

Einfallstor Mensch: Warum Social Engineering ein nicht zu unterschätzender Risikofaktor im Unternehmen ist

Cyberkriminelle beeinflussen Mitarbeiter des Unternehmens und dringen so in das Firmennetzwerk ein

Bochum (Deutschland), 5. März 2018

Im Jahr 2017 gab es im Mittel jede Minute 16 neue Malwaretypen für den Computer. Das fanden Analysten der G DATA Software AG heraus. Kriminelle aus dem Internet bedienen sich aber auch anderer perfider Tricks, um durch Manipulation von Mitarbeitern, im Fachjargon Social Engineering genannt, an vertrauliche Informationen des Unternehmens zu gelangen. G DATA zeigt worauf IT-Verantwortliche achten müssen.

Unternehmen fokussieren sich meistens auf den Schutz vor spezifischen Angriffsvektoren, die auf das Firmennetzwerk zielen. Angefangen bei Malware wie Ransomware, Trojaner, Viren, über Fehlkonfigurationen der Systeme bis hin zu DDOS-Attacken. Eine Schwachstelle, die von IT-Security-Verantwortlichen als Einfallstor häufig unterschätzt wird: Social Engineering.

Social Engineering: Cyberkriminelle lassen die Puppen tanzen

Längst sind die Tage vorbei, an denen Mitarbeiter in Personalabteilungen kryptische E-Mail-Bewerbungen von vermeintlichen Interessenten erhalten. Eine schlechte Grammatik oder Rechtschreibfehler haben früher als Indikator für eine unseriöse oder gefährliche Nachricht ausgereicht. Heutzutage bereiten sich Cyberkriminelle auf einen Angriff besser vor, denn auch sie haben dazugelernt. Laut Erkenntnissen aus der Studie „Social Engineering Attack Framework“ gibt es sechs Schritte, die ein solcher Angriff durchläuft:

- Schritt 1: Angriffsformulierung
- Schritt 2: Sammeln von Informationen
- Schritt 3: Vorbereitung
- Schritt 4: Beziehung herstellen
- Schritt 5: Beziehung manipulieren
- Schritt 6: Debriefing

Ein gutes Beispiel ist ein Recruiter eines Unternehmens, der häufig auf Social-Media-Plattformen zugreift, um nach geeigneten Bewerbern zu suchen. Scouting lautet das Stichwort. Scheint ein geeigneter Kandidat gefunden zu sein, so wird mit ihm Kontakt aufgebaut. Auch Kriminelle wissen das und erstellen sich Fake-Profilen, mit denen sie im passenden Moment mit dem Personalverantwortlichen in Kontakt treten. Der Täter versucht sich Informationen über den HR-Angestellten zu verschaffen bevor er Vertrauen bei seinem Gegenüber aufbaut und sendet ein Bewerbungsschreiben, bezugnehmend auf die sympathische Konversation über Social Media, an den HR-Angestellten. Dieses Konzept ist erfolgsversprechender, als initiativ eine standardisierte Bewerbung zu verfassen. Darin enthalten: Ein kurzer und knapper Text sowie ein Bild- und ein PDF-Anhang. Die E-Mail sowie die Anhänge werden geöffnet und die Malware auf dem Computer ausgespielt. Der Angreifer hat den Mitarbeiter folglich zum Öffnen der Dateien beeinflusst. Dahinter kann sich eine Ransomware befinden, bei der wichtige Dateien verschlüsselt werden und ein Lösegeld zum Entschlüsseln eingefordert wird. Das kann aber auch ein Trojaner sein, der die Tastaturanschläge aufzeichnet und an den Angreifer zurücksendet. In anderen Worten: Anmeldepasswörter

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Social Engineering verursacht finanzielle Schäden

Social Engineering wird überall dort eingesetzt, wo Menschen beeinflusst werden können und ein passender Schlüssel Geld für den Angreifer verspricht. Das können sowohl wertvolle Mitarbeiter-Informationen sein, direkte Zugangsdaten oder Zugriff zu geheimen Dokumenten, die ein Betriebsgeheimnis preisgeben. Laut einer [Studie des IT-Branchenverbands Bitkom von 2017](#) verursacht die digitale Spionage, Sabotage oder Datendiebstahl deutscher Unternehmen jedes Jahr einen Schaden von rund 55 Milliarden Euro. Da der Trend dieser Angriffsart aber an Beliebtheit gewinnt und somit steigt, ist inzwischen mit höheren Schadenssummen zu rechnen. Die Lösung gegen dieses Angriffsszenario sind Awareness-Trainings für Mitarbeiter.

Worauf müssen IT-Verantwortliche achten?

Der erste Schritt ist es, als IT-Verantwortlicher seine Mitarbeiter für Social Engineering zu sensibilisieren. Diesen Service bietet beispielsweise die G DATA Advanced Analytics an, ein Tochterunternehmen der G DATA Software AG. Mit einem Awareness-Training können Angriffe dieser Art leichter erkannt und verhindert werden. Beispielsweise lernen Mitarbeiter dort, dass E-Mails kritisch begutachtet werden sollen, am Telefon keine sensiblen Daten preisgegeben werden sollten und keine Links zu öffnen sind, die beispielsweise auf eine Login-Seite führen.

Ein weiterer, ebenso wichtiger Schritt ist [eine gute Sicherheitssoftware](#), die einen Phishing-Schutz bereitstellt. Viele Angriffe lassen sich so bereits im Vorfeld abfangen. Dadurch werden die Mitarbeiter deutlich entlastet und relevante E-Mails, die auch für die tägliche Arbeit wichtig sind, werden schneller bearbeitet. In anderen Worten: Das Risiko wird minimiert, auf einen Social-Engineering-Angriff hereinzufallen, der finanzielle Schäden verursachen könnte.

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299