«Social Engineering» Information und Prävention

Wie sehen mögliche Social Engineering Angriffe aus?

- Eine Person gibt sich als Techniker aus (z.B. einer Telefongesellschaft, eines Elektrizitätswerkes etc.) und versucht 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. (Phishing)
- Eine Person ruft Sie an und gibt vor eine Umfrage durchzuführen, um an sensitive Informationen (z.B. zum Einkommen, zu Sicherheitsmassnahmen etc.) zu gelangen.
- Zu Ihrem Arbeitsplatz kommt eine Person, die sich als Informatiker ausgibt und Ihnen vorgaukelt, an Ihrem PC Wartungsarbeiten verrichten zu müssen.

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

Schützen Sie sich, indem Sie:

- möglichst wenig persönliche Informationen über sich preisgeben. Insbesondere auf Sozialen Netzwerken wie Facebook, Xing etc. sollten Sie mit Informationen sehr sparsam umgehen.
- Passwörter grundsätzlich NIE einer anderen Person bekanntgeben. Auch einem Systemadministrator oder dem Chef nicht. Ein Passwort gehört Ihnen und NUR Ihnen!
- gegenüber E-Mail-Anfragen misstrauisch sind. Auch E-Mails von bekannten Absendern (Freunden) könnten gefälscht sein.

Social Engineering

Social Engineering ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Um an vertrauliche Informationen zu gelangen, wird sehr oft die Gutgläubigkeit und die Hilfsbereitschaft aber auch die Unsicherheit einer Person ausgenutzt. Von fingierten Telefonanrufen, über Personen die sich als jemand anderes ausgeben, bis hin zu Phishing-Attacken ist alles möglich.

Generell kann nur ein «gesundes» Mass an Misstrauen schützen. Oft hilft es auch zu hinterfragen welche Informationen man von sich preis gibt und gegenüber wem.

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 auf http://www.ebankingabersicher.ch.

Weitere Informationen: www.ebas.ch/socialengineering

«eBanking – aber sicher!» bietet E-Banking-Anwendern nützliche Sicherheitsinfos

eBanking aber sicher!

Auf der kostenlos zu nutzenden Webseite **www.ebankingabersicher.ch** finden Sie weitere praxisnahe Informationen über notwendige Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz