithmen nötig, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit auch langfristig zu erreichen [BSIGS]. Diese sind nicht nur aus Gründen der Informationssicherheit erforderlich, sondern ebenso Grundlage zur Erfüllung bestehender Dokumentations- und Nachweispflichten, sofern Blockchain für geschäftsrelevante Prozesse verwendet werden soll. Diese Anforderungen und Herausforderungen sowie mögliche Lösungsansätze werden im Folgenden näher beschrieben.

2 Anforderungen an Blockchain

Im Folgenden werden Anforderungen an Blockchain zur Nutzung für vertrauenswürdige digitale Prozesse aufgezeigt.

2.1 Nachweis- und Aufbewahrungspflichten

Sofern blockchainbasierte Verfahren zur Abbildung vertrauenswürdiger elektronischer Prozesse in Behörden und Unternehmen dienen sollen und damit innerhalb dieser Verfahren oder in Verbund mit angrenzenden Lösungen (z.B. Cloud zur Ablage der Daten selbst und nur Verbleib von Hashwerten in der Blockchain) geschäftsrelevante Unterlagen entstehen und abgelegt werden, so sind, wie in jedem IT-Verfahren, das zur Umsetzung elektronischer Geschäftsprozesse Anwendung findet, die einschlägigen Nachweis- und Aufbewahrungspflichten zu beachten [Ko13], [ISO15489], [Wi15], [We18]. Elektronische Unterlagen geben jedoch aus sich selbst heraus keine Hinweise zu deren Integrität und Authentizität, ebenso wenig können sie ohne technische Hilfsmittel wie Soft- und Hardware wahrgenommen oder gelesen werden. Gleichzeitig bestehen jedoch umfassende Dokumentations- und Aufbewahrungspflichten, deren Dauer zwischen zwei und 110 Jahre[2] oder dauernd[3] umfasst. Innerhalb dieser Zeit ist der eindeutige wie verlustfreie Nachweis von Authentizität, Integrität und Nachvollziehbarkeit der Unterlagen gegenüber Prüfbehörden, Gerichten, Dritten zu erbringen [To07], [Ko14], [KuSc16]. Teilweise beginnen diese Fristen erst zu einem Zeitpunkt in der Zukunft, so z.B., wenn das Produkt, auf das sich die Unterlagen beziehen, vom Markt genommen wird, wie dies im Bereich europäischer Zulassungsverfahren in Luftfahrt, Pharma oder Pflanzenschutzmittel der Fall ist. Um die erforderlichen Nachweise führen zu können, sind die Unterlagen inklusive Meta- und Prozessdaten dem Gericht resp. der Prüfbehörde vorzulegen, was deren Verkehrsfähigkeit erfordert. Die zum Nachweis notwendigen Informationen sind also inhärente Bestandteile der Unterlagen selbst [Ko13], [KuSc16], [Ro07]. Neben dem Nachweis der Authentizität und Integrität ist im Kontext elektronischer Unterlagen sowie der technischen Entwicklung über die o.g. teilweise jahrzehntelangen Aufbewahrungsfristen vor allem deren Verfügbarkeit, also Lesbarkeit zu gewährleisten. Branchenspezifisch kommen, neben der reinen, originären Visualisierung der Daten, spezifische technische Vorgaben hinzu wie deren maschinelle Auswertbarkeit oder die Reproduzierung in den Unterlagen dokumentierter Analyseergebnisse etc.

[2] 110 Jahre gelten z.B. im Personenstandswesen für die Registerdaten, siehe https://www.gesetze-im-internet.de/pstg/BJNR012210007.html, § 5

[3] ´Dauernd gilt z.B. für Bauakten oder im Kontext Endlagerung

IT-Sicherheit für Geschäftsprozesse im Finanzsektor

Steffi Rudel[1] · Torsten Bollen[2]

[1]Universität der Bundeswehr München
steffi.rudel@unibw.de

[2]Wincor Nixdorf
Torsten.Bollen@dieboldnixdorf.com

Zusammenfassung

Im vorliegenden Beitrag wird die Kurzfassung einer Fallstudie zur IT-Sicherheit in Kritischen Infrastrukturen beschrieben. Die Fallstudie stellt die Managementlösung PREVENT vor, die im Rahmen eines Forschungsprojektes im Förderschwerpunkt "IT-Sicherheit für Kritische Infrastrukturen" ITS|KRITIS des BMBF entwickelt wird. Die Managementlösung PREVENT stellt Banken Dashboards zur Verfügung, um durch nutzergerechte Aufbereitung eines Lagebildes bei der Risikoeinschätzung zu unterstützen. Dieses Lagebild erlaubt ein effektives und effizientes Risikomanagement für systemkritische Geschäftsprozesse. Die vollständige Fallstudie ist in der Quelle [LDR+18] veröffentlicht sowie unter www.itskritis.de kostenfrei verfügbar.

1 IT-Sicherheit im Bankwesen

Die vorliegende Fallstudie entstand in dem Forschungsprojekt PREVENT des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen" des Bundesministeriums für Bildung und Forschung (BMBF). Die Fallstudie beschreibt ein IT-Sicherheitsmanagementsystem der nächsten Generation für die als kritisch eingestuften Prozesse einer Bank: die Managementlösung PREVENT.

Für Banken ist seit Basel II das Risikomanagement von Finanztransaktionen ein wichtiges Thema. Diese Finanzrisiken werden vorrangig vom Basler Ausschuss für Bankenaufsicht in Zusammenhang mit der Eigenkapitalquote der Banken gesehen. Zunehmend treten heute jedoch die operativen Risiken in den Vordergrund. Dies sind Risiken, die sich aus Geschäftsprozessen, Menschen und Systemen, sowie deren Interaktion miteinander ergeben. Dieser Umstand findet entsprechende Beachtung u.a. in den Katalogen des IT Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2 Einordnung als Kritische Infrastruktur

Kritische Infrastrukturen (KRITIS) werden vom BSI grundsätzlich in verschiedene Sektoren untergliedert. Die Fallstudie mit den beteiligten Playern siedelt sich in dem Sektor Finanz- und Versicherungswesen an [BuSI16].

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 232-235.

Ausschlaggebend für die Einordnung als KRITIS ist die kritische Versorgungsdienstleistung. Die Abwicklung des Zahlungsverkehrs ist eine kritische Dienstleistung sowohl für Privatpersonen (Erhalt des Gehalts, Bezahlen von Rechnungen, Miete, etc.) als auch für Unternehmen. Sie hat damit eine sektorübergreifende Bedeutung und ist daher die wesentliche kritische Versorgungsdienstleistung des Finanzdienstleistungssektors [BuSI16].

Der Finanzsektor stellt unter den KRITIS eine Besonderheit dar, da hier die „Finanzmittel – im Gegensatz zu anderen Wirtschaftsbereichen – nicht nur die Rahmenbedingung für das Wirtschaften, sondern den Geschäftsgegenstand selbst darstellen" [BuSI16]. Als weitere Besonderheit sind in Bankenrechenzentren sowohl die Geschäftsprozesse als auch die Infrastruktur kritisch, da ausschließlich mit Daten und nicht mit physischen Waren gehandelt wird.

3 Managementlösung PREVENT

3.1 Hintergrund und Rahmenbedingungen

In Banken sind per Gesetz grundsätzlich die Vorstände für das Risikomanagement verantwortlich und haftbar zu machen. Aus diesem Grund soll dieser Managementebene mit der Managementlösung PREVENT ein Dashboard auf Basis eines Lagebildes (Compliance Status) zur Verfügung gestellt werden. Dieses soll helfen, Risiken in Echtzeit konkret einschätzen und bewerten zu können und anschließend geeignete Maßnahmen einleiten zu können.

3.2 Abhängigkeit zwischen Prozessen und Anwendungen

Grundsätzlich lassen sich die Prozesse und Anwendungen in einem Finanzunternehmen auf verschiedenen Ebenen betrachten. Die folgende Abbildung 1 visualisiert diese Ebenen.

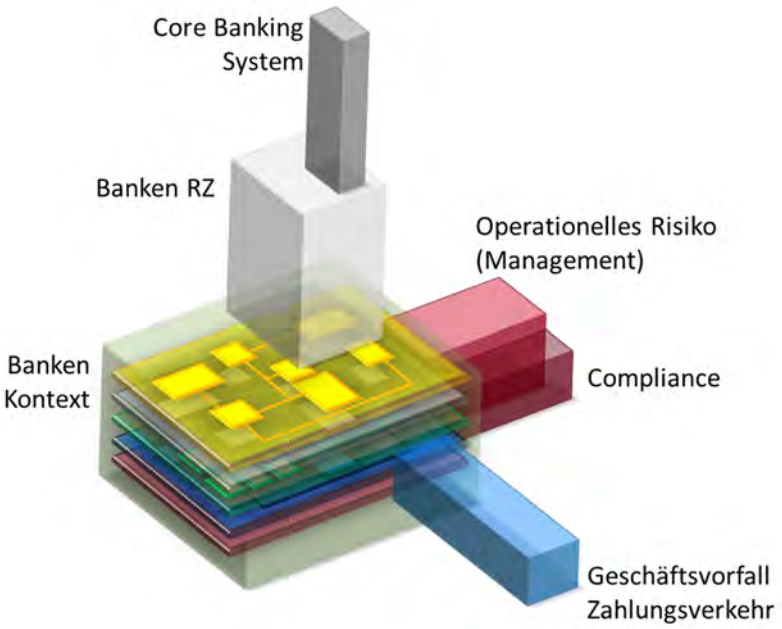

Abb. 1: Ebenen eines Finanzunternehmens

Tritt nun ein Vorfall auf einer der Ebenen auf, so darf dieser nicht isoliert auf dieser Ebene betrachtet werden. Vielmehr ist es wichtig, hier die Zusammenhänge zu erfassen. Denn um der

Managementebene ein aussagekräftiges Lagebild zur Verfügung zu stellen zu können, müssen die Risiken über alle Ebenen aggregiert werden.

Die folgende Abbildung 2 visualisiert daher den Zusammenhang zwischen den Ebenen und welche Auswirkungen ein Vorfall auf der Netzwerkebene auf die anderen Ebenen haben kann.

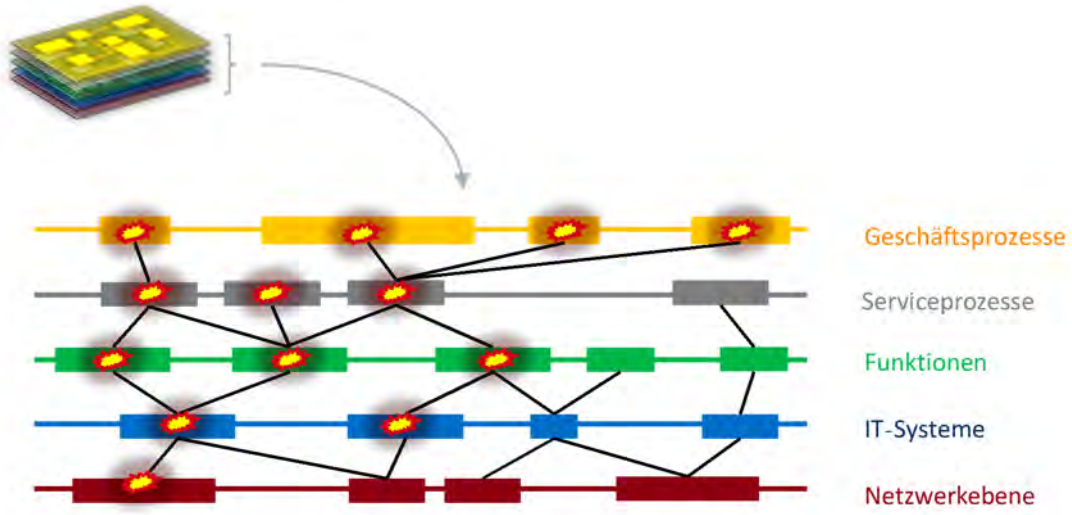

Abb. 2: Wechselwirkungen zwischen den Ebenen

3.3 Gemeinsames Lagebild zur Risikobeurteilung

Mit Hilfe der Managementlösung PREVENT sollen den Verantwortlichen fundierte Gründe für oder gegen eine Maßnahme zur Entscheidungsunterstützung an die Hand gegeben werden. Wirkungsketten sollen erkannt und potentielle Aggregationen von Risiken offengelegt werden.

Um dies umzusetzen, unterstützt die Managementlösung PREVENT bei

- der Modellierung von Businessprozessen,
- der Analyse von Betriebsprozessen und
- der Analyse der unterstützenden Infrastruktur auf Funktions-, Software und Netzwerk sowie Hardwareebene.

Dabei arbeitet PREVENT mit einer aus unterschiedlichen Quellen zusammengeführten Datenbasis. Die liefernden Quellen sind u.a: Log-Files, Zutrittskontrollsysteme oder eingesetzte SIEM-Systeme. Aus der sich ergebenden Datenbasis werden verschiedene Sichten bedarfsgerecht erzeugt. Als Herausforderungen sind hier die Big-Data-Analyse sowie das Erzeugen anwendungsgerechter Sichten zu meistern. Dadurch ist sichergestellt, dass jeder Nutzer die für sich nötige Sicht auf das Lagebild erhält.

So sollen Bedrohungspotentiale besser und schneller erkannt und im Lagebild abgebildet werden können, welches die Basis für proaktive Handlungsanweisungen geben kann.

Die folgende Abbildung 3 zeigt die implementierte Managementlösung PREVENT.

Ansatz zur Auswahl von Risikomanagement-Methoden

Martin Latzenhofer · Stefan Schauer
Sandra König · Christian Kollmitzer

Austrian Institute of Technology
{stefan.schauer | martin.latzenhofer
sandra.koenig | christian.kollmitzer}@ait.ac.at

Zusammenfassung

Es existiert eine Vielzahl an unterschiedlichen Risikomanagementframeworks. Bei einem ersten Kontakt mit den Publikationen ist es für den angehenden Risikomanager eine komplexe Aufgabe, das für die jeweilige Organisation in der aktuellen Situation und der individuellen Ziel- und Schwerpunktsetzung optimale Framework auszuwählen. Zudem kann diese Entscheidung nach dem Aufsetzen der Risikomanagementstrukturen in der Organisation nur unter sehr erschwerten Bedingungen revidiert und das Framework gewechselt werden, ohne hohe Sunk Costs zu generieren. Die European Network and Information Security Agency (ENISA) hat im Jahre 2006 eine Vergleichsmethodik entwickelt und die damals wichtigsten Risikomanagementframeworks anhand von 15 Kriterien verglichen. Die Grundidee des vorliegenden Artikels ist es, den Vergleich mit heutigen Frameworks nochmals durchzuführen, die Ergebnisse zu interpretieren und darüber hinaus zu diskutieren, ob die angelegten Bewertungskriterien heute noch zeitgemäß sind. Es werden Verbesserungsvorschläge dargestellt, welche die Potentiale der Frameworks für eine dezidierte Praxisanwendung insbesondere durch kleine und mittlere Unternehmen (KMU) besser sicht- und bewertbar machen. Hierbei wird argumentiert, dass die Schlüsselaspekte Detaillierungsgrad der Ausgestaltung, Organisationsgröße und -komplexität, Branchenrisiken, Risikomanagement-Knowhow und Ressourceneinsatz fokussierter in die Entscheidungskriterien einfließen sollten. Auch berücksichtigt der Methodenvergleich in der angewendeten Form weder Kaskadeneffekte, noch den Umgang mit inhärenter Unsicherheit oder die Anwendung neuerer Bewertungsmethoden.

1 Einleitung

Die Bedeutung von Risikomanagement als fundamentaler Ausgangspunkt für Entscheidungsfindung (Decision Making) ist seit dem letzten Jahrzehnt signifikant gestiegen. Einerseits wird Risikomanagement als probates Mittel gesehen, ex-ante auf eine Organisation oder ein System wirkende Gefahren, die sich in Kombination mit den Schwachstellen zu expliziten Bedrohungen gegen Werte in der Organisation auswachsen, vorab realistisch einzuschätzen und so den eigenen Ressourceneinsatz auf die Entwicklung, den Einsatz und die Überwachung von risikominimierenden Maßnahmen zu legen. Dabei achtet eine Organisation naturgemäß darauf, dieses möglichst effizient anhand ihrer ökonomischen Restriktionen wie Zeit, Geld oder Personalaufwand zu gestalten. Dies ist für den laufenden Betrieb wichtig, denn Risiken sind mannigfaltig, sehr vielschichtig und eben aufgrund der inhärenten Unsicherheit schwer fass- und einschätzbar.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 298-312.

Aufgrund dieser Problematik können Risiken vielfach nur qualitativ eingeschätzt werden, weil Aussagen über Häufigkeiten für eine seriöse quantitative Bewertung meist nicht in ausreichender Detailtiefe vorhanden sind. Auf der anderen Seite versucht man über Risikomanagement, insbesondere bei Compliance-Anforderungen, der vorhandenen Komplexität von Aufgaben in der Organisation zu begegnen und so die erforderlichen strukturgebenden Handlungsempfehlungen zu fokussieren. Zusammenfassend ist Risikomanagement für betriebswirtschaftlich operierende Organisationen ein Mittel zur Optimierung der eigenen Aktivitäten bei gleichzeitig angestrebter günstiger Ausrichtung des operativen Risikos.

Eine wesentliche Entscheidung für die Organisation bei der Einführung von Risikomanagementstrukturen betrifft die Wahl des zugrundeliegenden Risikoframeworks und damit des angewendeten Risikomodells. Bestehende Frameworks unterscheiden sich bei näherer Betrachtung signifikant hinsichtlich ihrer Struktur, der Detailtiefe, der Anwenderperspektive, inhaltlicher Schwerpunktsetzung und der Ausgestaltung. Dennoch können bei allen Ansätzen Gemeinsamkeiten in Herangehensweise, Begrifflichkeiten und Zielorientierung festgestellt werden. Somit stellt sich für den Risikomanager als auch den Prozess-Sponsor die Frage, wie man die Risikomanagementframeworks objektiv einem Vergleich unterziehen und bewerten kann, sodass man sich auf Basis der eigenen Rahmenbedingungen innerhalb der Organisation, der formulierten Zielsetzung und dem erforderlichen Detaillierungsgrad für das optimale – am besten für die jeweilige Situation passende – Risikomanagementframework entscheiden kann.

Die Europäische Agentur für Netz- und Informationssicherheit (European Network and Information Security Agency – ENISA) hat im Jahre 2006 im Rahmen eines Arbeitsprogramms über die Erhebung von Risikomanagement und Risikobewertungsmethoden einen Risikomanagementprozess [Tech08] definiert, der in nachfolgender Abbildung 1 dargestellt ist. Der Prozess identifiziert dabei sechs Phasen mit in Summe 15 Schritten und basiert auf verschiedenen internationalen Standards, Guidelines und Best Practices aus dieser Domäne oder anverwandten Gebieten, bei denen Risikomanagement die Grundlage bildet, wie beispielsweise Informationssicherheit. Zum Zeitpunkt der Definition des ENISA-Prozesses wurden die ISO/IEC 13335 [Inte04], ISO 17799 [Inte00], IT-Grundschutzkatalog [Bund13], NIST SP800-30 [StGF02] und OCTAVE [AlDo01a] als die relevantesten Frameworks angesehen. Obwohl diese mittlerweile alle überarbeitet, aktualisiert oder in anderen Rahmenwerken aufgegangen sind, haben die allgemeine Struktur und insbesondere diese 15 Schritte des ENISA-Prozesses weiterhin Gültigkeit.

Im Rahmen dieses Beitrages werden die von den Prozess-Schritten abgeleiteten Bewertungskriterien [Enis06] für einen Vergleich herangezogen und aktuelle Risikomanagementframeworks verglichen. Die sechs Phasen Bereichsbestimmung (Scoping), Risikobewertung (Risk Assessment), Risikobehandlung (Risk Treatment), Risikoakzeptanz (Risk Acceptance), Risikokommunikation, Risikosensibilisierung und Risikoberatung (Risk Communication and Risk Awareness Consulting) sowie Risikoüberwachung und Überprüfung (Risk Monitoring and Review) bilden den Rahmen für die 15 als Schritte bezeichneten Schlüsselaktivitäten. Diese werden nach einer vierstufigen Skala (von 0 bis 3) anhand ihres Detaillierungsgrades sowie deren jeweiliger Input und Output bewertet, der in einem abstrahierten Angleichungsprofil resultiert, das in weiterer Folge für die visuelle Darstellung und den Vergleich herangezogen wird.

Die im vorliegenden Beitrag analysierten Frameworks sind die ISO 31000 [Inte09], welche momentan den anerkannten allgemeinen Standard für Risikomanagement darstellt; ISO/IEC 27005 [Inte11], der mittlerweile mit sieben Jahren veraltet, aber in der Praxis weit verbreitet ist; NIST SP 800-30/-37/-39 [StGF02], [Nati10], [Nati11], der im US-amerikanischen Raum

wesentliche Bedeutung hat; COBIT for Risk [Info13] als speziell auf Risikomanagement ausgerichtete Variante des Governance-Frameworks; COSO ERM 2017 [CoPw17], die Aktualisierung des etablierten COSO-ERM-Frameworks sowie OCATVE Allegro [RJLW07] als praxisorientierter Prozess zur Implementierung von Risikomanagementstrukturen in Organisationen.

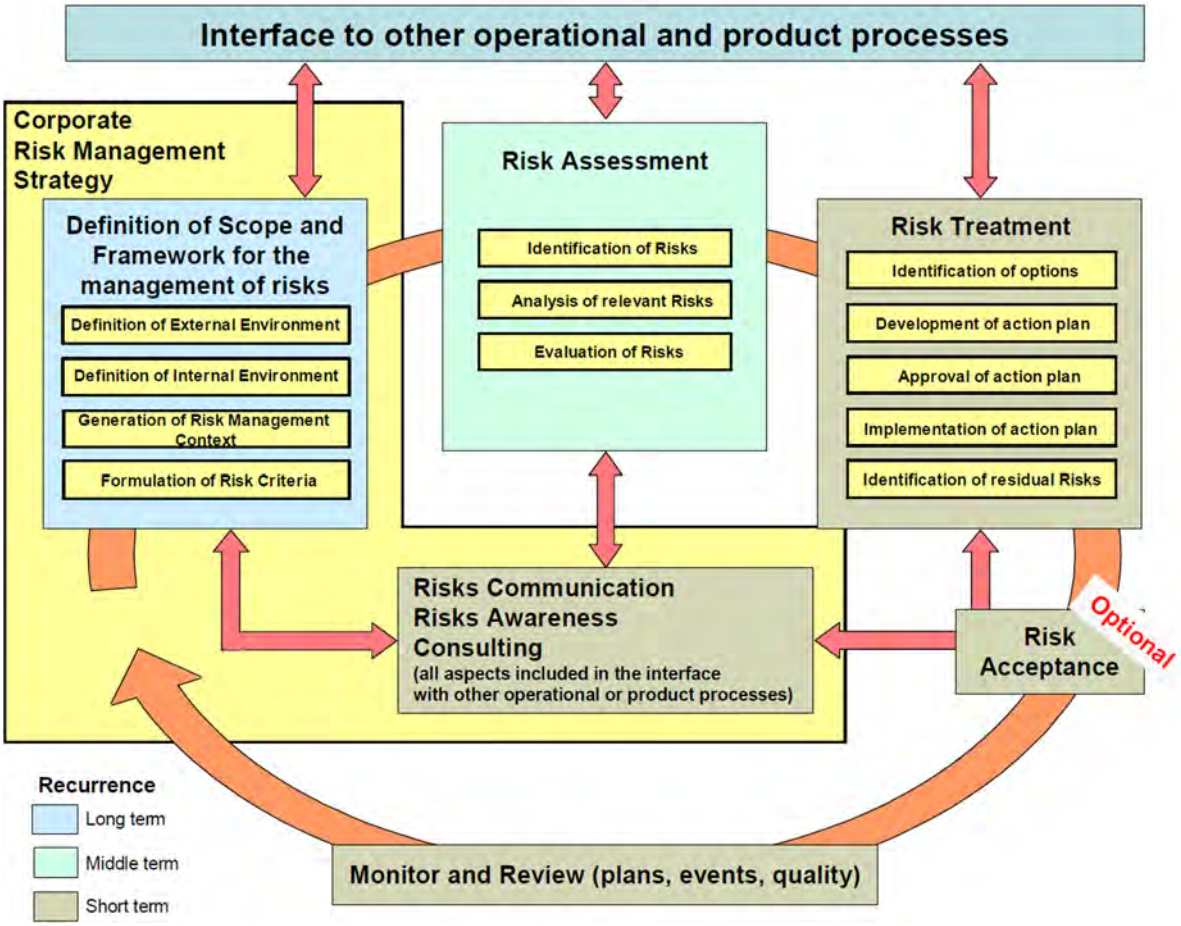

Abb. 1: ENISA Risikomanagementprozess [Tech08]

Nach der Durchführung der konkreten Bewertung der einzelnen Risikomanagementframeworks werden im Artikel die Einzelergebnisse im Gesamtvergleich kritisch betrachtet. Der Methodenvergleich zeigt, welche Frameworks in welchen Komponenten eine starke Akzentuierung aufweisen und so gute Unterstützung für die jeweilige Detailaufgabe bei der Einführung von Risikomanagementstrukturen in einer Organisation liefern können. Die Methodik wird anschließend kritisch gewürdigt und sinnvolle zukünftige Adaptierungen diskutiert.

2 Risikomanagementmethoden

In diesem Abschnitt werden die einzelnen Risikomanagementframeworks vorgestellt, welche für den Methodenvergleich betrachtet werden. Es folgt jeweils eine kurze Einführung zur Herkunft und Intention, eine rudimentäre Beschreibung der hinterlegten Prozessschritte sowie eine kurze Zusammenfassung der spezifischen Charakteristika. Für eine detailliertere Beschreibung sei hier auf die jeweiligen Referenzen aus der Literatur verwiesen.

Die Wirtschaft im Fokus von Cyber-Angriffen

Stefan Becker · Till Kleinert

Bundesamt für Sicherheit in der Informationstechnik
{stefan.becker | till.kleinert}@bsi.bund.de

Zusammenfassung

Während Cyber-Angriffe in den Anfangszeiten des Internets eher ein seltenes Phänomen waren, hat sich hieraus inzwischen eine hochprofessionelle Branche mit spezialisierten Dienstleistern im Darknet entwickelt. Täglich können neue Angriffe und Schadsoftware-Varianten beobachtet werden. Die zunehmende Vernetzung und Digitalisierung im Alltag eröffnet den Tätern gleichzeitig immer neue Möglichkeiten für Angriffe. Unternehmen sollten daher adäquate Schutzmaßnahmen implementieren und vorgefertigte Notfallpläne bereithalten. Der hier beschriebene Vortrag dient zur Einführung des Workshops „Incident Response - Korrektes Verhalten im Ernstfall“, in dem eine effiziente Bearbeitung von IT-Sicherheitsvorfällen im Unternehmen diskutiert werden soll.

1 Bedrohungslage

Im Jahr 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) pro Monat durchschnittlich fast 52.000 E-Mails abgefangen, die an Empfänger in der Bundesverwaltung gerichtet waren und im Anhang Schadsoftware mit sich bringen sollten. Dies geht aus dem Bericht „zur Lage der IT-Sicherheit in Deutschland 2017“ hervor, den das BSI jährlich veröffentlicht. Bei der Statistik der schadhaften E-Mails, die immer noch als häufigster Angriffsvektor für Attacken auf die Regierungsnetze verwendet werden, ist dabei eine Zunahme von 18% im Vergleich zum Vorjahr zu verzeichnen. Diese Steigerung geht insbesondere auf die zahlreichen Ransomware-Wellen – z.B. mit Locky oder Wannacry – zurück, die in den Vormonaten von sich reden machten und auch in Unternehmen und Privathaushalten für Probleme sorgten.

Auch andere Institutionen beschäftigen sich regelmäßig mit Straftaten im Cyber-Raum und können von ähnlichen Entwicklungen berichten. So stellt das Bundeskriminalamt im Lagebild Cybercrime von 2016 ein Zuwachs auf 253.290 Fälle „mit dem Tatmittel Internet“ fest. Das Bundesamt für Verfassungsschutz und der Digitalverband Bitkom kamen in einer gemeinsamen Studie zu dem Ergebnis, dass der deutschen Wirtschaft durch Cyber-Angriffe jährlich ein Schaden in Höhe von 55 Milliarden Euro entsteht.

Alle Quellen gehen von einer unverändert hohen Bedrohungslage aus. Organisationen aller Branchen und Größen sollten sich daher der ständigen Gefahr bewusst sein.

2 Aktuelle Vorfälle

Im Folgenden finden Sie eine Übersicht verschiedener IT-Sicherheitsvorfälle, mit denen sich das Bundesamt für Sicherheit in der Informationstechnik in den vergangenen Monaten befasst

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 323-328.

hat. Die Auswahl ist nur exemplarisch. Nahezu täglich können neue Incidents in den gängigen Fachmedien gefunden werden.

2.1 Schwachstellen in Content-Management-Systemen

Sachverhalt: Im April 2017 kam es zu einem Vorfall in einem Unternehmen, bei dem Angreifer durch Ausnutzung einer Sicherheitslücke in einer veralteten Plug-in-Version für ein Content-Management-System (CMS) unberechtigten Zugriff auf den Webserver erlangten, auf dem das CMS installiert war. Durch Verwendung einer sogenannten Reverse-Shell konnten die Angreifer anschließend auch auf die Daten eines weiteren auf diesem Server installierten CMS zugreifen und diese löschen. Weiterhin erhielten die Täter auf diesem Wege Zugriff auf einen Backup-Server und löschten ebenfalls die dort gespeicherten Datensicherungen der Content-Management-Systeme. Ende Januar 2017 hatte der Hersteller ein Update für das CMS veröffentlicht, das eine kritische Sicherheitslücke schloss. Bereits in den ersten Tagen nach Veröffentlichung des Updates nutzten Angreifer diese Sicherheitslücke bei noch nicht aktualisierten CMS-Installationen aus, um zehntausende Websites zu manipulieren.

Ursache und Schadenswirkung: CMS bieten komfortable Möglichkeiten, Websites zu erstellen und zu pflegen. Wie andere Software sind sie aber nicht frei von Fehlern und müssen regelmäßig gepflegt werden. Viele Betreiber handeln hierbei jedoch sehr nachlässig und spielen Updates, welche unter anderem Sicherheitslücken schließen, nicht oder erst mit langer Verzögerung ein. Nach einer Analyse von BleepingComputer waren im dritten Quartal 2016 über 60 Prozent der untersuchten Installationen des populären CMS „WordPress“ nicht auf dem aktuellen Stand, bei „Joomla“ sogar über 80 Prozent. Neben dem CMS selbst müssen auch installierte Plug-ins auf dem akuellen Stand gehalten werden. Auch dies wird von CMS-Betreibern häufig vernachlässigt und kann daher von Angreifern als Einfallstor für Kompromittierungen ausgenutzt werden. Die kompromittierten Websites werden dann unter anderem zur Verbreitung von Schadprogrammen, zur Manipulation der Ergebnisse von Suchmaschinen (BlackHat-SEO) oder zum Spam-Versand missbraucht. Auch sogenannte „Defacements“ zur Verbreitung politischer Botschaften finden regelmäßig statt.

Reaktion: CMS sind in der Regel aus dem Internet erreichbar und stehen daher oft im Fokus von Angreifern. Cyber-Kriminelle nutzen täglich bekannte Sicherheitslücken in veralteten Versionen gängiger CMS aus, um in großem Umfang damit verbundene Websites (automatisiert) zu kompromittieren. Im vorliegenden Fall wurde das nicht gepflegte CMS nur als Einfallstor für den Angriff auf das eigentliche Ziel ausgenutzt. Das primäre CMS war auf dem aktuellen Patch-Stand und durch ein sicheres Passwort geschützt.

Empfehlung: Der Vorfall verdeutlicht noch einmal, dass auf einem aus dem Internet erreichbaren Server installierte Software – auch ältere und gegebenenfalls nicht mehr genutzte – regelmäßig aktualisiert werden muss. Wesentlich ist hier, dass nicht nur das Basis-CMS aktualisiert weden muss, sondern auch alle installierten Plug-Ins, die häufig über keine automatischen Update-Funktionen verfügen.

2.2 DDoS-Angriff auf KrebsOnSecurity

Sachverhalt: Am 19. September 2016 meldete Octave Klaba vom französischen Webhoster OVH über Twitter zwei DDoS-Angriffe mit den extrem hohen Bandbreiten von 1.156 und 622

Gigabit pro Sekunde. Das Volumen der Angriffe übertraf die bisher größten verzeichneten Angriffe des DDoS-Mitigation-Dienstleisters Akamai um ein Vielfaches. Am Abend des folgenden Tages wurde das Weblog https://krebsonsecurity.com des Sicherheitsforschers Brian Krebs von einer massiven DDoS-Attacke mit etwa 620 Gigabit pro Sekunde getroffen. Brian Krebs hatte im Vorfeld der Angriffe kritisch über Anbieter von sogenannten Booter-Diensten berichtet, die kostenpflichtige DDoS-Attacken auf beliebige Ziele offerieren.

Ursache und Schadenswirkung: Neben der Größe waren auch die Angriffsmethoden auffällig. So wurde eine Kombination verschiedener Angriffsarten registriert, die bei DDoS-Angriffen in dieser Form bislang nicht vorkam. Aus technischer Sicht handelt es sich bei diesem Vorfall um das erste öffentliche Auftreten des Mirai-Botnetzes. Dieses Botnetz setzt sich überwiegend aus IoT-Geräten zusammen. Neben der schieren Größe des Botnetzes von mehreren hunderttausend Bots überraschte hier auch die technische Umsetzung. So ist Mirai in der Lage, sich selbstständig weiter zu verbreiten, indem bereits infizierte Systeme nach weiteren verwundbaren Geräten suchen und diese dann, wenn möglich, kompromittieren. Dabei wird eine Liste von Standard-Kennungen und -Kennwörtern verwendet, die bei Auslieferung der Geräte gesetzt sind. Systeme, bei denen die Kennwörter nach Auslieferung nicht geändert werden, können so schnell mit Mirai infiziert werden. Daneben gibt es weitere Mirai-Varianten, die Schwachstellen in Implementierungen, beispielsweise bei Routern, ausnutzen. Erfolgreich übernommene Systeme werden in das Botnetz eingegliedert und deaktivieren den Dienst, über den das Gerät kompromittiert wurde. Die Bot-Software selbst bietet neue DDoS-Angriffsmethoden wie GRE Flood oder DNS Water Torture, die durch eine effiziente Implementierung auch auf wenig leistungsfähigen Geräten eine hohe Paketrate erreichen.

Reaktion: Akamai gelang es nach einer Ausfallphase von wenigen Stunden, den Angriff abzuwehren. Da Akamai diese Dienstleistung jedoch im Rahmen eines kostenlosen, freiwilligen Angebots erbrachte, wurde sie aufgrund der anhaltenden Intensität und Dauer der Angriffe sowie der damit verbundenen Kostenaufwände zur Abwehr nicht dauerhaft zur Verfügung gestellt. Google hat sich daraufhin bereit erklärt, Krebs‘ Blog unter den kostenfreien Schutz von Google Project Shield zu stellen. Es ist seit diesem Zeitpunkt wieder dauerhaft verfügbar.

Empfehlung: Aufgrund der freien Verfügbarkeit des Quellcodes sowie der geringen technischen Hürde zum Aufbau eines eigenen Mirai-Botnetzes stellt Mirai eine massive Bedrohung dar. Die Implementierung funktionierender Angriffsmethoden ermöglicht vergleichsweise effiziente Angriffe mit bereits wenigen Tausend Bots. Erschwerend kommt hinzu, dass weltweit eine sehr hohe Zahl an technisch unzureichend gesicherten Systemen existiert, die über das Internet erreichbar und für die Ausnutzung bei solchen Angriffen anfällig sind. Hier besteht dringender Handlungsbedarf bei Herstellern und Anwendern dieser Systeme, um diese abzusichern. Nach Erkenntnissen des BSI finden dauerhaft Scan-Versuche durch Mirai-Systeme statt und ein verwundbares Gerät wird in weniger als einer Minute erfolgreich infiziert. In Deutschland befindet sich ein Großteil der Internetanschlüsse von Privatkunden hinter Routern. Wichtig ist daher, den Router, das Bindeglied zwischen Internet und Heimnetz, so zu konfigurieren, dass ein Durchgriff auf im Heimnetz befindliche vernetzte Geräte nicht möglich ist beziehungsweise dass die vernetzten Geräte keine direkte Freigabe zur Kommunikation über das Internet erhalten.

Kontextsensitive CAPTCHAS im Online-Banking

Tobias Urban[1] · René Riedel[1]
Ulrike Schmuntzsch[2] · Norbert Pohlmann[1]

[1]Institut für Internet-Sicherheit – if(is) Westfälische Hochschule
{urban | riedel | pohlmann}@internet-sicherheit.de

[2]Institut für Psychologie und Arbeitswissenschaft
Technische Universität Berlin
ulrike.schmuntzsch@mms.tu-berlin.de

Zusammenfassung

In der modernen Informationsgesellschaft nehmen Online-Transaktionen einen wichtigen Teil unseres täglichen Lebens ein. In dieser Arbeit stellen wir ein nutzerzentriertes Protokoll vor, dass es Nutzern erlaubt vertrauenswürdige und sichere Transkationen durchzuführen, selbst wenn sie ein nicht vertrauenswürdiges oder mit Schadsoftware infiziertes Gerät nutzen. Das Protokoll nutzt einen CAPTCHA-artigen Ansatz, der verhindert, dass ein Angreifer eine Transaktion verändert ohne, dass Server oder Client dies bemerken. Dazu stellen wir dem Nutzer eine Aufgabe, die kontextsensitive Informationen der Transaktion enthält. Die Aufgabe wird so gestellt, dass sie einfach von Menschen lösbar ist aber nur schwer automatisiert gelöst werden kann. Zur Evaluation des Systems haben wir eine Nutzerstudie ($n = 30$) durchgeführt und berechnet mit welcher Wahrscheinlichkeit ein Angreifer erfolgreich die richtige Antwort auf die Frage erraten kann. Wir zeigen, dass ein Großteil der Transaktionen ($> 94\%$) geschützt werden kann, während das System selbst nutzbar bleibt.

1 Einführung

Online-Banking und Online-Transaktionen sind ein bedeutender Teil der modernen Informationsgesellschaft und gewinnen stetig an Bedeutung. Allein zwischen 2007 und 2017 verdoppelte sich die Nutzung von 25 % auf 51% in Europa [1]. Dieses Wachstum, das Aufkommen von immer mehr Applikationen, die sich über Micro-Transaktionen finanzieren wird dazu führen, dass wir in Zukunft immer mehr Online-Transaktionen durchführen werden.

Betrüger haben den Bereich bereits auf unterschiedlichsten Wegen kompromittiert [2]. Laut offiziellen Angaben des Deutschen Bundeskriminalamts belief sich in Deutschland der finanzielle Schaden im Online-Banking zwischen 2014 und 2016 auf über 54 Millionen Euro [3].

Erfolgreiche Angriffe auf das Online-Banking werden durch sogenannte *Man-in-the-Browser* (MitB) Angriffe ermöglicht [4]. Bei diesem Angriffsvektor übernimmt die Angreiferin die vollständige Kontrolle über den Browser des Nutzers (z.B. durch bösartige Browser-Erweiterungen).

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 346-359.

Somit erlangt sie volle Kontrolle über z.B. die übertragenden Daten oder die Darstellung der Website auf dem Endgerät des Nutzers. In Bezug auf Online-Banking könnte die Angreiferin zum Beispiel den Zahlungsempfänger, der an den Server gesendet wird, einer Transaktion manipulieren dem Nutzer aber trotzdem noch den von ihm eingegebenen Empfänger anzeigen. Typischerweise wird als Verteidigungsstrategie gegen diesen Angriffsvektor ein zweiter Kanal verwendet, über den die Daten, welche die Bank erhalten hat, verifiziert werden können (z.B. das Smart Phone des Nutzers). Dementsprechend muss die Angreiferin auch den zweiten Kanal übernehmen, um das System erfolgreich anzugreifen.

In dieser Arbeit stellen wir ein Protokoll vor, dass Transkationen absichert, selbst wenn das Gerät des Nutzers mit Schadsoftware infiziert oder nicht vertrauenswürdig ist (z.B. ein Gerät in einem Internet-Café). Dabei wird kein weiterer Kanal als vertrauenswürdige Anzeige benötigt. Das Protokoll stellt mit hoher Wahrscheinlichkeit sicher, dass eine manipulierte Transaktion von dem Server oder Nutzer erkannt werden kann. Dazu wird das Prinzip von sog. CAPTCHAs *(„Completely Automated Public Turing Test To Tell Computers and Humans Apart”)* [5] auf das gegebene Problem angewendet (siehe Kapitel 3).

Wir adaptieren dieses Prinzip verwenden aber kontextsensitive Information aus der Transaktion, um diese abzusichern. Der Nutzer muss eine automatisch generierte Frage zu der Transaktion, die er durchführen möchte, beantworten. Bei der Manipulation einer Transaktion würden sich so zwei Szenarien ergeben: (1) Wenn die Angreiferin die Darstellung auf dem Client ändert passt die Antwort auf die Frage nicht zu der manipulierten Transaktion; oder (2) Wenn die Darstellung nicht geändert wird erkennt der Nutzer, dass die Transaktionsdaten geändert wurden. Die Angreiferin wird natürlich versuchen, die Antwort auf die Frage zu erraten. Dieser und weitere Angriffe auf das System werden in Kapitel 4 beschrieben. Die Auswirkungen der Angriffe auf das Protokoll werden in Kapitel 6 analysiert. Ein wichtiger Teil der IT-Sicherheit ist die Nutzbarkeit entwickelter Lösungen und ob diese von Nutzern akzeptiert werden. Daher haben wir eine Nutzerstudie ($n = 30$) für das entwickelte Protokoll durchgeführt, um dessen Nutzbarkeit zu überprüfen (siehe Kapitel 7).

Zusammengefasst liefert diese Arbeit die folgenden Beiträge:

- Wir adaptieren den CAPTCHA Mechanismus und wenden ihn im Online-Banking an.
- Wir stellen ein Protokoll vor, dass es erlaubt sichere Transkationen durchzuführen, selbst wenn dem Endgerät nicht vertraut werden kann oder mit Schadsoftware infiziert wurde.
- Wir analysieren das vorgestellte Protokoll in einer Nutzbarkeitsstudie.

2 Grundlagen

Wenn man sichere Online-Transaktionen durchführen will lassen sich die meisten auftretenden Probleme in drei Kategorien einteilen. Dies sind einerseits technische Probleme, die von Angreiferinnen ausgenutzt werden können und andererseits Limitierungen, die sich aus der Spannung zwischen Nutzbarkeit und Sicherheit ergeben.

1. **Gestohlene Anmeldedaten:** Wenn die Angreiferin die Kontrolle über das Konto des Nutzers erlangen will muss sie die Anmeldedaten des Nutzers stehlen. Heutzutage nutzen fast alle Web-Applikationen Nutzername und Passwort für die Authentifizierung. Daher muss die Angreiferin genau diese Informationen stehlen, um Zugang zu erhalten.

2. **Manipulation von Transaktionen:** Das Hauptproblem, bei der Durchführung der Autorisierung von Transaktionen ist, dass das verwendete Endgerät mit spezialisierter Schadsoftware infiziert wird, die der Angreiferin clientseitig volle Kontrolle über die Online-Banking Umgebung gibt (z.B. Ändern von Kontoständen oder Transaktionsempfängern) [4]. Dies wird von Angreifern genutzt, um komplexe *Social-Engineering* Angriffe durchzuführen, um beispielsweise private Daten zu stehlen (z.B. Handynummern) [6]. Daten, die an den Server gesendet werden, können von der Angreiferin geändert werden, ohne dass der Nutzer die Änderung bemerkt, was dazu führt, dass weder Client noch Server prüfen können, ob die übertragenden Daten verändert wurden. Auch eine TLS gesicherte Verbindung löst dieses Problem nicht, da die Manipulation vor bzw. nach dem Verschlüsseln durchgeführt werden.
3. **Vertrauenswürdige Anzeige:** Aus dem beschriebenen Problem ergeben sich zahlreiche weitere Problemstellungen. Eine Lösung ist die Nutzung eines unabhängigen Kommunikationskanals als „vertrauenswürdige Anzeige“ (z.B. ein Smart Phone oder externe TAN-Generatoren), um zu prüfen ob die Daten, die der Server erhalten hat tatsächlich die eingegebenen Daten sind. Der Vorteil von externen Geräten ist, dass diese praktisch nicht mit Schadsoftware infiziert werden können. Da zur Autorisierung von Transkationen ein spezielles Gerät benötigt wird, werden diese meist nur zuhause genutzt. Daher bevorzugen Nutzer das Smart Phone als zweiten Kanal [7], welches allerdings einfacher anzugreifen ist und bereits häufig erfolgreich angegriffen wurde [2].

3 Konzept

Das in dieser Arbeit vorgestellte Protokoll nutz neben einer digitalen Identität keine weitere Software oder Hardware Entitäten und könnte somit auf beliebigen Geräten genutzt werden, die über einen Web-Browser verfügen. Dies umfasst auch Geräte, die mit Schadsoftware infiziert sind oder Geräten denen nicht vollständig vertraut wird. Von nun an nutzen wir Online-Banking Überweisungen als Beispiel für Online-Transaktionen und beschreiben unseren Ansatz anhand dieses Beispiels. Im Allgemeinen lässt sich unser Ansatz aber auf alle Online-Transkationen anwenden (z.B. Einkaufen in einem Online-Shop).

3.1 Nutzung digitaler Identitäten

In dem Protokoll wird eine digitale Identität zur Authentifikation (2-Faktor-Authentifikation) und Autorisierung der Transaktion (digitale Signatur) genutzt. Die Transaktion wird digital signiert, um sie kryptografisch zu sichern und zu autorisieren. Wir können nicht davon ausgehen, dass die digitale Identität über eine geeignete Anzeige verfügt, um die Transaktionsdaten zu sichern. Daher stellen wir in dieser Arbeit den Ansatz kontextsensitiver CAPTCHAs vor, die diese Aufgabe übernehmen. Da eine physische Interaktion mit der digitalen Identität nötig ist, kann eine potentielle Angreiferin nicht unbemerkt eigene Transaktionen durchführen - und die CAPTCHAs lösen - nachdem sich ein Nutzer eingeloggt hat. Beispiele für solche digitalen Identitäten sind elektronische Personalausweise oder das YubiKey Token [8].

3.2 Adaption des CAPTCHA Prinzips

Wie bereits mehrfach erwähnt, kann der Nutzer der Anzeige seines Geräts nicht vertrauen. Zur Lösung dieser Herausforderung adaptieren wird das CAPTCHA Prinzip, um eine Transkation zu autorisieren.

Risikobasierte und adaptive Authentifizierung

René Riedel · Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
{riedel | pohlmann}@internet-sicherheit.de

Zusammenfassung

Die aktuellen Verfahren zur Authentifikation im Internet überfordern die digitale Gesellschaft zunehmend. Für immer mehr Dienste muss ein separater Registrierungs- oder Identifikationsprozess durchgeführt werden. Die Praxis zeigt: Sichere Passwörter sind für viele verschiedene Dienste inpraktikabel und hardwarebasierte digitale Identitäten schaffen aufgrund der fehlenden Akzeptanz bisher nur geringfügig Abhilfe. Ein vielversprechender Lösungsansatz für diese Problematik ist die Zentralisierung der Authentifikation durch sogenannte „Identity Provider". Große Unternehmen wie Google, Facebook oder Amazon bieten schon seit längerer Zeit die übergreifende Nutzung der bereits erstellten Konten für die Authentifizierung bei externen Diensten an. Der Vorteil bei diesem Konzept ist, dass potentiell nur noch wenige Identitäten im Internet benötigt werden und somit die Authentifizierung sowohl clientseitig, als auch serverseitig, effektiver gestaltet werden kann. Die bestehenden Konzepte weisen jedoch Probleme hinsichtlich der Skalierbarkeit auf, denn die konkreten Verfahren für die Authentifizierung können in der Regel nicht an den Bedarfsfall gebunden werden. Dieser Artikel knüpft an die fehlende Berücksichtigung der Skalierbarkeit an. Es wird ein High-Level Design eines skalierenden „Identity Providers" vorgestellt, der basierend auf einem berechneten Risikowert eine adaptive Auswahl der verwendeten Verfahren für die Authentifizierung ermöglichen soll. Die technologische Grundlage hierfür bildet ein vierter Faktor, der unteranderem aus „Device Fingerprints", Verhaltensmustern, Netzwerkkennzahlen und Sensordaten besteht.

1 Einführung

Die aktuell gängigsten Verfahren zur *Authentifikation* im Internet sind entweder unsicher oder sicher aber (sehr) komplex in der Handhabung. Als Beispiele hierfür kann die Authentifizierung mittels Passwort als unsicheres oder digitale Identitäten in Verbindung mit einem kostspieligen Kartenlesegerät als aufwändiges Verfahren betrachtet werden. Grundsätzlich bieten die bestehenden Verfahren nur eine grobe Unterscheidung von verschiedenen Sicherheitsniveaus: Für IT-Integratoren entsteht daraus das Problem, dass sie eine „Entweder-oder-Entscheidung" treffen müssen und somit die Verwendung eines bestimmten *Authentifikation*sverfahrens nicht an den Sinn und Zweck einer Anwendung binden können.

Dieser Artikel befasst sich deshalb mit neuen und handhabbaren Methoden zur *Authentifikation* im Internet, bei denen die Art der *Authentifikation* adaptiv an die durchzuführende Aufgabe angepasst wird. Ziel ist es also eine feinere Unterscheidung zwischen verschiedenen Sicherheitsniveaus und Anwendungshintergründen zu schaffen, um die Nutzbarkeit solcher Dienste zu verbessern.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 360-371.

Hierfür können beispielsweise bestehende Verfahren in Abhängigkeit von dem benötigten Sicherheitsniveau kombiniert werden, um somit Synergien zu erzielen. Als Ergebnis werden neue *Authentifikation*sverfahren geschaffen und die bestehenden Verfahren gestärkt. Neben den Funktionalitäten der bestehenden Verfahren, werden weitere Parameter für die Durchführung der Authentifizierung herangezogen. Hierbei kann es sich um Verkehrsdaten auf Netzwerkebene, Informationen über die Hard -und Software eines Informationssystems oder Profile über das Verhalten eines Nutzers handeln. Die gesammelten Informationen können für die Bewertung des Sicherheitsniveaus und des Restrisikos verwendet werden.

Damit aus der Kombination der bestehenden *Authentifikation*sverfahren keine weiteren unannehmbaren Komplexitäten entstehen, beschreibt dieser Artikel einen sogenannten *„Auth-Service“*, der in Form eines *„Identity Providers“* die benötigten Funktionalitäten für verschiedene Anwender zur Verfügung stellt.

Die Verwendung des *„Auth-Services“* erfolgt über eine einfache Schnittstelle, die in Form von sogenannten *„Service-Klassen“* realisiert wird: Ein Anwender könnte somit anhand der bereitgestellten *„Service-Klassen“* entscheiden, welches Sicherheitsniveau für seinen konkreten Anwendungshintergrund relevant ist. Eine Bank könnte in diesem Zusammenhang beim *„Auth-Service“* eine stärkere Authentifizierung für die Durchführung einer Transaktion anfordern, als der Betreiber eines Blogs für die Anmeldung auf einer Internetseite.

Basierend auf der ausgewählten Service-Klasse wird vom *„Auth-Service“* entschieden, welche zusätzlichen Parameter für die Authentifizierung herangezogen und welche Kombinationen der bestehenden Authentifikationsverfahren verwendet werden müssen.

Aus diesem Beispiel geht exemplarisch hervor, dass der Vorteil einer risikobasierten und adaptiven Authentifizierung Auswirkungen auf verschiedene Anwendergruppen hat. Für den Endanwender erleichtert sich in erster Linie die Durchführung einer *Authentifikation*. Darüber hinaus wird durch die Verwendung von weiteren Parametern im Hintergrund der Authentifizierung die Sicherheit des Endanwenders erhöht.

Für den IT-Integrator entsteht der Vorteil, dass er keine „Entweder-oder-Entscheidungen“ bei der Auswahl der benötigten Authentifikationsverfahren treffen muss, sondern vielmehr auf ein breites Spektrum an verschiedenen Schutzniveaus zugreifen kann. Ihm wird somit durch den *„Auth-Service*“ und der damit verbundenen adaptiven Authentifizierung ein flexibles und interoperables Werkzeug für einen zentralen Bestandteil von IT-Systemen zur Verfügung gestellt.

Im weiteren Verlauf dieser Arbeit werden die folgenden Ergebnisse vorgestellt:

- Es wird eine Definition der Begriffe „adaptiv“ und „risikobasiert“ vorgenommen
- Basierend auf den technischen und rechtlichen Rahmenbedingungen wird das tatsächliche Potential der risikobasierten und adaptiven Authentifizierung identifiziert
- Kritische Protokollabläufe des „Identity Lifecycle Managements“ werden im Kontext dieser Arbeit analysiert
- Es wird ein High-Level Design eines risikobasierten und adaptiven „Identity Providers“ als mögliches Referenzsystem vorgestellt

2 Begriffsbestimmung

Für den weiteren Verlauf dieses Artikels gelten die nachfolgenden Definitionen für die aufgelisteten Begriffe:

- **ID-Verifikation:** Dem Anwendungsfall entsprechende Überprüfung der angegebenen Eigenschaften einer Identität und Verbindung der überprüften Eigenschaften mit einem digitalen Merkmal im Rahmen der erstmaligen Registrierung einer digitalen Identität.
- **Authentifikation:** Erbringen eines Nachweises zu der Übereinstimmung von behaupteter und tatsächlicher Identität.
- **Adaptiv:** Eine Authentifizierung ist adaptiv, falls die Auswahl der benötigten Verfahren zur *ID-Verifikation* und *Authentifikation* nicht pauschal im Vorfeld für eine bestimmte Menge an Anwendungsfällen festgelegt wird, sondern auf Basis von Eingabeparametern E dynamisch zur Laufzeit für eine unbestimmte Menge ermittelt wird.
- **Risikobasiert:** Eine Authentifizierung ist risikobasiert, falls das gelernte Verhalten einer Person X mit den Eingabeparametern eines zukünftigen Request R abgeglichen wird und die Wahrscheinlichkeit $\mathrm{P(A)}\ mit\ A \coloneqq X\ hat\ R\ erstellt$ als Maß für die Authentizität von R verwendet wird.
- **Risikobasiert ∘ Adaptiv:** Die risikobasierte und adaptive Authentifizierung verwendet die Wahrscheinlichkeit P als Eingabeparameter E für die dynamische Ermittlung der benötigten Verfahren zur *ID-Verifikation* und *Authentifikation*. Die Sicherheitsanforderungen an die auszuwählenden Verfahren sind proportional zur Gegenwahrscheinlich von P, also $P(\bar{A})\ mit\ \bar{A} = X\ hat\ R\ nicht\ erstellt$.

3 Abgrenzung zu bestehenden Technologien

Die konkreten Anwendungsszenarien eines risikobasierten und adaptiven „Identity Providers“ und der damit verbundene Mehrwert im Vergleich zu den bestehenden Anbietern hängt sowohl von technischen, als auch von rechtlichen Rahmenbedingungen ab. Diese Abhängigkeiten werden in den nachfolgenden Unterkapiteln genauer beschrieben. Im Vergleich zu den verwandten Arbeiten wird das Potential der risikobasierten und adaptiven Authentifizierung genauer dargestellt.

3.1 Technische Rahmenbedingungen

Zu den technischen Rahmenbedingungen gehören die verschiedenen Faktoren, die bei der Bestätigung einer Identität grundsätzlich zum Einsatz kommen können. Eine Liste der verschiedenen Faktoren und konkrete Beispiele sind in Tabelle 1 aufgeführt (vgl. mit [1]). Im Internet werden aktuell die drei Faktoren: *Wissen*, *Besitz* und *Inhärenz* (einzeln oder in Kombination) verwendet. Die Kombination von zwei oder mehr Faktoren wird in diesem Kontext als *„Multi-Faktor-Authentifizierung“* (MFA) bezeichnet und bereits von den meisten *„Service Providern“* im Internet als zusätzliche Sicherheitsmaßnahme angeboten. Die Aktivierung der zusätzlichen Sicherheitsmaßnahme hat aktuell zur Folge, dass der Nutzer pauschal bei jeder Anfrage oder Transaktion die zusätzlichen Faktoren aktiv bestätigen muss. Aus Gründen der Effizienz (z.B. hohe Anschaffungskosten für externe Lesegeräte oder eine geringe Nutzbarkeit) hat sich im Internet der Spezialfall der MFA mit lediglich zwei Faktoren – die *„Zwei-Faktor-Authentifizierung“* (2FA) - durchgesetzt.

ML-gestützte Authentifizierung mit QR Code und Smartphone

Markus Hertlein

XignSys GmbH
hertlein@xignsys.com

Zusammenfassung

Die Welt wird immer digitaler und vernetzter. Dies führt zu einem massiven Angebot an digitalen Diensten für Privatpersonen und Unternehmen. Alle diese digitalen Dienste beherbergen eine Fülle an sensiblen persönlichen Informationen und Unternehmensdaten. Das hat zur Folge, dass heute jede Person eine Vielzahl von digitalen Identitäten besitzt, mit der sie sich im Internet bewegt. Der Schutz und die Verwendung der digitalen Identität, der Daten und Dienste liegt einer vorherigen Authentifizierung zu Grunde. Hier besteht die Notwendigkeit nach einer digitalen Identitylösung, die ein hohen Schutzbedarf liefert, zeitgleich aber flexibel für mehrere Use Cases geeignet ist und für den Endnutzer einfach zu verwenden ist. Ein QR Code basiertes Identity und Authentifikationssystems, das als Nutzerschnittstelle das Smartphone verwendet, erfüllt diese Anforderung [HeMP17] [CHCP18]. Durch die Erweiterung des Systems, um die Authentifizierung durch Nutzerverhaltensanalyse per Smartphone-Sensoren, mit maschineller Lerneinheit, wird sowohl die Sicherheit als auch die Benutzerfreundlichkeit gesteigert. Dazu wird in der vorliegenden Arbeit ein möglicher Ansatz zur Umsetzung beschrieben und bewertet.

1 Einleitung

Die Welt wird immer digitaler und vernetzter. Dies führt zu einem massiven Angebot an digitalen Diensten für Privatpersonen und Unternehmen. All die digitalen Dienste beherbergen eine Fülle an sensiblen persönlichen Informationen und Unternehmensdaten. Das hat zur Folge, dass heute jede Person eine Vielzahl von digitalen Identitäten besitzt, mit der sie sich im Internet bewegt. Digitale Identitäten sind für die Datendiebe interessant, da sie sensible Informationen beinhalten, die missbraucht werden können, um Betrug, strafbare Geschäfte, illegale Transaktionen etc. durchzuführen [Do18]. Dabei kann eine digitale Identität sowohl privat als auch geschäftlich sein. Um die Nutzung digitaler Identitäten und die damit verbundenen Daten vor unbefugten Zugriffen zu schützen, wird eine Authentifizierung durch den Eigentümer benötigt. Dabei ist die Nutzung von unsicheren Passwörtern immer noch die am häufigsten verwendete Form der Authentifizierung. Laut einer Umfrage auf Statista aus dem Jahr 2014 besitzen die Menschen mehrere Online-Passwörter. Doch bei Identitätsdiebstählen wurden in den letzten fünf Jahre mehr als 5 Milliarden digitale Identitäten und Passwörter gestohlen [Hert17]. Dabei sind nicht nur kleine und mittelständische Firmen von Angriffen betroffen, sondern auch Internet-Unternehmen mit mehr als drei Milliarden Nutzern. Sowohl der Umstand der Benutzerunfreundlichkeit, als auch die Unsicherheit bei der Verwendung aktueller Authentifizierungsverfahren erfordert einen neuen Ansatz, der die einfache und sichere Verwendung von digitalen Identitäten ermöglicht, in einer Vielzahl von Use Cases.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 372-382.

1.1 Ziele

Die vorliegende Arbeit stellt eine innovative Lösung der Authentifizierung für eine Vielzahl von Use Cases vor. Um ein möglichst hohes Maß an Sicherheit und Nutzerakzeptanz zu gewährleisten, soll die vorgestellte Authentifizierungslösung folgende Ziele abdecken:

1. Erhöhte Benutzerfreundlichkeit. Um den Nutzer aus der Verantwortung zunehmen, soll die Benutzerfreundlichkeit erhöht werden, indem Fehlverhalten minimiert wird und auftretendes Fehlverhalten toleriert wird und auch ungeübte und nicht technikaffine Personen ihre digitale Identität sicher nutzen können.
2. Erhöhte Sicherheit. Ein Fehlverhalten des Nutzers soll nicht zur Unsicherheit des Systems führen. Damit sollen auch Phishing und weitere aktuelle Angriffe auf Nutzer und die Authentifizierung von Informationssystemen nicht zur Unsicherheit oder den Identitätsdiebstahl führen.
3. Maximale Flexibilität. Ein Nutzer soll die Möglichkeit haben ein Authentifizierungsverfahren für eine Vielzahl und unterschiedliche Anwendungsfälle zu nutzen. Dabei sollen heute aktuelle Anwendungen, bspw. die Authentifizierung an Webseiten, aber auch zukunftsweisende Anwendungsfälle, wie z. B. die Authentifizierung im Internet der Dinge oder an elektrolade Säulen, unterstützt werden.
4. Erhöhung des Datenschutzes. Das Authentifizierungssystem soll bedarfsgerecht Nutzerdaten verarbeiten und bei der Ansammlung von personenbezogenen Daten, diese auf die für die Authentifizierung nötige Menge reduzieren. Es soll verhindert werden, dass ein Nutzer zu jedem Zeitpunkt, ggf. auch ohne Wissens des Nutzers authentifiziert und somit identifiziert werden kann.

1.2 Abgrenzung

Aktuellen Themen aus dem Bereich der ML gestützten Authentifizierung befassen sich mit der passiven kontinuierlichen Authentifizierung [SLY+16] [CeMC17] und der Analyse von Eingaben [Bart00]. Die hier vorliegende Arbeit, beschränkt sich im Vergleich zu den Arbeiten, der passiven kontinuierlichen Authentifizierung, auf die Nutzung der Smartphone-Sensoren bei der direkten Handlung des Scannens eines QR Codes [HeMP15b]. Damit soll die Belastung der Smartphone-Batterie reduziert werden und die Akzeptanz beim Nutzer erhöht werden. Der Nutzer empfindet eine kontinuierliche Erfassung und Auswertung der Daten der Smartphone-Sensoren als Überwachung, bspw. in dem die Interaktion mit dem Smartphone analysiert wird [MTSH18].

2 Verwendete Technologien

Damit die oben genannten Ziele erreicht werden können, muss ein Paradigmenwechsel bei der Authentifizierung stattfinden [HeMP15a]. Dabei sollen alten Verfahren im Ganzen, durch eine neue auf maschinelles Lernen beruhende Methode abgelöst werden. Dazu wird als Nutzerschnittstelle das Smartphone genutzt und als Schnittstelle zum Auslösen einer Authentifizierung, ein optischer Auslöser im Form eines QR Codes.

2.1 QR Codes

QR Codes sind 2D-Barcodes, die es ermöglichen bis zu 31.329 Bytes zu codieren. Die maximale Anzahl der zu codierenden Bytes hängt dabei von der Version des QR Codes (max. Version 40 mit 177 Spalten * 177 Zeilen) und weiteren Parametern abhängig. Dabei können Parameter die Stärke der Fehlerkorrektur sein und um welchen Inhalt (numerische, alphanumerisch, binär, …) es sich handelt. Fehlerkorrektur wird erzeugt, indem Teile des QR Codes redundant innerhalb der 2D-Matrix vorkommen [Hara02]. QR Codes finden im Bereich der Authentifizierung eine immer größer werdende Akzeptanz. Der Unterschied des Systems, das die Grundlage der hier vorliegenden Arbeit bildet, im Vergleich zu anderen Systemen die QR Codes für die Nutzerauthentifizierung nutzen, liegt in den im QR Code enthaltenen Daten. Es werden hier keine sensiblen Informationen gespeichert, wodurch das System auch für die Authentifizierung in Szenarien genutzt werden kann, bei dem statische und nicht dynamische QR Codes verwendet werden können [HePM15c].

2.2 Smartphone

Die Nutzung des Smartphones wird in der heutigen Zeit immer wichtiger und nimmt immer mehr Zeit im täglichen Leben eines jeden Menschen in Anspruch. Im Jahr 2016 nutzen 49 Millionen Menschen in Deutschland ihr Smartphone, wohingegen es nur rund 45,5 Millionen Menschen im Februar 2015 waren [Stat16a]. Bis 2019 wird vorausgesagt, dass 55,5 Millionen Menschen in Deutschland ein Smartphone für ihr tägliches Leben nutzen werden [Stat16a]. Zusätzlich nutzten 2014 knapp 54% der deutschen Bevölkerung mobiles Internet.

Damit hat das Smartphone den Weg in unsere Gesellschaft als technologischer Alltagsgegenstand gefunden. Neben der weiten Verbreitung ist die Interaktion mit dem Smartphone einfach zu erlernen, wodurch eine komfortable und benutzerfreundliche Nutzerschnittstelle gegeben ist [Do17].

Das Smartphone bietet neben den Anzeigekomponenten wie Bildschirm und Signal-LEDs, weitere Mitteilungskomponenten wie den Lautsprecher und Vibrationsmöglichkeiten, mit denen man dem Nutzer für unterschiedliche Ereignisse bei einer Authentifizierung, unterschiedliches Feedback geben kann.

Damit bildet das Smartphone eine einfach zu verwendende Nutzerschnittstelle. Der Nutzer muss zur Verwendung des Smartphones nicht trainiert werden, wodurch die Akzeptanz durch den Nutzer erhöht wird. Darüber hinaus bietet das Smartphone mit dem hochauflösenden Display eine sehr gute Möglichkeit, um dem Nutzer über Aktivitäten, verwendete Daten und Schritte während der Authentifizierung transparent zu Informieren. Damit kann die Sicherheit des Gesamtsystems gesteigert werden.

Das Smartphone besitzt aktive Eingabekomponenten, wie die Touchfunktionalität des Displays, mit denen der Nutzer eine bewusste und prüfbare Handlung durchführen kann. Bspw. das Bestätigen der Zustimmung der zu übertragenden Daten, um eine datenschutzkonforme und für den Nutzer transparente Handlung durchzuführen. Für die hier vorliegende Arbeit soll die Nutzerauthentifizierung anhand der verfügbaren passiven Sensoren durchgeführt werden. Passive Smartphone-Sensoren können dazu genutzt werden, Informationen, über den Kontext oder der Umgebung, in der sich ein Nutzer befindet, zu sammeln. Um die Akzeptanz durch den Nutzer weiter zu erhöhen, sollen für die passive Authentifizierung Sensoren genutzt werden, die keine weitere Berechtigung erfordern. Damit kann die passive Authentifizierung auch zu bestehenden Apps hinzugefügt werden, um auch hier die Sicherheit zu erhöhen.

Verwendung von Geolokationsdaten als Angriffsvektor für Social Engineering

Matteo Cagnazzo · Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
{cagnazzo | pohlmann}@internet-sicherheit.de

Zusammenfassung

Geolokationsdaten sind eine Bedrohung für Organisationen und Unternehmen. Vor kurzem wurde beispielsweise ein anonymisierter Datensatz veröffentlicht, allerdings sind die verwendeten Anonymisierungstechniken unzureichend. Private und eventuell geheime Standorte, beispielsweise Militärbasen in Kriegsgebieten, können damit aufgedeckt werden. Weiterhin können einzelne Personen gezielt identifiziert werden.

1 Einführung

Frei zugängliche Daten von privaten Firmen sind eine wichtige Quelle für unterschiedliche Forschungsbereiche. Es gibt viele Beispiele für die positive Nutzung von öffentlichen Daten in der Forschung zum Beispiel im Bereich des nicht-motorisierten Transportes oder Untersuchungen zur Exposition in Gebieten mit extremer Luftverschmutzung [SELA16] [SUN17].

Die aktuellen Entwicklungen und Erkenntnisse zeigen aber auch deutlich Probleme und Gefahren auf, die mit der Veröffentlichung solcher Datensätze einhergehen. Insbesondere die Betriebssicherheit (Opsec) und Privatheit von Individuen und großen Organisationen kann durch die Veröffentlichung solcher Daten gefährdet sein. Dieses Paper zielt darauf ab Gefahren aufzuzeigen und Awareness zu schaffen, dass solche Probleme existieren. Weiterhin werden mögliche Konsequenzen von betrieblichen- oder Privatsphäre Problemen angerissen und diskutiert. Das Kapitel 2 gibt Hintergrundinformationen für den Leser in den Bereichen Social Engineering, Privatsphäre und ortsbasierte Daten. Kapitel 3 zeigt Ergebnisse einer kleinen Fallstudie auf, welche durchgeführt wurde, um die Machbarkeit zu zeigen. Anschließend werden in Kapitel 4 mögliche Mitigierungsstrategien diskutiert. Im letzten Kapitel 5 werden die Ergebnisse diskutiert und weitere Forschungsfragen skizziert.

2 Hintergrundinformationen

Dieses Kapitel gibt einige theoretische Definitionen und Einführungen für ortsbasierte Daten, Social Engineering und Angriffstechnologien.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 383-391.

2.1 Ortsbasierte Daten

Ortsbasierten Daten enthalten Ortsinformationen in Form von Koordinaten und üblicherweise einen Zeitstempel. Diese Daten werden genutzt, um beispielsweise Geräte, Personen oder andere Entitäten zu orten. Das meistgenutzte System ist das Global Positioning System. Dieses arbeitet mit der Triangulation von Radiosignalen und Satelliten. [MISR06] gibt eine ausführliche Erläuterung und Überblick über diese Technologie. GPS wird in vielen Smartphones, mobilen Geräten oder Dingen im Internet der Dinge implementiert. Durch die ubiquitäre Vernetzung dieser Gegenstände wird es möglich, das Gerät jederzeit zu orten oder Informationen über den derzeitigen Aufenthaltsort zu versenden.

Diese Informationen werden von Applikationen genutzt, um zum Beispiel Laufstreckentracking zu ermöglichen. Ein großer Dienst in diesem Bereich ist das soziale Netzwerk Strava. Strava ist eine populäre Applikation, welche von Athleten jeglicher Leistungsklasse genutzt wird, um sportliche Aktivitäten mit anderen Sportlern zu vergleichen. Mit Hilfe von Applikationen wie Strava können Parameter wie zum Beispiel Laufdistanz, Laufzeit, Durchschnittsgeschwindigkeit, und Route mit anderen Nutzern geteilt werden. Dabei gibt es auch die Möglichkeit viele Metainformationen anzugeben, beispielsweise welches Laufschuhmodell oder welche Fitnessarmbanduhr wurde verwendet. Dienste wie Strava oder Suunto veröffentlichen anonymisierte Heatmaps der Aktivitäten ihrer Nutzer öffentlich zugänglich. Diese Daten wurden dann misbraucht, um militärische Stellungen überall auf der Welt, auch in Krisenregionen, aufzudecken [GUAR18]. Die Heatmap besteht aus drei Trillionen ortsbezogenen Daten in aggregierter Form. Die zeitlichen Komponenten der Daten wurden ebenfalls entfernt. Insgesamt hat allein Strava nach eigenen Angaben eine Milliarde Aktivitäten und zehn Millionen Nutzer in ihren Daten [STRA17].

Innerhalb der Fallstudie wird klar, wie schnell einzelne Nutzer anhand der Daten identifiziert werden können, beispielsweise als Soldaten auf einem Stützpunkt oder Arbeiter bestimmter Firmen. Durch die Kombination der Heatmap und den sogenannten „Segmenten“ ist dies möglich. Segmente sind „user-created-content“, das bedeutet Nutzer können Segmente anlegen um mit anderen Mitgliedern in einen virtuellen Wettstreit zu treten. Dafür wird nach dem absolvieren eines Laufes ein Streckenabschnitt innerhalb der Applikation markiert und benannt. Die Applikation erstellt nun eine Bestenliste für die einzelnen Segmente. Durch den virtuellen Wettstreit sollen die Nutzer der Applikation motiviert bleiben während sie joggen oder Rad fahren. Diese Segmente sind in der Standardeinstellung öffentlich. Man kann die Segmente nur für einen kleinen Personenkreis sichtbar machen, allerdings ist dann eines der „Key-Features“ der Applikation nicht funktional, der „virtuelle Wettstreit“ und die soziale Teilhabe an dem Erfolg des anderen.

2.2 Social Engineering

Social Engineering ist im Informationssicherheitskontext die Beeinflussung von potentiellen Opfern Informationen preiszugeben oder Handlungen durchzuführen durch soziale Manipulation. Diese Informationen oder Handlungen werden dann dafür genutzt ein informationsverarbeitendes System oder eines anderen Assets innerhalb eines Unternehmens zu manipulieren. Die Manipulation kann sich auf die Vertrauenswürdigkeit, Integrität oder die Verfügbarkeit auswirken. Täuschung und Manipulation sind die Grundlagen von Social Engineering-gestützten Angriffen.

Aktuelle technische Gegenmaßnahmen sind in der Regel gegen diese Angriffe unwirksam. Darüber hinaus haben viele Opfer von Social Engineering Angriffen die Meinung, dass sie gut darin sind, diese Angriffe zu erkennen, es aber eigentlich nicht sind [KROM15]. Es gibt mehrere Stufen innerhalb der Taxonomie eines erfolgreichen Social Engineering-Angriffs, wie in Abbildung 1 zu sehen ist. Vor allem wenn der Angriff darauf abzielt, ein Unintentional Insider Threat (UIT) zu beinhalten. [BURE13] definiert einen UIT wie folgt: „Ein Unintentional Insider Threat ist (1) ein gegenwärtiger oder ehemaliger Mitarbeiter, Auftragnehmer oder Geschäftspartner (2), der Zugriff auf das Netzwerk, System oder Daten einer Organisation autorisiert hat oder hatte und (3) durch Aktion oder Unterlassung ohne böswillige Absicht (4) verursacht Schaden oder erhöht wesentlich die Wahrscheinlichkeit eines zukünftigen ernsthaften Schadens für die Vertraulichkeit, Integrität oder Verfügbarkeit des Informations- oder Informationssystems der Organisation“.

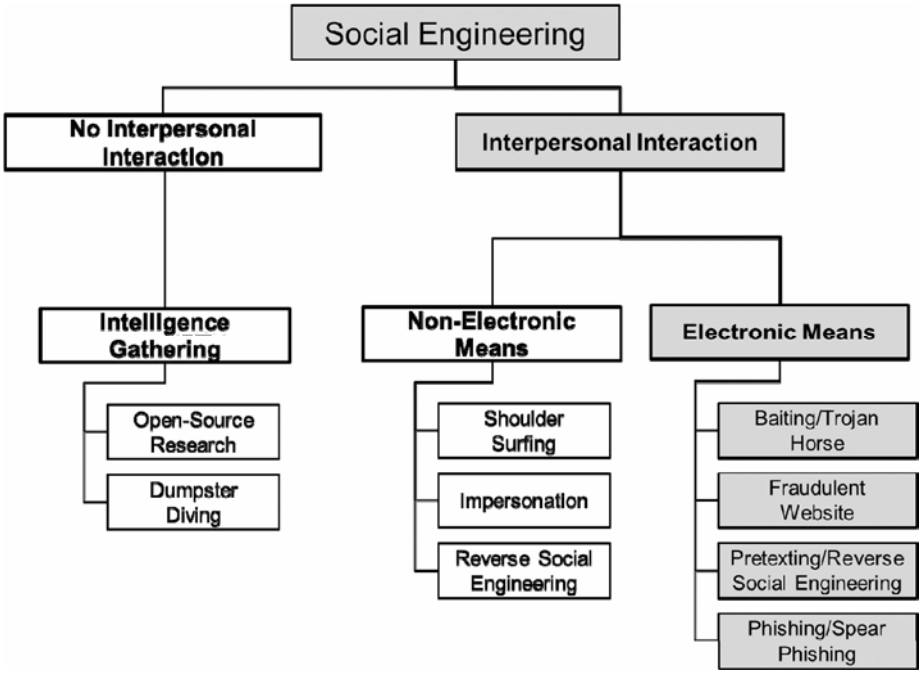

Abb. 1: Taxonomie eines Social Engineering Angriffs [GREI14]

Diese Insider-Bedrohungen, unabhängig davon ob beabsichtigt oder nicht, gelten als eines der größten Risiken für die betriebliche und organisatorische Sicherheit. Die beiden Bedrohungen unterscheiden sich in Bezug auf Motivation, Indikation und andere Unterschiede. Daher ist es wichtig, diese Bedrohungen zu erforschen und ihr Aufkommen zu verstehen [BURE13]. Für die von uns durchgeführte Fallstudie werden wir Open Source Informationen von Personen mit standortbezogenen Informationen aus Fitnessapplikationen verknüpfen. Aus den gesammelten Informationen lassen sich gezielte Pretexte und zielgruppenspezifisches (Spear) Phishing entwickeln.

Beim Pretexting wird ein erfundenes oder echtes Szenario verwendet, um die Chancen zu erhöhen, dass ein Opfer die Vertraulichkeit, Integrität oder Verfügbarkeit seines Unternehmens gefährdet. Unter normalen Bedingungen würde das Opfer eine solche Handlung nicht durchführen, aber durch die geschickte Wahl eines Pretext kann ein potentielles Opfer motiviert werden, auf bösartige Links oder Anhänge zu klicken.