Social Engineering & Visual Hacking

Informationen über zwei erstaunlich unbekannte Angriffsmethoden

von RA Thilo Märtin[1] und Severin Maier[2]

Einleitung

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 genutzten Drittanbietern sollte für jeden betrieblichen oder externen Datenschützer ein Thema sein und die Abwehr dieser Angriffe 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 anderen Techniken versucht ein Angreifer in das IT-System zu gelangen.

Doch für erfolgreiche Angriffe braucht es nicht immer High-Tech oder gar Technik überhaupt. Um zwei besondere Formen des Hackings geht es im folgenden Beitrag: das **Social Engineering** und das **Visual Hacking**. Beide Angriffsmethoden sind im Verhältnis zu ihrem Vorkommen erstaunlich unbekannt: Social Engineering ist die von Angreifern am zweithäufigsten genutzte Methode, um an Unternehmensdaten zu gelangen – 19 Prozent der Angriffe gehen auf das Konto von Social Engineers, wie eine Studie des Verbandes BITKOM herausfand. Häufiger ist nur der Diebstahl von IT- oder Kommunikationsgeräten.

Das amerikanische Ponemon Institute wiederum führte einen Feldversuch über Visual Hacking durch. Das 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.

Social Engineering

Was also ist 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 bzw. Emotionen genutzt: Autoritätshörigkeit, Stolz auf die eigene Arbeit, Tendenz zur unbürokratischen Hilfe in Notlagen, Vertrauen oder Angst. Diese Liste ließe sich, wahrscheinlich beliebig lange, fortsetzen. Sie verdeutlicht aber schon jetzt ein wichtiges Detail des Social Engineering: 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

[1] Thilo Märtin ist Rechtsanwalt und Partner bei MKM+PARTNER Rechtsanwälte Nürnberg.
[2] Severin Maier ist Student der Politikwissenschaften sowie des Öffentlichen Rechts und arbeitet als freier Autor.

zum Einsatz kommen, bspw. kompromittierte Mails. In der Regel bilden aber **öffentlich zugängliche** Informationen die Basis für einen Angriff mittels Social Engineering.

Methoden

Einem Social Engineer steht ein vielseitiges Repertoire an Methoden zur Verfügung, um seinen Angriff durchzuführen. Einige dieser Methoden sollen an dieser Stelle vorgestellt werden.

Pretexting

Der bekannte Social Engineer Christopher Hadnagy, selber mit jahrelanger Erfahrung in der IT-Sicherheits-Branche, bezeichnet Pretexting (von engl. *pretext* – Scheingrund, Vorwand, Ausrede) treffend als das Schlüpfen in eine andere Haut. Um Pretexting glaubwürdig durchführen zu können, ist viel Vorbereitung notwendig. Es ist mehr als das bloße Verkleiden oder Lügen an der Pforte – auch wenn dies als Pretexting betrachtet werden kann. Ein erfolgreicher Pretexter erzeugt quasi eine vollkommene Illusion für sein Opfer: Habitus, Kleidung, die Art des Sprechens und mitgeteilte Informationen schaffen ein glaubwürdiges, aber dennoch falsches und nur vorgespieltes, Szenario.

Beispiel: Ein Angreifer macht ein Lokal aus, in dem viele Mitarbeiter des anvisierten Unternehmens mit Geschäftspartnern zu Mittag essen. Er isst selber über einen längeren Zeitraum dort zu Mittag und analysiert Dresscode und Umgangsweise der Angestellten. Zudem erfasst er relevante Gesprächsinhalte über aktuelle Projekte und deren Mitwirkende: aufgetretene Probleme, beteiligte Firmen und die Namen der Mitarbeiter, anstehende Urlaube und Termine. Mit diesem Wissen kann er bei einem Anruf oder Eindringen in die Geschäftsräume seine Beteiligung an dem Projekt glaubhaft vorspielen. Hier ist auch die Macht einer Visitenkarte nicht zu unterschätzen: aus einem nicht nachvollziehbaren Grund wird immer als wahr angenommen, was auf einer Visitenkarte steht.

Prävention: Pretexting stellt weniger eine Angriffsform dar, als das Schaffen eines Szenarios in welchem der Angriff erfolgen soll. Hilfe bieten profane Mittel: fest definierte Abläufe zur Informationsfreigabe oder für Zutritte, idealerweise erfolgen beim Schutz sensibler Informationen mehrere Stufen der Prüfung. Dabei ist wichtig: Egal wie überzeugend ein Gegenüber selbst oder mit seiner Geschichte wirken mag, sind die Leitfäden strikt zu beachten. So können viele Vorfälle verhindert werden. Benötigt man z.B. Passwörter oder Ausweisdokumente zur Informationsfreigabe, erschwert das dem Pretexter den Angriff – denn diese muss er erst bekommen bzw. fälschen. Menschen an solchen Kontrollpunkten sollten sich nicht durch Emotionen oder vorgetäuschten Zeitdruck unter Stress setzen lassen. Es sollte definiert werden, welche Informationen von einer bestimmten Personengruppe wirklich benötigt werden und ob diese freizugeben sind.

Tipp: Sind die Informationen, die Sie schützen wichtig für Ihr Unternehmen, scheuen Sie nicht den Aufwand, solche Situationen zu üben und die verantwortlichen Mitarbeiter zu sensibilisieren.

Nachteil: Ein Nachteil der strikten Leitlinien ist, dass sie unflexibel sind. Bringt der Pretexter die Leitfäden in Erfahrung, kann er sich exakt auf die einzutretenden Abläufe vorbereiten. Um diese in Erfahrung zu bringen, ist eine andere Methode des Social Engineering geeignet: das Elizitieren.

Elizitieren

Elizitieren (von engl. *elicit* – herauslocken, entlocken) meint Reize auf einen Menschen so wirken zu lassen, dass bei ihm ein bestimmtes Verhalten ausgelöst wird – i.d.R. das Mitteilen von Informationen. Die amerikanische National Security Agency definiert Elizitieren als „subtile Extraktion von Informationen während einer offenbar normalen und harmlosen Unterhaltung". Ein Social Engineer ist in der Lage sein Gegenüber so zu beeinflussen, dass dieser von sich aus Informationen mitteilt. Um das zu erreichen gibt es verschiedene Möglichkeiten. Zum Beispiel das Appellieren an das Ego der Zielperson, Bekunden von gemeinsamen Interesse oder absichtlich falsche Aussagen, die Gegenreaktionen provozieren.

Beispiel: Der Angreifer wählt eine Situation mit lockerer Atmosphäre, bspw. eine Abendveranstaltung der lokalen Unternehmervereinigung, an der auch die Zielperson teilnimmt. Bei ein, zwei Cocktails an der Bar erwähnt der Angreifer die Vorteile und besondere Qualität einer bestimmten Datenbank oder eines Programms, die Zielperson stimmt zu (1. Schritt: gemeinsames Interesse). Im nächsten Schritt behauptet der Angreifer, dass eine weitergehende Sicherung von Daten aber nicht möglich sei (2. Schritt: absichtlich falsche Aussage). Die Zielperson widerspricht und klärt bereitwillig auf (3. Schritt: Elizitieren von Informationen). Durch die Kombination von Schritt 1 und 2 erzeugt der Angreifer sogar das Gefühl, dass die Zielperson in dem Gebiet gemeinsamer Interessen kompetenter ist.

Prävention: Auch hier können Leitfäden und definierte Abläufe helfen, speziell für Situation außerhalb des Arbeitsplatzes, z.B. Messen, Veranstaltungen, Fortbildungen usw. Was darf gesagt werden? Welche Details dürfen erwähnt werden?

Nachteil: Lassen die Leitfäden zu wenig Freiraum, wirkt wohl fast jedes informelle Gespräch unnatürlich und steht der eigenen Informationsgewinnung im Weg.

Tipp: Besonders das Abwehren von Fragen sollte geübt werden. Dazu ist es nötig diese als solche zu erkennen und sodann ggf. mit diplomatischem Fingerspitzengefühl zu umgehen. Alternativ kann dies auch geradeheraus geäußert werden: „Es tut mir leid, aber über diese Angelegenheiten kann ich mich nicht so ausführlich äußern".

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, soziale Netzwerke usw. Unterstützt wird die Informationssammlung von profanen und ausgefeilten Methoden: das sog. **dumpster diving** (zu Deutsch: das Fischen nach Informationen im Müll) fördert regelmäßig brauchbare Informationen zu Tage – nicht ordnungsgemäß vernichtete Unterlagen, Visitenkarten, Kalender oder Scans. Selbst geschredderte Blätter können wieder zusammengesetzt werden, wenn der Schredder sie nur in Streifen schneidet.

Beispiel: 2014 wurden in Berlin zwei Baucontainer mit Büro-Ordnern gefunden. In den Ordnern fanden sich nicht vernichtete Unterlagen zum Flughafen BER: detaillierte Baupläne und Grundrisse sowie Kontrollberichte. Einen solchen Fund könnte man für einen Angreifer, der sich Zutritt zu Sicherheitsbereichen verschaffen will, wohl als Jackpot bezeichnen.

Technische Hilfsmittel können GPS-Tracker zum Lokalisieren der Zielperson, Keylogger auf dem Rechner der Zielperson zum Abgreifen von Passwörtern oder Werkzeuge zum Öffnen von Türen sein, z.B. Dietriche oder sog. White Plastics – Magnetkarten zum Beschreiben mit Zugangsdaten.

Prävention: Passwörter in regelmäßigen Abständen ändern, bestimmte Passwortstärken verwenden, keine USB-Sticks unbekannter Herkunft nutzen, keine unbekannten oder unangemeldeten IT-Techniker an die Systeme lassen.

Tipp: Öffnen Sie keine Email-Anhänge von unbekannten Personen! „Das tut doch heute keiner mehr", werden Sie vielleicht sagen. Aber sensibilisieren Sie sich selbst für ungewöhnliche Situationen: Was machen Sie, wenn ein potenzieller Kunde anruft, Ihnen einen attraktiven Großauftrag in Aussicht stellt und noch während des Gesprächs ein PDF dazu sendet – öffnen Sie dieses völlig unkritisch? Oder sind Sie vorsichtig und überprüfen es trotz Virenscanner noch einmal separat? Auf diese Art und Weise handelt man sich schnell einen Keylogger ein, der wichtige Passwörter und Benutzernamen nach außen transportiert.

Wie könnte ein Social Engineer-Angriff aussehen?

Social-Engineer-Angriffe sind in der Regel nicht sofort zu erkennen, speziell wenn sich der Angreifer durch öffentlich zugängliche Informationen oder (durch eventuell zuvor ausgeführte Angriffe oder ehemalige Unternehmenszugehörigkeit erlangte) interne Informationen entsprechend vorbereitet hat. Ein Angriff könnte folgendermaßen aussehen:

- Der Angreifer recherchiert in öffentlichen Quellen und an zugänglichen Plätzen, um Informationen über sein Ziel zu ermitteln.
    - Auf Xing findet er von Mitarbeitern die Unternehmenszugehörigkeit, Dauer der Anstellung, Name und Ausbildung und eventuell Vorgesetzte heraus.
    - Mittels der Google-Suche lässt sich unter Umständen die Durchwahl zum Vorzimmer herausfinden. So umgeht er die Zentrale und kann behaupten, die Durchwahl bei früheren Kontakten erhalten zu haben. Damit schafft er zusätzlich Vertrauen.
    - Auf Facebook erfährt der Angreifer eventuell private Informationen des Ziels, z.B. Hobbies, Sportarten oder Vorlieben. Die kann er nutzen, um Gemeinsamkeiten mit dem Ziel vorzutäuschen.
    - Im Papiermüll findet sich ein Lieferschein eines IT-Dienstleisters, der Hardware geliefert hat.
- Der Angreifer gibt sich am Telefon als eine bestimmte Person aus, bspw. als System-Administrator des IT-Dienstleisters. Da er im Internet die Unternehmensgröße recherchiert hat weiß er, dass das Vorzimmer nicht alle externen Dienstleister kennen wird.

- Durch einen schon früher getätigten Anruf ist dem Angreifer bekannt, dass das Management für ein paar Tage nicht im Haus ist.
- Der Angreifer täuscht vor, Angestellter des externen IT-Dienstleisters und von einem Manager beauftragt zu sein, technische Probleme zu lösen. Um diese zu beheben müsste er aber noch Einstellungen per Fernzugriff auf dem Computer des Managements anpassen.
- Die Zweifel des Vorzimmers räumt er durch das Schüren von Angst aus dem Weg: Wenn er nicht per Fernzugriff arbeiten kann, finde das Management bei der Rückkehr kein funktionsfähiges System vor, die Reparatur verzögere sich um einige Tage. Zudem würde er Probleme mit seinem Chef bekommen, wenn er das Problem heute nicht behebe. Außerdem könne das Vorzimmer ja parallel sehen, was er auf dem Rechner mache.

- Das Vorzimmer willigt ein, der Angreifer erhält Zugriff auf den Computer des Managements, der Angriff ist erfolgreich.

Visual Hacking

Visual Hacking ist ebenfalls eine prinzipiell **nicht-technische** Angriffsmethode. Bei ihr handelt es sich um eine wirklich **simple** Vorgehensweisen, 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?

Visual Hacking ist einfach erklärt. Es meint 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 Geräte. Visual Hacks lassen sich dadurch kostenneutral durchführen.

Methoden

Grundsätzlich sind zahllose Möglichkeiten und Situationen denkbar, in denen Visual Hacks vorkommen können. Auch Kombinationen aus bspw. Social Engineering und Visual Hacking sind denkbar. Die zwei folgenden dürften vermutlich am häufigsten vorkommen:

- Shoulder Surfing: Der Angreifer positioniert sich neben oder hinter der Zielperson (bspw. am Bahnhof oder im Zug) und sieht den Bildschirm des Smartphones, Tablets, Laptops o.ä. ein.

- Offen zugängliche Arbeitsplätze: Der Angreifer betritt offen zugängliche Büros und sammelt Informationen, bspw. von nicht blicksicheren Bildschirmen, am Arbeitsplatz notierten Passwörtern, nicht verschlossenen Aktenschränken und herumliegenden Dokumenten.

Beispiel: Der Manager eines Unternehmens nutzt die Bahn für eine Geschäftsreise. Durch ein vorhergehendes Telefonat mit dem Vorzimmer weiß der Angreifer den Abreisetag und dass der Manager die Bahn nutzt. Auf der Homepage des Unternehmens hat der Angreifer ein Foto gefunden und lädt dieses auf sein Smartphone, um die Zielperson am Bahnhof identifizieren zu können. Er

besteigt denselben Zug und setzt sich neben seine Zielperson, die während der Fahrt mit dem Laptop arbeitet. Ohne Sichtschutzfolie kann der Angreifer wichtige Informationen einsehen.

Prävention: Alle Bildschirme sollten mit Sichtschutzfolien ausgestattet werden (Bedenken Sie: die Folie schützt nur in bestimmten Winkeln!). Achten Sie auf Ihre Umgebung: Vermeiden Sie die Bearbeitung sensibler Daten in allzu großer Öffentlichkeit. Am Arbeitsplatz sollten Richtlinien festlegen, wo Akten abgelegt werden dürfen, wann welche Akten zu vernichten sind, Aktenschränke sind zu verschließen – dies gilt insbesondere für Bereiche mit Publikumsverkehr (Wer hat noch nicht eine Reihe von Patientenakten beim Arzt auf dem Anmeldetresen liegen sehen?). Im Unternehmen sollte eine Clean Desk Policy eingeführt werden, d.h. keine nicht gebrauchten oder sensiblen Informationen auf Schreibtischen liegen lassen bzw. auf dem Startbildschirm verknüpfen. Bildschirme sperren, wenn niemand am Arbeitsplatz ist. Ordner in der Datenablage, die sensible Informationen beinhalten, mit Passwörtern schützen. In der Öffentlichkeit sollte die Bildschirmhelligkeit reduziert werden, um Angreifern Blicke zu erschweren.

Fazit

Social Engineering und Visual Hacking sind Low-Tech oder Non-Tech Angriffe, einfach und effektiv. Unternehmen können sich aber auch einfach und effektiv dagegen schützen. Zum einen sollten Schulungen der Mitarbeiter und klare Richtlinien zum Einsatz kommen. **Schaffen Sie Awareness für diese beiden Angriffsmethoden, sensibilisieren Sie ihr Unternehmen**. Da die Basis eines Social Engineering-Angriffs oftmals öffentliche Informationen sind, sollte 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, der testet sein Unternehmen (regelmäßig) unter realen Bedingungen. Lebensmittel-Discounter bspw. führen regelmäßig „Probe-Ladendiebstähle" durch, um das eigene Personal zu testen. Bereits ein einmaliger Test-Angriff durch einen Social Engineer oder einen Visual Hacker wird Schwachstellen und die Anwendung von Richtlinien aufzeigen und das Unternehmen sensibilisieren.

Weitere Informationen zu Methoden, Tools und Sensibilisierung für dieses Thema finden sich unter http://www.social-engineer.org (englisch).