Inhaltsverzeichnis:

1.	Aktuelle Gefahren/Bedrohungen/Hinweise	Seite 2
1.1	Kostenfallen: Button-Lösung im Internet wirksam	Seite 2
2.	Social Engineering – psychosoziales Hacking am Menschen	Seite 2
2.1	Was ist Social Engineering?	Seite 2
2.2	Phänomenologische Erscheinungsformen	Seite 4
2.3	Prävention und Handlungsempfehlungen	Seite 5
2.4	Tipps zur Weitergabe an Unternehmen und ihre Mitarbeiter	Seite 5
2.5	Tipps zur Weitergabe an Privatpersonen	Seite 6

1. Aktuelle Gefahren/Bedrohungen/ Hinweise

1.1 Kostenfallen: Button-Lösung im Internet wirksam

Das am 01.08.2012 in Kraft getretene Gesetz zum besseren Schutz der Verbraucher vor Kostenfallen im elektronischen Geschäftsverkehr hat sich bewährt – das teilt das Bundesjustizministerium mit. Hintergrund der damaligen Gesetzesinitiative war die hohe Zahl von Opfern sogenannter Abo-Fallen. Vermeintlich kostenfreie Dienste im Internet wurden durch versteckte Abo-Verträge zu Kostenfallen für die Verbraucher. Diesem Betrug wurde durch die gesetzliche Button-Maßnahme Einhalt geboten, wie man dem Bericht zur Evaluation entnehmen kann. Anbieter von kostenpflichtigen Abo-Diensten sind laut Gesetz verpflichtet, den Kunden auf alle vertraglichen Pflichten hinzuweisen, die dieser durch Klick auf einen entsprechenden Button bestätigen muss. Versteckten Kostenfallen wurde damit gesetzlich ein Riegel vorgeschoben.

Dennoch zeigt die Evaluation auch, dass weiterhin ein erheblicher Handlungsbedarf bei der Verbraucherinformation und -aufklärung besteht. Insbesondere bei Zulässigkeit und Ausgestaltung der Buttons herrscht bei den Verbrauchern oftmals Misstrauen. Es wird darauf verwiesen, „…dass die heute zulässigen Button-Beschriftungen und Darstellungsanforderungen von Verbraucherinnen und Verbrauchern nicht als derart intuitiv nachvollziehbar empfunden werden, als dass sich eine rechtliche Zulässigkeit für sie sofort erschließt“. Daher sollte – so der Evaluationsbericht – im Rahmen repräsentativer Verbraucherbefragungen oder durch verhaltenswissenschaftliche Experimente erhoben werden, „…welche Informationen und Gestaltungselemente für Verbraucherinnen und Verbraucher bei Online-Käufen tatsächlich relevant sind und wie diese im besten Fall ausgestaltet sein sollten“.

Quelle:
Bundesministerium der Justiz und für Verbraucherschutz
http://www.bmjv.de/SharedDocs/Kurzmeldungen/DE/2014/20140904_Button_Loesung.html

2. Social Engineering – psychosoziales Hacking am Menschen

2.1 Was ist Social Engineering?

Klassische Bedrohungen im weltweiten Datenverkehr sind weitläufig bekannt. Hacken und Datenspionage, digitale Erpressung mittels Ransomware, Viren, Trojaner und andere Schadsoftware – alles technische Mittel, die von Cyberkriminellen genutzt werden, um eigene finanzielle oder ideologische Ziele zu erreichen. Technische Sicherungen erschweren Straftätern jedoch ihre Machenschaften.

Das größte Risiko geht aber nicht von der Technik, sondern vom Menschen aus. Wer sich beispielsweise als Unternehmens- oder Behördenmitarbeiter in digitalen Netzen bewegt, trägt auch sensible Informationen über diese mit sich: Zugangsdaten zum Firmennetzwerk, zu Cloud-Diensten oder Inhalte über vertrauliche Projekte oder Produktinnovationen.

Straftäter gehen daher mehr und mehr dazu über, am Schwachpunkt Mensch anzusetzen und die benötigten Informati-

onen mittels geschickter psychologischer Techniken und arglistiger Täuschung zu erfragen. Diese Vorgehensweise bezeichnet man als Social Engineering oder auch Social Hacking.

Ziel der Täter:
Täter wollen Informationen abgreifen und zwar indem sie sich geschickt an bestimmte Personen annähern. Diese Annäherung kann persönlich erfolgen, beispielsweise wenn Kriminelle als Handwerker auftreten und zielsicher um Zugang zum Serverraum eines Unternehmens bitten (Human Based Social Engineering). Dies ist ein Leichtes, wenn der Täter vorher bei der Assistentin des verantwortlichen Administrators telefonisch erfragt hat, dass dieser nicht anwesend ist. Um einen Mitarbeiter zum Öffnen des Serverraums zu bewegen, üben die Täter zusätzlich Druck aus, indem sie einen technischen Notfall vortäuschen.

Der Aufbau einer persönlichen Beziehung kann auch telefonisch oder elektronisch (Computer Based Social Engineering) erfolgen, um Passwörter oder Zugangsnamen zu erhalten.
Wichtigste Grundlage für die Täter ist eine lückenlose Legende, die sich durch öffentlich zugängliche Informationen leicht stützen lässt.

Ein klassischer Fall des Social Engineerings ist auch der kostenlose oder gefundene USB-Stick, der am eigenen Rechner ausgelesen wird. Die dort vom Cyberkriminellen versteckte Schadsoftware installiert sich unbemerkt, damit sind der PC und das eigene Netzwerk dem Zugriff der Täter ausgeliefert.

Die Technik des Social Hackings existiert bereits viele Jahre und wurde vor allen durch Kevin Mitnick, einen der in den 1980er und -90er Jahren meistgesuchtesten Hacker weltweit, entwickelt. Ihm gelang es unter anderem, sich mehrfach Zugang zum Pentagon zu verschaffen. Social Hacker nutzen bei der Beeinflussung der Zielpersonen vor allem sechs Konstanten menschlichen Verhaltens:

Reziprozität: Der Mensch leistet anderen einen Gefallen, um später eine Gegenleistung zu erhalten bzw. fordern zu können.

Konsistenz: Der Mensch neigt in den meisten Fällen dazu, konsequent zu sein und zu wirken, sich treu zu bleiben und einen Weg, den man selbst eingeschlagen hat, auch zu Ende zu gehen.

Soziale Bewährtheit: Die Orientierung des Individuums an offensichtlich bewährten Handlungsweisen der sozialen Vergleichsgruppe in ähnlichen Situationen.

Sympathie: Offenheit gegenüber vertrauenswürdigen, sympathischen Menschen. Interesse an charakterlich gleichen Menschen.

Autorität: Autoritätshörigkeit gegenüber offensichtlich höher gestellten Personen.

Knappheit: Das Bedürfnis, bei Knappheit von Gütern oder Zeit entsprechend priorisiert handeln zu müssen und Drucksituationen schnell meistern wollen.

Orientiert sich der Täter an diesen Grundsätzen und richtet seine Strategie entsprechend auf die Opfer aus, ist der Aufwand verglichen mit dem Nutzen weitaus geringer als bei aufwendigen technischen Angriffen auf ausgefeilte Sicherheitssysteme – besonders bei Unternehmen. Erleichtert werden Social Engineering-Angriffe durch im Internet veröffentlichte Leitfäden – diese zeigen, wie Angriffe am besten konzipiert werden.

2.2 Phänomenologische Erscheinungsformen

Social Engineering spielt sowohl im Internet als auch in anderen Bereichen des gesellschaftlichen Lebens eine große Rolle. Aus polizeilicher Sicht sind jedoch besonders Wirtschaftsunternehmen von dieser Art des Datenabfangens betroffen.

Denn Tätern reichen schon wenige Kenntnisse über Organisationsstrukturen eines Unternehmens, um Mitarbeiter in ein Gespräch zu verwickeln. Sie nennen dabei plausibel unterschiedliche Gründe, um den Mitarbeiter zur Herausgabe von Daten oder der Zugangsberechtigung zu bewegen – spiegeln äußerst dringliche Entscheidungsfindung bis hin zum technischen Notfall im System vor.

Aber auch Privatpersonen werden oft Opfer derartiger Angriffe – die wohl bekannteste Form des Social Hackings gegen Privatpersonen ist der Enkeltrick. Dem Opfer wird telefonisch die Notsituation (Knappheit) einer vermeintlich verwandten Person (Sympathie) vorgegaukelt und dieses so zu Geldauszahlungen „überredet“ (Konsistenz). Die zugrunde liegende Straftat ist ein Betrug.

Ähnliche Methoden zeigen sich bei Betrugsfällen an der Haustür bzw. bei Diebstählen aus Wohnungen. Dem Opfer wird suggeriert, die Polizei (Autorität), Handwerker oder alte Bekannte hätten eine Bitte oder benötigen eine Gefälligkeit (Reziprozität). Lässt das Opfer die Personen in seine Wohnung, kommt es entweder zur freiwilligen Übergabe von Geld, weil das arglose Opfer von der Geschichte und der Sympathie getäuscht ist, oder zu Diebstählen. Das Veröffentlichen von sensiblen personenbezogenen Daten in sozialen Netzwerken spielt den Tätern dabei oft in die Karten, weil Adressen, Vorlieben, Hobbies usw. als Ansatzpunkte für Social Engineering verwendet werden.

Einen klassischen Fall des Computer Based Social Engineering stellt Phishing dar. Dem Online-Banking-Kunden oder Online-Käufer wird per E-Mail eine beispielsweise auf technischen Problemen der Bank begründete gefälschte Internetseite präsentiert, auf der Zugangsdaten oder sogar TAN eingetragen werden sollen. Weil sie die Richtigkeit der Informationen und der Notwendigkeit der Maßnahme vertrauen, werden nach wie vor viele Personen Opfer derartiger Betrugsfälle.

2.3 Prävention und Handlungsempfehlungen

Trotz der beschriebenen psychologisch bedrohlichen Szenarien sollten präventive Handlungsempfehlungen weder bei Mitarbeitern von Unternehmen noch bei Privatpersonen Misstrauen oder Angst fördern. Stattdessen sollte an den gesunden Menschenverstand appelliert werden, um im Ernstfall Sachverhalte entsprechend hinterfragen zu können.

Folgende Punkte könnten zur Erklärung beitragen:

- Kann die Geschichte stimmen? Wer kann diese zusätzlich beurteilen?
- Verlangt mein Gegenüber etwas Ungewöhnliches? Fordert mein Gegenüber eine Gegenleistung für einen Gefallen, um den man nie gebeten hat?
- Bleibt wirklich keine Zeit für Nachfragen? Immer Bedenkzeit und ggf. Rückruf erbitten und selbst nachrecherchieren.
- Teilt mein Gegenüber auffällig meine Interessen und tut er dies sehr offen und schnell kund? Setzt mein Gegenüber ein überzogenes Vertrauensverhältnis voraus?
- Hat die Autorität meines Gegenübers eine solide Basis? Hinterfragen Sie Anordnung von Ihnen unbekannten Autoritäten. Scheuen Sie sich im Zweifelsfall nicht, auch höhere Vorgesetzte nach der Richtigkeit der Angaben zu fragen.

2.4 Tipps zur Weitergabe an Unternehmen und ihre Mitarbeiter

Unternehmer sollten ihre Mitarbeiter darüber aufklären, dass Abwehrmechanismen beispielsweise gegen Social Engineering innerhalb eines Unternehmens notwendig sind. Damit die Sicherheitsvorgaben umgesetzt werden können, müssen Rahmen geschaffen werden, die Awareness fördern sowie Kommunikationswege und Vertraulichkeitsstufen festlegen. Trotzdem sollte Vertrauen gegenüber Mitarbeitern vorherrschen und ihnen Wege aufgezeigt werden, wie mit Problemlagen umgegangen werden sollte. Dazu müssen Vorgesetzte Mitarbeitern ermöglichen, sich auch in schwierigen Situationen an sie wenden zu können.

Grundsätzlich gilt für Mitarbeiter in Unternehmen:

- Erteilen Sie keine Auskünfte, zu denen Sie nicht ausdrücklich ermächtigt sind. Geben Sie nur so wenige Informationen wie nötig preis. Hinterfragen Sie auch Autoritätspersonen, die Ihnen nicht bekannt sind.
- Bedenken Sie, dass Sie als Mitarbeiter auch Informationen über das Unternehmen haben, die für Außenstehende interessant sein können.
- Seien Sie in den Räumlichkeiten, aber auch im Unternehmens-Netzwerk aufmerksam und melden Sie Auffälligkeiten Ihrem Vorgesetzten.
- Gehen Sie sorgsam und bedacht mit sensiblen Informationen um. Sei es bei öffentlich geführten Telefonaten über Unternehmensinterna, der Arbeit mit mobilen Geräten in der Öffentlichkeit oder bei der Verwendung mobiler Speicher. Auch im eigenen Büro sollten Sicherheitsbestimmungen beachtet werden.

2.5 Tipps zur Weitergabe an Privatpersonen

- Seien Sie vorsichtig, wenn angebliche Verwandte oder Freunde um Geld oder sensible Daten bitten. Rufen Sie stattdessen bei dem Verwandten oder Freund unter der Ihnen bekannten Nummer an und fragen sich nach dem Anliegen. Sollten Sie niemanden erreichen, geben Sie der Forderung des Bittstellers nicht nach. Erfragen Sie beim Anrufer Dinge, die nur der richtige Verwandte/Bekannte wissen kann. Informieren Sie die Polizei, z. B. wenn Unbekannte Geld von Ihnen erbitten.
- Lassen Sie keine fremden Personen in Ihre Wohnung. Wenn sich Personen an der Haustür als Mitarbeiter von Firmen und Behörden ausgeben, fragen Sie telefonisch bei der jeweiligen Stelle nach, ob dies stimmt. Lassen Sie sich nicht durch Ausweise täuschen.
- Seriöse Firmen fragen vertrauliche Zugangs- und Passwortdaten niemals am Telefon oder per E-Mail ab. Achten Sie bei der Eingabe sensibler Daten grundsätzlich auf eine sichere Verbindung, erkennbar am „https“ in der Browserzeile.
- Veröffentlichen Sie so wenig wie möglich persönliche Daten in sozialen Netzwerken und machen Sie Ihr Profil nur für Freunde sichtbar.
- Wenn Sie Opfer geworden sind: Erstatten Sie Anzeige bei der Polizei.

Quellen:

Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html

Programm Polizeiliche Kriminalprävention der Länder und des Bundes
Infoblatt „Enkeltrick“
http://www.polizei-beratung.de/themen-und-tipps/betrug/enkeltrick.html#

Bundesministerium für Wirtschaft und Technologie
Informationsbroschüre „Gefahr durch Social Engineering“

Trendmicro
E-Guide „Was steckt hinter Social Engineering“

LANline – IT, Netze, Infrastruktur
„Social Engineering erkennen“
http://www.lanline.de/fachartikel/social-engineering-erkennen.html