Funkkolleg 2016/2017

Sicherheit

Zusatzmaterial zur Sendung 08:
Social Hacking -
Der Enkeltrick in der Cyberworld

vhs Die Volkshochschulen in Hessen

TECHNISCHE UNIVERSITÄT DARMSTADT

HESSEN Hessisches Kultusministerium

hr iNFO

Zusatzmaterial zur Folge 08
Social Hacking – Der Enkeltrick in der Cyberworld

Livestream und Podcast: www.hr-inforadio.de

Interessierte Hörerinnen und Hörer finden auf dieser Seite weiterführende Informationen zu den einzelnen Sendungsthemen als Zusatzmaterial. Die Materialien wurden zum Zugriffszeitpunkt 06.01.2017 erstellt von:
Markus Stegeman, Fachgebiet Wirtschaftsinformatik | Software Business & Information Management, Technische Universität Darmstadt

Inhalt

1. Forschungsstudien

Social Engineering: Passwort im Tausch gegen Schokolade

Für Computerhacker ist es sehr aufwendig, einen Trojaner zu programmieren und in die Rechner von Privatpersonen und Unternehmen einzudringen. Sie greifen daher zunehmend auch auf psychologische Strategien zurück, um Computernutzer so zu manipulieren, dass sie freiwillig ihre Zugangsdaten preisgeben. Die Methoden sind als „Social Engineering“ bekannt.

Zum ersten Mal haben Psychologen der Universität Luxemburg in einer großangelegten Studie mit 1208 Teilnehmern untersucht, wie Menschen bereits mit kleinen Gefälligkeiten dazu gebracht werden können, ihre Passwörter mit ihnen vollkommen unbekannten Personen zu teilen. Das Ergebnis ist überraschend.

Quelle: Universität Luxemburg: Social Engineering: Passwort im Tausch gegen Schokolade, 04.05.2016

Link:
http://wwwde.uni.lu/forschung/flshase/inside/news_events/social_engineering_passwort_im_tausch_gegen_schokolade

2. Industrienahe Studien

Social Engineering-Studie – Cyberkriminelle nutzen menschliche Schwächen aus

Geiz, Neugier, Eitelkeit – häufig sind es weniger die Raffinessen anderer, sondern vielmehr unsere eigenen Schwächen, die uns Opfer von Cyberkriminellen werden lassen, zeigt eine Studie des IT-Security-Lösungsanbieters Kaspersky Lab zum sog. Social Engineering. Cyberkriminelle machen sich bei ihren Angriffsstrategien und –techniken psychologische Erkenntnisse zunutze und richten diese daran aus.

Quelle: Perspektive Mittelstand: Social Engineering-Studie. Cyberkriminelle nutzen menschliche Schwächen aus, 20.11.2014

Link: http://www.perspektive-mittelstand.de/Social-Engineering-Studie-Cyberkriminelle-nutzen-menschliche-Schwaechen-aus/management-wissen/6008.html

Social Engineering: Wie Nutzer „gehackt“ werden

Social Engineering, also die Angriffsmethode, das Vertrauen der Nutzer auszunutzen und die Anwender ungewollt zu einer Datenweitergabe zu verleiten, wird immer beliebter unter den Datendieben. Der Grund: Nutzer lassen sich nicht so einfach automatisch absichern, wie dies bei Hard- und Software zumindest teilweise möglich ist. Eine Datenschutzunterweisung sollte daher immer wieder einmal das Thema Social Engineering aufgreifen.

Viele IT-Sicherheitsforscher halten die Nutzer sogar für die größte Schwachstelle überhaupt. Die „Sicherheitslücken“ bei den Nutzern lassen sich auch nicht automatisch durch Einspielen von Patches beheben. Tatsächlich sind es Datenschutzbeauftragte, die eine Behebung der menschlichen „Schwachstellen“ vornehmen sollten.

Quelle: Schonschek, Oliver: Social Engineering: Wie Nutzer „gehackt“ werden, Datenschutz PRAXIS, 23.03.2015

Link: https://www.datenschutz-praxis.de/fachartikel/social-engineering-wie-nutzer-selbst-gehackt-werden/

Social Engineering – Wie Soft Skills zur Sicherheitsfallen werden können

Neben dem Angriff auf technische Weise werden Unternehmen bei der Methode des Social Engineering durch direkte Kontaktaufnahme über das Telefon, auf Messen, über soziale Netzwerke und über andere Kommunikationskanäle ausspioniert.

Die von der Corporate Trust GmbH durchgeführte Studie "Industriespionage 2012" ergab bei einer Befragung von 6.924 deutschen Unternehmen in 70,5 % der Fälle eine wissentliche Informationsweitergabe und Datendiebstahl durch Social Engineering. Hierbei stellt sich die Frage, warum diese Methode so erfolgreich ist.

Quelle: Leitwerk: Social Engineering – Wie Soft Skills zur Sicherheitsfalle werden können, 2012

Link: http://www.leitwerk.de/themen/it-sicherheit/social-engineering-wie-soft-skills-zur-sicherheitsfalle-werden-koennen/

3. Sonstiges

3.1. Literatur

Psychologische Grundlagen des Social Engineering

Social Engineering ist eine Angriffsstrategie, die nicht die Technik als Opfer auserkoren hat. Stattdessen wird hier lieber – und vor allem effizienter – der Mensch bzw. sein Verhalten angegriffen. Ein Angreifer verwendet verschiedene Strategien und Taktiken, um aus Benutzern der Systeme Informationen wie Passwörter oder IP-Adressen herauszuholen. Mit Hilfe dieser Informationen kann er erfolgreiche Angriffe gegen Zielsysteme fahren.

Quelle: Schumacher, Stefan: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder (94), S. 52-59, 2010

Link: http://ds.ccc.de/pdfs/ds094.pdf

Als weiterführende Literatur empfehlen wir:

- Hadnagy, Christopher: Die Kunst des Human Hacking, mitp Verlag, Frechen, 2011

3.2. Video/Audio

Social Hacking: Wenn der Datendieb anruft

Hacker greifen mitunter sogar zum Telefon, um ihren Opfern sensible Daten zu entlocken. "Social Hacking" heißt die Methode, um an Passwörter und Zugangsberechtigungen von Privatpersonen zu kommen. Dabei gehen die Kriminellen geschickt und vor allem dreist vor. In diesem Beitrag des Bayrischen Rundfunks (BR) wird Social Hacking näher erläutert.

Link: http://www.ardmediathek.de/radio/Notizbuch-Service-Bayern-2/Social-Hacking-Wenn-der-Datendieb-anruf/Bayern-2/Audio-Podcast?bcastId=5936850&documentId=34132160

Mediathek der Allianz für Cyber-Sicherheit

Die Partner der Allianz für Cyber-Sicherheit stellen neben Dokumenten, Dienstleistungen und Seminaren auch regelmäßig Videos und andere multimediale Inhalte zur Verfügung. Diese befassen sich häufig - aber nicht ausschließlich - mit Informationen zur Prävention von Cyber-Angriffen. Hierzu zählen insbesondere Inhalte zur Sensibilisierung von Mitarbeitern.

Link: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Mediathek/mediathek.html

3.3. Webseiten

DSIN – Verhaltensregeln zum Social Engineering

Der Verein „Deutschland sicher im Netz“ (DsiN) stellt nützliche Informationen zum Thema Social Engineering und entsprechende Verhaltensregeln für Internetnutzer zur Verfügung.

Am Beispiel einiger besonders gefährdeter Lebens- und Arbeitsbereiche macht die Broschüre Unternehmer und ihre Mitarbeiter auf konkrete Risiken durch Social Engineering-Attacken im Arbeitsalltag aufmerksam und gibt einen kompakten und allgemein verständlichen Überblick.

Link: https://www.sicher-im-netz.de/news/verhaltensregeln-zum-social-engineering

3.4. Forschungsgruppen

Forschungsgruppe SECUSO der TU Darmstadt

Im Mittelpunkt der Forschung steht der Mensch: Die Forschungsgruppe SECUSO der TU Darmstadt will die menschlichen Faktoren in den Bereichen Sicherheit und Privatsphäre genauer untersuchen. Ziel ist es, Mechanismen zu entwickeln, die zum einen die Sicherheit und Privatsphäre der Benutzer adäquat schützen, zum anderen aber auch sehr benutzerfreundlich sind. Zudem werden Sensibilisierungs- und Schulungsmaßnahmen für diese Thematik entwickelt. Um diese Ziele zu erreichen ist die Forschungsgruppe sehr interdisziplinär aufgebaut. Sie wird u.a. unterstützt durch mehrere Bundesministerien sowie durch das Hessische Ministerium für Wissenschaft und Kunst. Ein wichtiger Bestandteil der Forschung befasst sich mit dem Social Engineering.

Link: https://www.secuso.informatik.tu-darmstadt.de/de/secuso/

3.5. Zeitschriften

Psychologische Mechanismen hinter Social Engineering

Die Entwicklung technologischer IT-Sicherheitsmaßnahmen ist weit fortgeschritten: Anti-Viren-Programme, Next Generation Firewalls, Intrusion Prevention-Systeme und Advanced Threat Defense Appliances. Doch eine Kette ist bekanntlich immer nur so stark wie ihr schwächstes Glied: der Mensch. Auf welche kognitiven Schwächen Hacker dabei abzielen, verrät dieser Artikel.

Quelle: Krause, Marco: Psychologische Mechanismen hinter Social Engineering, IT Administrator, 08.06.2015

Link: http://www.it-administrator.de/themen/sicherheit/fachartikel/185259.html

Social Engineering: Das Hacken des menschlichen Betriebssystems

Social Engineering, manchmal auch die Wissenschaft und Kunst des Menschen-Hackings genannt, ist durch die wachsende Zahl von E-Mails, Sozialen Netzwerken und anderen Formen elektronischer Kommunikation in letzter Zeit immer beliebter geworden. Im Bereich der IT-Sicherheit wird dieser Begriff meist genutzt, um eine Vielzahl von Techniken zu beschreiben, die von Kriminellen genutzt werden, um ihre Opfer zu manipulieren und dadurch vertrauliche Informationen zu erhalten oder die Opfer dazu zu bringen, Dinge zu tun, die ihren Computer kompromittieren könnten.

Quelle: Pontiroli, Santiago: Social Engineering: Das Hacken des menschlichen Betriebssystems, Kaspersky Lab, 20.12.2013

Link: https://blog.kaspersky.de/social-engineering-das-hacken-des-menschlichen-betriebssystems/2186/

4. Personen

Die Biographie Kevin Mitnicks liest sich wie das Drehbuch zu einem Kinofilm. In einem ähnlichen Katz-und-Maus-Spiel mit dem Originaltitel „Catch me if you can“ brillierte Leonardo di Caprio neben vielen hübschen Stewardessen. Erfolgreiches Social Engineering entspricht ganz diesem Filmklischee.

Mitte der neunziger Jahre war Mitnick der meistgesuchte Computerhacker. Nach einer mehrjährigen Gefängnisstrafe, bei der er sich als ausgewähltes Opfer einer Medienkampagne sowie der rigiden US-amerikanischen Rechtsprechung ansah, brilliert er heute mit Krawatte und Anzug. Der Berater gibt Tipps für probate Schutzmaßnahmen in der IT. Er ist korrekt gekleidet und gefragter Gastredner auf Kongressen.

Link: http://www.zdnet.de/39152145/risikofaktor-mensch-die-kunst-des-social-engineering/