Kiteworks

2023

Prognose zum Umgang mit dem Risiko der Offenlegung sensibler Inhalte

15 Einschätzungen für die Kommunikation sensibler Inhalte auf der Grundlage von Erkenntnissen über Cyberkriminalität, Cybersicherheit und Compliance

REPORT

Einleitung: Das Risiko der Offenlegung sensibler Inhalte erkennen

Unternehmen müssen das Datenschutzrisiko managen und dabei geschickt durch ein Minenfeld navigieren, in dem sich Cyber-Bedrohungen, Gesetze und Technologieoptionen ständig weiterentwickeln. Unsere Prognose für 2023 enthält 15 Vorhersagen zum Datenschutz und zur Einhaltung gesetzlicher Vorgaben, die Führungskräfte aus den Bereichen IT, Sicherheit, Risikomanagement und Compliance kennen müssen, um ihre Risikolage im Jahr 2023 proaktiv zu steuern. Diese Vorhersagen spiegeln zukunftsorientierte Analysen von den Kiteworks-Experten wider, die über jahrzehntelange Erfahrung in den Bereichen Cybersicherheit, Compliance und Technologie verfügen.

Die Flut von Daten, einschließlich vertraulicher Inhalte, nimmt weiterhin stark zu, da immer mehr Unternehmen datengesteuerte Geschäftsmodelle einführen. In praktisch jeder Abteilung, jeder Branche und jedem Sektor (öffentlich und privat) hat das Datenvolumen explosionsartig zugenommen, und es gibt keine Anzeichen dafür, dass sich dieser Trend verlangsamt. Das betrifft auch sensible Inhalte, die früher lokal gespeichert oder durch manuelle Prozesse erstellt und weitergegeben wurden, auf die jedoch inzwischen von jedem Gerät oder Standort aus einfach zugegriffen werden kann. Da vertrauliche Inhalte, die leicht zugänglich sind, anfälliger für unbefugten Zugriff sind, ist eine umfassende Nachverfolgung und Kontrolle zur Verwaltung von Sicherheits- und Compliance-Risiken von entscheidender Bedeutung.

Diese Prognose soll Unternehmen dabei helfen, die Risiken zu bewältigen, indem sie die neuesten Cyber-Bedrohungen durch unvorsichtige oder böswillige Mitarbeiter, Cyber-Kriminelle - Einzeltäter als auch organisierte Verbrechersyndikate - und Schurkenstaaten aufzeigt. Der Ausblick berücksichtigt verschiedene Cybersecurity-Technologien und -Verfahren sowie sich weiter entwickelnde Compliance-Standards, die alle dem Schutz vertraulicher Inhalte dienen.

Zunahme der Kommunikation mit sensiblen Inhalten

1. Der Austausch sensibler Daten ist zwar riskant, aber geschäftlich erforderlich

Unternehmen werden auch in Zukunft auf die gemeinsame Nutzung von Daten zurückgreifen, um Wettbewerbsvorteile zu erzielen. Bei einigen dieser Daten handelt es sich um sensible Inhalte wie personenbezogene Daten, geschützte Gesundheitsinformationen, Finanzdaten, Details zu Fusionen und Übernahmen, Forschung und Entwicklung (F&E) sowie geistiges Eigentum. Letzteres umfasst u. a. Informationen über Produktionspläne, Produktdesign, Marketing- und Markteinführungsstrategien oder DNA-Sequenzen. Der digitale Austausch dieser vertraulichen Daten erfolgt sowohl innerbetrieblich als auch mit externen Parteien wie Beratern, Lieferanten, Partnern und Aufsichtsbehörden.

All dies führt zu einem rasanten Wachstum in den Bereichen File Sharing und Managed File Transfer (MFT). Es wird prognostiziert, dass der Markt für die Synchronisierung und gemeinsame Nutzung von Dateien in Unternehmen bis 2027 mit einer durchschnittlichen jährlichen Wachstumsrate (Compound Annual Growth Rate, CAGR) von 28,1 % wachsen wird,[1] während für den MFT-Markt im gleichen Zeitraum eine CAGR von 28,3 % erwartet wird.[2]

Vertrauen ist ein zentrales Element bei der Freigabe von Daten. Gartner geht davon aus, dass Unternehmen, die bei Partnern und Kunden Vertrauen schaffen können, bis 2023 in der Lage sein werden, sich an 50 % mehr Kunden- und Partner-Ökosystemen zu beteiligen, was wiederum zu erweiterten Möglichkeiten der Umsatzgenerierung führen wird.[3] Da Daten, einschließlich sensibler Inhalte, über verschiedene Kommunikationskanäle - E-Mail, Dateifreigabe, Managed File Transfer, Web-Formulare und APIs (Application Programming Interfaces) - versendet, ausgetauscht und empfangen werden, benötigen Unternehmen eine Lösung, die die Nachverfolgung und Kontrolle über alle Kanäle hinweg konsolidiert, um sicherzustellen, dass die Daten geschützt sind und die Prozesse den gesetzlichen Anforderungen entsprechen.

2. Unsicherer Versand von E-Mails mit sensiblen Inhalten bleibt ein erhebliches Risiko

Auch wenn die Akzeptanz von Kommunikationskanälen wie Chat und SMS weiter zunimmt, bleibt E-Mail für viele Unternehmen eine wichtige Stütze - insbesondere für die Kommunikation mit externen Parteien. Das E-Mail-Volumen steigt daher weiter an. Es wird erwartet, dass die Gesamtzahl der versendeten E-Mails im Jahr 2023 im Vergleich zu 2020 um fast 12 % steigen wird (auf 347,3 Milliarden).[4] Ein höheres E-Mail-Volumen bedeutet unweigerlich ein höheres Abfangrisiko. Laut einer aktuellen Studie des Ponemon Institute meldet fast ein Viertel (23 %) der Unternehmen jeden Monat mehr als 30 Sicherheitsvorfälle im Zusammenhang mit der Nutzung von E-Mails seitens der Mitarbeiter.[5] Eine beträchtliche Anzahl davon stand im Zusammenhang mit Fehlzustellungen - d. h. E-Mails, die an unbeabsichtigte Empfänger gesendet wurden -, die von Verizon für etwa 15 % aller Datenschutzverletzungen im Jahr 2021 verantwortlich gemacht wurden.[6]

Vertrauen ist ein zentrales Element bei der Freigabe von Daten. Gartner geht davon aus, dass Unternehmen, die bei Partnern und Kunden Vertrauen schaffen können, bis 2023 in der Lage sein werden, sich an 50 % mehr Kunden- und Partner-Ökosystemen zu beteiligen, was wiederum zu erweiterten Möglichkeiten der Umsatzgenerierung führen wird.

Cyberattacken legen vertrauliche Daten offen

3. Mandantenfähiges Cloud-Hosting bietet Cyberangreifern einen idealen Nährboden

Cyberkriminelle haben es zunehmend auf mandantenfähige Lösungen in der Cloud abgesehen. Für ein paar tausend Dollar können Angreifer eine Cloud-Instanz von Microsoft oder anderen Softwareanbietern erwerben und mithilfe sogenannter Sandboxes Schwachstellen aufspüren und komplexe Exploits zum Abfangen sensibler Inhalte entlang der Software Supply Chain entwickeln. Da die Daten verschiedener Mandanten in einer mandantenfähigen Cloud-Umgebung nebeneinander liegen, kann ein Sicherheitsversagen bei einem Mandanten die Systeme, Anwendungen und Inhalte anderer Mandanten, die sich in der gleichen Instanz befinden, gefährden.[7]

Unternehmen sollten sich daher für Single-Tenant-Hosting-Lösungen mit einem dedizierten Server entscheiden, der von anderen Mandanten isoliert ist. Doch das ist nur der Anfang. Sie müssen entscheiden, wer den Server verwaltet und die volle Verantwortung für die Sicherheit der auf dem Server enthaltenen Inhalte übernimmt. Wenn Unternehmen und ihre Cloud Access Security Broker (CASB)-Anbieter sich die Verantwortung teilen, werden Annahmen darüber getroffen, “wer was macht”, was zu Sicherheitslücken und Fehlkonfigurationen führen kann. Dadurch kann jeder, der über eine Internetverbindung verfügt, auf die vertraulichen Inhalte auf diesen Servern zugreifen. Unternehmen müssen daher sicherstellen, dass die Daten auf diesen Single-Tenant-Cloud-Lösungen sowohl bei der Lagerung als auch bei der Übertragung verschlüsselt sind, wobei der Verschlüsselungscode im alleinigen Besitz des Unternehmens ist und den Anforderungen des National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), der International Organizational for Standardization (ISO) und SOC 2 entspricht.

4. Externe Parteien in der Lieferkette erhöhen das Risiko

Drittanbieter, Auftragnehmer, Rechtsberater und andere externe Unternehmen werden immer mehr zur Zielscheibe. Vertrauliche Informationen, die über die verschiedenen Kommunikatitonskanäle an Dritte weitergegeben werden, können für Ransomware, IP-Diebstahl und Erpressung (öffentliche Bloßstellung, Markenschädigung) ausgenutzt werden. In einer Anfang des Jahres veröffentlichten Umfrage stellte PwC fest, dass mehr als die Hälfte der Unternehmen entweder gerade damit begonnen hat oder noch plant, Verfahren zum sogenannten Third-Party-Risk-Management einzuführen.[8] Es überrascht nicht, dass Verizon in seinem jüngsten Data Breach Investigations Report feststellte, dass die Lieferkette für 62 % der Systemeinbrüche verantwortlich war und 39 % der Datenschutzverletzungen auf kompromittierte Geschäftspartner zurückzuführen waren.[9] Diese Statistiken sollten Unternehmen daran erinnern, dass ihre Richtlinien, Verfahren und Technologieinvestitionen im Bereich der Cybersicherheit nur so gut sind wie ihr schwächster Partner in der Lieferkette.

Kriminelle Akteure können eine Cloud-Instanz von Microsoft oder anderen Softwareanbietern erwerben, Schwachstellen aufspüren und komplexe Exploits zum Abfangen sensibler Inhalte entlang der Software Supply Chain entwickeln.

5. Angriffe durch Schurkenstaaten sind auf dem Vormarsch

Cyberspionage-Angriffe durch Schurkenstaaten haben im Jahr 2022 drastisch zugenommen. Der Anteil der Angriffe auf kritische Infrastrukturen stieg im vergangenen Jahr von 20 % auf 40 %.[10] Schurkenstaaten - Nordkorea, China, Russland und der Iran[11] - werden auch in Zukunft Angriffe auf hochwertige Ziele wie Lieferketten verüben, die Zugang zu Hunderten oder Tausenden von Unternehmen bieten. Unternehmen müssen ihre Kommunikation mit sensiblen Inhalten auch weiterhin mit äußerster Sorgfalt gegen diese vier Staaten und ihre zunehmende Fähigkeit, raffinierte Angriffe zu entwickeln, absichern.

6. Cyberangreifer werden immer raffinierter - und immer gefährlicher

Zwar gibt es immer noch einzelne kriminelle Akteure, doch Cyber-Hacking hat sich zu einem milliardenschweren Unternehmen entwickelt (mit F&E-Budgets und Organisationshierarchien), für das vertrauliche Daten - sowohl im ruhenden Zustand als auch bei der Übertragung - ein Hauptziel darstellen. Diese finanzstarken kriminellen Organisationen setzen fortschrittliche Technologien wie künstliche Intelligenz (KI) ein, um Informationen zu sammeln, Anwendungen und Netzwerke zu infiltrieren, diese zu durchsuchen, um sensible Inhalte zu finden und diese, ohne entdeckt zu werden, abzufangen, wenn sie gesendet, geteilt, empfangen und/oder gespeichert werden. Der Einsatz fortschrittlicher persistenter Bedrohungen mit Hilfe von KI, maschinellem Lernen und Automatisierung ermöglicht es ihnen, ihre Präsenz im Netzwerk oder in den Anwendungen zu verschleiern und monatelang unentdeckt zu bleiben, um Terabytes vertraulicher Inhalte zu rauben und zur Erpressung und/oder zum Verkauf im Dark Web zu missbrauchen.

Finanzstarke kriminelle Organisationen setzen fortschrittliche Technologien wie künstliche Intelligenz (KI) ein, um Informationen zu sammeln, Anwendungen und Netzwerke zu infiltrieren, diese zu durchsuchen, um sensible Inhalte zu finden und diese, ohne entdeckt zu werden, abzufangen, wenn sie gesendet, geteilt, empfangen oder gespeichert werden.

Cybersecurity-Strategien und -Technologien entwickeln sich weiter, um den mit der Kommunikation sensibler Inhalte verbundenen Risiken zu begegnen

7. Inhaltsdefiniertes Zero Trust und ein Private Content Network für die Kommunikation mit sensiblen Inhalten

Die meisten Unternehmen sind entweder dabei, eine Zero-Trust-Sicherheitsstrategie einzuführen oder haben dies bereits getan, um auf die Defizite der Sicherheit am Netzwerkrand und die zunehmende Raffinesse von Cyberangriffen zu reagieren. Zero Trust geht davon aus, dass Benutzern, Anwendungen und Infrastrukturen nicht vertraut werden kann, und wendet Richtlinien für den Zugriff mit den geringsten Rechten an, um ihre vertraulichsten Inhalte zu schützen.

Der Vorstoß für Zero Trust auf US-Bundesebene in Form der Executive Order 14028 und der nachfolgenden Memoranden wird sich in erweiterten Zero-Trust-Standards im privaten Sektor niederschlagen.[12] Da sensible Inhalte das ultimative Ziel von Cyberkriminellen sind, setzt sich zunehmend die Erkenntnis durch, dass ein inhaltsbezogenes Zero-Trust-Konzept erforderlich ist. Derzeit stellen unstrukturierte Daten, die ohne angemessene Nachverfolgung und Kontrolle versendet oder mit anderen gemeinsam genutzt werden, ein erhebliches Risiko dar. So entstand das Private Content Network, ein dediziertes System, das die digitale Kommunikation hochsensibler Informationen - sowohl intern als auch extern - schützt. Es nutzt inhaltsbezogene Zero-Trust-Richtlinien, um Content-Assets, Benutzer und Aktionen zu verwalten.[13]

8. Least-Privilege-Zugang und Authentifizierung werden unabdingbar

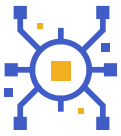
Der Zugriff mit den geringsten Rechten und die Authentifizierung sind die Grundvoraussetzungen für Zero Trust. In seinem jüngsten M-Trends Report hat Mandiant festgestellt, dass gestohlene Zugangsdaten 11 % der ursprünglichen Infektionsvektoren ausmachen.[14] Mit gestohlenen Zugangsdaten, die auf unterschiedlichste Weise erlangt werden können (Dark Web, Phishing usw.), verschaffen sich Cyberkriminelle und Schurkenstaaten Zugang zu Ihrem Netzwerk, Ihren Anwendungen und Inhalten. Unternehmen geben zahlreiche potenzielle Auswirkungen gestohlener Zugangsdaten an, wobei der Verlust sensibler Daten ganz oben auf der Liste steht (35 %).[15]

Um dem Risiko des Identitätszugriffs, der Authentifizierung und des Diebstahls von Zugangsdaten entgegenzuwirken, benötigen Unternehmen einen Zero-Trust-Ansatz, der Richtlinien zur Minimierung von Rechten mit Hilfe der Multifaktor-Authentifizierung (MFA) anwendet, um die Gefahr des Diebstahls von Zugangsdaten einzudämmen. MFA ist heute die Standardmethode für den Zugriff auf Netzwerke und Anwendungen. Ungeachtet dessen, wo sich Ihre sensiblen Inhalte befinden (lokal, in einer Private Cloud oder in der Public Cloud), ist MFA - einschließlich SAML 2.0 und Kerberos SSO - entscheidend für die Nachverfolgung und die Zugriffskontrolle.

Da sensible Inhalte das ultimative Ziel von Cyberkriminellen sind, setzt sich zunehmend die Erkenntnis durch, dass ein **inhaltsbezogenes Zero-Trust-Konzept** erforderlich ist. Derzeit stellen unstrukturierte Daten, die ohne angemessene Nachverfolgung und Kontrolle versendet oder mit anderen gemeinsam genutzt werden, ein erhebliches Risiko dar.

9. Immer mehr Unternehmen entscheiden sich für den Alleinbesitz ihrer Verschlüsselungscodes

Die Verschlüsselung und Verwaltung von Schlüsseln werden für Cloud-Anbieter und ihre Kunden zunehmend zu einem Problem. Viele der Kunden sind lediglich Mitverwalter ihrer Verschlüsselungscodes, so dass Strafverfolgungs- und Sicherheitsbehörden, Anwälte und andere Stellen den jeweiligen Kunden "umgehen" und den Cloud-Anbieter zur Herausgabe der Verschlüsselungscodes auffordern können, was dieser dann auch tun muss, um Zugriff auf die vertraulichen Inhalte des Kunden zu gewähren. Die Europäische Union und einzelne europäische Länder haben darauf reagiert und die französische Blocking-Verordnung sowie Standardvertragsklauseln in der General Data Protection Regulation (GDPR/DSGVO) erlassen, um die persönlichen Daten ihrer Bürger zu schützen. Die US-Bundesregierung, die verhindern will, dass ein Sicherheitsproblem zu einem diplomatischen Problem wird, hat kürzlich eine Executive Order mit dem Namen "Privacy Shield 2.0" erlassen, die Schutzmaßnahmen zum Schutz der persönlichen Daten von EU-Bürgern verspricht.[16]



10. Die Beseitigung von Schwachstellen in Bibliotheken und Software von Drittanbietern wird immer wichtiger

Die Anzahl der im Jahr 2022 veröffentlichten Common Vulnerabilities and Exposures (CVE) ist gegenüber 2021 um 35 % gestiegen.[17] Da ein erheblicher Prozentsatz des Software-Codes aus offenen Quellen stammt, sollten Unternehmen ihre Software Supply Chain kontinuierlich überprüfen. Um das von CVEs ausgehende Risiko zu mindern und dadurch den Schweregrad der Schwachstellenausnutzung und die Auswirkungen zu reduzieren, erhöhen Unternehmen proaktiv - und zunehmend aggressiv - die Sicherheit ihrer Software-Lösungen und fügen mehrere Sicherheitsebenen hinzu.[18] Als Teil ihres Risikomanagement-Ansatzes können sie ein CVE sogar auf der Grundlage dieser entschärfenden Sicherheitsfaktoren neu bewerten. (CVEs werden auf einer Skala von 1 bis 10 je nach Schwere des Risikos, das sie darstellen, bewertet).

11. KI wird immer häufiger zur Erkennung von Anomalien bei Datenfreigaben und -transfers eingesetzt

Künstliche Intelligenz (KI) birgt ein nahezu grenzenloses Potenzial in der gesamten Cybersicherheitslandschaft, einschließlich der fortschrittlichen Erkennung von Bedrohungen und dem Schutz sensibler Inhalte. Insbesondere kann die KI-Technologie anomale Datenfreigaben und -transfers erkennen. Durch die Integration von KI-Funktionen in Tools für die Kommunikation sensibler Inhalte und für das Security Operations Center (SOC), wie z. B. Security Information and Event Management (SIEM) und Security Orchestration, Automation and Response (SOAR), können Sicherheitspersonal und Interventionsteams Echtzeitwarnungen erhalten, so dass sie sofort Maßnahmen ergreifen können, um die Auswirkungen gefährlicher Aktivitäten zu verringern.

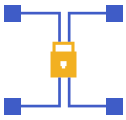
12. Unternehmen werden mehr Ressourcen für die Verbesserung und die Integration von Sicherheitsmaßnahmen einsetzen

Die Integration und Konsolidierung von Investitionen in Cybersecurity-Technologien ist für viele Unternehmen nach wie vor ein zentrales Thema, und dies gilt sicherlich auch für die Kommunikation sensibler Inhalte. IT-, Sicherheits-, Risiko- und Compliance-Teams arbeiten effizienter und effektiver, wenn sie Bedrohungs- und Compliance-Daten in einem einzigen Dashboard konsolidieren können.[19] Die Integration von Antivirus-Funktionen zur Überprüfung auf Malware und andere Viren, die in E-Mails, Dateifreigaben, Managed File Transfer und APIs enthalten sind, ist ein wichtiger Ansatzpunkt. Die Integration von Netzwerk- und Web Application Firewall- und Intrusion Prevention System (IPS)-Funktionen schafft Sicherheitsebenen, die sensible Inhalte hinter Service-Ebenen mit Zugriffskontrollen mit geringst möglichen Befugnissen schützen.

Die Automatisierung von Prozessen im Bereich der Cybersicherheit ist ebenso wichtig. Content Disarm and Reconstruction (CDR) erkennt und entfernt automatisch ausführbare Inhalte in eingehenden E-Mails, Dateifreigaben, MFT und APIs, während die Inhalte an den Empfänger weitergeleitet werden. Data Loss Prevention (DLP) kontrolliert ausgehende E-Mails, Dateifreigaben, MFT und APIs, um sowohl versehentliche als auch absichtliche Datenverluste zu verhindern. Der Aufbau von API-Verbindungen mit SOC-Überwachungs- und Incident-Response-Tools wie SIEM und SOAR ermöglicht es SOC-Teams, die Kommunikation mit sensiblen Inhalten zu überwachen und Echtzeitwarnungen zu erhalten, wenn Angriffe oder Anomalien auftreten.

KI-Technologie kann anomale Datenfreigaben und -transfers erkennen. Durch die Integration von KI-Funktionen in Tools für die Kommunikation sensibler Inhalte und das SOC, können Sicherheitspersonal und Interventionsteams Echtzeitwarnungen erhalten, so dass sie sofort Maßnahmen ergreifen können, um die Auswirkungen gefährlicher Aktivitäten zu verringern.

Risikomanagement durch Nachverfolgung und Kontrolle des digitalen Austauschs sensibler Daten



13. Anpassung an neue und erweiterte Datenschutzbestimmungen

Praktisch jedes Land der Welt hat in irgendeiner Form ein Datenschutzgesetz erlassen, das regelt, wie Informationen gesammelt werden, wie die von der Datenerfassung Betroffenen darüber informiert werden und wie die Daten zu verwenden sind. Unternehmen, die sich nicht an diese unzähligen Gesetze halten, müssen mit Geldstrafen und Bußgeldern, Gerichtsverfahren und sogar dem Verbot der Geschäftstätigkeit in einem bestimmten Land rechnen. Die negative Publicity, die der Verstoß eines Unternehmens gegen ein Datenschutzgesetz nach sich zieht, kann sich auch nachteilig auf dessen Marke auswirken.

Die Datenschutzlandschaft ist derzeit sehr weitläufig und wird sich noch weiter ausdehnen. Der HIPAA (Health Insurance Portability and Accountability Act) regelt den Datenschutz in Bezug auf geschützte Gesundheitsinformationen. FISMA, GLBA, PCI DSS (Payment Card Industry Data Security Standard) und andere regeln den Schutz von Finanzdaten und personenbezogenen Daten. Die EU-Datenschutzverordnung GDPR (General Data Protection Regulation, dt. DSGVO) war einer der ersten Versuche, den Datenschutz über mehrere Regionen hinweg zu regeln. Da es in den USA keine nationale Datenschutzverordnung gibt, haben verschiedene US-Bundesstaaten vor kurzem Datenschutzgesetze eingeführt. Kalifornien war der erste mit der Verabschiedung des CCPA (California Consumer Privacy Act). Vier weitere US-Bundesstaaten haben ähnliche Datenschutzgesetze verabschiedet, die im Jahr 2023 in Kraft treten werden:[20] Virginia (Consumer Data Protection Act, 1. Januar 2023), Colorado (Privacy Act, 1. Juli 2023), Utah (Consumer Protection Act, 31. Dezember 2023) und Connecticut (Data Protection Act, 1. Juli 2023).

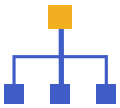
Als Reaktion auf die Verabschiedung dieser vier neuen bundesstaatlichen Gesetze sowie den anhaltenden globalen Fokus auf den Datenschutz wird im Jahr 2023 die Überwachung und Kontrolle des Datenschutzes sowie der Schutz dieser Daten beim Senden, Teilen, Empfangen und Speichern immer wichtiger. Die Nichteinhaltung von Gesetzesänderungen in bestehenden und neuen Datenschutzgesetzen ist keine Option.

14. Geofencing beim Austausch vertraulicher Daten wird zunehmen

Sicherheit und Datenschutz zwischen Ländern sind eine wachsende Anforderung für globale Unternehmen. Die Notwendigkeit des Schutzes und der Kontrolle vertraulicher Daten, die innerhalb und zwischen bestimmten Gerichtsbarkeiten ausgetauscht werden, hat in den letzten Jahren exponentiell zugenommen - sowohl in Bezug auf die Einhaltung gesetzlicher Vorgaben als auch hinsichtlich der Sicherheitsmaßnahmen. Um zu verhindern, dass vertrauliche Daten unbefugt an bestimmte geografische Gebiete gesendet oder freigegeben werden - sowohl innerhalb eines Unternehmens als auch extern an Dritte - sollten Unternehmen Geofencing-Kontrollen einsetzen, die das Senden,

Die Datenschutzlandschaft ist derzeit sehr weitläufig und wird sich noch weiter ausdehnen.

Freigeben und Empfangen von einzelnen Dateien und Ordnern blockieren, die diesen Gerichtsbarkeiten zugeordnet sind. Kontrollen der Datensouveränität beschränken die Speicherung einzelner Dateien auf das Heimatland des Datenbesitzers. Zusätzlich zur Verwendung von Sperr- und Überwachungslisten sollten Unternehmen inhaltsbezogene Zero-Trust-Richtlinien zur Nachverfolgung und Kontrolle umsetzen.



15. Die Anwendung von Best Practices für Cybersecurity-Kontrollen und -Frameworks setzt sich immer mehr durch

Der Einfluss von Cybersecurity-Frameworks wie ISO 27001, NIST CSF und SOC 2 wird sowohl im öffentlichen als auch im privaten Sektor weiter zunehmen und sich durchsetzen. Die Einhaltung der in diesen Rahmenwerken enthaltenen Best Practices-Standards ermöglicht es Unternehmen, ihre Risiken effektiver zu kontrollieren. Dementsprechend werden sich die Unternehmen bei der Bewertung des Risikos der Offenlegung sensibler Inhalte zunehmend auf Cybersecurity-Frameworks stützen.

Ein Teil der Aufmerksamkeit wird auf Regierungsebene erzeugt werden. Die Zero-Trust-Prinzipien, die in der US-Verordnung 14028 und nachfolgenden Memoranden niedergelegt sind, konzentrieren sich zum Beispiel stark auf die Gefährdung vertraulicher Daten. Das Gleiche gilt für die Cybersecurity Maturity Model Certification (CMMC), welche die NIST 800-171 und 800-172 als Grundlage für ihre Verfahren zur Kontrolle des Austauschs und der Speicherung sensibler Inhalte innerhalb der Lieferkette des US-Verteidigungsministeriums (DoD) verwendet. Gleichzeitig sieht der private Sektor direkte Vorteile in der Verwendung von Cybersecurity-Frameworks, und ihre Nutzung zur Kontrolle des Risikos der Offenlegung sensibler Inhalte wird im Jahr 2023 weiter zunehmen.[21]

Erkenntnisse aus unserer Prognose zu den Risiken im Zusammenhang mit dem Datenschutz

Die rasante Entwicklung von Cyberangriffen durch Cyberkriminelle und Schurkenstaaten hat die Cybersicherheit für die meisten Unternehmen an die Spitze der Prioritätenliste gerückt. Da vertrauliche Daten das Ziel vieler Cyberangriffe sind, sind Unternehmen gezwungen, die Art und Weise, wie sie ihre sensiblen Inhalte schützen, zu überdenken. Der geschäftliche Wert des Datenaustauschs und die erweiterte Lieferkettenlandschaft erhöhen gleichzeitig das Risiko der Preisgabe vertraulicher Daten. Daher müssen Unternehmen über geeignete Sicherheitskontrollen und -verfahren verfügen, um den digitalen Austausch sensibler Inhalte innerhalb und außerhalb ihres Unternehmens zu schützen.

Da die Gesetzgeber in verschiedenen geografischen Regionen bestehende Datenschutzbestimmungen erweitern und neue erlassen, nimmt die Komplexität der Einhaltung und des Nachweises des Datenschutzes gegenüber den Aufsichtsbehörden noch weiter zu. Unternehmen müssen mehr Governance-Kontrollen und Nachverfolgungsfunktionen einrichten, um nachzuweisen, dass der Versand, die Weitergabe und die Verwendung sensibler Daten mit den Datenschutzbestimmungen in allen Ländern, in denen sie tätig sind, übereinstimmen.

Unternehmen werden im Jahr 2023 eine Menge zu beachten haben. Der Umgang mit vertraulichen Daten und die Vermeidung ihrer Offenlegung müssen oberste Priorität haben. Dies erfordert einen strategischen Compliance-, Governance- und Sicherheitsansatz für Ihren digitalen Austausch sensibler Daten.

Um zu verhindern, dass vertrauliche Daten unbefugt an bestimmte geografische Gebiete gesendet oder freigegeben werden — sowohl innerhalb eines Unternehmens als auch extern an Dritte - sollten Unternehmen Geofencing-Kontrollen einsetzen.

Quellenangaben

[1] "Enterprise File Synchronization and Sharing (EFSS) Market: Growth, Trends, COVID-19 Impact, and Forecasts (2022-2027)," Mordor Intelligence, abgerufen am 9. November 2022.

[2] "Managed File Transfer Market: Growth, Trends, COVID-19 Impact, and Forecasts (2022-2027)," Mordor Intelligence, abgerufen am 9. November 2022.

[3] Laurence Goasduff, "Data Sharing Is a Business Necessity to Accelerate Digital Business," Gartner, 20. Mai 2021.

[4] "Number of sent and received e-mails per day worldwide from 2017 to 2025," Statisa, Februar 2021.

[5] "Email Data Loss Prevention: The Rising Need for Behavioral Intelligence," Ponemon Insitute, 18. Mai 2022.

[6] "2022 Data Breach Investigations Report," Verizon, Juni 2022.

[7] Wayne Brown, Vince Anderson, und Qing Tan, "Multitenancy: Security Risks and Countermeasures," Network-Based Information Systems, September 2012.

[8] "2022 Global Digital Trust Insights," PwC, Oktober 2021.

[9] "2022 Data Breach Investigations Report," Verizon, Juni 2022.

[10] "Microsoft Digital Defense Report 2022," Microsoft, abgerufen am 9. November 2022.

[11] "Mandiant Cyber Security Forecast 2023," Mandiant, 2. November 2022.

[12] "How Federal Agencies Can Comply With the Data Requirement in Executive Order 14028," Kiteworks, Februar 2022.

[13] "Kiteworks Launches the Private Content Network," Kiteworks Presse-Information, 11. August 2022.

[14] "M-Trends 2022," Mandiant Special Report, Februar 2022.

[15] "Benchmarking Security Gaps & Privileged Access: Global survey of cybersecurity leaders," Delinea, September 2022.

[16] "FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework," The White House, 7. Oktober 2022.

[17] Jason Villaluna, "2022 Trustwave SpiderLabs Telemetry Report," Trustwave, 25. August 2022.

[18] "Kiteworks Hardened Virtual Appliance Provides Multiple Security Layers to Dramatically Reduce Vulnerability Exploit and Impact Severity," Kiteworks, November 2022.

[19] Jim Boehm, et al., "Cybersecurity trends: Looking over the horizon," McKinsey, 10. März 2022.

[20] Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," Wirecutter, 6. September 2021.

[21] Adamu A. Garba and Aliyu M. Bade, "An Investigation on Recent Cyber Security Frameworks as Guidelines for Organizations to Adopt," International Journal of Innovative Science and Research Technology, Volume 6, Issue 2, Februar 2021.

Kiteworks

www.kiteworks.com