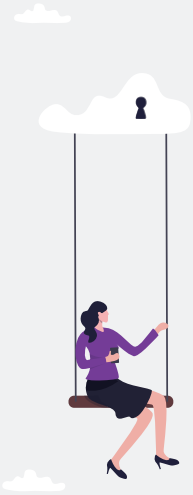
proofpoint.

E-BOOK



Schutz für Microsoft 365

So schützt eine dedizierte Sicherheitslösung Anwender und Daten und steigert den Wert Ihrer Cloud-Investition

Einführung

In der modernen Geschäftswelt sind nur wenige Tools so wichtig wie Microsoft 365. Für viele Unternehmen ist die Plattform die Grundlage für die Remote-Arbeit, die weltweite Zusammenarbeit und die Cloud (und steht meist als Synonym für diese Begriffe).

Leider ist sie aufgrund ihrer Allgegenwärtigkeit und zentralen Rolle bei der Arbeit auch ein bevorzugtes Ziel für Cyberangreifer – und häufig der wichtigste Vektor zur Kompromittierung von Opfern. Gleichzeitig rücken durch den beschleunigten Wechsel zur Remote- und Hybrid-Arbeit insiderbezogene Bedrohungen sowie Datenverlustrisiken in den Fokus der Sicherheitsmaßnahmen.

Heutige hochentwickelte Angriffe nutzen nicht nur technische Exploits, sondern auch Phishing- und Social-Engineering-Taktiken. Damit sollen die Anwender zur Installation von Malware, zur Weitergabe von Anmeldedaten oder anderer vertraulicher Informationen sowie zur Überweisung von Geldern verleitet werden. Zudem erhöhen die Bedrohungsakteure die Zahl und den Umfang dieser personenzentrierten Angriffe und richten dadurch größere Schäden an als je zuvor.

Massen-Mailings, Spam und gefährliche E-Mails senken den Wert Ihrer Investition in Microsoft 365. Große Mengen dieser unerwünschten E-Mails beeinträchtigen nicht nur die Arbeitsproduktivität, sondern bringen die ohnehin schon stark ausgelasteten Sicherheits- und IT-Teams an ihre Grenzen.

Microsoft 365 ist zwar ein unverzichtbares Collaboration-Tool, allerdings empfehlen Experten wie Gartner und Forrester den Einsatz einer umfassenden Lösung für E-Mail-, Cloud- und Datensicherheit statt der plattformeigenen Angebote.[1,2]

Dieses E-Book befasst sich mit aktuellen Bedrohungen sowie empfohlenen Vorgehensweisen zum Schutz von Anwendern und Daten und gibt Empfehlungen zu Funktionen, die die Sicherheit von Microsoft 365 verbessern können.

1 Mark Harris, Peter Firstbrook u. a. (Gartner): „Market Guide for Email Security“ (Market Guide für E-Mail-Sicherheit), Oktober 2021.

2 Jess Burn, Joseph Blankenship u. a. (Forrester): „Best Practices: Phishing Prevention“ (Bewährte Methoden zum Verhindern von Phishing), November 2021.

ABSCHNITT 1

So nehmen Angreifer Ihre Microsoft 365-Anwender ins Visier

Wenig überraschend beginnen die meisten gezielten Angriffe mit einer E-Mail.

Die Bandbreite der E-Mail-Angriffe reicht von Phishing bis zu Malware – und bei E-Mails fällt es Angreifern besonders leicht, den Faktor Mensch auszunutzen, um Anmeldeinformationen, Daten und mehr zu stehlen. Diese Bedrohungen können Ihr Unternehmen finanziell schwer treffen. Die durchschnittlichen Kosten einer Datenkompromittierung liegen weltweit bei einem Rekordwert von 4,35 Millionen US-Dollar und sind damit im Vergleich zu den letzten drei Jahren um sage und schreibe 43 % gestiegen.[3] Dieser Wert ist in den USA mit 9,44 Millionen US-Dollar und einem Anstieg von 15 % gegenüber 2019 sogar noch höher.[4]

3 Ponemon Institute: „Cost of a Data Breach 2022“ (Kosten von Datenkompromittierungen 2022) und „Cost of a Data Beach 2019“ (Kosten von Datenkompromittierungen 2019), Juli 2022 bzw. August 2019.

4 ebd.

66 %

der Unternehmen verzeichneten im Jahr 2021 mindestens einen personalisierten Spearphishing-Angriff

Phishing

In den mehr als 20 Jahren seit der ersten Einstufung als Bedrohung hat sich Phishing zu einem kommerziellen Geschäft entwickelt. Cyberkriminelle setzen für den Diebstahl von Anmeldedaten, Geld und wertvollen Informationen eine große Vielfalt an Techniken ein.

Heute gehen Angreifer beim Phishing in mehreren Stufen vor und sind in der Lage, viele herkömmliche Schutzmaßnahmen zu überwinden. Angriffe können sehr breit gefächert oder äußerst gezielt erfolgen. Häufig kommt Malware zum Einsatz, in anderen Fällen jedoch nicht. Einige Cyberkriminelle verteilen ihre Phishing-E-Mails sogar über legitime Marketingdienste, um Spamfilter und andere Abwehrmaßnahmen zu umgehen.

Bei etwa 66 % der Unternehmen kam es 2021 zu mindestens einem personalisierten Spearphishing-Angriff und bei 65 % zu mindestens einem BEC-Angriff (Business Email Compromise, auch als Chefmasche bezeichnet)[5] (siehe „Business Email Compromise (BEC) und Nachahmung von Lieferanten“ auf der nächsten Seite).

Unabhängig von der Vorgehensweise sind Phishing-Angriffe meist äußerst erfolgreich. Tatsächlich haben 83 % der Unternehmen im letzten Jahr einen erfolgreichen Phishing-Angriff verzeichnet. Im Vorjahr waren es noch 57 %.[6]

Malware

Das AV-TEST Institut verzeichnet täglich über 450.000 neue Malware-Varianten und gefährliche Anwendungen.[7] Doch der Kreativität der böswilligen Akteure sind damit noch lange keine Grenzen gesetzt.

Beim Auswählen neuer Ziele sind sie äußerst einfallsreich. Sie nutzen automatisierte Tools, um in Profilen von sozialen Netzwerken nach Informationen über Ihre Mitarbeiter zu suchen. Sie wissen, wo Ihre Anwender arbeiten (und in welcher Position), ob sie verheiratet sind und wo sie in der Vergangenheit gearbeitet haben. Sie kennen ihre Interessen, Hobbys und viele weitere Details.

Diese Informationen dienen mehreren Zwecken: der Identifizierung von Anwendern, die über die gewünschten Daten oder den richtigen Zugriff verfügen, und als Köder für E-Mails, die die Anwender zum Klicken bewegen sollen. Fallen die Empfänger auf den Köder herein, werden Schaddaten im System abgelegt.

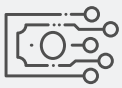
5 Proofpoint: „State of the Phish 2022“, Februar 2022.
6 ebd.
7 AV-TEST Institut: „Malware (https://www.av-test.org/en/statistics/malware/)“, im August 2022 abgerufen.

Business Email Compromise (BEC) und Nachahmung von Lieferanten

BEC- und Lieferantenbetrug sind neue und schwerwiegende Bedrohungen. Das FBI schätzt, dass diese Angriffe bei den Opfern seit 2016 Kosten von mehr als 43 Milliarden US-Dollar (an realen und potenziellen Verlusten) verursacht haben.

Bei den Angriffen werden Autoritätspersonen, Geschäftspartner, Kunden oder Lieferanten imitiert. Häufig werden dabei gefälschte E-Mail-Adressen oder Doppelgänger-Domains verwendet. In einigen Fällen nutzen die Angreifer ein legitimes, aber kompromittiertes E-Mail-Konto. Dieser Missbrauch kann mit Microsoft 365 allein nahezu nicht erkannt werden. Ganz unabhängig von den gewählten Taktiken ist das Ziel immer das gleiche: die Opfer dazu zu bewegen, Geld zu überweisen oder umzuleiten.

Eine typische BEC-E-Mail scheint zum Beispiel von einem vertrauenswürdigen Lieferanten zu stammen, der einen Mitarbeiter der Finanzabteilung um Folgendes bittet:



Bank-überweisungen

Umleitung einer Zahlung

Änderung von Bankverbindungen

In den meisten Fällen geht das überwiesene Geld dabei direkt an die Cyberbetrüger. Im Durchschnitt werden mit jedem BEC-Angriff fast 180.000 US-Dollar erbeutet.

BEC-E-Mails beschränken sich jedoch nicht nur auf betrügerische Überweisungen, sondern fordern die Empfänger in anderen Fällen zur Weiterleitung von personenbezogenen Informationen, Lohnabrechnungen sowie anderen sensiblen Daten auf.

Die Angriffsziele sind Personen auf jeder Unternehmensebene, ganz unabhängig vom Geschäftsbereich, der Abteilung oder dem Team, in dem sie tätig sind. Deshalb müssen Sie den BEC-Schutz möglicherweise auf alle Mitarbeiter ausweiten.

Kontenkompromittierung

Durch die Kompromittierung eines vertrauenswürdigen Microsoft 365-Kontos gelangen die Angreifer an eine Fülle von Informationen, die sie für eine Vielzahl anderer Angriffe nutzen können.

Häufig werden dabei bevorzugt Anwender mit umfassenden Berechtigungen ins Visier genommen. Wenn die Angreifer Zugang zu den E-Mail-Konten der Geschäftsführung oder leitenden Angestellten der Personalabteilung haben, können sie auf nahezu alle Daten im Netzwerk zugreifen. Zudem können sie die Vertrauensbeziehungen der Geschäftsführung ausnutzen, um damit BEC-Angriffe gegen Geschäftspartner durchzuführen. Dies führt nicht nur zu Unterbrechungen der normalen Abläufe, sondern kann auch die wertvollste Ressource Ihres Unternehmen beschädigen: die Reputation.

Hochentwickelte Taktiken

Bei fast allen diesen Angriffen werden eine oder mehrere Formen der subtilen Manipulationskunst des Social Engineering genutzt. Dabei werden die Opfer durch Täuschung dazu bewegt, gegen ihr eigenes Interesse zu handeln.

Per Social Engineering werden sie dazu verführt, auf unsichere Links zu klicken, schädliche Anhänge zu öffnen, Gelder umzuleiten und vertrauliche Daten herauszugeben.

Eine der Entwicklungen, die wir am wenigsten erwartet hatten, war die starke Zunahme von Angriffen per Telefon, die sehr direkte Interaktionen erfordern. Bei den per E-Mail verschickten Ködern kommen keine Malware oder schädlichen URLs zum Einsatz, sodass sie ohne zusätzliche Sicherheitsmaßnahmen für Microsoft 365 häufig unerkannt bleiben. Die Opfer sollen dazu verleitet werden, einen Fake-Kundendienst anzurufen.

Wenn das Opfer den Köder geschluckt hat, weist der Angreifer es per Telefon an, ihm Remote-Zugriff auf seinen Computer zu geben oder Malware manuell herunterzuladen. Laut unseren Daten gibt es jeden Tag mehr als 100.000 Angriffsversuche dieser Art.

ABSCHNITT 2

Warum „gut genug“ nicht mehr ausreicht

Die integrierten Sicherheits- und Compliance-Funktionen von Microsoft 365 können in begrenztem Maße weiterhelfen. Da sich die Bedrohungen häufen und weiterentwickeln, benötigen Sie jedoch möglicherweise weitere Sicherheitsebenen.

Durch die hektischen Bemühungen im Zuge der notwendigen Einführung von Remote- und Hybrid-Arbeit nahm die Cybersicherheit in einigen Fällen einen geringeren Stellenwert ein. Nachdem das Schlimmste der COVID-19-Pandemie überstanden ist, wollen viele nun ihre Cloud-Investitionen ausbauen.

Unzureichender Schutz vor Cyberbedrohungen und Datenverlust kann zu kostenintensiven Kompromittierungen führen, die Ihrer Marke und Reputation schaden und Ihr Unternehmen finanziell schwer treffen können. Deshalb ist es für Ihre Sicherheit und Compliance wichtig, dass Sie die in Microsoft 365 enthaltenen Schutzfunktionen erweitern.

Heutige Angriffe richten sich gegen Menschen

Cyberkriminelle wissen, dass die meisten Personen in Ihrem Unternehmen vorrangig Microsoft 365 einsetzen, während alle anderen Unternehmenstools erst an zweiter Stelle kommen. Viele dieser Anwender haben Zugang zu Geldmitteln oder hochwertigen Daten, während andere Mitarbeiter weniger offensichtliche Schwachstellen, Angriffsprofile und Zugriffsrechte haben.

Angreifer ködern Anwender mittels Social Engineering, sodass diese:

Infizierte Anhänge öffnen

Schädliche Websites aufrufen

Assets weitergeben (z. B. Anmelde- oder Finanzdaten)

Mittels OAuth dauerhaften Zugriff auf Konten gewähren

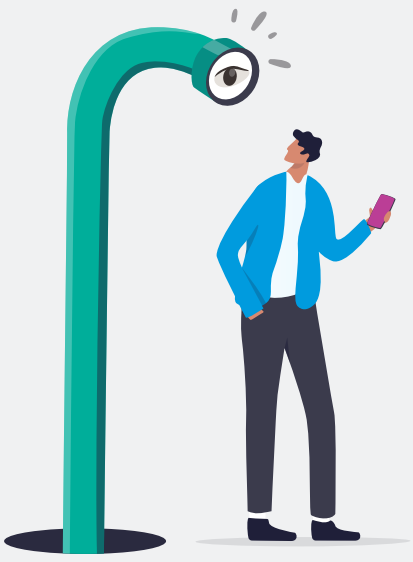
Sobald sich die Cyberkriminellen mithilfe von Malware, gestohlenen Anmeldedaten oder über OAuth Zugang zum System des Anwenders verschafft haben, können sie Ihre Mitarbeiter, Daten und Systeme angreifen.

Daher ist es nicht überraschend, dass das Thema Sicherheit nun auch in der Führungsetage von Unternehmen angekommen ist. Der Schutz Ihrer Microsoft 365-Umgebung ist inzwischen eine geschäftskritische Entscheidung – und effektive Cybersicherheitsansätze müssen sich heute in erster Linie auf den Menschen konzentrieren.

Was Sie nicht sehen, können Sie auch nicht schützen

Der Schutz Ihrer Microsoft 365-Bereitstellung vor externen Bedrohungen und durch Insider ausgelösten Datenverlust erfordert eine gemeinsame Grundlage: Transparenz.

Um Angriffe effektiv erkennen und darauf angemessen reagieren zu können, benötigen Sie die hierfür erforderlichen Informationen. Ohne Schutzfunktionen mit der Möglichkeit, umfangreiche und detaillierte Berichte zu generieren, müssen Sie nach der sprichwörtlichen Nadel im Heuhaufen suchen.



Das Blockieren von Bedrohungen, bevor diese die Posteingänge der Anwender erreichen, hat zwei wichtige Vorteile. Erstens erhalten Sie einen Überblick über den vollständigen Angriff, nicht nur über die letzten Phasen, nachdem der Schaden bereits eingetreten ist. Zweitens können Sie Bedrohungen durch frühzeitiges Abfangen – am besten schon, ehe sie die Anwender erreichen – stoppen, bevor sie Ihre Umgebung kompromittieren.

Aus dem gleichen Grund ist der Überblick, der durch die MIP-Funktionen (Microsoft Information Protection) bereitgestellt wird, für den Schutz von Daten oder die Reaktion auf Datenverlust-Zwischenfälle unverzichtbar. Sie müssen wissen, wo sich Ihre vertraulichen Daten befinden und was Ihre Anwender damit machen. Zudem benötigen Sie Kontext, um zu verstehen, ob ein Insider-Risiko durch einen fahrlässig handelnden, kompromittierten oder böswilligen Anwender verursacht wird.

Dies ist besonders in der heutigen schnelllebigen Geschäftswelt von Bedeutung. Daten entwickeln sich so schnell weiter wie die nächste Innovation oder Firmenübernahme. Zur Gewährleistung ihrer Sicherheit benötigen Sie prädiktive Funktionen, die auf vertrauliche Daten hinweisen, sodass Sie diese schützen und von Ihrer Investition in die MIP-Funktionen profitieren können.

Isolierte Funktionen für Sicherheit, DLP und Compliance sind nicht nachhaltig

In der sich beständig verändernden Bedrohungslandschaft koordinieren Cyberkriminelle ihre Angriffe über mehrere Vektoren und kompromittieren häufig Anwenderkonten, um den dazugehörigen Zugriff auf wichtige Daten, Systeme und andere Ressourcen zu missbrauchen.

Deshalb ist eine integrierte mehrschichtige Verteidigung unverzichtbar. Doch eine effektive Lösung muss sich auch mit dem Rest Ihres Ökosystems für Sicherheit, Informationsschutz und Compliance vernetzen. Das umfasst sowohl Ihren E-Mail-Schutz als auch Ihr DLP-System (Data Loss Prevention) bis hin zum CASB (Cloud Access Security Broker) und Ihrer Identitätsmanagement-Plattform.

Die intelligente und automatisierte Koordinierung vereinfacht die Verhinderung, Erkennung und Abwehr von Bedrohungen, die Ihre Mitarbeiter über Microsoft 365 erreichen.

Bedrohungen

Durch die flächendeckende Migration zu OneDrive, Teams und anderen Microsoft 365-Produktivitätsanwendungen wird Datensicherheit zur Herausforderung. Sie müssen in der Lage sein, die von Ihren Mitarbeitern erstellten, abgerufenen und weitergegebenen Daten zu identifizieren und abzusichern.

Das ist mit Microsoft 365 allein nicht immer einfach. Die integrierte Bedrohungserkennung der Plattform bietet Ihnen möglicherweise nicht den nötigen Überblick über Cyberbedrohungen, Anwenderaktivitäten und Datenbewegungen für E-Mails, die Cloud und Endpunkte.

Datenverlust

Alle Anwender stellen in gewissem Maße ein Risiko für Unternehmen dar. Jeder ist jedoch auf seine ganz eigene und immer neue Art und Weise gefährlich. Einige Anwender sind böswillig, viele sind nachlässig und noch andere wurden eventuell kompromittiert. Deshalb schützen universelle Sicherheits- und Datenzugangsrichtlinien nicht vor Insider-Risiken und Bedrohungen, die Personen über Microsoft 365 angreifen.

Sie benötigen Transparenz und Kontrollen, die die Mitarbeiter, Daten und Bedrohungen als Kontext und in Echtzeit berücksichtigen. Nur dann können Sie Datenverlust und Missbrauch im gesamten Unternehmen verhindern.

Unerwartete E-Mail-Ausfälle können enorme geschäftliche Auswirkungen haben

Ein zuverlässiger E-Mail-Zugang ist für den Geschäftsbetrieb heute unverzichtbar und ein unerwarteter Ausfall kann kostspielige Konsequenzen haben. Der Zugang zu E-Mails muss daher rund um die Uhr gewährleistet werden.

Ausfälle von Microsoft 365 kommen unweigerlich vor, aber sie sollten Ihren Geschäftsbetrieb nicht zum Stillstand bringen. Deshalb benötigen Sie Funktionen für störungsfreien Geschäftsbetrieb, die die Produktivität Ihrer Anwender auch bei einem Ausfall von Microsoft 365 gewährleisten.

ABSCHNITT 3

Berechnen des Werts von verbesserter Sicherheit

Wenn Sie auf eine dedizierte Sicherheitslösung für Ihre Microsoft 365-Bereitstellung verzichten, sparen Sie auf den ersten Blick Geld.

Ein mangelhafter Schutz Ihrer Investition wird Sie jedoch sehr wahrscheinlich Zeit, Daten, Geld und auch Ihre Reputation kosten. Nachfolgend erfahren Sie, wie Sie durch die Erweiterung der in Microsoft 365 integrierten Funktionen mehr Compliance und Sicherheit erzielen.

Für Sicherheitsteams

Sicherheit war schon immer ein schwieriger Job und die aktuellen hochentwickelten Bedrohungen erschweren die Situation noch weiter. Sicherheit wird aufgrund von Compliance-Vorschriften und bekannt gewordenen Angriffen nun auch auf Vorstandsebene diskutiert. Dabei geht es nicht allein um Effizienz, sondern um einen Überblick über die Bedrohungen, die Ihre Mitarbeiter gefährden, sowie um die damit verbundenen Risiken für Ihr Unternehmen.

Bedrohungen

Ohne Überblick und Daten über die wichtigsten Sicherheitsprobleme kann erheblich Zeit verloren gehen. Laut dem Ponemon Institute hat die Erkennung und Reaktion auf Kompromittierungen mit 1,44 Millionen US-Dollar den größten Anteil an den Kosten.[8] Das ist ein Anstieg von 16 % gegenüber dem Vorjahr und das erste Mal in sechs Jahren, dass diese Kosten höher sind als die Umsatzverluste aufgrund von Kompromittierungen.

Um ihre Ziele umzusetzen, missbrauchen Angreifer die Tools, die Ihre Anwender nutzen. Ganz gleich, ob es um die Erpressung mit wichtigen SharePoint-Dateien, die Übertragung von schädlichen Dateien über OneDrive oder die Ausnutzung von Schwachstellen in Microsoft Teams geht – Microsoft 365-Anwender sehen sich mit einer Flut von Bedrohungen konfrontiert und benötigen zusätzliche Sicherheitsebenen.

Stellen Sie sich folgende Fragen:

- Wie viel Produktivität geht dadurch verloren, dass die Schäden E-Mail-bezogener Zwischenfälle behoben werden müssen?
- Wie viel Zeit geht durch die Erkennung und Behebung kompromittierter Konten und durch die Untersuchung, Priorisierung und Bestätigung von Bedrohungen verloren? Und wie viel Zeit verbringen Sie mit der Bereinigung von schädlichen Anhängen oder URLs in E-Mails, die in die Postfächer Ihrer Anwender gelangt sind?
- Wie quantifizieren Sie das Risiko, das dadurch entsteht, dass Ihre Anwender diesen E-Mails über einen längeren Zeitraum ausgesetzt sind?
- Wie viel Zeit geht dadurch verloren, dass isolierte Sicherheitsprodukte Bedrohungen nicht schnell eindämmen und die Reputation Ihres Unternehmens schützen können? (Diese Zeitspanne kann pro Warnmeldung von Stunden bis Tagen reichen.)
- Wie viel Zeit benötigen Sie zusätzlich, um die gezielten Bedrohungen für Ihre Umgebung zu verstehen, wenn Sie nicht den vollen Überblick haben?
- Wie groß sind die Auswirkungen auf die Sicherheit, wenn Anwender bei einem Ausfall der Microsoft 365-E-Mails ihre privaten E-Mail-Adressen nutzen? (In einer Untersuchung von Gartner wurden die Kosten auf über 300.000 US-Dollar pro Stunde geschätzt.[9] Beachten Sie dabei, dass einige Microsoft-Ausfälle mehrere Tage dauern.[10])
- Wie viel wären Sie bei Angriffen, die durch Microsoft 365 allein nicht erkannt werden, bereit zu zahlen, um Dateien freizukaufen – und wie hoch wären stattdessen die Kosten für die Wiederherstellung der Abläufe?

8 Ponemon Institute: „Cost of a Data Breach Report 2022“ (Kosten von Datenkompromittierungen 2022), Juli 2022.

9 Andrew Lerner (Gartner): „The Cost of Downtime“ (Die Kosten von Ausfallzeiten), Juli 2014.

10 Ed Targett (Computer Business Review): „Microsoft Office 365 Outage: Day Two as Enterprise User Grumbles Grow“ (Ausfall von Microsoft Office 365: Tag zwei und die Beschwerden der Unternehmensanwender nehmen zu), Januar 2019.

Datenverlustprävention und Informationsschutz

Unternehmen drohen jederzeit Datenverluste. Böswillige Insider können Daten weitergeben. Externe Kriminelle können sie stehlen. Und selbst bei gutwilligen Mitarbeitern besteht die Gefahr, dass sie unwissentlich wertvolle Unternehmensressourcen kompromittieren.

Allein im Jahr 2021 meldeten Unternehmen 1.882 Datenkompromittierungen, ein sprunghafter Anstieg von 68 % gegenüber 2020.[11] (Die Zahl umfasst Datenkompromittierungen und Datenlecks.)

Die durch Datenkompromittierungen entstehenden Haftungsfragen haben das Thema Sicherheit bis in die Führungsetagen getragen. Daher muss die Sicherheit von Microsoft 365 einer genauen Prüfung unterzogen werden.

Überprüfen Sie die Möglichkeiten zur Suche nach sensiblen Daten (einschließlich verschiedenen Dateitypen), zur Behebung von Problemen auf mehreren Kanälen, zur Richtliniendurchsetzung sowie zur Meldung von Richtlinienproblemen. Ergänzen Sie die nativen Funktionen mit einer Lösung, die Richtlinien auf ausgehende E-Mails, OneDrive, SharePoint und Teams anwenden kann, sowie Einblicke in E-Mails, Endpunkte und die Cloud bietet.

Datenkompromittierungen entstehen durch böswillige, fahrlässig handelnde oder kompromittierte Anwender. Es gibt also kein Patentrezept zur Behebung dieser Bedrohungen. Stattdessen benötigen Sie Kontextinformationen und Einblicke, um die genaue Ursache ermitteln zu können.

Folgende Faktoren sollten Sie berücksichtigen:

- Welchen Wert haben die Daten, die Angestellte beim Verlassen des Unternehmens aus Microsoft 365 mitnehmen?
- Wie hoch wären die Kosten durch gestohlene oder offengelegte Daten, wenn Ihre DLP-Lösung nicht die kritischsten Ressourcen in den Kanälen schützen kann, die Ihre Mitarbeiter nutzen? Können Sie sensible Daten in E-Mails, der Cloud und auf Endpunkten erkennen? Und können Sie die vielen verschiedenen Dateitypen erkennen, die eventuell sensible Informationen erhalten?
- Haben Sie die Möglichkeit, Richtlinien zentral zu definieren?
- Können Sie schnell bestimmen, welche Inhalte und Aktionen eine Richtlinienwarnung ausgelöst haben? Haben Sie die nötigen Kontextinformationen, um ermitteln zu können, ob ein Insider-Zwischenfall durch einen böswilligen, einen fahrlässig handelnden oder einen kompromittierten Anwender verursacht wurde? Genügen die Informationen, um richtig darauf zu reagieren?
- Sind Sie sicher, dass Ihr geistiges Eigentum vollständig geschützt ist?
- Verfügen Sie über einen Workflow zur Vorfallreaktion, mit dem Sie Probleme beheben können? Können Sie mithilfe automatischer Reaktionen Inline-Blockierungen für E-Mails, Dateifreigaben, Microsoft Teams und Microsoft SharePoint-Websites durchführen und Probleme beheben? Benötigen Sie für jeden dieser Kanäle eine separate DLP-Lösung? Wie gewährleisten Sie, dass diese Richtlinien synchronisiert und konsistent dokumentiert werden?
- Erhalten Sie bei der Untersuchung von DLP-Warnungen ein aussagekräftiges und leicht verständliches Gesamtbild über das Geschehene? Können Sie diese Informationen problemlos an die Rechts- und Personalabteilung weitergeben?
- Können Sie sehen, wer Zugriffsrechte für Daten und Systeme hat, und können Sie Richtlinien für Einzelpersonen und Personengruppen erstellen?

11 Identity Theft Resource Center: „First Half 2022 Data Breach Analysis“ (Analyse der Datenschutzverletzungen für das 1. Halbjahr 2022), Juli 2022.

- Können Sie schnell riskante Drittanbieter-Anwendungen ermitteln, die Ihre Anwender nutzen, und Ihr Unternehmen vor diesen Anwendungen schützen?
- Haben Sie neben der Nutzung von integrierten oder benutzerdefinierten Detektoren zur Identifizierung vertraulicher Daten die Möglichkeit, mithilfe von künstlicher Intelligenz und Machine Learning dynamisch aus Daten zu lernen, um Risiken aufzudecken?
- Kann die Lösung die Genauigkeit Ihrer DLP-Richtlinien verbessern?

Für IT-Abteilungen

Als IT-Administrator sollten Sie die Kosten für Ausfallzeiten und Support berücksichtigen.

(Dienst-)Verfügbarkeit

Microsoft 365 verspricht zwar eine Verfügbarkeit von 99,99 %, aber Ausfälle kommen vor. (Ein kurzer Blick auf den Twitter-Status-Feed von Microsoft zeigt, wie häufig Dienstprobleme auftreten.)

Wenn Sie die Sicherheit Ihrer Microsoft 365-Umgebung verbessern und diese Kosten senken möchten, stellen Sie sich folgende Fragen:

- Wie stark hängen Ihre Geschäftsabläufe von E-Mails ab? Wie groß sind die Auswirkungen, wenn E-Mails von bestehenden oder potenziellen Kunden aufgrund eines E-Mail-Ausfalls verloren gehen?
- Wie häufig gibt es Störungen des E-Mail-Dienstes in Microsoft 365?
- Wie schnell erhält die IT eine Warnmeldung bei einem Ausfall?
- Verfügen Sie über genügend Daten sowie einen ausreichenden Überblick, um zuverlässige Prognosen zum Zeitpunkt der Wiederherstellung des Dienstes geben zu können?
- Welche Sicherheits- und Compliance-Risiken ergeben sich, wenn gutmeinende Mitarbeiter auf private E-Mail-Adressen ausweichen, um ihre Arbeit zu erledigen?

E-Mail-Nachverfolgungen und Meldungen zu nicht gesendeten Nachrichten (NDR)

„Wo ist meine E-Mail?“ Diese Frage wird täglich an IT- und Sicherheitsexperten gerichtet.

Überprüfen Sie Ihren Prozess genau und stellen Sie sich folgende Fragen:

- Wie viel Zeitaufwand ist für den Support bei solchen Problemen akzeptabel?
- Wie häufig werden Indizes zu Nachrichtenprotokollen erstellt? Wie lange werden diese Protokolle gespeichert?
- Werden Ergebnisse zu Suchabfragen innerhalb von Minuten oder Stunden zurückgegeben?
- Verläuft die Suche in alten und neuen Protokollen unterschiedlich?
- Verfügen Sie über die erforderlichen Suchkriterien, um Protokolle schnell zu finden? Sind die bei der Suche erhaltenen Ergebnisse ausreichend?
- Welche Schritte sind erforderlich, um den Support für detailliertere Informationen zu kontaktieren?
- Welche Auswirkungen haben False Positives auf die Anzahl der gefundenen Nachrichten und den Zeitaufwand?

Zur Bereinigung der E-Mails und Systeme erforderlicher Zeitaufwand

Nach der Kompromittierung von Systemen kann die IT-Abteilung Stunden oder gar Tage damit beschäftigt sein, auf infizierten Systemen neue Images aufzuspielen.

Außerdem sollte die IT-Abteilung diese E-Mails entfernen, um eine erneute Infektion zu verhindern, was schnell vorkommt, wenn ein Anwender unbewusst erneut auf den Inhalt zugreift oder die betroffene E-Mail unbedacht an einen anderen Anwender weiterleitet.

Dieser Prozess beeinträchtigt sowohl die IT-Abteilung als auch die Produktivität der Mitarbeiter typischerweise einen vollen Arbeitstag lang. Stellen Sie sich folgende Fragen:

- Für wie viele Systeme muss unnötigerweise ein Re-Imaging durchgeführt werden?
- Verfügt die IT-Abteilung über Tools, um Infektionen zu bestätigen und Systeme zu priorisieren, die gefährdet sind, aber nicht kompromittiert wurden?
- Wie viel Zeit verbringt die IT-Abteilung mit der Bereinigung von Nachrichten?

Für Compliance-Mitarbeiter

Compliance ist eine ernsthafte Angelegenheit. Unzureichende Compliance kann hohe Kosten zur Folge haben und Ihrem Unternehmen schaden. Auf Rechenzentrumsebene hält Microsoft 365 alle wichtigen Vorschriften ein, z. B. die Datenschutzgrundverordnung der Europäischen Union (DSGVO), den HIPAA (Health Insurance Portability and Accountability Act), ISO 27001 und andere.

Doch die Plattform verfügt über begrenzte Möglichkeiten zur Archivierung und Überwachung der E-Mail-Daten, damit diese Informationen bei Rechtsstreits oder Audits schnell zur Verfügung stehen. Die fehlende rechtssichere Aufbewahrung der Datensätze und Workflows kann großen Zeit- und Ressourcenaufwand bedeuten und Kosten für Rechtsstreitigkeiten nach sich ziehen.

Sie benötigen wahrscheinlich einen Microsoft 365-Tarif, der Compliance-Funktionen beinhaltet, oder Sie müssen diese Funktionen als Add-in-Abonnement kaufen, damit Sie die folgenden Vorschriften lückenlos einhalten können:

- USA: Financial Industry Regulatory Authority (FINRA)
- USA: Securities and Exchange Commission (SEC)
- Kanada: Investment Industry Regulatory Organization (IIROC)
- Großbritannien: Financial Services Act

Diese Vorschriften sollen Investoren schützen, indem sie sicherstellen, dass die US-amerikanischen, britischen und kanadischen Sicherheitsbranchen fair und ehrlich arbeiten. Geldbußen für die Nichteinhaltung können in die Millionen gehen. Zu den Zusatzkosten gehören die Kosten für die Implementierung zusätzlicher Sicherheitsmaßnahmen, Audits sowie für potenzielle Schäden für die Reputation.

Stellen Sie sich bei der Bewertung der standardmäßig verfügbaren Microsoft 365-Funktionen diese wichtigen Fragen:

- Wenn Ihr Unternehmen sich in einem Rechtsstreit befindet, unterstützt Microsoft 365 Sie bei der Bereitstellung von Datensätzen zu allen Kommunikationen und Transaktionen, die von bestimmten Anwendern getätigt wurden (unter Berücksichtigung von sozialen Netzwerken und Enterprise-Collaboration-Tools)? Was passiert, wenn mehrere Fälle gleichzeitig laufen?
- Wie zuverlässig können Sie im Fall eines Rechtsstreits festlegen, dass Inhalte aufgrund gesetzlicher Aufbewahrungspflichten nicht gelöscht werden dürfen?
- Wie viel Zeit benötigt Ihre IT-Abteilung für die Durchführung von E-Discovery und Datenexporten? Wie schnell werden Suchvorgänge durchgeführt? Bietet Microsoft ein Service Level Agreement (SLA), das die Parameter für diese wichtige Funktion definiert? Wo erfolgt die Verarbeitung der Suchvorgänge?
- Sobald Sie den Datensatz gefunden haben, der exportiert werden soll, können Sie die Dateien automatisiert auf eine bestimmte FTP-Website hochladen? Oder müssen Sie Zeit für die manuelle Durchführung dieses Workflow-Schritts einplanen? Welche Verzögerungen ergeben sich, bis die Teams die erforderlichen Daten überprüfen können?
- Können Sie alle von Ihrem Unternehmen generierten Compliance-Inhalte erfassen und speichern? Wie sieht es mit Daten von Social-Media-Plattformen aus?
- Wie zuverlässig können Sie Inhalte überwachen? (Für einige Vorschriften müssen Sie Inhalte überwachen und stichprobenhaft untersuchen können.) Wird dafür die neueste Technologie verwendet oder erfolgt dieser Schritt mithilfe einfacher Schlüsselwortabfragen?

12 Andrew Peck, Jennifer Feldman u. a. (New York Law Journal): „Defensible deletion: The proof is in the planning“ (Begründete Datenlöschung: Planung ist alles), Januar 2021.

13 Chris Matthews (MarketWatch): „SEC fines JPMorgan $125 million for failing to keep records“ (SEC verdonnert JPMorgan zu Strafe in Höhe von 125 Mio. USD wegen fehlender Datenaufbewahrung), Dezember 2021.

ABSCHNITT 4

Minimiertes Risiko, optimierter Betrieb und niedrigere Kosten – Warum Proofpoint anders ist

In Anbetracht der aktuellen komplexen und sich ständig ändernden Bedrohungs- und Compliance-Landschaft ist ein neuer Ansatz für den Schutz vor Bedrohungen sowie Datenverlust und zur Gewährleistung von Compliance erforderlich.

Deshalb bietet Ihnen Proofpoint einen einzigartigen personenzentrierten Ansatz mit folgenden Vorteilen:

- Der branchenweit effektivste Schutz vor Bedrohungen und Datenverlust
- Verwertbare Einblicke und Kontextinformationen für interne und externe Bedrohungen
- Ein moderner, integrierter Ansatz zur Verhinderung von Bedrohungen, Datenverlust und Compliance-Verstößen
- Hervorragende Anwenderführung

Nachfolgend erfahren Sie, wie wir Ihnen helfen, die Sicherheit von Microsoft 365 zu erweitern.

Erweiterter Schutz vor Phishing, BEC-Angriffen und anderen Bedrohungen

Unser KI-gestütztes Erkennungsmodul stoppt mithilfe von Verhaltensanalysen eine breite Palette an Bedrohungen – einschließlich schwer erkennbarer Bedrohungen, die keine schädlichen Anhänge oder URLs nutzen (z. B. BEC-Angriffe).

Jeden Monat erkennen und blockieren wir 2,2 Millionen BEC-Bedrohungen mithilfe von Machine Learning und Verhaltensanalysen, die mit Billionen Datenpunkten trainiert wurden. Wir bieten Ihnen detaillierte Forensikanalysen, damit Sie nachvollziehen können, warum eine Nachricht als BEC eingestuft und blockiert wurde.

Zudem erhalten Sie Einblicke in folgende Bereiche:

- Wer in Ihrem Unternehmen von BEC-Bedrohungen ins Visier genommen wird
- Die am häufigsten eingesetzten gegen Ihr Unternehmen BEC-Taktiken
- Welchen BEC-Bedrohungen Ihr Unternehmen im Laufe der Zeit ausgesetzt ist

Unsere integrierte ganzheitliche Lösung bietet Ihnen umfangreiche Einblicke in böswillige Aktivitäten und Anwenderverhaltensweisen und kann somit weitere aktuelle Bedrohungen stoppen. Außerdem automatisiert unsere Lösung wichtige Teile der Reaktion auf Zwischenfälle, sodass Sie Ihre Anwender umfassend schützen können.

Eine prädiktive URL-Analyse scannt und neutralisiert verdächtige URLs, bevor sie zugestellt werden und wenn Anwender darauf klicken. Sie können Anhänge mit dubiosen URLs blockieren und verdächtige URLs umschreiben – unabhängig davon, ob diese in Textdateien (TXT), Rich-Text-Dateien (RTF) oder als HTML auftreten.

Dank einer durchschnittlichen Analysedauer von weniger als drei Minuten blockieren wir unsichere Anhänge schon bevor Anwender die Gelegenheit haben, damit zu interagieren – und ohne die Produktivität der Anwender zu beeinträchtigen. Wir unterstützen eine große Auswahl an Dateitypen jenseits von Office-Dokumenten, darunter PDF- und HTML-Dateien.

Für besonders gefährdete Anwender und riskante Websites öffnet unsere URL Isolation-Technologie unbekannte Links aus E-Mails in einer sicheren, abgeschlossenen Umgebung. Dadurch halten Sie Bedrohungen von Ihrer Umgebung fern.

Zudem mahnen konfigurierbare E-Mail-Warnhinweise für Ein-Klick-Meldungen die Anwender zu besonderer Vorsicht und erleichtern ihnen die Meldung potenziell schädlicher Nachrichten.

Der branchenweit effektivste Schutz für Ihre Daten

Schützen Sie Ihre Daten vor externen und internen Bedrohungen mit personenzentriertem Kontext, der die Zusammenhänge zwischen Inhalten, Verhaltensweisen und Bedrohungen aufzeigt. Unsere Zeitleistenansicht fügt die Ereignisse hinter jeder DLP-Warnung zu einem Gesamtbild zusammen. Dies ermöglicht eine schnelle Einschätzung der Absichten des Anwenders und eine problemlose Zusammenarbeit mit der Rechts- und Personalabteilung zwecks einer angemessenen Reaktion.

Wir vereinfachen die Erstellung, Anwendung und Durchsetzung einheitlicher Richtlinien für E-Mail, Cloud und Endpunkte, sodass Sie Ihre Daten schützen und geltende Vorschriften einhalten können.

Unser KI-gestütztes Datenklassifizierungsmodul unterstützt Ihr DLP-Programm und optimiert Ihre Abläufe. Sie können aus Hunderten vortrainierten Klassifizierern auswählen oder von unserem DLP-Modul benutzerdefinierte Klassifizierer aus Beispieldokumenten erstellen lassen. Das Modul lernt dynamisch aus den Daten in der Cloud und in lokalen Repositories und schlägt Wörterbücher vor, die sich mit einem Klick auf alle Kanäle anwenden lassen.

Mittels integrierter algorithmischer Analysen, unseres intelligenten Identifikatormoduls und Wörterbüchern können Sie den Schwerpunkt auf die Einrichtung und Pflege der spezifischen Datenrichtlinien Ihres Unternehmens legen. Dank standardmäßigen DLP-Workflows ist es zudem leichter, Verstöße zu finden, zu beheben und zu melden.

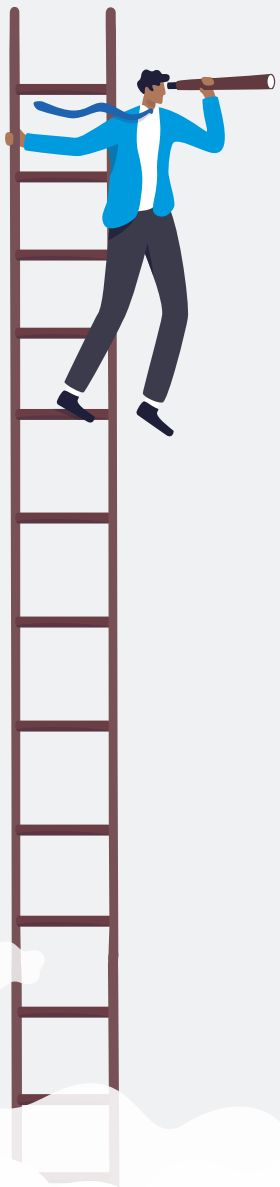
Schutz vor Kontoübernahmen

Mit unserem mehrstufigen Ansatz helfen wir Ihnen, Ihr Microsoft 365-Konto bei verdächtigen Aktivitäten mit Echtzeitwarnungen, automatischer Behebung und risikobasierten Zugriffsberechtigungen zu schützen.

Wenn es zu Zwischenfällen kommt, können Sie in unserem intuitiven Dashboard frühere Aktivitäten und Warnungen untersuchen. Unsere robusten Richtlinien weisen in Echtzeit auf Probleme hin, behandeln kompromittierte Konten, stellen schädliche Dateien unter Quarantäne und sorgen dafür, dass die erforderliche Authentifizierung basierend auf dem aktuellen Risiko erfolgt.

Die Integration in Okta erlaubt die Identifizierung einer Vielzahl von ungewöhnlichen und unsicheren Aktivitäten:

- Erfolgreiche, aber verdächtige Anmeldungen bei Microsoft 365
- Fehlgeschlagene Anmeldeereignisse
- Unerwartete Zugriffe auf Geschäftsanwendungen
- Rechteerweiterungen, die Zugriff auf wichtige Cloud-Ressourcen ermöglichen
- Rechteerweiterungen, die Anwender von den üblichen Authentifizierungsfaktoren befreien



Verbesserte Transparenz und Sicherheit in der Cloud

Wir bieten Ihnen einen personenzentrierten Ansatz für den Schutz vor Cloud-Bedrohungen. Außerdem decken wir Schatten-IT auf und verwalten Cloud- sowie Drittanbieter-OAuth-Anwendungen.

Wir bieten Schutz für Anwender, vertrauliche Daten und Cloud-Anwendungen vor externen Bedrohungen und Compliance-Risiken und erweitern so die integrierten Microsoft 365-Sicherheitsfunktionen erheblich. Identifizieren Sie Ihre Very Attacked People™ und wenden Sie risikobasierte Kontrollen an, um deren Konten zu schützen.

Blitzschnelle und umfassende Reaktion auf Zwischenfälle

Schädliche E-Mails werden automatisch aus Posteingängen entfernt. Dies umfasst auch Nachrichten, die von Anwendern gemeldet oder nach der Zustellung als unsicher eingestuft wurden. Wenn schädliche Nachrichten erkannt werden, entfernen wir sie automatisch aus den Posteingängen der Anwender, auch wenn sie bereits an andere Anwender weitergeleitet wurden. Durch diese Funktion muss Ihr Sicherheits- und Nachrichtenteam weniger Zeit für die Untersuchung und Behebung von E-Mail-Bedrohungen aufwenden.

Zudem können wir Kontoübernahmen beheben, bevor diese Ihren Daten, Abläufen, Geschäftsbeziehungen und Ihrem Ruf langfristig schaden können.

Intelligente und schnelle Archivierung

Wir garantieren Ihnen, dass Ihre Suchvorgänge unabhängig von der Größe Ihres Archivs maximal 20 Sekunden dauern – nicht Minuten oder Stunden.

Unser Cloud-basiertes Archiv unterstützt mehr als 500 Dateitypen in der Cloud und lokal, nicht nur E-Mails. Wir unterstützen eine unbegrenzte Anzahl an einbeziehbaren E-Discovery-Fällen, rechtlichen Sperrfristen und Datenexporten – ganz gleich, ob es sich um 10.000 oder 100.000 (oder auch mehr) Postfächer handelt.

Programme zur Sensibilisierung für Sicherheit, die Anwenderverhalten verändern

Wir bieten eine umfangreiche Auswahl an ansprechenden Inhalten auf Grundlage tatsächlich eingesetzter Angriffstechniken. Die Schulungsmaterialien basieren auf unseren eigenen Bedrohungsdaten und den Wissenslücken Ihrer Anwender. Zudem lassen sie sich auf die speziellen Sicherheitsanforderungen in Ihrem Unternehmen und mit den Zeitplänen Ihrer Mitarbeiter abstimmen.

Über die Grundlagenschulungen zur Steigerung des Sicherheitsbewusstseins hinaus bieten wir Phishing-Simulationen und nachträgliche Schulungen für Anwender, die auf Angriffe hereingefallen sind. Lernfortschritte lassen sich unkompliziert nachverfolgen und in Berichten zusammenfassen, sodass Sie Verbesserungspotenzial erkennen und Ihre Anwender unterstützen können.

Erstklassiger Support

Wir kümmern uns um die vollständige Installation und Anpassung Ihrer Bereitstellung und nutzen dabei die neuesten Branchenentwicklungen sowie empfohlene Vorgehensweisen. Nach der Bereitstellung erhalten Sie Support rund um die Uhr an 365 Tagen im Jahr – ganz ohne komplizierte Service-Add-ons.

Unser Unternehmen erreicht dauerhaft eine Kundenzufriedenheit von mehr als 95 % und eine jährliche Verlängerungsrate von mehr als 90 %. Daher ist es nicht überraschend, dass über die Hälfte der Fortune 100-Unternehmen zu unseren Kunden zählen.

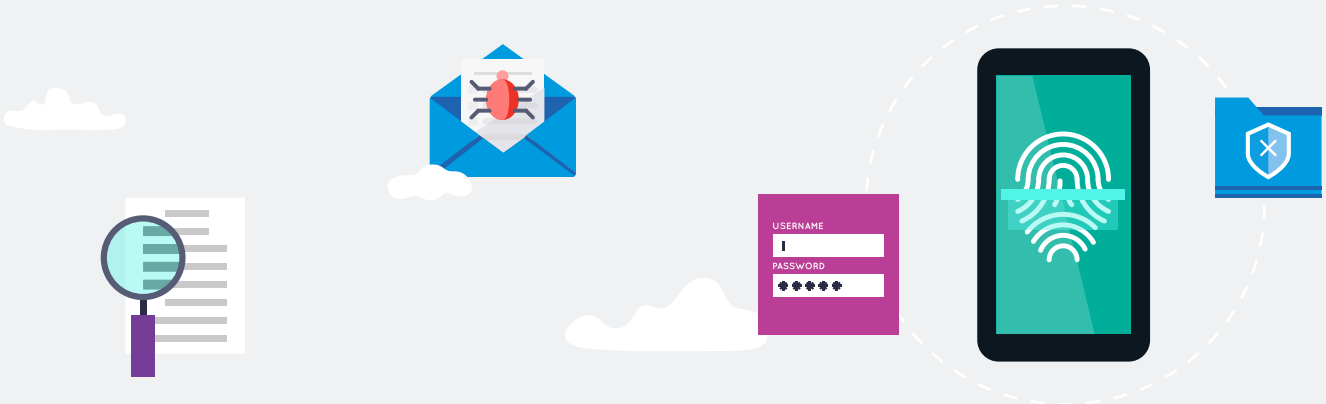
Lückenlose, vollständig integrierte Sicherheit, die Abläufe optimiert

Unsere umfassende integrierte Sicherheitsplattform kombiniert leistungsfähigen, effektiven E-Mail-, Cloud- und Informationsschutz zur Bewältigung der drängendsten Sicherheits- und Compliance-Probleme unserer Zeit. Wir integrieren zudem erstklassige Sicherheitsanbieter wie Palo Alto Networks, Okta und CrowdStrike, sodass Sie Ihren Workflow optimieren können und Ihr Sicherheitsteam schneller und besser arbeiten kann.

Das Ergebnis ist eine integrierte, personenzentrierte Sicherheitslösung, die Ihre Microsoft 365-Umgebung schützt.

Durch unseren bewährten Sicherheits- und Compliance-Ansatz für Microsoft 365 erhalten Sie folgende Vorteile:

- Minimierung von Risiken
- Entlastung wichtiger Sicherheits- und IT-Ressourcen
- Geringere Kosten
- Höhere Effektivität und Effizienz Ihrer Sicherheitsabläufe



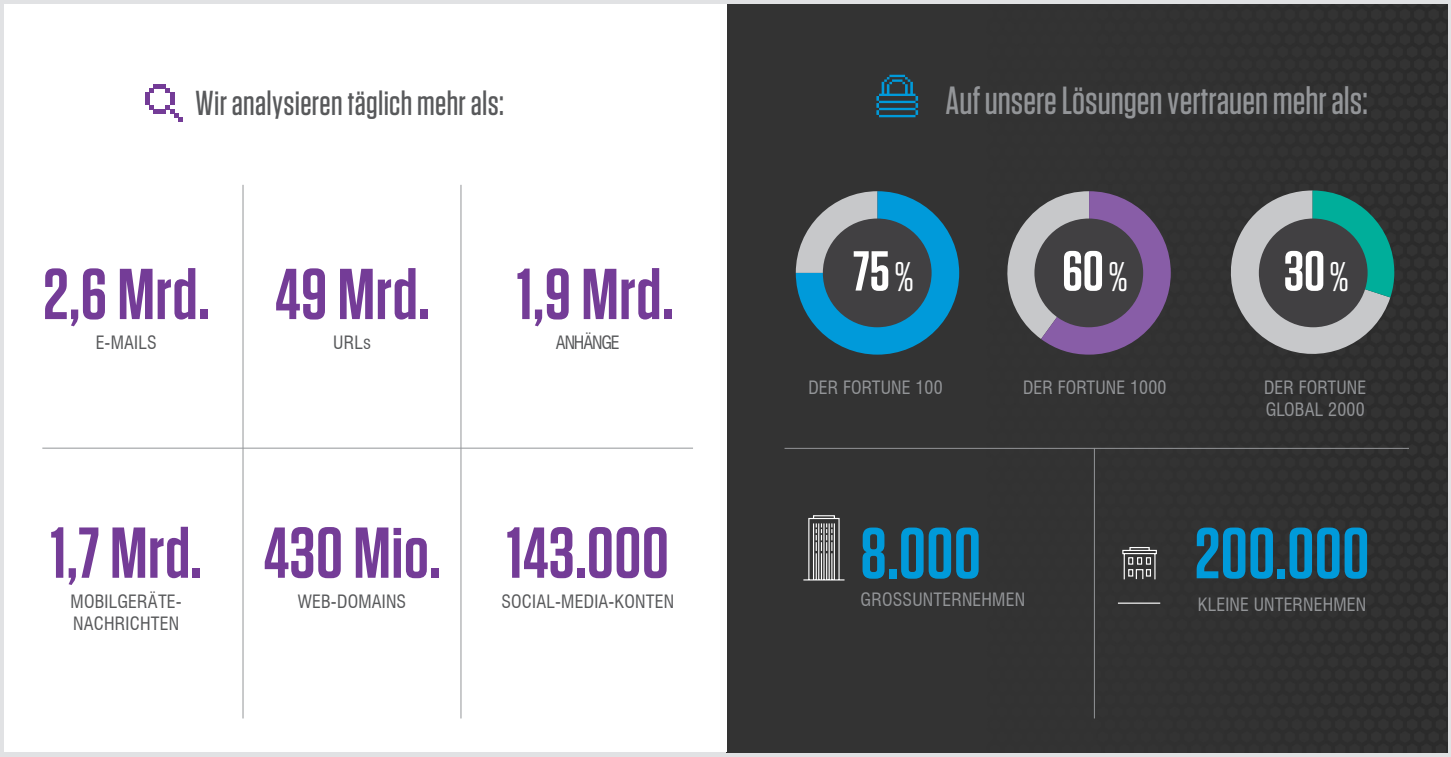
ABSCHNITT 5

Gehen Sie den nächsten Schritt

Weitere Informationen zu Proofpoint und darüber, wie wir Sie bei der Verbesserung Ihrer Microsoft 365-Bereitstellung mit personenzentrierter Sicherheit und Compliance für E-Mails, die Cloud und Endpunkte unterstützen können, finden Sie unter proofpoint.com.

Informationen zu Proofpoint

Proofpoint Nexus Threat Graph verbindet die branchenweit beste Sicherheitsforschung, Technologie und Bedrohungsdaten, um Sie in allen Angriffsphasen zu schützen. Kein anderer Anbieter verfügt über umfangreichere Einblicke in die Mechanismen aktueller Cyberangriffe.



WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0501-004-04-02 10/22