NTT Security ermittelt das Sicherheitsrisiko von Geschäftsleitungen

Management Hack – wie schlimm ist es?

NTT Security erweitert seine umfangreiche Angebotsreihe um den «Management Hack». Mit dem Einsatz spezieller Social-Engineering-Techniken wird dabei überprüft, inwiefern Führungskräfte selbst ein Sicherheitsrisiko darstellen.

Technische IT-Sicherheitssysteme sind immer nur so stark wie ihr schwächstes Glied – dabei geht es nicht nur um neue Technologien und Softwarelösungen, sondern auch um den «Risikofaktor Mensch». Die Minimierung dieser potenziellen Schwachstelle durch die Schulung der Security Awareness und Etablierung unterstützender technischer Lösungen muss immer ein wichtiger Baustein einer präventiven Sicherheitsstrategie sein.

Die «Schwachstelle Mensch»

Wie es konkret um die «Schwachstelle Mensch» für die IT-Sicherheit eines Unternehmens bestellt ist, ermittelt NTT Security im neuen «Management Hack». Im Fokus steht dabei die Führungsebene eines Unternehmens, das heisst der gesamte C-Level wie CEO, CFO oder CIO. Die Management-Ebene ist ein attraktives Ziel für jeden Hacker, da dieser Personenkreis in der Regel uneingeschränkten Zugriff auf vertrauliche Unternehmensdaten geniesst. Nicht selten profitieren Manager auch von besonderen Privilegien: So werden Sicherheits-Policies und -Standards ausgesetzt oder aufgelockert, um zum Beispiel das Login zu vereinfachen – mit fatalen Folgen.

Nach entsprechender Abstimmung mit dem Auftraggeber – in der Regel mit dem CISO oder dem Leiter des IT-Betriebs – werden simulierte, personalisierte Social-Engineering-Angriffe durchgeführt, von denen die im Fokus stehenden Personen im Idealfall nichts wissen. Dabei wird analysiert, wie verantwortungsbewusst die Managementebene in Sachen Security Awareness und IT-Sicherheit ist. Im Anschluss werden konkrete Schwachstellen aufgezeigt und Massnahmen, wie zum Beispiel Security-Awareness-Schulungen, empfohlen.

Allgemein umfasst das Service-Angebot des «Management Hack» von NTT Security die Überprüfung der IT-Sicherheit, der physischen Sicherheit (Objektschutz) und die Analyse von mensch-

lichem Fehlverhalten. Konkret nutzt der Sicherheitsspezialist hierzu unter anderem Social-Engineering-Techniken wie Phishing und das personalisierte Spear-Phishing in Kombination mit Malware- oder Brute-Force-Angriffen auf Passwörter.

Social-Engineering-Angriffe simulieren

Die Simulation eines Social-Engineering-Angriffs erfolgt beispielsweise in folgenden Schritten:

- Aufbau einer Phishing-Webseite, die eine Kunden- oder eine dem Kunden bekannte Webseite simuliert
- Gestaltung einer Phishing-Mail, die auf die Phishing-Webseite leitet
- Versand der Phishing-Mails an das Management des Auftraggebers
- Abfangen von Login-Informationen oder anderen vertraulichen Daten
- Erstellung eines detaillierten Reports mit Statistiken zur aktuellen Sicherheitslage und Massnahmenempfehlungen zur Verbesserung der Sicherheit

Erstaunliche wie erschreckende Ergebnisse

Mehrere solcher «Management Hack»-Projekte hat NTT Security bereits in Skandinavien durchgeführt. «Die Ergebnisse haben selbst uns überrascht. So erhielten wir vielfach in nur zehn Minuten Zugriff auf unternehmenskritische Daten, etwa Business-Pläne, M&A-Planungen, Warenwirtschaftssysteme, Domain-Controller, User-Namen oder Passwörter. Auch administrative Zugangsdaten wurden oft gefunden», erklärt Kai Grunwitz, Senior Vice President EMEA bei NTT Security. «Die damit verbundenen Gefahren für ein Unternehmen liegen auf der Hand. So kann sich ein Angreifer mit Administratorrechten frei im Netzwerk bewegen und oft für lange Zeit unbemerkt auf kritische Informationen zugreifen.»

Erhöhung des Sicherheitsbewusstseins

Der neue Service von NTT Security zielt auf eine Erhöhung des Sicherheitsbewusstseins auf Vorstands- und Geschäftsleitungsebene ab – letzten Endes aber auch auf die Etablierung einer neuen Sicherheitsstrategie und -kultur im gesamten Unternehmen. «Unsere ersten Projekte haben gezeigt, dass auf Unternehmensseite durchaus Handlungsbedarf besteht», so Grunwitz. «Der Reifegrad in Bezug auf Cyber-Security ist auf Managementebene, vorsichtig ausgedrückt, noch eher gering ausgeprägt.»

Im Anschluss an die Tests analysiert NTT Security in Workshops gemeinsam mit dem Kunden die Ergebnisse. Auf Wunsch unterstützt NTT Security dann das Unternehmen bei der Konzeption und Umsetzung einer umfassenden Sicherheitsstrategie, welche auch die Führungsebene einbezieht und zukünftig vor etwaigen Social-Engineering-Angriffen zuverlässig schützt.

Weitere Informationen

zum «Management Hack» von NTT Security finden sich unter www.nttsecurity.com/de-ch/management-hack-service