Die Tricks der Datendiebe

Bericht VKÖ

Die X-Werke entwickeln seit sechs Jahren eine – streng geheime – Turbine für Kurzstrecken-Lenkraketen. Eines Tages ruft der Entwicklungsleiter, Dr. V, noch spätabends im Werk an und ersucht den Diensthabenden höflich, aber bestimmt um die Übersendung aller Konstruktionspläne, da er unterwegs sei und daher keinen Zugriff auf seinen PC habe, aber „ganz dringend“ etwas überprüfen müsse.

Einige Tage später gerät das Werk plötzlich unter Beschuss. Ganz zufällig wurden die dabei eingesetzten Raketen nach genau jenen geheimen Bauplänen entwickelt, die im guten Glauben weitergegeben wurden.

Manipulation durch Vertrauensmissbrauch

Keine Frage: Die X-Werke wurden Opfer eines sogenannten Social Engineers.

Mit Social Engineering bezeichnet man eine betrügerische Manipulation, die auf die Beschaffung geheimer Daten abzielt und besonders in den USA zunehmend zur Gefahr wird. Social Engineers nutzen typisch menschliche Verhaltensmuster wie die Mechanismen der Vertrauensbildung für ihre Zwecke aus.

Vertrauen zu Autoritäten kann fatal enden

Unser glücklicherweise nur fiktives Beispiel mit dem Lenkraketen zeigt den klassischen Fall eines solchen Vertrauensmissbrauchs, der darauf basiert, dass wir seit Jahrtausenden darauf konditioniert sind,

Autoritäten zu vertrauen und Freunde bzw. Verbündete zu unterstützen.

Die Frage, ob Dr. V wirklich Dr. V ist, wurde aufgrund dieser Konditionierung entschieden. Soll heißen: Es braucht nur jemand überzeugend genug als Dr. V aufzutreten – und er kann dessen Bekanntheitsgrad und Machtstellung nach Herzenslust missbrauchen ...

Hauptmann von Köpenick

Der Mechanismus der Manipulation durch geschickte Vorspiegelung falscher Tatsachen ist seit eh und je geläufig. Denken wir nur an Friedrich Wilhelm Voigt, einen der berühmtesten Betrüger der Kriminalgeschichte. Der ostpreußische Schuhmacher hatte sich bei einem Trödler eine Unform besorgt.

Als Hauptmann verkleidet, „requirierte“ er am 16.10.1906 kurzerhand zehn Berliner Gardisten. Mit Hilfe dieser Soldaten fuhr er nach Köpenick und beschlagnahmte dort „auf allerhöchsten Befehl“ die Stadtkasse des Rathauses.

Er quittierte die Übernahme des Geldes auch ordnungsgemäß – mit dem Namen des Gefängnisdirektors, bei dem er zuletzt wegen Diebstahls und Urkundenfälschung einsaß.

Dass der dreiste Hochstapler zehn Tage später gefasst wurde, verdankte die Polizei dem Hinweis eines ehemaligen Zellengenossen. Voigt wurde zu vier Jahren Haft verurteilt, doch begnadigte Kaiser Wilhelm II. den „genialen Kerl“, wie er ihn nannte, nach zwei Jahren. Mit der Technik des Social Engineerings werden heutzutage auf oft ähnlich verblüffende Weise brisante Unternehmensdaten beschafft.

Die Mitleidsmasche

Der „blinde“ Bettler, der stets als Erster die am Boden liegende Münze sieht, und seine angeblich ebenfalls grausam behinderten Kollegen

beweisen immer wieder, dass das Spiel mit dem Mitleid bestens funktioniert.

Wir Menschen sind aufgrund unserer biologischen Vergangenheit mitfühlende und solidarisch handelnde Wesen. Nichts ist daher leichter, als diese Eigenschaften zu missbrauchen.

So darf sich der „bemitleidenswerte Passagier“ mit seinem angeblich gebrochenen Bein über ein kostenloses Upgrade auf dem Langstreckenflug freuen. Und der Preis für so ein bisschen Gips ist im Gegensatz zu dem eines Platzes in der ersten Klasse doch wirklich vernachlässigenswert …

Höret die Signale

Wie aber kann man Angriffe durch Social Engineers verhindern?

Die einfachste und zugleich wirksamste Abwehrmethode ist die Sensibilisierung.

Ein altes Sprichwort sagt, dass der bekannte Feind weniger gefährlich sei als der unbekannte Freund. Dies trifft im Bereich Social Engineering in besonderem Maß zu. Mitarbeiter, die auf etwaige Attacken durch SEs vorbereitet sind, lassen sich weniger leicht manipulieren.

Einhalten von Dienstvorschriften

Weiteren Schutz erreicht man durch striktes Einhalten von Dienstvorschriften wie Protokollen, Zugangsberechtigungen und Kontrollen.

Wenn der Zugang zu sensiblen Informationen per Telefon unmöglich ist, kann man einen Großteil etwaiger Angriffe abwehren.

Generell gilt: Je mehr Personen Zugang zu vertraulichen Informationen haben, desto leichter wird es, ein manipulierbares Individuum zu finden.

Verräterischer „Sondermüll“

Zwei weitere besonders interessante „Informationsquellen“ für Social Engineers sind die Website und der Papiermüll eines Unternehmens.

Das omnipräsente komplexe Organigramm aller 50.000 Mitarbeiter mag das Ego des Eigentümers aufbauen – leider hilft es dem Social Engineer beim Ausspionieren wichtiger Fakten der Unternehmenshierarchie.

Kenntnisse geschickt nutzen

Beim Angriff kann er dann seine Kenntnisse geschickt nutzen, wenn er sich z. B. auf den – leider angeblich nicht erreichbaren - Vorgesetzten der Kontaktperson beruft, um seiner Forderung nach der Preisgabe vertraulicher Daten Nachdruck zu verleihen. Und welche Sekretärin lässt sich nicht einschüchtern, wenn ihr Chef dem angeblichen Aufsichtsratsvorsitzenden die prompte Übermittlung brisanter Zahlen oder Fakten versprochen hat?

Die logische Konsequenz für Unternehmen lautet kurz und ergreifend: „take it offline“ – also kein Organigramm oder ähnliche Informationen im Internet.

Besondere Vorsicht

Besondere Vorsicht gilt auch für den Papiermüll. Das sicherste Passwort nützt nichts, wenn es mit schöner Regelmäßigkeit vollständig ausgedruckt im Altpapier landet.

Social Engineers wühlen leidenschaftlich gern in entsorgten Dokumenten. Shredder kosten wenig, machen Spaß und lösen das Problem.

Social Engineering gilt in den USA seit Jahren als zunehmend gefährliche Angriffsart für Industriespionage und sonstige Wirtschaftskriminalität.

Österreich ist hinsichtlich dieser Kriminalität eine Insel der Seligen. Doch der diesbezügliche GAU ist nur mehr eine Frage der Zeit.

Tam Hanna

Literaturtip:

Social-Engineering-Forscher Kevin Mitnick und William Simon, *Die Kunst der Täuschung: Risikofaktor Mensch (2003),* weiter informieren.