mimecast

Der Mittelstand. BVMW e.V. Bundesverband

Ratgeber

Cybergefahren für den Mittelstand

Liebe Unternehmerinnen, liebe Unternehmer,

durch die aktuellen Entwicklungen bei großen KI-Sprachmodellen wie ChatGPT ist künstliche Intelligenz und die Digitalisierung wieder Gegenstand einer breiten gesellschaftlichen Debatte geworden. Dies muss nach Ansicht des Bundesverbandes Der Mittelstand (BVMW) mit einer stärkeren Förderung der digitalen Bildung, der schnelleren Digitalisierung der öffentlichen Verwaltung und der digitalen Souveränität einhergehen. Damit die deutsche Wirtschaft und insbesondere der deutsche Mittelstand auch zukünftig wettbewerbsfähig bleiben, brauchen wir einen Boost bei der Digitalisierung und digitalen Transformation in Deutschland. Mit seiner Digitalen Agenda des Mittelstands nimmt der BVMW deshalb die Politik, die Gesellschaft und auch die Wirtschaft in die Pflicht, der Digitalisierung noch größere Aufmerksamkeit beizumessen.

Digitalisierung bietet aber nicht nur Chancen, sondern auch Risiken: Cyberangriffe finden längst nicht mehr nur auf die Infrastruktur von Großunternehmen statt. Drei von zehn mittelständischen Unternehmen in Deutschland sind allein in den Jahren 2018 bis 2020 von Cyberkriminellen angegriffen worden. Auch eine aktuelle Kurzumfrage unter BVMW-Mitgliedern in Bayern zeigt: Die Unternehmen sind sich der Gefahren bewusst und haben bereits vielfältige Mechanismen wie regelmäßige Backups, Zwei-Faktor-Authentisierung und E-Mail-Security-Lösungen installiert. Die Wahrscheinlichkeit eines Cyberangriffs wird dabei sehr unterschiedlich eingeschätzt: Fast die Hälfte der Befragten hält einen Angriff auf das eigene Unternehmen für wahrscheinlich – ein gleichgroßer Anteil glaubt aber auch, dass ein Angriff „wenig wahrscheinlich“ ist. Über die Art möglicher Hackerattacken herrscht hingegen Einigkeit: Ransomware-Angriffe sind die mit Abstand am häufigsten genannte Bedrohung.

Der BVMW unterstützt seine Mitglieder aktiv dabei, die Digitalisierung im Mittelstand voranzutreiben. Die schon im dritten Jahr erfolgreiche Partnerschaft mit Mimecast soll dazu beitragen, das Bewusstsein für digitale Sicherheitslösungen weiter zu erhöhen und konkrete Lösungsmöglichkeiten für den Mittelstand aufzuzeigen.

Ihr

Achim von Michel

Der Mittelstand.BVMW in Bayern, Beauftragter für Politik

Der Mittelstand.
BVMW e.V.
Bundesverband

Cybergefahren sind Unternehmensgefahren

203 Milliarden Euro haben Angriffe deutsche Unternehmen 2022 gekostet. Das ist das Ergebnis einer Studie im Auftrag des Digitalverbands Bitkom, für die mehr als **1.000 Unternehmen** über alle Branchen hinweg repräsentativ befragt wurden. Als wäre die Summe nicht schon erschreckend genug: So gut wie jedes Unternehmen wurde oder kann zum Opfer werden. **84 Prozent** der befragten Unternehmen waren betroffen, weitere **9 Prozent** gehen davon aus. In den vergangenen fünf Jahren hat sich die Schadenssumme damit fast verdoppelt **(in den Jahren 2018/2019 waren es laut Bitkom „nur" 103 Milliarden Euro)**. Cybergefahren nehmen also drastisch zu und betreffen Unternehmen aller Branchen und jeglicher Größe! Gleichzeitig gehen Angreifer, die immer häufiger aus dem organisierten Verbrechen kommen, immer professioneller vor. Die Sorgen in der Wirtschaft vor den Folgen einer Cyberattacke wachsen: **45 Prozent** der Unternehmen sind überzeugt, dass Cyberattacken ihre geschäftliche Existenz bedrohen können, **42 Prozent** rechnen mit einem starken Anstieg der Attacken.

Mittelständische Unternehmen sollten deshalb wachsam sein. Es ist ein leichtsinniger Trugschluss, sich auf Argumente wie **„unser Unternehmen ist zu klein und zu uninteressant für Cyberangreifer"**, **„wir sind durch unsere Cyberversicherung bestens abgesichert"** oder **„wir sind noch nicht so digital"** zu verlassen und darauf zu hoffen, Cybergefahren dadurch entgehen zu können!

Hier nur zwei Beispiele für Cyberangriffe: **Anfang 2022 traf es die Unfallkasse Thüringen (UKT)**. Cyberkriminelle verschlüsselten das gesamte System vollständig, so dass – einfach ausgedrückt – nichts mehr ging. **Der Angriff erfolgte dabei gezielt, wie eine Sprecherin im Januar 2022 bestätigte.** Infolge der Attacke konnten die Angestellten auf keinerlei Versichertendaten mehr zugreifen oder Zahlungen bearbeiten, ebenso wenig war es Mitgliedern noch möglich, Arbeitsunfälle digital zu melden. Selbst die Telefonanlage fiel kurzzeitig aus, ebenso der E-Mail-Server. Ursache für den totalen Systemausfall war eine Ransomware, die sämtliche Server der Unfallkasse verschlüsselt hatte. Auch der Großcaterer und Tiefkühlproduzent **Apetito**, der Einrichtungen wie Krankenhäuser, Kindergärten, Firmenkantinen, Schulen und Seniorenheime mit Essen versorgt, reihte sich 2022 in die Opfer-Statistik ein. **Die erfolgreiche Hacker-Attacke legte sämtliche Server lahm, sodass es Kunden u.a. nicht mehr möglich war, ihre Bestellungen abzugeben.**

Die Unternehmensführung sollte sich im Klaren sein, dass Cyberrisiken kein IT-Thema sind. Cybergefahren sind Risiken, die Einfluss auf das gesamte Unternehmen haben und somit ein ernstzunehmendes Geschäftsrisiko darstellen. Die Kosten eines erfolgreichen Ransomwareangriffs können für Unternehmen dramatisch sein. Fatal ist, dass es im Durchschnitt mehr als neun Monate dauert, um eine Datenschutzverletzung zu entdecken und einzudämmen. Angesichts **hoher Inflationsraten, einer schwierigen Wirtschaftssituation und geopolitischer Spannungen, die zu einer hohen wirtschaftlichen Volatilität führen,** können es sich Unternehmen nicht leisten, eine schwache Sicherheitsarchitektur zu haben, die sie anfällig für Angriffe auf ihre Daten macht und die Stabilität ihrer Organisation gefährdet.

Die gute Nachricht: Während externe Faktoren wie Kriege und Naturkatastrophen oder wirtschaftliche Einflüsse wie Inflationen nicht oder nur schwer beeinflussbar sind, können sich Unternehmen auf Cybergefahren einstellen und bestmögliche Vorbereitungen treffen. So sagte **Bitkom-Präsident** Achim Berg bei der Vorstellung der Bitkom-Studie, dass **„[…] Unternehmen mit geeigneten Maßnahmen und Vorsorge dafür sorgen können, dass Angriffe abgewehrt oder zumindest der Schaden begrenzt wird."**

Das tückische Trio der Cybergefahren: Ransomware, Phishing und Spoofing

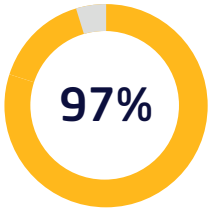
Der wichtigste Angriffsvektor ist nach wie vor die E-Mail. Es gibt viele verschiedene Arten von E-Mail-Bedrohungen, mit denen Cybersecurity-Profis konfrontiert sind, aber die drei häufigsten sind nach wie vor:

- **Phishing:** Phishing (vom englischen „fishing“ = Angeln) ist ein Sammelbegriff für Versuche, über Spam-Mails oder Direktnachrichten sowie über fingierte Webseiten oder Profile an die persönlichen Daten eines fremden Benutzers zu gelangen. Ziel von Phishing sind der Eigentums- und Datenklau.

- **Ransomware:** Ransomware sind Schadprogramme, die auf die Blockade des Computersystems oder die Verschlüsselung der Betriebs- und Nutzerdaten abzielen, und meistens über das Einfallstor E-Mail ins Unternehmen gelangen. Ein gutes Beispiel für Ransomware ist Emotet. Diese Schadsoftware verbreitet sich sehr schnell selbständig und kann damit besonders hohen Schaden anrichten.

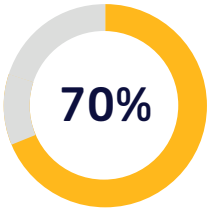
- **Spoofing:** Der Begriff E-Mail-Spoofing bezeichnet das Nachbauen beziehungsweise Fälschen einer E-Mail-Adresse. Ziel ist es dabei, den Empfänger glauben zu lassen, dass die Nachrichten von einer anderen Person stammen. E-Mail-Spoofing ist ein beliebtes Mittel von Cyberkriminellen, um an sensible Daten oder Geld zu gelangen.

Laut des jährlichen Mimecast-Reports zur **E-Mail-Sicherheit State of Email Security (SOES)** haben **84 Prozent** der Sicherheitsentscheider in den letzten **12 Monaten** eine Zunahme von mindestens einer Art dieser Angriffe festgestellt, von denen Phishing am weitesten verbreitet ist: Im Jahr 2022 gab es schätzungsweise **255 Millionen Phishing-Versuche**, ein Anstieg von **61 % gegenüber** dem Vorjahr. Schlimmer noch: Mehr als **70 %** dieser E-Mails wurden vom Empfänger geöffnet. Gibt es irgendjemanden, der noch nie eine verdächtig aussehende E-Mail erhalten hat – oder schlimmer noch, eine E-Mail, die scheinbar von einer vertrauenswürdigen Partei stammte, es aber nicht war? Aus diesem Grund fürchten sich Unternehmen vor Phishing - denn es ist einfach, jemanden dazu zu verleiten, eine mit Malware verseuchte E-Mail zu öffnen und diese E-Mail dann an andere weiterzuleiten, wodurch die Bedrohung weiterverbreitet wird. Es ist daher kaum überraschend, dass **90 Prozent** der Sicherheitsverletzungen in Unternehmen auf Phishing zurückzuführen sind. Im vergangenen Jahr waren praktisch alle der diesjährigen SOES-Befragten **(97 Prozent)** das Ziel eines Phishing-Angriffs. Die Mehrheit **(59 Prozent)** hat mehr Angriffe erlebt als in den Vorjahren. Und von allen Befragten gaben **80 Prozent** an, dass sie mindestens einen Angriff erlebt haben, bei dem sich die Bedrohung von einem infizierten Benutzer auf einen anderen ausgebreitet hat.



waren Ziel eines Phishing-Angriffs

Phishingversuche



Öffnungsrate von Phishing-Emails

Zwei Drittel der diesjährigen SOES-Befragten **(66 Prozent)** gaben an, Opfer von **Ransomware** geworden zu sein, aber in diesem Fall waren kleinere Unternehmen stärker betroffen. Bei den Unternehmen mit **250 bis 500 Mitarbeitern** gaben sieben von zehn Befragten **(70 Prozent)** zu, dass ein Ransomware-Angriff ihr Geschäft geschädigt hat, während **73 Prozent** der Unternehmen mit **1.000 bis 5.000 Mitarbeitern** dasselbe bestätigten. Von den Großunternehmen mit **10.000 oder mehr Mitarbeitern** wurde weniger als die Hälfte **(46 Prozent)** durch Ransomware geschädigt. Auch Unternehmen in bestimmten Branchen wurden häufiger Opfer von Ransomware. Von den Unternehmen in den Branchen Verbraucherdienste **(87 Prozent),** Energie **(83 Prozent),** Gesundheitswesen **(80 Prozent)** und Medien und Unterhaltung **(86 Prozent)** wurden mehr als acht von zehn durch einen Ransomware-Angriff ernsthaft geschädigt.

Auch **E-Mail-Spoofing** bleibt ein ernstes Risiko. Fast alle SOES-Befragten **(91 Prozent)** waren sich der Versuche bewusst, ihre E-Mail-Domäne zu missbrauchen, und fast die Hälfte **(44 Prozent)** sahen eine Zunahme dieser Art von Aktivitäten im Jahr **2022**. Auch das Spoofing von Web-Domains ist weit verbreitet, wobei Unternehmen wiederholt Versuche aufdeckten, ihre Websites zu klonen. Im Durchschnitt stellten die Unternehmen im vergangenen Jahr **10 solcher Versuche fest.** Während die meisten Unternehmen behaupteten, dass sie zumindest minimal auf Spoofing vorbereitet sind, sagte weniger als ein Drittel **(29 Prozent)** von sich, dass sie vollständig auf die unrechtmäßige Nutzung ihrer E-Mail-Domänen vorbereitet sind. Und obwohl fast neun von zehn **(88 Prozent)** der SOES-Befragten angaben, dass ihre Unternehmen daran interessiert sind, in den nächsten 12 Monaten **DMARC (Domain-based Message Authentication, Reporting and Conformance)** zu verwenden, um E-Mail-Spoofing zu vereiteln, hat es deutlich weniger als ein Drittel **(27 Prozent)** tatsächlich bereits implementiert.

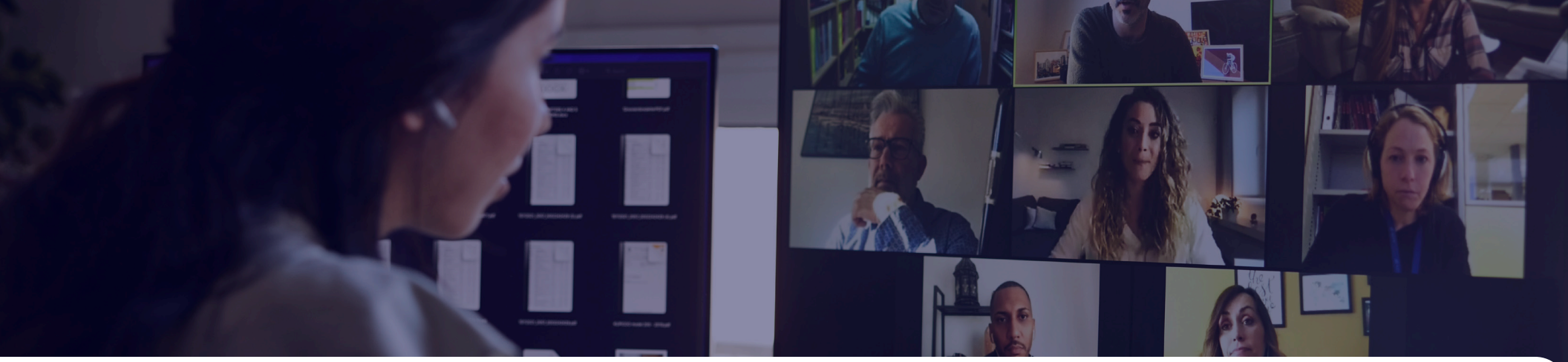
> "Gelebte Cybersicherheit erfordert die Implementierung eines vielschichtigen Modells. Modernste E-Mail-Security Lösungen helfen nicht nur dabei die Mitarbeiter vor schadhaften Links zu beschützen, vielmehr verhindern sie auch koordinierte Attacken wie (Spear) Phishing oder Spoofing."
>
> **Group CISO & Vice President CANCOM**

Herausforderungen für die IT-Sicherheit: Collaboration-Tools als neues Einfallstor für Kriminelle

Durch Corona hat sich die gewohnte Arbeitswelt weiterentwickelt: Collaboration-Tools wie **Microsoft Teams, Zoom, Slack, WebEx und Co.** haben sich während der Pandemie ihren Weg in den Arbeitsalltag vieler Unternehmen gebahnt – und sie sind geblieben. Diese vermehrte und vielfältigere Kommunikation haben Cyberkriminelle erkannt und sich darauf als Angriffspunkte neu orientiert und spezialisiert.

Die Vorteile der Tools liegen auf der Hand – Unternehmen schätzen erhöhte **Flexibilität, örtliche und zeitliche Unabhängigkeit der Mitarbeiter, schnellere und effizientere Kommunikation sowie vereinfachten Datenaustausch und erhöhte Produktivität.**

Neben den vielen Vorteilen bringen **Collaborations-Tools gleichermaßen neue Risiken für die IT-Sicherheit mit sich.** Die Gefahren beruhen primär darauf, dass diese Tools meist außerhalb der Kontrolle der Unternehmens-IT liegen, z.B.



- **Menschliche Fehler wie das Teilen von Passwörtern oder das Hereinfallen auf Phishing-Attacken durch Unachtsamkeit können Cyberkriminellen den Weg in das Unternehmensnetzwerk ermöglichen.** Phishing-Attacken über Collaboration-Tools können zum Beispiel in Form von gefälschten Einladungen zur Teilnahme an einem Microsoft Teams-Call erfolgen. Ein falscher Klick und das Netzwerk könnte mit Malware infiziert werden.

- **Ungeplante Zugriffe von Dritten auf vertrauliche Inhalte stellt ein Sicherheitsrisiko dar.** Dies könnte passieren, wenn externe Personen einen zeitlich begrenzten Zugriff auf ein bestimmtes Projekt erhalten, oder Partner zusätzliche Zugriffe auf Inhalte bekommen, die eigentlich nicht für seine Augen bestimmt waren.

- **Zunahme von Schatten-IT: Mitarbeitende könnten sich unautorisierte Collaboration-Tools aus dem Netz herunterladen, die nicht von der Unternehmens-IT freigegeben sind.** Wenn diese ohne Befugnis genutzt werden, entstehen jedoch Gefahren im Bereich IT-Sicherheit, Datenschutz und Compliance.

Es gibt Möglichkeiten, die mit den Collaboration-Tools einhergehenden Sicherheitsrisiken zu minimieren:

- **Ergänzende Security-Software:** vor allem Sicherheitslösungen aus der Cloud lassen sich schnell und einfach implementieren und können Unternehmen zusätzlichen Schutz bieten.

- **Organisatorische Maßnahmen:** die Ergänzung der Unternehmensrichtlinien für den Umgang mit Collaboration-Tools zur Minimierung von Sicherheitslücken.

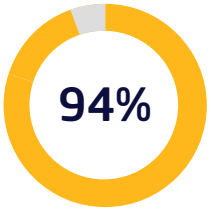
- **Security-Awareness-Trainings** als sinnvolle Maßnahme zur Reduzierung von Risiken, die durch menschliche Fehler entstehen.

Microsoft 365 – der Liebling von Unternehmen und Cyberkriminellen

Microsoft 365 (M365) verbindet die Apps der Office-Familie mit intelligenten Cloud-Diensten, wie dem E-Mail-Dienst Exchange, der Webanwendung SharePoint oder dem Kommunikationstool Teams. Mit Erfolg: Während Microsoft Office seit Jahrzehnten den De-facto-Standard in unseren Büros markiert, ist Cloud Computing die Grundlage moderner digitaler Kommunikation. Von der E-Mail an den Kunden über den Chat mit der Chefin bis zum virtuellen Meeting: Mit der Funktionsintegration von **M365 gestaltet Microsoft** nahtlos vernetzte Arbeitswelten und entwickelte sich vom Office-Giganten zu einem führenden Cloud-Anbieter. Die von Mimecast in Zusammenarbeit mit statista entstandene Studie **„Wie sicher ist Microsoft 365“** ergab: Auf **200 befragte IT-Entscheider** mittlerer und großer Unternehmen in Deutschland, die **M365** nutzen, **kommen nur 12**, die es nicht nutzen. **Effiziente Zusammenarbeit, ortsunabhängige schnelle Kommunikation und der bequeme Austausch von Daten** sind die wesentlichen Vorteile von **M365. 93 Prozent** der Unternehmen teilen heute auch vertrauliche Informationen, wie Preislisten, Verträge oder sogar Login-Daten, per E-Mail. Maximale Sicherheit ist dabei unverzichtbar. Microsoft verspricht, dass Daten in der Cloud vertraulich bleiben – dennoch schätzen nur **30 Prozent** der IT-Entscheider die Sicherheit von **M365 als sehr hoch ein.**

Die massenhafte Verbreitung von **M365** hat auch dazu geführt, dass sich Angreifer verstärkt auf diese beliebte Produktivitätsplattform konzentrieren. Mehr als **90 % der Angriffe** erfolgen per E-Mail, und oft sind sie so konzipiert, dass sie in der heutigen, Microsoft-abhängigen Welt erfolgreich sind. Umso wichtiger, dass Unternehmen einen Extra-Schutz für **M365** implementieren.

Experten empfehlen, die bestehende Sicherheit von **M365** durch einen Drittanbieter zu ergänzen. Mimecast bietet umfassende Sicherheitslösungen, die auf **M365** zugeschnitten und nahtlos integrierbar sind. Eine KI-gestützte Erkennung blockiert auch die raffiniertesten E-Mail-basierten Bedrohungen. Einfach zu verwaltende Add-Ons reduzieren das Gesamtrisiko, die Komplexität und die Kosten zusätzlich – allen voran das unabhängige Mimecast Cloud Archive, mit dem Unternehmen z.B. Daten des Kommunikationstools Teams zuverlässig, sicher und verschlüsselt archivieren können.



der Unternehen nutzen M365

teilen vetrauliche Informationen über M365

scätzen Sicherheit von M365 als sehr hoch ein

Cyberversicherung – Grundabsicherung ersetzt nicht die eigene Prävention

Ein Cyberangriff oder Informationsdiebstahl durch Hacker oder Innentäter kann erheblichen oder gar existenzgefährdenden Schaden im Unternehmen anrichten und zu Folgenkosten durch Schadenersatzansprüche von betroffenen Dritten führen. **Eine Cyberversicherung kann einen Angriff oder dessen Schäden nicht verhindern. Sie mildert die finanziellen Schäden infolge des Angriffs jedoch ab.** Weiterhin hilft sie häufig mit weiteren Serviceleistungen, um im Notfall schnellstmöglich zum Normalbetrieb zurückzukehren. Häufig gibt es ein Zusammenspiel von erforderlichen **(Mindest-)** Schutzmaßnahmen, um eine Cyberversicherung abschließen zu können, und der Höhe der Versicherungsprämie. **Die aktive Reduzierung des Risikos kann dazu beitragen, die Versicherungsprämie zu optimieren.**

Gerade für mittelständische Unternehmen können **Cybersicherungen** sinnvoll sein, sie sollten aber nicht das einzige Mittel zur Absicherung bleiben.

Es mag finanziell sinnvoll sein, sich gegen Cyberrisiken zu versichern, aber selbst die beste Cyber-Versicherung kann nur Schäden begrenzen, die bereits entstanden sind; sie kann nicht verhindern, dass der Schaden überhaupt erst entsteht. **Das kann nur ein eigener Cyber-Vorsorgeplan leisten.**

Security-Ökosystem statt vieler Einzellösungen

Der Markt für Security-Lösungen ist extrem vielfältig und komplex. Und meist sind in Unternehmen auch mehrere Lösungen parallel im Einsatz. Verschiedene Sicherheitslösungen sammeln unterschiedliche Informationen zu Cyberrisiken. Je besser diese Informationen zwischen den einzelnen Systemen ausgetauscht werden, desto umfassender sind sie und können größtmöglichen Schutz bieten.

Am besten für Herausforderungen im Bereich der Cybersicherheit gerüstet sind diejenigen Unternehmen, die Sicherheitstools und -plattformen einsetzen, die eine umfangreiche Bibliothek von Schnittstellen (APIs) und Drittanbieterintegrationen bieten. Vor allem ein integriertes Framework ermöglicht es Unternehmen, ihre individuellen Umgebungen effektiv zu steuern, indem es Tools konsolidiert und menschliche Fehler reduziert. Durch die Zusammenarbeit mit einem breiteren Spektrum von Sicherheitsanbietern profitieren Unternehmen, die API-Integrationen nutzen, vom kombinierten Wissen aller integrierten Plattformen und können so die allgemeine Sicherheitslage erheblich verbessern. Der umfassende Zugriff auf aktuelle Bedrohungsdaten ermöglicht es den Sicherheitsteams, Präventions-, Untersuchungs- und Reaktionspläne über mehrere Sicherheitskontrollen hinweg abzustimmen und die Geschwindigkeit ihrer Erkennungs- und Abhilfemaßnahmen zu erhöhen. Angesichts der weit verbreiteten Einführung von Cloud-basierten, hybriden Arbeitsumgebungen wird immer deutlicher, dass die Sicherheitsarchitekturen von Unternehmen aus skalierbaren, eng integrierten Lösungen bestehen müssen, die das richtige Gleichgewicht zwischen automatisierten Präventions-, Erkennungs- und Reaktionsfunktionen bieten, um Daten über ihren gesamten Lebenszyklus hinweg effektiv zu schützen.

Ein offenes API-Integrations-Framework verbindet die kritischen Funktionen und Prozesse, die von grundlegenden Sicherheitstools ausgeführt werden – E-Mail-Sicherheit, Endgerätesicherheit, Websicherheit, NDR, Datensicherheit – zu einem einzigen vernetzten Framework, das gemeinsam arbeitet und zentralisierte Bedrohungsdaten über das gesamte Ökosystem hinweg austauscht. Durch die Verbindung aller Teile des Puzzles erhalten Unternehmen die Ressourcen, um ihre Präventions- und Erkennungsfunktionen in komplexen Umgebungen zu verbessern.

KI als Cyber-Superheld: Wie künstliche Intelligenz die Sicherheit verbessert

Künstliche Intelligenz ist derzeit in aller Munde – doch was bedeutet sie im Kontext der Cybersicherheit? KI und maschinelles Lernen sind für die Informationssicherheit mittlerweile unverzichtbar geworden, da diese Technologien in der Lage sind, Millionen von Datensätzen schnell zu analysieren und eine Vielzahl von Cyber-Bedrohungen aufzuspüren – von Malware-Bedrohungen bis hin zu fragwürdigem Verhalten, das zu einem Phishing-Angriff führen könnte. Allerdings gilt auch bei der KI: Wie bei allen neuen Technologien sind Cyberkriminelle sehr findig und nutzen die Vorteile so schnell wie möglich für ihre eigenen Zwecke, so dass sich auch hier eine Art Wettrüsten anbahnt.

Vielen Unternehmen wird die Notwendigkeit des Einsatzes von KI in ihrer Sicherheitsumgebung zunehmend bewusst, wie eine aktuelle Studie von techconsult in Kooperation mit Mimecast zum Thema KI-Einsatz in der Cybersecurity zeigt. Rund die Hälfte der befragten Unternehmen in Deutschland und der Schweiz verwendet demnach bereits KI-gestützte Security-Lösungen. Weitere 34 Prozent planen, entsprechende Lösungen innerhalb des nächsten Jahre zu implementieren. Ob zur Automatisierung von Security-Prozessen, der Vermeidung von menschlichen Fehlern oder der Erkennung und Abwehr von Bedrohungen – KI ist ein mächtiges Werkzeug im Security-Kontext und kann Unternehmen maßgeblich dabei helfen, ihre Sicherheitsmaßnahmen zu verbessern und potenzielle Risiken frühzeitig zu erkennen und abzuwehren.

Drei Viertel der befragten Unternehmen, die bereits KI-gestützte Lösungen nutzen, setzen diese hauptsächlich für die Abwehr von Bedrohungen und die E-Mail-Sicherheit ein. Angesichts der Tatsache, dass E-Mail-Postfächer nach wie vor das bevorzugte Ziel von Cyberkriminellen sind, steht außer Frage, wie wichtig eine robuste E-Mail-Sicherheit ist. In diesem Zusammenhang kann künstliche Intelligenz den entscheidenden Vorteil bringen, indem sie den E-Mail-Verkehr überwacht, verdächtige Aktivitäten erkennt und Schadsoftware identifiziert und meldet bzw. direkt blockiert. Auch Datenschutz und Compliance sowie die Automatisierung von Security-Prozessen nennen die befragten Unternehmen der KI-Studie als wichtige Einsatzfelder.

Rund die Hälfte der Unternehmen sehen die schnellere Erkennung von bekannten und unbekannten Bedrohungen als den größten Vorteil des KI-Einsatzes im Cybersecurity-Bereich an. Auf Platz 2 landete die schnelle und automatisierte Reaktion auf Bedrohungen, denn gerade hier kommt es auf Geschwindigkeit an. Abwehrmechanismen müssen schnell aktiviert werden, um die Bedrohung zu eliminieren, bevor sie Schäden anrichten kann.

Weitere Vorteile liegen in der erhöhten Präzision und Effizienz bei der Gefahrenabwehr sowie in der Lernfähigkeit der KI. Dadurch, dass sie das alltägliche und normale Verhalten der Unternehmensumgebung und ihrer Nutzer erfasst, ist die Technologie in der Lage, ungewöhnliche Verhaltensweisen schneller und effizienter zu erkennen als es ein Mensch könnte. So können auch Gegenmaßnahmen ohne zeitliche Verzögerung in die Wege geleitet werden. KI entlastet außerdem die durch Personal- und Fachkräftemangel stark beanspruchten IT-Teams und trägt damit zusätzlich zu einer Minimierung menschlicher Fehler bei.

Fazit

Mittelständische Unternehmen sind gut beraten, sich jetzt intensiv mit ihrem Cyberrisikoprofil auseinander zu setzen und ihre Cybersecurity-Strategie gegebenenfalls anzupassen. Denn noch nie war das Risiko, von einem Cyberangriff betroffen zu sein, so hoch. Die Frage ist nicht, ob ein Angriff passiert, sondern wann. Das hauptsächliche Einfallstor für Cyberkriminelle ist zwar nach wie vor die E-Mail, durch die immer stärkere Nutzung von Collaborationstools wächst die Zahl der möglichen Angriffsvektoren jedoch stetig. Und bei der Nutzung von M365 sollten Unternehmen darüber nachdenken, für eine zusätzliche Sicherheitsschicht zu sorgen. Am besten mit einem Anbieter, der die gefährlichsten E-Mail-Bedrohungen wirksam blockiert und der vielfältige Integrationsmöglichkeiten im gesamten Cybersecurity-Ökosystem bietet. Denn Cyberversicherungen können nur Schäden ausgleichen. Schäden verhindern kann nur der unternehmenseigene Vorsorgeplan.

Der Mittelstand. BVMW e.V. Bundesverband

Der Bundesverband mittelständische Wirtschaft (BVMW) vertritt die Interessen der mittelständischen Wirtschaft, vernetzt Unternehmen und bietet Leistungen und Unterstützung z. B. im Zusammenhang mit Digitalisierung und Technologietransfer an.

www.bmvw.de

mimecast

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 Email- und Collaboration Security auf das nächste Level.

www.mimecast.com/de