Pressemitteilung

Rapide zunehmendes Social Engineering: Metadaten besser schützen!

München, 17. Dezember 2014. Nicht alles ist Gold, was glänzt: Wenn also ein IT-Manager auf Facebook von einer unglaublich hübschen, ihm völlig unbekannten jungen Dame geaddet wird, ist das meistens weniger „großes Glück“, sondern der Beginn eines simplen Social-Engineering-Angriffs auf die Informationen, zu denen der Manager Zugang hat. (1) Wenn letzterer ein paar Stunden später einen flirtigen Chat hinter sich und ein paar sexy Bilder aus einem Fotokatalog sowie einen Trojaner auf seinem Rechner hat, der nun jede Tastatureingabe nach Fernost weitermeldet, ist das einerseits ein schöner Erfolg für den Hacker hinter dem hübschen Facebook-Foto; andererseits aber äußerst ärgerlich für die Organisation, der der Manager in unserem Beispiel angehört. Weil sie einfach gut funktioniert, besser und schneller als die langwierige Suche nach technischen Schlupflöchern, setzt sich die Social Engineering Masche weltweit immer mehr durch und passt sich immer besser der jeweiligen Zielgruppe an. (2) „Wie dumm – wäre mir aber nicht passiert!“, denken viele. Wahrscheinlich dachten das auch die rund 2500 Probanden, die bei einem international angelegten Test an ihrem Arbeitsplatz auf einen ähnlich simplen Trick hereinfielen: 2500 von insgesamt rund 12.000, also gut jeder Fünfte. (3)

Die Schwelle, gutgläubig solchen Fishing-Mails nachzugeben, erhöht sich mit der Zeit vermutlich, so dass Hacker gerne auf den Schein des Vertrauten setzen: Besitzt er bereits eine geringe Menge an Informationen über die anzugreifende Person, vertraut ihm diese eher. In diesem Zusammenhang werden Verbindungsdaten, auch als Metadaten bekannt, zum Schlüssel. Ein Beispiel: Wer würde skeptisch reagieren, wenn kurz nach dem Absenden einer Mail an einen DAX-30-Vorstand dessen angebliche Assistenz anruft und bittet, die Mail noch einmal an dessen private Mail-Adresse vorname.nachname@irgendwas.de zu schicken, weil sich der Anhang auf dem Gerät des Chefs angeblich nicht öffnen lässt? In diesem Beispiel genügen die Metadaten einer einzigen Mail (Absender, Empfänger, genaue Zeit, Dateinamen und -größen), um ohne weiteres einen erfolgversprechenden Social Engineering Angriff zu starten und wertvolle Informationen zu stehlen.

Metadaten sind also keineswegs harmlos. Nach heutigem Stand der Forschung lassen

sie sich auf drei verschiedene Arten schützen (4):

> *1. wenn die Botschaft nicht an einen, sondern an eine Gruppe von Empfängern geht, wobei nur einer den richtigen Schlüssel zum Öffnen besitzt. Das Freenet-Projekt folgt dieser Methode und lässt sich privat gut nutzen, für Firmen ist es aber weniger geeignet. (5)*
>
> *2. mit dem Einsatz von Mix-Netzen. Hier werden Nachrichten über mehrere Zwischenstationen (Mix-Knoten) geleitet. Auch damit lässt sich die Anonymisierung der Kommunikationsbeziehung erreichen. Die Sicherheitssoftware TOR nutzt diese Technik, die so gut schützt, dass die National Security Agency (NSA) annimmt, dass jeder, der einen Server dieses Netzwerks betreibt, terrorverdächtig ist, und deshalb in Echtzeit die Kommunikation desselben rastert. Je engmaschiger aber ein Raster ist, desto einfacher wird es, die Anonymität wieder zu zerstören. (6)*
>
> *3. mit der in Deutschland entwickelten Sealed-Cloud-Technologie (7). Sie setzt an zwei Punkten an: Zum einen sichert sie ein Rechenzentrum so ab, dass die Daten nicht nur beim Transport zum und vom Datenzentrum und im Speichersystem in der Datenbank geschützt sind, sondern auch während ihrer Verarbeitung. Zum Zweiten werden die ein- und ausgehenden Datenströme nach Volumen und Zeit verschoben (de-korreliert), so dass sich zwischen den Verbindungen keine Bezüge herstellen lassen. Eine beispielhafte Anwendung der Sealed Cloud Technologie ist der Online-Speicher- und -Kommunikationsdienst IDGard (8), der den Schutz von Metadaten auch für kleine und mittlere Unternehmen erschwinglich macht.*

Für Anwälte, Wirtschaftsprüfer, Ärzte und Datenschutzbeauftragte, die zu den sogenannten Geheimnisträgern gehören, ergibt sich aus diesem Wissen und dem §203 StGB sogar eine Pflicht, Verbindungs- oder Metadaten als personenbezogene Daten besonders zu schützen. Ähnliches gilt nach § 353b StGB für den öffentlichen Dienst. Inzwischen sehen Rechtsexperten im Ansatz der Sealed Cloud Technologie einen gangbaren Weg, um sogar den Geheimnisträgern den Einsatz von Cloud

Pressemitteilung

Computing rechtlich zu ermöglichen (9). Denn diese Technologie kann sowohl Inhalte als auch Metadaten schützen.

Druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de

(1) http://de.wikipedia.org/wiki/Social_Engineering_%28Sicherheit%29#Bekannte_Social_Engineers
(2) Zum Beispiel http://www.onlinepc.ch/internet/schweiz/social-engineering-und-phishing-gegen-schweizer-746008.html und http://www.funkschau.de/telekommunikation/artikel/111660/
(3) http://www.heise.de/newsticker/meldung/Spearphishing-Jeder-Fuenfte-geht-in-die-Falle-2461982.html
(4) Datenschutz Praxis Ausgabe 01/15, S. 4 ff.
(5) https://freenetproject.org/?language=de
(6) https://www.torproject.org/
(7) https://de.wikipedia.org/wiki/Sealed_Cloud und http://www.sealedcloud.de
(8) https://de.wikipedia.org/wiki/IDGARD und http://www.idgard.de
(9) Kroschwald, S., Informationelle Selbstbestimmung in der Cloud, Dissertation, Kassel 2015, i. E.

Über Uniscon GmbH –

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service IDGARD für Unternehmen basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

Pressekontakt
Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 110
presse@uniscon.de
www.uniscon.de

PR-Agentur
Xpand21, Doris Loster

Pressemitteilung

Alter Teichweg 9m
22081 Hamburg
0170 / 215 31 72
uniscon@xpand21.com
www.pr-agentur-xpand21.de