box

Schützen Sie Ihre Inhalte vor Cyberbedrohungen und Datenverlust

Inhalte machen Ihr Unternehmen aus

Wertvolle Ressourcen wie Kundenverträge, Produktspezifikationen, Patente und Marketingmaterialien sind das Herzstück jedes Prozesses – unabhängig von Ihrer Branche. Ihre Inhalte sind jedoch ständig von böswilligen Hackern und sogar von wohlmeinenden Mitarbeitenden bedroht.

Der Zugriff auf Unternehmensnetzwerke war vor Corona besser kontrollierbar, da die Mitarbeitenden sich entweder im Büro befanden und über lokale Anmeldeinformationen und Netzwerkdaten gesichert waren oder ein VPN für den Zugriff auf Systeme nutzten. In beiden Fällen greifen Mitarbeitende über unternehmenseigene Mechanismen auf Geschäftsinhalte zu. Mit der Umstellung auf hybride Arbeitsumgebungen ist dies jedoch nicht ihr einziger Zugangspunkt.

Sie benötigen einen völlig neuen Ansatz zum Schutz der Inhalte, der Ihre Kunden unterstützt und den Handlungsspielraum Ihrer Teams erweitert – jederzeit, überall und auf jedem Gerät.

Die globalen Kosten für Ransomware werden

im Jahr 2023 voraussichtlich 30 Milliarden US-Dollar übersteigen.[1]

Aktuelle Bedrohungslandschaft: Innerhalb und außerhalb des Unternehmens

Bedrohungen für Ihre Inhalte können sowohl von externen als auch von internen Quellen ausgehen. Eine Möglichkeit, diese Bedrohungsarten zu betrachten, sind inhalts- bzw. nutzerorientierte Bedrohungen. Sie schaffen unterschiedliche, sich aber überschneidende Arten von Risiken.

Externe Bedrohungen

Inhaltsorientierte externe Bedrohungen stellen operationelle Risiken dar.

Malware

Cyberkriminelle suchen nach Sicherheitslücken, um Schadsoftware (Malware) zu installieren. Diese dient dazu, private Geräte, Dienste oder Netzwerke auszunutzen und Inhalte zu stehlen, um daraus finanziellen Nutzen zu ziehen (z. B. durch Verkauf). Zu den Inhalten, auf die es Cyberkriminelle abgesehen haben, gehören u. a.:

- Sensible Finanz- und Rechtsunterlagen, die Auswirkungen auf den Geschäftsbetrieb und die Reputation haben
- Personenbezogene Daten (PII) von Mitarbeiter:Innen und Kunden, die unter Vorschriften wie die DSGVO fallen
- Geschützte Gesundheitsdaten (PHI), die unter Vorschriften wie HIPAA fallen

2,5 Millionen US-Dollar

Durchschnittliche Kosten eines Malware-Angriffs auf ein Unternehmen im Jahr 2023.[2]

Ransomware

Kriminelle, die sich auf diese Untergruppe von Malware spezialisiert haben, erkennen den Wert Ihrer Inhalte und erpressen Sie damit. Sie wissen, dass Ihr Geschäft ohne diese Inhalte zum Stillstand kommen würde. Das Volumen von Ransomware ist drastisch gewachsen und verzeichnete im Jahr 2022 einen Anstieg von 13 %.[3] 79 % der Unternehmen waren bereits von einem Ransomware-Angriff betroffen[4]. Diese Art von Angriffen ist von Natur aus lukrativ und aufgrund von „Ransomware-as-a-Service“ im Dark Web relativ einfach zu bewerkstelligen.

Im Frühjahr 2021 attackierten Ransomware-Angreifer beispielsweise die Colonial Pipeline, die größte Erdölpipeline der USA, und forderten (und erhielten) 5 Millionen US-Dollar. Der Angriff legte den Betrieb für mehr als eine Woche lahm, was zu Benzinknappheit und Preissteigerungen führte.

1,4 Millionen US-Dollar

Durchschnittliche Wiederherstellungskosten nach einem Ransomware-Angriff im Jahr 2021[5]

Interne Bedrohungen

Nutzerorientierte interne Bedrohungen stellen finanzielle Risiken und das Risiko einer Rufschädigung dar.

Datenverluste oder -gefährdungen verringern – selbst wenn sie versehentlich auftreten – den Nettowert Ihrer Inhalte und verursachen finanzielle Verluste und Rufschädigungen. Das typische Ziel sind personenbezogene Daten, die über das Dark Web weiterverkauft werden können.

Globale Marken wie Alibaba (1,1 Milliarden Nutzer), LinkedIn (700 Millionen Nutzer), Facebook (533 Millionen Nutzer) und Marriott (500 Millionen Kund:Innen) kamen in den letzten drei Jahren aufgrund von Datenlecks in Verlegenheit und hatten juristische Probleme. Und die Stilllegung der Pipeline wurde durch ein geleaktes Kennwort für ein VPN-Konto verursacht.

File-Sharing

E-Mail-Angriffe fallen unter die Kategorie des Social Engineering, bei dem menschliches Verhalten ausgenutzt wird. Daher birgt die gemeinsame Arbeit an Inhalten mithilfe von E-Mail-Anhängen Risiken. Anhänge aus scheinbar seriösen E-Mails können Malware in die Geräte von Anwender:Innen einschleusen, die sich dann schnell über Unternehmenssysteme ausbreitet.

Fast 3 GB

an unnötigen und anfälligen Dateiinhalten wird pro Mitarbeiter:In und Jahr durch die allgegenwärtige Verwendung von E-Mail-Anhängen in Verbindung mit dem vorherrschenden Nutzerverhalten in Unternehmen generiert[6]

Fahrlässigkeit

Fahrlässigkeit tritt selbst in den besten Unternehmen auf. Trotz regelmäßiger Erinnerungen an sichere Praktiken treten Fehler auf, z. B. das Senden eines vertraulichen Dokuments an den falschen E-Mail-Empfänger.

307.111 US-Dollar

durchschnittliche Kosten, verursacht durch Vorfälle im Zusammenhang mit der Fahrlässigkeit von Mitarbeitenden oder Auftragnehmern

Böswillige Aktivitäten

Böswillige Aktivitäten von Mitarbeitenden oder Auftragnehmern, die Inhalte stehlen wollen, stellen ebenfalls eine ernsthafte interne Bedrohung dar.

756.760 US-Dollar

durchschnittliche Kosten, verursacht durch kriminelle und vorsätzliche Verstöße durch Insider

So löst Box inhaltsorientierte Risiken

Die Content Cloud verfolgt einen vierstufigen, automatisierten Ansatz, um Inhalte vor externen Bedrohungen zu schützen

Zugriff auf vertrauliche Inhalte verhindern

Schädliche Dateien auf Ihrem Computer können mit anderen Anwender:Innen geteilt werden. Ransomware kann sich jedoch nicht weiter verbreiten, sobald sie sich im Cloud-Speicher von Box befindet. Alle Dateien werden im Ruhezustand verschlüsselt und verfügen nicht über eine Umgebung, von der aus sie ausgeführt werden können. Box ermöglicht Anwender:Innen die Zusammenarbeit unter Einhaltung der Datenkonformität – und ohne dass anfällige E-Mail-Anhänge ausgetauscht werden müssen. Darüber hinaus können Sie mit den Smart Access-Funktionen von Box Shield Ihre Inhalte mit einem permanenten Label klassifizieren, das die Freigabe von Inhalten außerhalb Ihres Unternehmens einschränkt.

Schädliche Aktivitäten erkennen

Untersuchungen zeigen, dass Automatisierung und künstliche Intelligenz (KI) die durchschnittlichen Kosten einer Sicherheitsverletzung um 79 % senken, wenn sie in vollem Umfang eingesetzt werden.[7] Box Shield verwendet kontextabhängiges maschinelles Lernen (ML), um externe, von Dritten freigegebene Inhalte sowie interne Inhalte beim Hochladen und beim Ausführen von Aktionen wie Freigeben, Vorschau und Download zu scannen. Shield erkennt bösartige Merkmale (selbst die von ausgefeilterer Malware) innerhalb der Inhalte nahezu in Echtzeit und kennzeichnet die Datei automatisch als schädlich. Dank der Deep-Learning-Technologie von Box Shield können IT- und Sicherheitsteams potenzielle Bedrohungen effizient und strukturiert bekämpfen.

Shield generiert außerdem eine detaillierte Sicherheitswarnung, damit Sicherheits- und IT-Teams schnell handeln können. Sie können diese Warnungen im Shield-Dashboard anzeigen oder veranlassen, dass Box sie mithilfe nativer Integrationen an Ihr SIEM sendet. Die Warnung zeigt Ihnen, wer die Datei hochgeladen hat und enthält außerdem alle Bedrohungsinformationen über die Malware sowie die bisherigen dateibezogene Aktivitäten. So kann Ihr Team die am besten geeignete Reaktion auswählen. Um Unterbrechungen zu minimieren, können Administrator:Innen Inhalte mit geringem Risiko in Shield als sicher markieren.

Die Content Cloud verfolgt einen vierstufigen, automatisierten Ansatz, um Inhalte vor externen Bedrohungen zu schützen

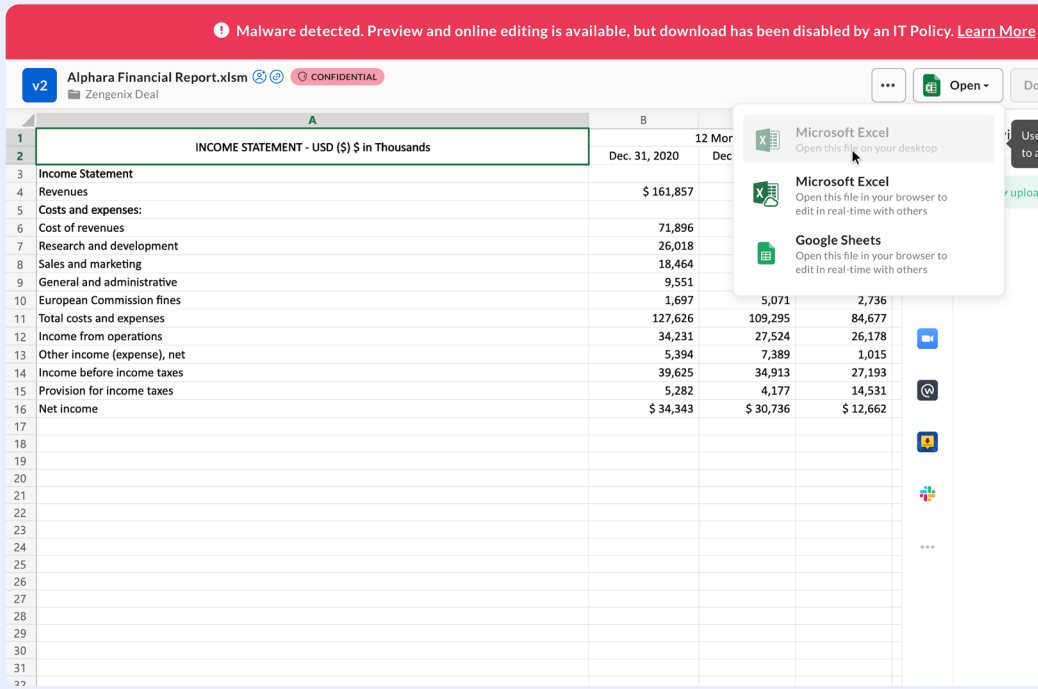
Inhalte eindämmen, um Verbreitung zu verhindern

Sobald Shield schädliche Inhalte identifiziert hat, werden Downloads und die lokale Bearbeitung eingeschränkt, um die Verbreitung auf mehr Anwender:Innen und Geräte zu verhindern. Die Anwender:Innen sehen eine Malware-Benachrichtigung auf der Nutzeroberfläche von Box, können aber trotzdem eine sichere Vorschau der Datei online einsehen und bearbeiten. So bleiben die Teams produktiv.

Das Problem durch Zugriff auf eine frühere Version beheben

Wenn Ihre Systeme mit Malware infiziert sind, können Sie Ihre Inhalte trotzdem in der Content Cloud einsehen, während sich Ihr Team mit der Bedrohung auseinandersetzt.

Da Box bei jedem Speichern eine neue Dateiversion erstellt, können Sie nach einem Ransomware-Angriff betroffene Dateien ohne Beschädigung der ursprünglichen Daten löschen und auf frühere Versionen wichtiger Dateien zugreifen. Wenn Ihnen Developer-Ressourcen zur Verfügung stehen, können Sie mithilfe der Box API ein anwenderdefiniertes Skript schreiben, das alle infizierten Dateien auf eine nicht betroffene Version zurücksetzt.



Denken Sie daran, dass Sie jederzeit Unterstützung von Fachleuten erhalten können. Box verfügt über mehrere Ressourcen, die Ihnen beim Zugriff auf Ihre Inhalte helfen.

So löst Box benutzerorientierte Risiken

Box verfolgt einen mehrgleisigen Ansatz bei internen Bedrohungen, der Ihre Mitarbeitenden, Auftragnehmer:Innen und andere Anwender:Innen von der Sicherheitslast befreit und ihnen gleichzeitig ein reibungsloses Weiterarbeiten ermöglicht.

Zero-Trust-Infrastruktur

Box ermöglicht Ihnen den Schutz Ihrer Inhalte mit einer „Zero Trust"-Haltung. Anstatt davon auszugehen, dass bestimmte Inhalte oder Anwender:Innen vertrauenswürdig sind, wird kontextsensitive Intelligenz verwendet, um Personen bei allgemeinen Aktivitäten wie dem Hochladen oder Freigeben von Daten auf verdächtiges Verhalten zu prüfen. Box Device Trust unterstützt Sie bei der Durchsetzung der Sicherheitsrichtlinien Ihres Unternehmens, indem Sie Mindestanforderungen für Geräte definieren, die für den Zugriff auf Box verwendet werden.

Null-Toleranz für ein mangelhaftes Benutzererlebnis

Schutz funktioniert nur, wenn Ihre Mitarbeitenden ihn auch anwenden. Wenn die Sicherheitsmaßnahmen das Benutzererlebnis beeinträchtigt, finden Anwender:Innen einfache Wege, um sie zu umgehen. Box bietet eine äußerst sichere Erfahrung, mit der Anwender:Innen Inhalte einfach freigeben und gemeinsam bearbeiten können, ohne sie zu gefährden. Mit Box Shield können Administrator:Innen den Anwender:Innen die Möglichkeit geben, einmalige Zugriffsausnahmen mit administrativ festgelegten geschäftlichen Begründungen zu erlauben und so die Sicherheit erhöhen, ohne die Produktivität zu beeinträchtigen.

Erkennung von anomalem Verhalten

Box Shield nutzt ML-gestützte Erkennung anomaler Verhaltensweisen, um potenzielle Bedrohungen wie kompromittierte Konten und Datendiebstahl zu erkennen und Sicherheitsteams mit Warnmeldungen auf dem Laufenden zu halten. Die Erkennung anomaler Downloads von Shield identifiziert Kontoinhaber:Innen, die möglicherweise vertrauliche Inhalte stehlen. Die Erkennung verdächtiger Standorte kennzeichnet den Zugriff von einem ungewöhnlichen oder ausgeschlossenen geografischen Standort oder einer Host-IP-Adresse. Die Erkennung verdächtiger Sitzungen erkennt potenziell schädliche Zugriffe, die durch ungewöhnliche Zeichenfolgen des Nutzer-Agents, abnormale IDs, ungewöhnliche Anwendungstypen, neue IP-Adressen und eine unwahrscheinlich schnelle Änderung des Anmeldeortes gekennzeichnet sind.

Zentralisierte Content-Ebene in der Cloud

Die Bereitstellung all Ihrer Inhalte in der Content Cloud erleichtert die sichere Zusammenarbeit – selbst zwischen Teammitgliedern, die über verschiedene Regionen und Zeitzonen verteilt sind, und unabhängig davon, welches Gerät sie verwenden. Zentralisierte Inhalte vereinfachen zudem das Informationsmanagement und die Governance, sodass Ihre Inhalte sicherer und immer auf dem neuesten Stand sind.

Sicherheit, die Ihre Inhalte begleitet

Box Shield erweitert die zentralen Sicherheitsfunktionen der Content Cloud um eine weitere Ebene, darunter integrierte Multifaktor-Authentifizierung (MFA), Single Sign-On (SSO), Wasserzeichen und die Verwaltung von KeySafe-Verschlüsselung. Zusammen gewährleisten diese Sicherheitsvorkehrungen, dass Sie jederzeit und überall auf die wertvollen Inhalte Ihres Unternehmens zugreifen und daran zusammenarbeiten können, ohne die Sicherheit zu beeinträchtigen. Mit Box lässt sich nahtlos in Tausende gängiger Anwendungen integrieren, sodass Sie und Ihr Team ganz nach Ihren Wünschen arbeiten können.

Finanzielle Vorteile: Wie die Sicherheit von Box den ROI steigert

In einer von Box in Auftrag gegebenen Studie analysierte Forrester kürzlich die wirtschaftlichen Auswirkungen der Content Cloud. Die Content Cloud wirkt sich auf unterschiedliche Arten auf das Geschäftsergebnis aus. Einige davon beziehen sich direkt auf die Inhaltssicherheit.[8]

Gesamteinsparungen

1.125.000 US-Dollar an Einsparungen bei Netzwerksicherheit, Governance und Compliance, einschließlich Risikominimierung von Datenschutzverletzungen und optimierter Überwachung des Zugriffs auf Inhalte mit Box Shield

Nutzerorientiertes Risiko

580.000 US-Dollar an Einsparungen bei Datenmissbrauch durch unbeabsichtigte Datenlecks

Überwachung des Zugriffs auf Nutzerdaten

237.000 US-Dollar an Einsparungen durch Überwachung des Zugriffs auf Personaldaten

Kosten durch Drittanbieter

245.000 US-Dollar eingesparte Kosten für Sicherheits- und Compliance-Lösungen und Zertifizierungen von Drittanbietern

Data Governance

63.000 US-Dollar an Einsparungen durch einfachere Data Governance

Die Content Cloud: Ein sicherer Ansatz

Unternehmen investieren viel Zeit und Mühe in die Beseitigung von Sicherheitsrisiken in ihren Systemen und Anwendungen – und das zu Recht. Aber um die Sicherheit wirklich zu verbessern, muss der Schwerpunkt auf den Inhalten selbst liegen.

Hier kommt die Content Cloud ins Spiel. Sie ist ein bewährter Ansatz zur Verwaltung Ihrer wertvollsten Daten mit einer zentralen, sicheren Plattform für den gesamten Lebenszyklus von Inhalten. Box steht Ihnen bei jedem Schritt unterstützend zur Seite.

box

Box (NYSE:BOX) ist die Content Cloud, eine zentrale Plattform, die es Unternehmen ermöglicht, den gesamten Content-Lebenszyklus zu verwalten, von überall aus sicher zu arbeiten und führende Anwendungen zu vernetzen. Box wurde 2005 gegründet und genießt das Vertrauen von 69 % der Fortune 500-Unternehmen, darunter AstraZeneca, General Electric, JLL und Nationwide. Box hat seinen Hauptsitz in Redwood City, Kalifornien und weitere Niederlassungen weltweit, inklusive Deutschland.

Weitere Informationen über die Content Cloud und dazu, auf welche Arten sie Freigabe und Zusammenarbeit unterstützt, ohne die Sicherheit zu beeinträchtigen, finden Sie unter box.com/shield.

[1] Tech.co, „Ransomware Statistics 2023: Key Trends, Insights and Quested Questions ", 2023

[2] PurpleSec, „2023 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends", 2023

[3] IBM, Cost of Data Breach report, 2022

[4] Splunk 2022 Cybersecurity Report

[5] Sophos, „State of Ransomware 2022"

[6] Data Driven Investor, 2Email Attachments Generate Nearly 6,000 Unnecessary and Unsecure Files per Employee per Year", 2020

[7] IBM, Cost of a Data Breach report, 2022

[8] Forrester, The Total Economic Impact™ of the Box Content Cloud, Juni 2021
*im Auftrag von Box durchgeführte Studie von Forrester Consulting (Juni 2021); die Gesamtwerte basieren auf einem Verbundunternehmen mit 5.000 Mitarbeitenden.