Künstliche Intelligenz in der Cybersicherheit

Die Zukunft der E-Mail-Security

Unterstützt durch

mimecast™

Inhalt

Vorwort

Seien es E-Mails mit schadhaften Anhängen, Phishing-Mails oder Ransomware, die E-Mail gilt weiterhin als größter Angriffsvektor für Cyberkriminelle. Dabei werden Angriffsmuster immer komplexer und raffinierter, und lassen sich teilweise nicht einmal mehr von Menschen als solche erkennen. Denn die Cyberkriminellen erhöhen nicht nur die Frequenz der Angriffe, sie erfinden sich jeden Tag neu und wissen ganz genau, wie sie traditionelle Sicherheitsmaßnahmen umgehen können. Herkömmliche Security-Systeme können mit der Vielzahl an unterschiedlichen Angriffen kaum noch mithalten. Um sich den neuen Gegebenheiten anzupassen, steht Unternehmen beispielsweise der Einsatz von Künstlicher Intelligenz innerhalb der Sicherheitsumgebung zur Verfügung.

Doch wie sieht es mit dem Einsatzgrad von KI im Security-Kontext aus? Welche Einsatzfelder werden verstärkt durch KI unterstützt? Welche Vorteile sehen Unternehmen im Einsatz von KI und welche Hürden müssen überwunden werden?

Um diese Fragen zu beantworten, wurden im Rahmen dieser Studie 200 Entscheidende oder stark am Entscheidungsprozess beteiligte Personen zu ihrem KI-Einsatz im Security-Umfeld, den Vorteilen, Problemfeldern und spezifischen E-Mail-basierten Themen befragt. An der Befragung im September 2022 nahmen 103 Entscheidende aus Deutschland sowie 97 Entscheidende aus der Schweiz aus mittleren und großen Unternehmen jeglicher Branchen teil.

Künstliche Intelligenz auf dem Vormarsch

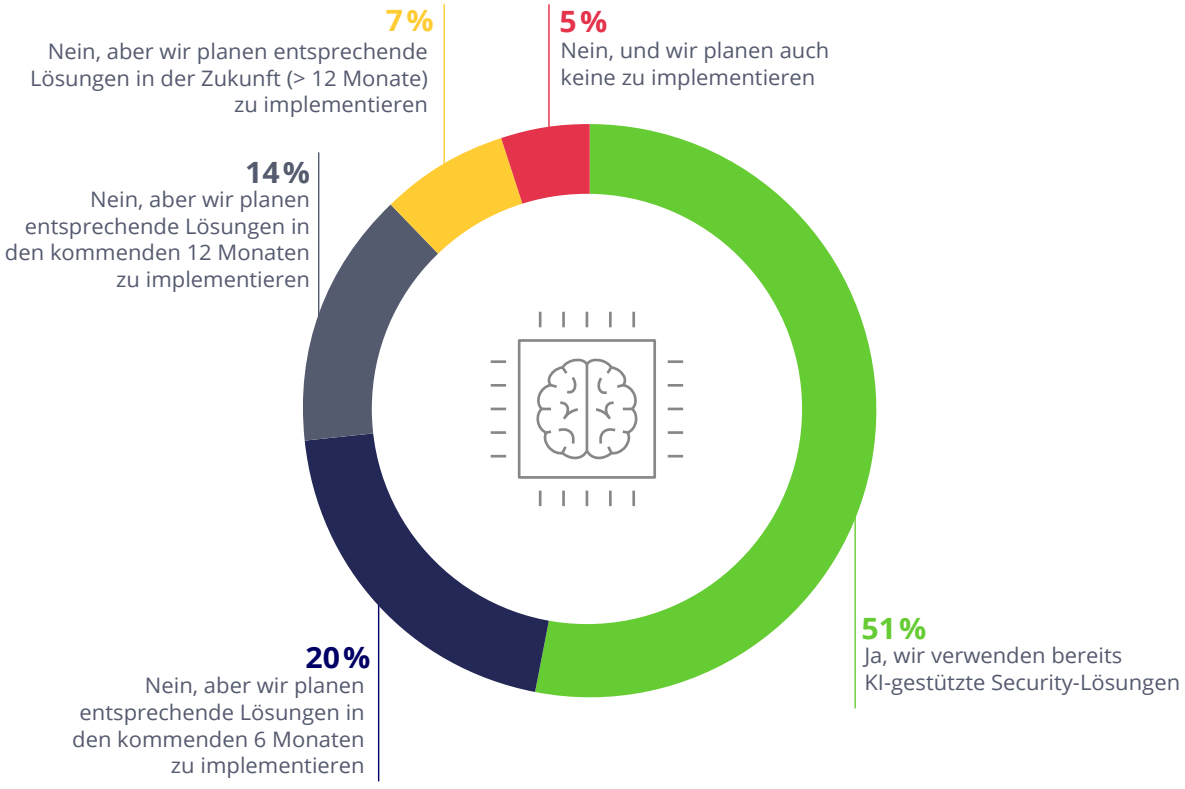
Das World Economic Forum hat jüngst Cybercrime als eines der potenziell gefährlichsten Risiken für die Gesellschaft ernannt, sogar noch vor terroristischen Akten. Insbesondere im Rahmen der Pandemie verschärfte sich das Risiko noch einmal deutlich. Denn für Cyberkriminelle eröffneten sich durch den digitalen Wandel vieler Unternehmen mehr Gelegenheiten, in Unternehmensnetzwerke einzudringen und Schaden anzurichten. Die immer wieder an neue Gegebenheiten angepassten Angriffsstrategien können traditionelle IT-Sicherheitsarchitekturen schnell an ihre Grenzen bringen und die Tore für Cyberkriminelle weit öffnen.

Eine gute Möglichkeit, um sich selbst vor den immer komplexeren Angriffsverfahren zu schützen, ist der Einsatz von Künstlicher Intelligenz in der eigenen Security-Umgebung. Künstliche Intelligenz unterstützt Unternehmen dabei, den Cyberkriminellen einen Schritt voraus zu sein. Mithilfe von maschinellem Lernen erweitert die KI die eigenen Kenntnisse stetig und „lernt", wie sich Bedrohungen verändern und wie diese zu bekämpfen sind.

Viele Unternehmen haben die Notwendigkeit des Einsatzes von KI in ihren Security-Umgebungen bereits erkannt. Schon heute verwendet über die Hälfte der Unternehmen in ihrer Security-Landschaft Lösungen, die in irgendeiner Art und Weise Künstliche Intelligenz integriert haben. Die Einsatzgrade sind dabei in Unternehmen ab 750 Mitarbeitenden mit mehr als 55 Prozent tendenziell höher als dies bei Unternehmen mit weniger als 750 Mitarbeitenden (45 Prozent) der Fall ist.

In den kommenden Monaten soll sich der Anteil an Unternehmen, die auf KI in ihren Security-Umgebungen setzen, laut eigener Aussage deutlich erhöhen. So möchte ein knappes Fünftel der Unternehmen bereits in den kommenden 6 Monaten entsprechende Lösungen implementieren. Immerhin 14 Prozent planen, innerhalb der nächsten 12 Monate auf KI zu setzen, und weitere 7 Prozent peilen dies für die nächsten Jahre an. Nur die allerwenigsten Unternehmen (5 Prozent) verschließen sich gegenüber dem Einsatz von KI-gestützten Security-Lösungen vollständig.

Einsatzgrade Künstlicher Intelligenz



Basis: 200 Unternehmen

Bedrohungsabwehr im Fokus

Künstliche Intelligenz kann im Security-Kontext eine Vielzahl von Aufgaben abdecken – sei es zur konkreten Abwehr von Bedrohungen, der Automatisierung von Prozessen oder auch der proaktiven Vermeidung von menschlichen Fehlern. Bei den Unternehmen, die bereits KI-gestützte Security-Lösungen verwenden, ist insbesondere die Abwehr von Bedrohungen im Fokus. Knapp drei Viertel der Unternehmen geben an, dass sie KI vor allem bei der E-Mail-Sicherheit sowie der Erkennung und Abwehr von Bedrohungen einsetzen. Dies verwundert wenig, sind doch vor allem die E-Mail-Postfächer das mit Abstand beliebteste Ziel von Cyberkriminellen. Zwar schützen Unternehmen ihre E-Mail-Postfächer gegen Gefahren, doch den gängigen Sicherheitsmechanismen ausweichende oder schwer zu entdeckende E-Mail-Bedrohungen können oftmals nicht von traditionellen E-Mail-Security-Lösungen bekämpft werden.

Eine KI-gestützte E-Mail-Security-Lösung könnte beispielsweise bei auffälligem Verhalten einen Alarm auslösen und so das Security-Team auf den Plan rufen.

Man kann aber auch noch einen Schritt weiter gehen und KI für die Automatisierung von Security-Prozessen verwenden, wie es knapp ein Drittel der Unternehmen bereits tut. Nicht nur fehlt es Unternehmen oftmals an Ressourcen, um Attacken und Anomalien manuell aufzuspüren und zu bekämpfen. So manche ungewöhnliche Angriffsmethode kann unter Umständen von Menschen viel zu spät oder auch gar nicht entdeckt werden. Und in puncto Bedrohungsbekämpfung gilt: Geschwindigkeit ist gefragt. Abwehrmechanismen müssen so schnell greifen, dass die Bedrohung möglichst im Keim erstickt wird, bevor sie Schaden anrichten kann.

KI-Security-Einsatzfelder

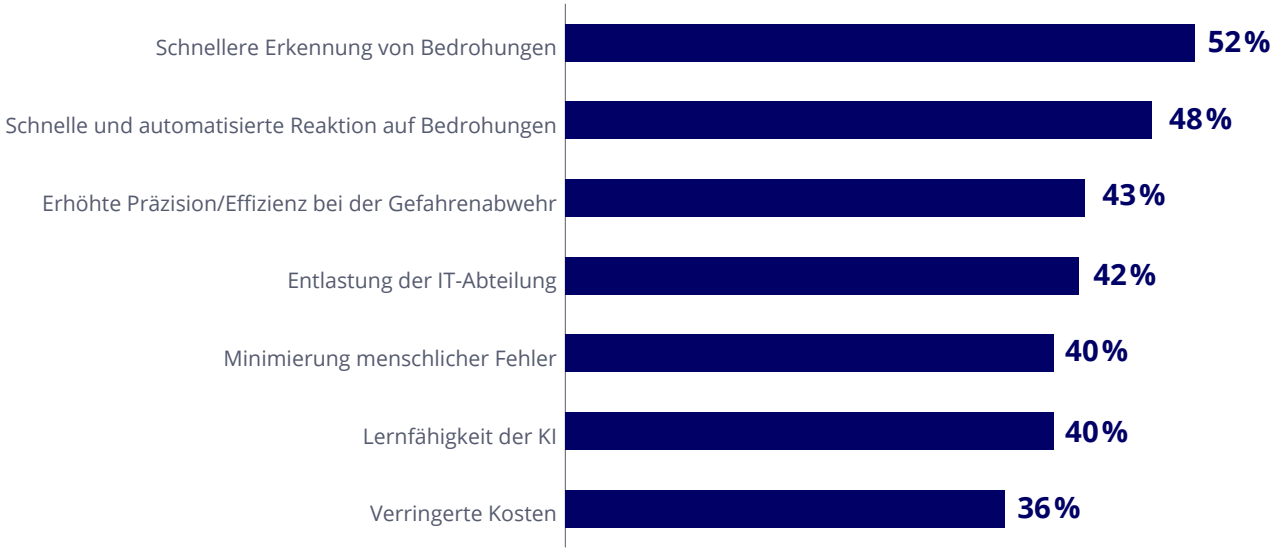
Basis: 102 Unternehmen | Mehrfachnennungen

Und ebenjene Geschwindigkeit wird auch von den Unternehmen als einer der wichtigsten Vorteile erkannt. So wurden die Teilnehmenden im Rahmen dieser Studie gebeten, die aus ihrer Sicht drei größten Vorteile von KI absteigend von Rang eins bis drei zu platzieren. Auf diese ersten drei Ränge wurden zumeist Themen gesetzt, die direkt mit der Abwehr von Gefahren verbunden sind. 52 Prozent der Unternehmen reihten dort die schnellere Erkennung bekannter und unbekannter Bedrohungen ein.

Dicht dahinter mit 48 Prozent folgt die schnelle und automatisierte Reaktion auf jene Bedrohungen. Komplettiert wird die Top 3 von der erhöhten Präzision bei der Abwehr der Gefahren (42 Prozent).

Aber: Am häufigsten auf die erste Position, dafür weniger auf Rang zwei und drei, wurde die Entlastung der IT-Abteilung gesetzt. Vor allem angesichts eingeschränkter Budgets oder Mangel an qualifiziertem Personal können KI-gestützte Lösungen für eine wesentliche Entlastung sorgen, wodurch sich IT-Abteilungen anderen strategischen Aufgaben widmen können.

Vorteile von Künstlicher Intelligenz



Basis: 200 Unternehmen | Mehrfachnennungen

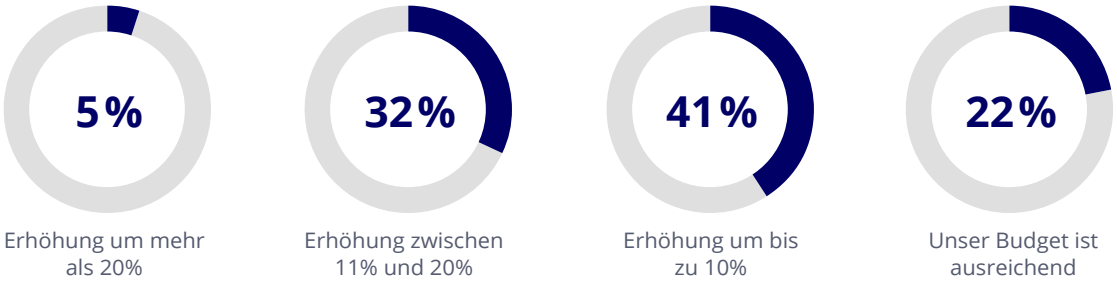
Budgets verhindern KI-Einsatz

Obwohl Künstliche Intelligenz einen Mehrwert bedeuten kann, hat fast die Hälfte der befragten Unternehmen bisher noch keine KI-Lösung im Security-Kontext implementiert. Jene Unternehmen, die noch in der Planungsphase sind, berichten von konkreten Problemfeldern, die den Einsatz bisher verhindert haben.

Die häufigsten Gründe, die bisher gegen den Einsatz von KI im Security-Umfeld sprachen, sind zum einen das fehlende Budget für entsprechende Anschaffungen (37 Prozent). Zum anderen sehen Unternehmen eine problematische Einbindung in die bestehende Security-Landschaft (37 Prozent).

Dass die Budgets nicht ausreichen, um KI erfolgsversprechend im Security-Kontext zu implementieren, zeigt sich anhand der Frage, um wie viel Prozent die Budgets ansteigen müssten. Um in Zukunft KI im eigenen Unternehmen wirksam einsetzten zu können, braucht es entsprechende Erhöhungen der zugrundeliegenden Security-Budgets. Und dies gilt nicht nur für jene Unternehmen, die bisher noch keine KI einsetzen, sondern auch für diejenigen, die KI bereits im Einsatz haben. Für 41 Prozent der Unternehmen wären Erhöhungen bis 10 Prozent nötig. Ein knappes Drittel würde zwischen 11 und 20 Prozent mehr Budget benötigen. Mehr als 20 Prozent Budgeterhöhung bräuchten lediglich 5 Prozent der Unternehmen. Das vorhandene Budget als ausreichend bewerten ein gutes Fünftel der Unternehmen.

Budgetpläne hinsichtlich KI-Einsatz

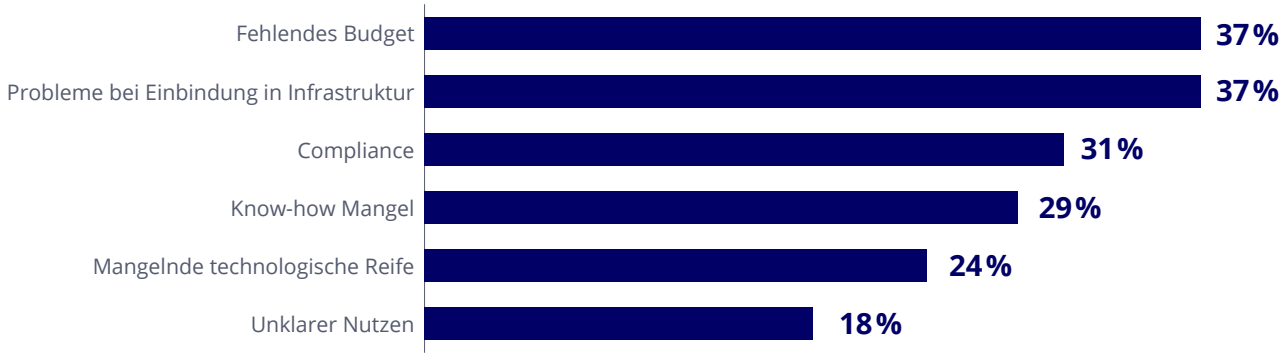


Basis: 200 Unternehmen

Aber auch Bedenken hinsichtlich Compliance und Datenschutz (31 Prozent) sind nicht zu vernachlässigen. Immerhin müssen sehr viele Daten erhoben werden, um der KI die Fähigkeit zu geben, selbstständig auf Sicherheitsvorfälle zu reagieren.

Es existieren jedoch einige Unterschiede bezüglich der Stärke der Problemfelder. So klagen tendenziell kleinere Unternehmen mit unter 750 Mitarbeitenden vermehrt über fehlende Budgets (42 Prozent), während Unternehmen mit mehr als 5000 Mitarbeitenden deutlich öfter den Nutzen von KI in Frage stellen (35 Prozent).

Gründe für den fehlenden KI-Einsatz

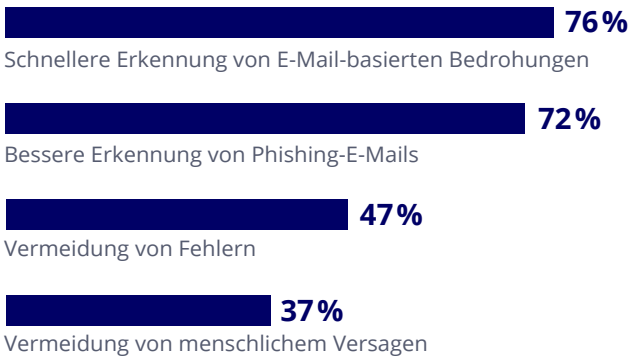


Basis: 91 Unternehmen | Mehrfachnennungen

Klassisches Einsatzfeld: E-Mail-Security

Bereits eingangs konnte festgestellt werden, dass Künstliche Intelligenz vor allem im Bereich der E-Mail-Sicherheit eingesetzt wird. Folgend stellt sich die Frage, was genau KI im Umfeld von E-Mail-Security bewirken kann. Diesbezüglich waren sich die Teilnehmenden der Studie im Großen und Ganzen einig. Mit Künstlicher Intelligenz lassen sich ihrer Meinung nach E-Mail-basierte Bedrohungen sowie Phishing-Mails schneller und besser erkennen; drei Viertel der Unternehmen sehen dies so. Dies gelingt vor allem dadurch, dass KI-Lösungen die Unternehmensumgebungen oder auch das Benutzerverhalten analysieren und „lernen", was der Normalzustand ist. Dadurch erkennen sie anormale Verhaltensweisen deutlich früher und wehren neue und bislang unbekannte E-Mail-basierte Bedrohungen schneller ab, als dies bei starren, richtlinienbasierten Security-Ansätzen der Fall ist.

Verbesserungsmöglichkeiten durch KI

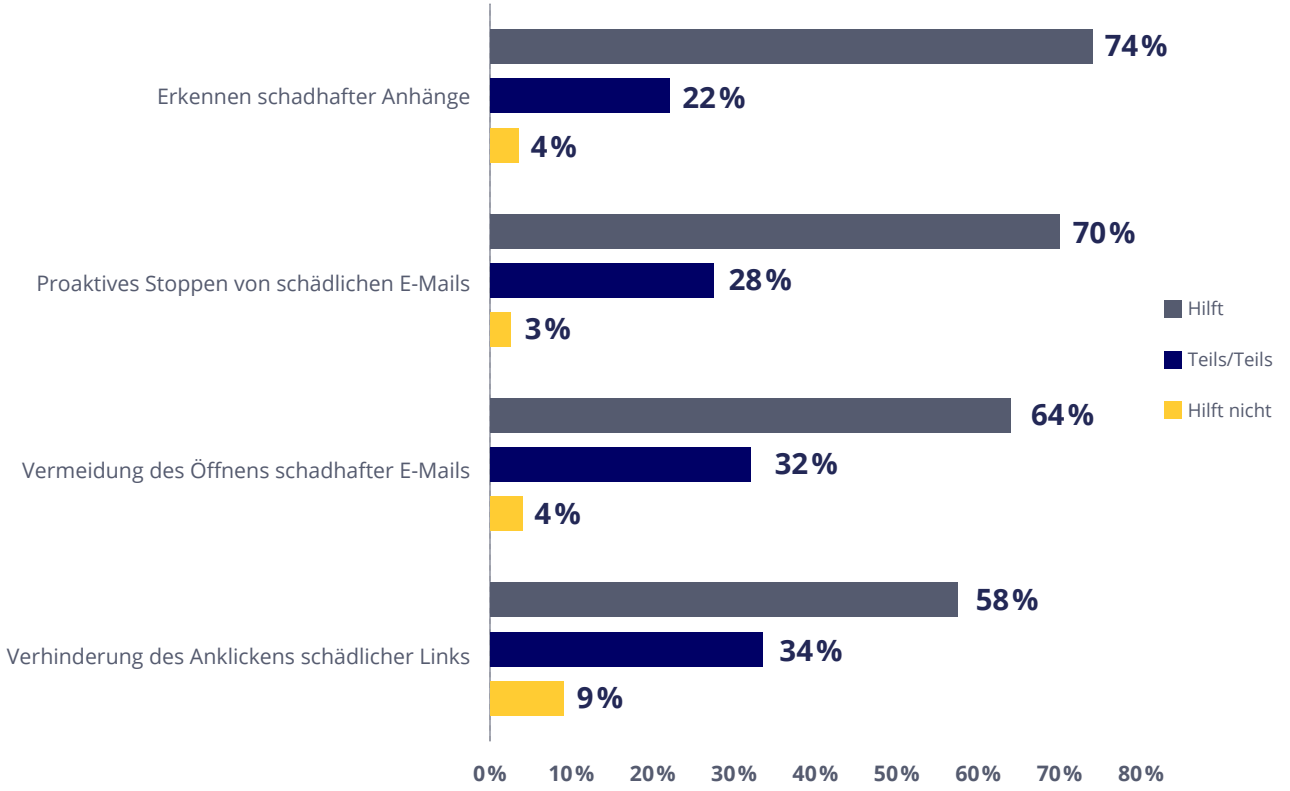


Basis: 91 Unternehmen | Mehrfachnennungen

Der Mensch ist immer noch die größte Sicherheitsbedrohung für Unternehmen. Der Großteil aller Sicherheitsvorfälle wird durch menschliche Fehler verursacht, beispielsweise wenn durch unbedarfte Mitarbeitende gefährliche Anhänge in seriös wirkenden E-Mails angeklickt werden und so die Netzwerke mit Schadsoftware infiziert werden.

Mithilfe von Künstlicher Intelligenz lassen sich diese menschlichen Fehler weitgehend minimieren. Besonders beim Erkennen von schadhaften Anhängen in seriös wirkenden E-Mails wird der Künstlichen Intelligenz ein hohes Potenzial zugeschrieben: Fast drei Viertel der befragten Unternehmen sehen KI in diesem Punkt als hilfreich an.

Nutzen von Künstlicher Intelligenz



Basis: 200 Unternehmen | Mehrfachnennungen

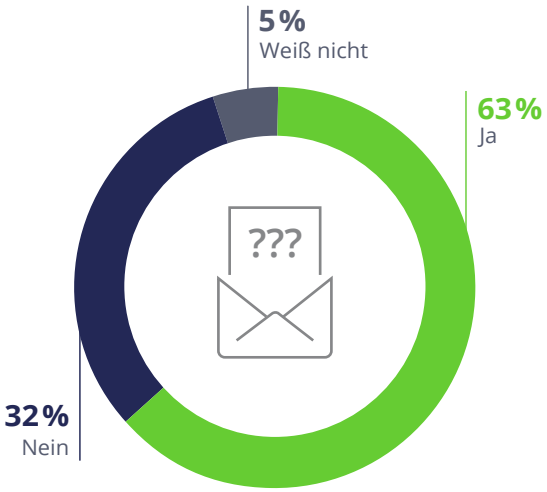
Ein Phänomen, das im Zuge der Pandemie und der Zunahme von Home Office zu erkennen war, ist die Häufung von falsch adressierten bzw. zugestellten E-Mails (misaddressed e-mails). In einem solchen Fall werden E-Mails mit beispielsweise vertraulichen Informationen durch Mitarbeitende versehentlich an nicht berechtigte Empfänger versandt. Fast zwei Drittel der Unternehmen mussten eine Zunahme falsch adressierter Mails feststellen.

Mehr als die Hälfte dieser Unternehmen gab zudem an, dass sich die Anzahl solcher E-Mails in den letzten Jahren zwischen 10 und 20 Prozent erhöht hat. Bei einem weiteren Drittel waren bis zu 10 Prozent häufiger falsch zugestellte E-Mails zu erkennen.

Mithilfe von KI-gestützten E-Mail-Security-Lösungen können solche falsch adressiert und zugestellten E-Mails massiv reduziert werden. Dabei analysiert die Security-Lösung die ausgehende Kommunikation und „lernt" mittels Machine Learning das normale Verhalten des Menschen hinter dem E-Mail-Konto. Bei Anomalien schlägt sie Alarm. So lassen sich Datenverluste verhindern und die Fehleranfälligkeit des Faktor Mensch fällt weniger ins Gewicht.

Besonders persönliche (56 Prozent) oder vertrauliche Informationen (52 Prozent) wurden am häufigsten an nicht berechtigte Empfänger gesendet. Eine falsch versandte Mail mit sensiblen Informationen stellt eine Datenpanne dar und kann je nach Schwere und regulatorischen branchenspezifischen Auflagen nicht nur zu hohen Bußgeldern führen, auch Folgen wie beispielsweise Reputationsschäden oder der Verlust von geistigem Eigentum können dem Unternehmen langfristig die Position am Markt kosten.

Zunahme falsch adressierter E-Mails seit Pandemiebeginn



Basis: 200 Unternehmen

Fazit

Die E-Mail ist für Cyberkriminelle der wichtigste Angriffsvektor, um in Unternehmensnetzwerke einzudringen. Da jedoch nahezu jedes Unternehmen über einen E-Mail-Schutz verfügt, versuchen Cyberkriminelle mit immer raffinierteren Methoden die traditionellen Schutzmechanismen auszuhebeln.

Und da ihnen dies immer wieder gelingt, ist es für Unternehmen unabdingbar, ihre E-Mail-Sicherheitslösungen auf den Prüfstand zu stellen und neue, moderne Technologien zum Schutz des Unternehmens zu nutzen. Denn nur wer schnell und effektiv auf neue und unbekannte Bedrohungsarten reagieren kann, ist in der Lage, das eigene Unternehmensnetzwerk vor Schaden zu bewahren.

Um diesen hohen Grad an Geschwindigkeit und Präzision in der Bedrohungsabwehr zu erreichen, empfiehlt es sich, auf eine E-Mail-Security-Lösung zu bauen, die sich der Vorteile von Künstlicher Intelligenz bedient. Damit werden nicht nur Angriffe von außen, wie z.B. E-Mails mit schadhaften Anhängen oder Phishing-Versuche, im Keim erstickt. Auch interne Gefahren auf Basis menschlicher Fehler lassen sich minimieren. So kann die KI beispielsweise versehentliche Datenverluste, die durch den Versand einer E-Mail mit vertraulichen Informationen an falsche Empfänger entstehen könnten, erkennen und verhindern.

Der kontinuierliche Lernprozess der KI des alltäglichen normalen Verhaltens der Unternehmensumgebung und deren Nutzer versetzt die Lösung in die Lage, anormale Verhaltensweisen schneller und effizienter zu erkennen und Gegenmaßnahmen zu ergreifen, als dies für den Menschen je möglich wäre. Und bei einem erfolgreichen Angriff gilt: Jede Sekunde zählt. Denn je weiter sich der Angreifer im Netzwerk ausbreiten kann, desto mehr Schaden kann er anrichten.

Zur Studie

Die Studie "KI in der Cybersicherheit" wurde von der techconsult GmbH im Auftrag von Mimecast konzipiert und durchgeführt. 103 Unternehmen aus Deutschland und 97 Unternehmen aus der Schweiz ab 100 Mitarbeitenden wurden zu ihrem Einsatzgrad von KI-Technologien im Rahmen von Cybersecurity, ihren Herausforderungen bei der Implementierung sowie E-Mail-Security-spezifischen Themen befragt. Die Stichprobe umfasste alle Branchen. Ansprechpartner waren in erster Linie IT-Entscheidende.

Branche

Industrie	24 %
Handel	7 %
Dienstleistung*	51 %
Banken und Versicherung	7 %
Öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen	12 %

Größenklassen

100 bis 749 Mitarbeitende	60%
750 bis 4.999 Mitarbeitende	40%
5.000 oder mehr Mitarbeitende	20%

Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Weitere Informationen

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**
Tel.: +49-561-8109-0
Fax: +49-561-8109-101
Web: **www.techconsult.de**

Kontakt techconsult

Raphael Napieralski
Analyst
techconsult GmbH

E-Mail: **raphael.napieralski@techconsult.de**
Tel.: +49-561-8109-0

Über techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Über Mimecast

Work Protected™ Seit 2003 verhindert Mimecast, dass guten Unternehmen Schlimmes widerfährt, indem es ihnen ermöglicht, geschützt zu arbeiten. Wir ermöglichen es über 40.000 Kund:innen, Risiken zu minimieren und die Komplexität einer Bedrohungslandschaft zu bewältigen, die von bösartigen Cyberangriffen, menschlichem Versagen und technologischen Fehlern geprägt ist. Mimecast bringt Ihre Email- und Collaboration Security auf das nächste Level.

Kontakt

Mimecast Germany GmbH
Kistlerhofstraße 172
81379 München

Tel: +49 89 904 200 800
Web: https://www.mimecast.com
E-Mail: info@mimecast.com

mimecast™