



Cyber-Security

Die Risiken werden immer noch unterschätzt



Cyber-Kriminalität ist zunehmend zu einer existenziellen Bedrohung geworden. Doch bei vielen Mitarbeitern ist der Wissenstand darüber weiterhin auf einem relativ niedrigen Niveau. Wie groß die Lücke tatsächlich ist, zeigen die Ergebnisse eines aktuellen Quiz unter den Lesern der CIO.



Das Wissen über die Cyber-Bedrohungen ist selbst unter den IT-Experten nicht sonderlich hoch, dabei ist das ein wesentlicher Schlüssel für alle Abwehrmaßnahmen.

Die Automatisierung dieser Prozesse fand bisher meist innerhalb der Grenzen einer bestimmten Business-Anwendung statt. Ein Warenwirtschaftssystem beispielsweise bestellt selbsttätig ein neues Kontingent von einem bestimmten Produkt, sobald der Lagerbestand ein unteres Limit erreicht hat. Oder ein CRM-System verschickt selbsttätig eine Mail an jemanden, der sich IT-Sicherheit liegt schon lange nicht mehr alleine in der Verantwortung von Experten, sondern aller Mitarbeiter. Nur mit einer gehörigen Portion an Skepsis sowie dem nötigen Basiswissen kann jeder Mitarbeiter dazu beitragen, dass weder er selbst noch das gesamte Unternehmen kompromittiert werden. Das Cyber-Sicherheitsunternehmen Mimecast wollte es genauer wissen und hat zusammen mit der CIO ein entsprechendes Quiz für deren Leser ausgearbeitet.

Faktenwissen „hat noch Luft nach oben“

Inzwischen haben mehr als 400 Personen die Fragen beantwortet und es zeigt sich, dass es noch erhebliche Lücken gibt. Am gravierendsten ist die Diskrepanz zwischen Wissen und Wirklichkeit bei der Einschätzung der Schäden, die durch Mitarbeiter verursacht werden. Auf die Frage „Was schätzen Sie, wie viel Prozent der Mitarbeitenden sind an wie viel Prozent der Sicherheitsvorfälle beteiligt?“ entschieden sich 51 Prozent der Quizteilnehmer für die Antwort „35 Prozent der Mitarbeiter sind an 60 Prozent der Sicherheitsvorfälle beteiligt.“ Die richtige Antwort lautete jedoch: „8 Prozent der Mitarbeiter sind an 80 Prozent aller Vorfälle beteiligt“. Doch das wurde nur von mageren 18 Prozent der Teilnehmer beantwortet. Etwas besser waren die Ergebnisse bei den Fragen: „Wie hoch sind die durchschnittlichen Kosten für ein Datenleck in Deutschland?“ und „Wieviel Prozent der Unternehmen hatten in den letzten zwölf Monaten mindestens einen Sicherheitsvorfall zu verzeichnen?“. Die richtige Antwort bei der ersten Frage war 4,9 Millionen Euro und wurde von 23 Prozent der Teilnehmer angeklickt. Doch fast doppelt so viel (43 Prozent) entschieden sich für die falsche Antwort: 1,2 Millionen Euro. Das heißt, die Schäden sind durchschnittlich viermal so hoch, wie die meisten Teilnehmer vermuten. Bei der zweiten Frage ist es ähnlich. Die richtige Antwort lautete „78 Prozent hatten in den letzten zwölf Monaten einen Sicherheitsvorfall“. 24 Prozent entscheiden sich für diese Antwort, doch 47 Prozent meinen, dass nur 42 Prozent einen solchen Vorfall hatten.

Die menschliche Komponente – wichtiger als Technologie

In der IT-Security gibt es sehr viele Abkürzungen, doch einige wenige sollte man als CISO oder Sicherheitsverantwortlicher unbedingt kennen, beispielsweise HRM. Das Kürzel steht für „Human Risk Management“ und umschreibt das IT-Security-Risk, dass von den Mitarbeitern ausgeht, beziehungsweise, die Minimierung dieser Einflüsse. Mimecast kommt in einem Bericht zu der Erkenntnis, dass „das menschliche Risiko heute die größte Lücke in der Cyber-Sicherheit ist und oftmals zu wenig beachtet wird“.

In dem Quiz wurde der Wissensstand zu diesem bedeutenden Security-Bereich abgefragt. Immerhin kannten 32 Prozent der Teilnehmer die Abkürzung und den Begriff. Das war aber nur Platz zwei hinter der falschen Antwort „Hacker Risk Management“, die von 45 Prozent angeklickt wurde. Immerhin wussten 20 Prozent, was sich im Detail hinter HRM verbirgt:

- Erkennen und Messen menschlicher Sicherheitsverhaltensweisen
- Einleitung von Richtlinien- und Schulungsmaßnahmen basierend auf dem menschlichen Risiko
- Schulung und Befähigung der Belegschaft, sich selbst und ihr Unternehmen vor Cyber-Angriffen zu schützen
- Aufbau einer positiven Sicherheitskultur

Mimecast verfolgt das Konzept eines gezielten Managements nutzerzentrierter Risiken im Rahmen einer konsolidierten Human Risk Management (HRM) Plattform. Ein innovativer und ganzheitlicher Ansatz, der die menschliche Komponente der Cybersicherheit in den Fokus rückt. Die Plattform bietet Einblicke in Risikoprofile von Nutzern und Unternehmen. Sie ermöglicht es Sicherheitsteams, Nutzer anhand dieser Profile gezielt zu schulen und, wenn nötig, verstärkt zu schützen.

Über Mimecast

Mimecast ist eine KI-gestützte, API-fähige und vernetzte Human Risk Management-Plattform. Sie wurde entwickelt, um Unternehmen vor dem gesamten Spektrum von Cyberbedrohungen zu schützen. Dafür integriert sie moderne, benutzerfreundliche Technologie mit Strategien für das Erkennen von Risiken und den Aufbau von Sicherheitskompetenz, die immer den Nutzer im Fokus behalten. Darauf ausgelegt, unsichtbare Risiken sichtbar zu machen und Dateneinblicke so aufzubereiten, dass sie als Entscheidungsgrundlage dienen können, eröffnet sie Unternehmen proaktive Handlungsmöglichkeiten. Sie hilft, Kommunikations- und Kollaborationslandschaften zu schützen, kritische Daten zu sichern, Mitarbeiter aktiv in das Risikomanagement einzubeziehen und eine Sicherheitskultur zu fördern, die mit Unternehmenszielen wie Geschäftskontinuität und Steigerung der Produktivität in Einklang steht. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich dynamisch entwickelnden Bedrohungslandschaft einen Schritt voraus zu sein. Von internen Risiken bis hin zu externen Gefahren – Mimecast bietet Kunden mehr. Mehr Sichtbarkeit. Mehr Einblicke. Mehr Agilität. Mehr Sicherheit.

Im dritten Quartal 2024 wurde Mimecast in der Forrester Wave™ für „Human Risk Management Solutions“ als „Strong Performer“ gelistet.

[Mehr zu Mimecast](#)