Awareness gegen Cyber-Attacken

Jeden Tag erreichen uns über die verschiedensten Medien Mitteilungen und unterschiedlichste Nachrichten (Xing, LinkedIn usw.) über Cyber-Attacken. Neben monetären und Reputationsschäden kommt es dabei vor allem zu Daten- und Informationsverlusten. Die Frage ist: Wie kann es sein, dass Dritte die an sich hohen Sicherheitsvorkehrungen einer Bank überwinden?

Bei den Daten- und Informationsverlusten kann es sich sowohl um vertrauliches unternehmensbezogenes Datenmaterial als auch um Daten von Mitarbeitern und dritten Personen handeln. Begründeter Weise drängt sich die Frage auf, wie so etwas denn überhaupt passieren kann. Schließlich sind komplexe Sicherheitsvorkehrungen mittlerweile gelebte Praxis. So gehören in Organisationshandbüchern umfangreiche Passwortrichtlinien und Schulungskonzepte ebenso zum Standard wie technisch hoch entwickelte Firewalls und ein kontinuierliches Patchmanagement.

Hinter all den technischen Sicherheitsvorkehrungen gibt es eine weitere Verteidigungslinie, die durch die Mitarbeitenden selbst gebildet wird. So schützt jeder Mitarbeiter seinen Arbeitsplatz beispielsweise mit seinem individuellen Passwort, das kein anderer kennt und das auch niemandem gegenüber kommuniziert werden darf. Doch der Alltag sieht anders aus: Der Administrator möchte Ihre Benutzerdaten; Sie geben diese weiter. Doch tatsächlich war der „Administrator“ nicht „Ihr“ Administrator von Ihrer Bank. Und: Der wahre Administrator würde auch niemals nach Ihrem Passwort fragen. Bereits diese kleine Unachtsamkeit reicht aus, um den Datenhaushalt einem unkalkulierbaren Risiko auszusetzen. Dass so etwas nur „jemand anderem“ passieren kann, ist leider ein weit verbreiteter Irrtum.

Der unerwartete Moment, die kleine Unaufmerksamkeit

Die hoch technologisierten und entwickelten Sicherheitsvorkehrungen können nicht alle Einfallstore für Kriminelle absichern. Das ist diesen sehr bewusst und sie nutzen diese Tatsache zu ihrem Vorteil. So wie technische Schwachstellen direkt angegriffen werden, wird auch der kleinste Moment der menschlichen Unachtsamkeit direkt ausgenutzt. Ein greifbares Beispiel ist der Straßenverkehr. Hier wissen wir, wie oft und wie schnell man sich ablenken lässt und kurz unachtsam wird. Auch hier kann ein kleiner Moment entscheidend sein.

Dieser kleine, kurze und unerwartete Moment macht uns angreifbar. Damit repräsentiert er den Hauptaktionsbereich der Awareness. Awareness bedeutet in diesem Sinne, dass sich Banken und insbesondere die Mitarbeitenden ein Bewusstsein für diesen kurzen Moment der Unachtsamkeit und die damit verbundenen Risiken erarbeiten und nachhaltig etablieren. Awareness heißt damit nichts anderes als die Schärfung des Bewusstseins für betrügerische Handlungen.

Dieses Bewusstsein ist durch entsprechende Maßnahmen aktiv zu schaffen und einzuüben. Im BSI Standard 200-4, der sich mit dem Business Continuity Management (BCM) befasst, welches sich mit Notfall- und Krisensituationen beschäftigt, heißt es dazu: „Zudem erhalten sie In-

formationen direkt von Führungskräften sowie im Rahmen von Schulungen und Awareness-Maßnahmen."

Eine Frage der Unternehmenskultur

In der Folge wird ersichtlich, wie eng Awareness-Maßnahmen und Notfallmanagement zusammenhängen und wie wichtig es ist, dass beide Bereiche fester Bestandteil der Unternehmenskultur werden:

Sowohl BCM als auch Awareness betreffen grundsätzlich das gesamte Institut und haben in Konsequenz Auswirkungen auf jeden Mitarbeiter. Auch thematisch sind die bestehenden Notfallprozesse mit den Notfallübungen und den daraus resultierenden nachhaltigen Awareness-Maßnahmen und -Prozessen eng zu verzahnen. So sollte auch die Personalabteilung bei allen Entscheidungen und Maßnahmen im Kontext BCM involviert werden, die wesentlichen Einfluss auf die Rechte und Pflichten der Mitarbeiter haben. Daneben kann das Personalmanagement bei der Planung von Schulungen und Awareness-Maßnahmen unterstützen, um die Integration in die Kultur der Institution zu erhöhen.

Auch in einem anderen Informationssicherheitsstandard, der ISO/IEC 27001, Maßnahme A 7.2.2, ist Folgendes niedergeschrieben:

„Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, bekommen ein angemessenes Bewusstsein durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind."

Regelmäßige Übungen, Schulungen und insbesondere regelmäßige Informationen an die Mitarbeitenden sind also unerlässliche Maßnahmen, die in der Bank verankert sein müssen.

Im Rahmen einer Dreijahresplanung ist ein jährlicher Übungsplan aus unserer Sicht unerlässlich.

Schlussendlich sind in der BAIT II Tz. 4.9 folgende Regelungen und Maßnahmen dokumentiert:

„Weiterhin ist innerhalb der Bank durch ein kontinuierliches und zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm das Bewusstsein der Beschäftigten für Informationssicherheit zu schärfen und dabei insbesondere auf die Eigenverantwortung sowie auf die grundsätzlichen Vorkehrungen und Regelungen der Bank einzugehen."

Über alle Regelungen, Vorschriften und Empfehlungen ist zusammenfassend zu sagen, dass es in Zukunft eine ganzheitliche, prozessuale und individuelle Planung der Awareness-Maßnahmen benötigt. Diese Maßnahmen sind zentral zu installieren, durchzuführen, zu messen und schlussendlich zu überwachen.

Eine Bank benötigt demnach ein ganzheitliches Maßnahmenprogramm, das alle Themeninhalte berücksichtigt und dabei insbesondere den Menschen in den Fokus setzt. Denn tatsächlich sind 95 % aller Cybersicherheitsvorfälle auf menschliche Unachtsamkeit zurückzuführen (Quelle: World Economic Forum – The Global Risks Report 2022).

AwarenessCircle

Die Aufgabe ist also, technologisierte Prozesse in Einklang mit den Anwendern und deren Aufmerksamkeit zu bringen – und zwar dauerhaft bzw. wiederkehrend. Diese Anforderungen aufnehmend haben wir – basierend auf unseren Erfahrungen bei 180 Mandaten im Bereich Informationssicherheit/Notfallmanagement – eine ganzheitliche und nachhaltig wirkende Lösung aufgebaut, den AwarenessCircle. Unsere Herangehensweise sieht kurz erläutert wie folgt aus:

1. Security-Awareness-Plattform:

- Inbetriebnahme der Plattform in Absprache mit dem Kunden
- Durchführung der individuellen Maßnahmen durch individuelle Schulungspakete
- Auswertung nach definierbaren Gruppen in der Bank und Vergleich mit Benchmark-Gruppen
- Einbeziehung ISB und Berichtserstellung für die Quartalsberichte unserer Kunden
- Laufende Unterstützung und Nachhalten der Maßnahmen in der Bank

2. Awareness-Paket Mitarbeiter

- Halbtages Workshop in der Bank
- Schulung der Mitarbeitenden oder individueller Abteilungen
- Bei Bedarf Abgleich der Notfallplanung mit den abgeleiteten Awareness-Maßnahmen
- Erstellung einer dreijährigen Awareness-Planung
- Sensibilisierungsmaßnahmen von bestimmten Bereichen nach Absprache mit der Bank. Es ist zu beachten, dass knapp 30 % der Angriffe über E-Mails erfolgen; weitere knapp 40 % erfolgen über das Telefon.

Bleibt noch anzumerken, dass alle hier aufgeführten Awareness-Maßnahmen ergänzende bzw. weiterführende Maßnahmen sind, die zusätzlich zu den bisherigen Aufgaben der Informationssicherheit umzusetzen sind.

Zusammenfassend liegt das Thema Awareness im ureigenen Schutzinteresse der Bank, ist spätestens mit den neuen BAIT aber auch verpflichtend umzusetzen. Es gilt, nachhaltige Prozesse für Awareness in der Bank zu schaffen. Damit verbindet sich das Ziel, das Risiko für Cyber-Attacken deutlich zu minimieren – und zwar indem die notwendige Bewusstheit und Aufmerksamkeit zum Alltag aller Mitarbeitenden gemacht wird. ▬

Chantal Pfeffer
Abteilungsleiterin
Informationssicherheit & Datenschutz,
E-Mail: chantal.pfeffer@dz-cp.de

Reinhold Gillich
Beauftragter
Informationssicherheit & Datenschutz,
E-Mail: reinhold.gillich@dz-cp.de