Social Engineering

Um an vertrauliche Informationen zu gelangen, nutzen Kriminelle oft die Gutgläubigkeit, Hilfsbereitschaft oder Unsicherheit einer Person aus. Ob fingierte Telefonanrufe, falsche Polizisten oder Phishing-Attacken – Angriffsziel ist beim Social Engineering immer der Mensch. Der beste Schutz ist «gesundes Misstrauen».

Schützen Sie sich vor Social Engineering Angriffen, indem Sie...

- möglichst wenig persönliche Informationen über sich preisgeben. Insbesondere auf Sozialen Netzwerken sollten Sie mit Informationen sehr sparsam umgehen.
- Passwörter oder TAN-Codes grundsätzlich nie einer anderen Person bekanntgeben – auch einem Systemadministrator oder dem Chef nicht. Ein Passwort gehört Ihnen und nur Ihnen!
- bei Anfragen per E-Mail oder Telefon misstrauisch sind. Auch E-Mails von bekannten Absendern und Anrufe von bekannten Telefonnummern können gefälscht sein!

Social Engineering Angriffe haben zum Ziel, Ihnen persönliche oder vertrauliche Informationen (z.B. Zugangsdaten, Passwörter etc.) zu entlocken, um diese dann unbefugt einzusetzen.

Kriminelle versuchen als ersten Schritt möglichst viele Informationen über das Opfer zu sammeln. Denn anhand dieser Informationen lässt sich das Opfer leichter täuschen. Zum Beispiel kann sich der Kriminelle anschliessend als eine Ihnen bekannte Person ausgeben.

Ideal, um an Informationen zu gelangen, eignet sich das Internet. Vor allem Soziale Netzwerke (https://www.ebas.ch/soziale-medien-und-netzwerke/) wie z.B. Facebook, Xing, Instagram etc. beinhalten sehr viele persönliche Informationen. Anhand dieser Daten kann der Angreifer gezielt auf eine Person zugehen und wirkt, dank den gesammelten Informationen, vertrauenswürdig.

Wie können Sie sich effektiv schützen?

Leider gibt es keine technischen Massnahmen, welche vor Social Engineering schützen. Da ein Angreifer menschliche Charaktereigenschaften wie Hilfsbereitschaft, Unsicherheit, Gutgläubigkeit und das grundlegende Vertrauen zu anderen Personen gezielt ausnutzt, ist es sehr schwierig, einen Social Engineering Angriff zu entdecken und abzuwehren.

Generell schützt nur ein «gesundes Mass an Misstrauen» gegenüber fremden – aber auch gegenüber (vermeintlich) bekannten Personen. Oft hilft es auch, sich zu hinterfragen, was man für Informationen von sich Preis gibt, und an wen.

Informieren Sie im Verdachtsfall Ihr Finanzinstitut

Sollte Ihnen bezüglich E-Banking etwas verdächtig vorkommen, geben Sie nichts preis und informieren Sie umgehend Ihr Finanzinstitut. Die Koordinaten finden Sie hier (https://www.ebas.ch/partner/) .

Beispiele von Social Engineering Angriffen

- Eine Person gibt sich als Techniker aus (z.B. einer Telefongesellschaft, eines Elektrizitätswerkes etc.) und ver-

Copyright © 2024 – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

sucht so Zugang in Ihr Haus oder ins Unternehmen zu erlangen.

- Sie erhalten eine E-Mail, welche Sie auffordert einen Link aufzurufen und ein Login zu tätigen oder persönliche Informationen preis zu geben.
- Eine Person ruft Sie per Telefon an und will Ihnen für eine Umfrage gewisse Fragen stellen (z.B. zum Einkommen, zu Sicherheitsmassnahmen am Computer etc.).
- Ein Angreifer fälscht den Absender einer E-Mail und gibt sich so als bekannte Person aus (möglicherweise enthält der Anhang eine Malware).
- Am Arbeitsplatz kommt eine Person, die sich als Informatiker ausgibt und Ihnen vorgaukelt, an Ihrem Computer Unterhaltsarbeiten verrichten zu müssen.
- Social Engineering Angriffe gehen sogar so weit, dass sich Personen gezielt auf eine Stelle in einem Unternehmen bewerben, um dann spezifische Informationen zu stehlen.

Social Engineering ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Technische Schutzmassnahmen existieren nicht. Generell kann daher nur ein gesundes Misstrauen schützen.

Copyright © 2024 – Alle Rechte vorbehalten. Hochschule Luzern – Informatik