MKM + PARTNER
DATENSCHUTZ

TRAU, SCHAU, WEM!

Awareness schaffen: Für viele Unternehmen sind Social Engineering und Visual Hacking erstaunlicherweise immer noch unbekannte Angriffsmethoden von außen.

Autoren: Thilo Märtin, Severin Maier

Wer sich mit dem Schutz von Daten seines Unternehmens und seiner Kunden befasst, der kommt um ein Thema nicht herum: Hacking. Der Angriff auf das eigene IT-System oder das von Drittanbietern genutzte sollte für jeden betrieblichen oder externen Datenschützer ein Thema sein. Und die Abwehr derartiger Angriffe sollte auf der To-do-Liste ganz weit oben stehen. Das gängige Bild des Hackings dürfte immer noch ein technisches sein: Mittels Viren, Rootkits, Trojanern und anderer Malware versucht ein Angreifer, in das IT-System zu gelangen. Doch für erfolgreiche Angriffe braucht es nicht immer Hightech beziehungsweise Technik überhaupt. Zwei besondere Formen des Hackings sind Social Engineering und Visual Hacking. Beide Angriffsmethoden sind im Verhältnis zu ihrem Vorkommen erstaunlich unbekannt. Social Engineering ist die von Angreifern am zweithäufigsten angewandte Methode, um an Unternehmensdaten zu gelangen – 19 Prozent der Angriffe gehen auf das Konto von Social Engineers, wie eine Studie des Verbands BITKOM zeigt. Häufiger ist nur der Diebstahl von IT- oder Kommunikationsgeräten. Das amerikanische Ponemon Institute wiederum führte einen Feldversuch über Visual Hacking durch. Ergebnis: Mitarbeitern des Instituts, die sich als vorübergehende oder externe Angestellte der untersuchten Unternehmen ausgaben, gelang es in 38 von 43 Fällen, nur durch Einsehen von nicht blicksicheren Daten sensible Informationen zu entwenden. 50 Prozent dieser „Visual Hacks“ waren in weniger als 15 Minuten erfolgreich.

MKM + PARTNER
DATENSCHUTZ

Social Engineering

Was ist nun Social Engineering? Die Definitionen hierüber gehen auseinander. Dennoch kann man sich auf eine gemeinsame Basis einigen. Social Engineering ist eine Angriffsmethode, mit der ein Angreifer mittels Manipulation von Menschen versucht, Zugang zu bestimmten Informationsquellen zu erhalten. Für die Manipulation werden gezielt elementare menschliche Eigenschaften beziehungsweise Emotionen genutzt: Autoritätshörigkeit, Stolz auf die eigene Arbeit, Tendenz zur unbürokratischen Hilfe in Notlagen, Vertrauen oder Angst. Diese Liste lässt sich, wahrscheinlich beliebig lange, fortsetzen. Sie verdeutlicht aber schon jetzt ein wichtiges Detail des Social Engineerings: Es handelt sich um eine nicht technische Angriffsmethode. Social Engineers „hacken" primär Menschen und nicht Computer. Dennoch können zur Vorbereitung oder Unterstützung zusätzlich technische Mittel zum Einsatz kommen, wie etwa kompromittierte Mails. In der Regel bilden aber öffentlich zugängliche Informationen die Basis für einen Angriff mittels Social Engineering.

Vorbereitung und Hilfsmittel

Die Vorbereitung ist für einen Social Engineer von enormer Bedeutung. Je mehr Informationen er hat, desto besser kann er sich auf seinen Angriff vorbereiten. Die Vorbereitungen können simpel oder ausgefeilt sein und mit oder ohne (technische) Hilfsmittel ablaufen. Die Basis bilden oftmals öffentlich zugängliche Informationen: Suchmaschinen, Branchenverzeichnisse, Nachrichten, Telefonbücher oder soziale Netzwerke usw. Unterstützt wird die Informationssammlung von profanen und ausgereiften Methoden. Das sogenannte Dumpster Diving (zu Deutsch: Fischen nach Informationen im Müll) fördert häufig brauchbare Informationen zutage – nicht ordnungsgemäß vernichtete Unterlagen, Visitenkarten, Kalender oder Scans. Selbst geschredderte Blätter können wieder zusammengesetzt werden, wenn der Schredder sie nur in Streifen schneidet.

Visual Hacking

Visual Hacking ist ebenfalls eine prinzipiell nicht technische Angriffsmethode. Bei ihr handelt es sich um wirklich simple Methoden, die aber erstaunlich erfolgreich und verbreitet sind. Visual Hacking dürfte wohl die Angriffsmethode mit dem besten Kosten-Nutzen-Verhältnis für den Angreifer sein. Aber warum? Und was ist eigentlich Visual Hacking? Gemeint ist das Erlangen von Informationen durch das Sehen von Dingen, die nicht für die Augen des Angreifers bestimmt sind. Folglich braucht der Angreifer kein technisches Know-how oder keine Geräte.

Visual Hacks lassen sich dadurch kostenneutral durchführen. Grundsätzlich sind zahllose Möglichkeiten und Situationen denkbar, in denen Visual Hacks vorkommen können. Die zwei folgenden dürften vermutlich am häufigsten vorkommen:

1. Shoulder Surfing: Der Angreifer positioniert sich neben oder hinter der Zielperson (beispielsweise im Bahnhof oder im Zug) und sieht den Bildschirm des Smartphones, Tablets, Laptops oder Ähnliches ein.
2. Frei zugängliche Arbeitsplätze: Der Angreifer betritt frei zugängliche Büros und sammelt Informationen, etwa von nicht blicksicheren Bildschirmen, am Arbeitsplatz notierten Passwörtern, nicht verschlossenen Aktenschränken und herumliegenden Dokumenten.

Ausblick

Social Engineering und Visual Hacking sind auch in Kombination denkbar. Beide Methoden sind einfach und effektiv. Die Unternehmen können sich aber auch einfach und effektiv dagegen schützen. Zum einen sollten Schulungen der Mitarbeiter und klare Richtlinien zum Einsatz kommen. Es ist nötig, ein Bewusstsein für diese beiden Angriffsmethoden zu schaffen beziehungsweise die Mitarbeiter im Unternehmen zu sensibilisieren. Da die Basis eines Social-Engineering-Angriffs oftmals öffentliche Informationen sind, sollte zum anderen geprüft werden, welche Informationen öffentlich zugänglich sind und ob dies unbedingt erforderlich ist. Technischen Schutz – vor allem gegen Visual Hacking – bieten Zutrittskontrollen, verschlüsselte Datenträger, versperrte Aktenschränke und Sichtschutzfolien. Wer sichergehen will, lässt sein Unternehmen (regelmäßig) unter realen Bedingungen testen. Bereits ein einmaliger Testangriff durch einen Social Engineer oder Visual Hacker wird Schwachstellen und die Anwendung von Richtlinien aufzeigen sowie das Unternehmen sensibilisieren.

> SCHAFFEN SIE AWARENESS – KEINE ANGRIFFSMETHODE IST ZU BANAL. DIE FOLGEN KÖNNEN SCHWERWIEGEND SEIN.

THILO MÄRTIN: ist Rechtsanwalt und Partner von MKM+PARTNER Rechtsanwälte PartmbB, Nürnberg. Er ist spezialisiert auf Fragen des IT-Rechts, des Datenschutzes sowie gewerblichen Rechtsschutzes.

SEVERIN MAIER: ist Student der Politikwissenschaft und des Öffentlichen Rechts und arbeitet als selbständiger Autor.