Security Awareness: Mit Schulungen stärken Sie das IT-Sicherheitsbewusstsein Ihrer Mitarbeiter.

Faktor Mensch in der IT-Sicherheit – Teil 2: Security Awareness – Stärken Sie das IT-Sicherheits-bewusstsein Ihrer Mitarbeiter

Im ersten Teil dieser kleinen Serie zum Thema IT-Sicherheit wurde bereits darauf hingewiesen, dass neben wichtigen technischen Maßnahmen zur IT-Sicherheit vor allem der Faktor Mensch als das schwächste Glied in der gesamten Sicherheitskette eine gewichtige Rolle spielt. Die beste Technik nützt also nichts, wenn statt der Technik der menschliche Benutzer durch sogenannte Social Engineering- oder Human Hacking-Angriffe manipuliert wird. Angreifer finden es offensichtlich einfacher, das Vertrauen von Personen auszunutzen als sich in technisch sichere IT-Systeme zu hacken.

Während im ersten Teil der Serie der sichere Umgang mit E-Mails als ein konkreter Baustein zu mehr Sicherheitsbewusstsein im Focus stand, stehen jetzt umfassendere Security Awareness-Schulungen im Mittelpunkt. Diese Schulungen sollten einen essentiellen Bestandteil Ihrer Gesamtstrategie zur IT-Sicherheit in Ihrem Unternehmen sein.

Social Engineering – Die Kunst der Täuschung

Forscher gehen davon aus, dass ca. 80 Prozent der menschlichen Entscheidungen gefühlsbasiert getroffen werden. Der menschliche Verstand hat demnach in vielen Fällen wenig Mitspracherecht. Und genau diesen Umstand nutzt Social Engineering bzw. Human Hacking aus. Das Angriffsziel sind also nicht die IT-Systeme, sondern deren Benutzer, um diesen sensible Informationen zu entlocken oder sie zu sicherheitskritischen Handlungen zu verleiten. Dies stellt oftmals die erste Phase einer größeren Cyber-Attacke dar.

Zu den wichtigsten und gleichzeitig ungünstigsten Persönlichkeitsmerkmalen, die ausgenutzt werden, zählen Hilfsbereitschaft, Unerfahrenheit, Gutgläubigkeit, Neugier, Gier oder der Wunsch nach Liebe. Je genauer die potentiellen Opfer im

Human Hacking - Angriffsziel ist der Menschen, um ihm sensible Informationen zu entlocken und ihn zu sicherheitskritischen Handlungen zu verleiten.

Vorfeld ausspioniert werden, desto größer sind anschließend die Erfolgsaussichten. Eine Studie hat gezeigt, dass alleine durch eine personalisierte Anrede in einer gefälschten Mail die Erfolgsquote zum Öffnen eines gefährlichen Links oder eines verseuchten Dateianhangs von 20 Prozent auf 56 Prozent steigen kann. Hilfreich für Human Hacker sind in diesem Zusammenhang vor allem die sozialen Medien wie Facebook und Twitter. Wer in diesen Medien viel Privates preisgibt, braucht sich über entsprechend vertraulich anmutende Mails nicht zu wundern.

Während die meisten Angriffe über gefälschte Mails und Webseiten laufen und dabei vor allem die Unerfahrenheit der Benutzer ausnutzen, zielen beispielsweise auf dem Mitarbeiterparkplatz scheinbar zufällig liegen gelassene und manipulierte USB-Sticks auf die menschliche Neugier ab.

Prominente Beispiele für erfolgreiche Social Engineering-Angriffe sind täglich der Presse zu entnehmen. Zu den spektakulärsten Fällen gehört beispielsweise der Angriff auf Hillary Clinton in deren Wahlkampf um die amerikanische Präsidentschaft. Damals fiel ihr Wahlkampfmanager auf eine gefälschte Mail herein und gab die Zugangsdaten zu ihrem Postfach preis. In der Folge wurden zahlreiche Mails von Hillary Clinton veröffentlicht.

Security Awareness-Schulungen als essentieller Baustein für mehr IT-Sicherheit

Wenn technische Maßnahmen alleine also höchstens ausreichen, um IT-Systeme zu schützen, nicht aber deren menschliche Benutzer, bedarf es zusätzlicher Maßnahmen. Dies sind sogenannte Security Awareness-Schulungen, um das Sicherheitsbewusstsein aller Mitarbeiter regelmäßig zu schulen und das richtige Abwehrverhalten im Angriffsfall anzutrainieren.

Solche Schulungen können klassische „Klassenraumschulungen" sein oder auch online erfolgen. Wichtig in beiden Fällen ist aber eine Teilnehmerquote nahe 100 Prozent.

Social Awareness - regelmäßige Schulungen trainieren den Mitarbeitern das richtige Abwehrverhalten an.

Die Inhalte der Security Awareness-Schulungen können vielfältig sein, müssen regelmäßig wiederholt und immer wieder an neue Angriffsmuster angepasst werden.

Mitarbeiter sollten lernen…

- Internet-Adressen (URL) richtig zu verstehen und im Zweifelsfall zu misstrauen,
- mit Mails generell skeptisch umzugehen, den vermeintlichen Absendern gegebenenfalls zu misstrauen, auf die Anrede zu achten, Nötigungen oder Drohungen zu ignorieren und vor allem Links in Mails am besten zu ignorieren, da das tatsächliche Ziel dieser Links ganz einfach zu verschleiern ist,
- sichere Kennwörter zu benutzen (siehe Infobox),
- den Bildschirm beim Verlassen des Büros zu sperren und auch
- im privaten Umfeld die gleichen Vorsichtsmaßnahmen walten zu lassen.

Social Engineering-Audit als Weckruf für das eigene Unternehmen

In vielen Fällen konzentrieren sich aber die Bemühungen der Unternehmen um mehr IT-Sicherheit leider immer noch ausschließlich auf technische Maßnahmen. Weniger aus Unwissenheit, vielmehr aus einem trügerischen Gefühl der Sicherheit vernachlässigen viele Organisationen dieses wichtige Thema Security Awareness. Es bedarf also offensichtlich einer besonderen Motivation bzw. eines entsprechenden Weckrufs. Dieser Weckruf kann im Rahmen eines sogenannten Social Engineering-Audits erfolgen. Dieses Audit zeigt auf, wie es tatsächlich um das IT-Sicherheitsbewusstsein im Unternehmen steht. Das Audit erbringt dabei in der Regel den Beweis, dass eben doch nicht alle Mitarbeiter mit den Gefahren vertraut sind, die von Social Engineering ausgehen.

Die Aufgabe lautet also, mit klassischen Social Engineering-Methoden die Erfolgswahrscheinlichkeit eines echten (bösartigen) Angriffs einzuschätzen. Dieser simulierte Angriff durch die (guten) Auditoren kann dabei per Mail, vor Ort am Unternehmenssitz und/oder per Telefon erfolgen. Ziel des Angriffs sollten möglichst viele Mitarbeiter sein, um eine gute Einschätzung des durchschnittlichen Gefahrenpotentials zu erlangen.

Um das Ergebnis nicht zu verfälschen, ist es wichtig, keine Insiderinformationen zu verwenden. Die Auswertung des simulierten Angriffs erfolgt anonym ohne jeglichen Hinweis auf die Mitarbeiter und deren positives oder negatives Verhalten. Im Anschluss werden alle erhobenen Daten wieder vollständig gelöscht.

Sie möchten noch mehr für die IT-Sicherheit in Ihrem Unternehmen tun? Die INFOSERVE GmbH berät Sie gerne zu technischen und organisatorischen Maßnahmen. Wir stellen Ihr Unternehmen mit einem umfassenden IT-Sicherheitskonzept von der Analyse der IST-Situation über die Bereitstellung der entsprechenden Sicherheitsinfrastrukur bis hin zur Awareness-Schulung auf sichere Füße. ■

INFOSERVE
>eurodata-Gruppe