clearswift
by HelpSystems

LEITFADEN *(Cybersicherheit)*

Verringern informatischer Sicherheitsrisiken in Microsoft 365

Das Cloud-gestützte Produktivitätsversprechen von Microsoft 365

Mit seinen integrierten Anwendungen und intuitiven Funktionen hat sich Microsoft 365 (vormals Office 365) seit seiner Einführung im Jahr 2011 stetig zu einem Produktivitätsmagnaten für Unternehmen entwickelt. In der Tat verzeichnete Microsoft im ersten Quartal des Geschäftsjahres 2020 monatlich 200 Millionen Nutzer, wobei die kommerzielle Nutzung im Vergleich zum vierten Quartal 2020 um 19 % gestiegen ist.

Microsoft 365 bietet mehrere Ebenen von Funktionen, die alle die Cloud nutzen, um Fachleuten auf der ganzen Welt die Möglichkeit zu geben, mit Leichtigkeit zu kommunizieren und zusammenzuarbeiten. Aber bieten die nativen Funktionen der Anwendung die Informationssicherheit und den effektiven Schutz vor Cyberangriffen, die in der heutigen Bedrohungslage erforderlich sind?

In diesem Leitfaden untersuchen wir die in Microsoft 365 integrierte Cybersicherheits-Funktionalitäten und zeigen auf, wo diese nicht umfassend genug sind, um die steigenden Risiken von heute zu bewältigen.

Die heutige Bedrohungslage zeigt keine Reduzierung der Geschäftsrisiken

Es ist kein Geheimnis: Cyberangriffe sind eine kontinuierliche Bedrohung für Unternehmen und ihre sensiblen Daten. Was Microsoft 365 betrifft, entwickeln sich die Cyberkriminellen an mehreren Fronten weiter und versuchen mit diversen Verfahren, an wertvolle Daten zu gelangen. Einige dieser Techniken umfassen:

- **Phishing-Betrug:** Es wird immer schwieriger, gegen Microsoft 365-Benutzer gerichtete Phishing-Kampagnen zu erkennen, da sie clever sind und realistisch aussehen. Diese tarnen sich als harmlos aussehende Kommunikation, wie z. B. eine Besprechungsanfrage eines Mitarbeiters oder ein falscher Live-Chat. Sobald der Benutzer auf den Link klickt, wird er auf die Phishing-Website umgeleitet, die als Microsoft 365-Seite getarnt ist.
- **Malware:** Von einer legitim erscheinenden E-Mail-Adresse eingeschleuste und in Abbildungen eingebettete Malware infizieren Netzwerke, sobald ein Benutzer die betreffende Datei öffnet. Dies kann sogar im PreView-Modus passieren, eine Sicherheitslücke in Microsoft 365, die die Quelle eines Dokuments vor dem Start der Vorschau nicht überprüft. Malware ist oft in Dokumenten versteckt, die Mitarbeiter tagtäglich sehen. Beispielsweise erhält die Finanzabteilung eine Bestellung als PDF-Datei oder die Personalabteilung empfängt einen Bericht. Die Gefahr besteht darin, dass der Empfänger keine Ahnung hat, dass etwas nicht in Ordnung ist, und diese Bedrohungen können ein Netzwerk für Tage, Wochen oder Monate infiltrieren, bevor sie entdeckt werden – falls sie entdeckt werden.
- **Das Umgehen der Sicherheit von Microsoft 365:** Beim NoRelationship-Angriff umgingen die Hacker im Jahr 2019 die nativen Sicherheitsfilter von Microsoft 365, denn diese untersuchen nicht immer die kompletten Dokumente auf Bedrohungen. Vielmehr katalogisieren diese Sicherheitssysteme die externen Links einer Datei mithilfe von xml.rels-Dateien. Die Cyberangreifer entfernten diese Dateien und vermieden damit den Sicherheitsalarm.

Außerdem ist aufgrund der COVID-19-Pandemie die Zahl der Homeoffice-Mitarbeiter drastisch angestiegen, und zur möglichst schnellen Einrichtung von Microsoft 365 übergehen viele Unternehmen die Sicherheitsprotokolle, was natürlich die Verwundbarkeit erhöht. In einer Umfrage unter 250 Informationstechnologie-Leitern und Verantwortlichen der Informationssicherheit bei Finanzdienstleistern in den USA, Großbritannien, den Niederlanden, Deutschland und Australien bestätigte fast die Hälfte der Teilnehmer, COVID-19 habe ihre Pläne zur digitalen Umstellung beschleunigt. Hierzu zählt auch der Übergang zu Microsoft 365. Außerdem erklärten 56 % der Befragten ihre Absicht, die Investitionen im Folgejahr auf die Sicherheit der Cloud, von Microsoft 365 und der E-Mails zu konzentrieren. Seit dem COVID-19-Ausbruch verzeichnen 45 % der großen Finanzinstitute zunehmende Cyberangriffe.

Unbeabsichtigte Datenfreigabe - Vorfälle werden passieren

Andere Situationen verdeutlichen versehentliche, aber nicht weniger schädliche Formen, in denen die falschen Informationen an die falsche Person gesendet werden. Möglicherweise macht ein Kundenbetreuer eine Datei einem Kunden zugänglich, merkt aber nicht, dass sich in einer Tabellenspalte Personal- oder Kreditkartendaten verbergen. Oder ein CEO bemerkt nicht, dass sensible Metadaten im Eigenschaftsfeld oder nicht akzeptierte Änderungen noch in der Versionshistorie eines M&A-Berichts vorhanden sind.

Oder in einem Preisangebot ist das vorherige, an einen anderen Kunden gerichtete Angebot nicht gelöscht worden. Eventuell gibt ein hochrangiger Militär-Angestellter ein Dokument mit einem Foto weiter, ohne zu bemerken, dass dieses Foto streng geheime eingebettete Ortsangaben enthält.

Folgen und Auswirkungen von Datenschutz-Verletzungen

Wie auch immer Daten verloren gehen: Wenn sie in falsche Hände geraten, bedeuten sie mitunter hohe Kosten und Risiken für ein Unternehmen. Zu den Kosten gehören Lösegeldforderungen von Tätern und Geldstrafen von Aufsichtsbehörden für die Nichteinhaltung von Datenschutzgesetzen. Cyber-Angriffe mit der Absicht, Störungen zu verursachen, können interne Abläufe durcheinander bringen, was oft zu Ausfallzeiten beim Kunden führt. Derartige Auswirkungen können die Reputation zerstören und potenziell zu Kundenverlusten führen.

Verhindern von Datenlecks aus E-Mails

Um das Risiko einer Datenverletzung zu vermeiden, müssen Unternehmen ihre geschäftlichen Kommunikationskanäle absichern. Datenlecks durch E-Mails sind an der Tagesordnung. Um das Risiko zu minimieren, müssen E-Mail-Sicherheits-Tools tief in die Nachrichten und Anhänge hinein scannen, um sensible oder kritische Informationen zu identifizieren, bevor sie das Unternehmen verlassen.
Microsoft 365 ist gut für den Umgang mit Spam und Malware und bietet verschiedene Ebenen der E-Mail-Sicherheit, wie z. B. Tools zur Bewältigung der regulatorischen Kontrolle durch Archivierung und grundlegende Verschlüsselung. Es werden Regel-Vorlagen bereitgestellt, die Ihnen den Einstieg in die Policies erleichtern, aber diese bieten in der Regel nicht die tiefgreifende Inhaltsprüfung (Deep Content Inspection), die für echte Sicherheit erforderlich ist.

Die Sicherheitsmängel von Microsoft 365

Alle Microsoft 365-Kunden sind automatisch durch Antiviren- und Antispam-Funktionen geschützt, aber der Grad des Schutzes hängt von dem Paket ab, das Ihr Unternehmen verwendet. Was den Schutz vor Datenverlusten, Cyber-Bedrohungen und Verwaltungsfunktionen betrifft, haben Clearswift-Kunden zahlreiche Bedenken geäußert.

- DLP-Kontrollen sind nicht sehr umfassend und können schwer effektiv zu konfigurieren sein
- Die Regelungen erfordern in Microsoft 365 eine Konfiguration an mehreren Admin-Konsolen. Für die Suche nach einem Schlüsselwort muss zum Beispiel eine Transport Rule eingerichtet werden, während für die Erkennung einer Kreditkartennummer die Richtlinie in den Konfigurationseinstellungen für Sicherheit und Compliance konfiguriert wird
- Das Programm erkennt keine sensiblen Angaben (etwa Personaldaten) in Bilddateien, z. B. in Bildschirmfotos oder in eingescannten Dokumenten.
- Außerdem ist Microsoft 365 nicht in der Lage, Metadaten (die zu Datenlecks führen können) oder in Dokumenten oder Bilddateien verborgene Malware zu entfernen.
- Selbst **mit** der Sandboxing-Analyse von Anhängen ist der Schutz vor Ransomware begrenzt.
- Das Programm umfasst keine Möglichkeiten, ausgehende E-Mails in Quarantäne zu senden. Nur das Zurückweisen, das Aufheben der Sendefreigabe und das Umleiten zum Administrator sind möglich.
- Microsoft 365 blockiert nur ausführbare Dateiformate (gemäß Dateinamen). Die Überwachung anderer Dateien hängt von den Regelungen über die Dateiformate ab, also zum Beispiel über Xlsx, Xlsm, Xlsb (etc.), aber nicht „Excel".
- Das Programm ist nicht in der Lage, neue individuelle Dateiformate (im Dateinamen angegeben) zu definieren.
- Seine Mitteilungsoptionen sind begrenzt (nur an den Sender, Empfänger oder Administrator).
- Vorhandene Listen (mit Ausdrücken oder unangemessenen Sprachelementen) lassen sich nicht wiederverwenden. Microsoft stellt einige Klassifikatoren zur Verfügung, um Bedrohungen, Profanität, Lebensläufe, Quellcode und Belästigungen abzudecken. Sie sind jedoch dabei, ihren Offensive Language Classifier zu verwerfen, da er zu viele falsche positive Ergebnisse erzeugt.
- Das Programm bietet keine Mittel zur Vervielfältigung von Regeln und zur Einführung bindender Regeln nach abweichenden Kriterien und ohne Vorlage (z. B. gemäß Sender, Empfänger oder verletzendem Sachverhalt).
- Komplexe Kundenkonfigurationen erschweren manchmal die Policy-Regeln.
- Die Fehlermeldungen sind irreführend oder nicht hilfreich, obwohl manche die Tool-Tipps nützlich finden.
- Die Berichterstattung bietet keine hinreichend umfassenden und gleichzeitig leicht verständlichen Details, die bei Verletzungen der Datensicherheit aber notwendig sind. Darüber hinaus ist zu beachten, dass jede Berichterstellung über Daten, die älter sind als einen Tag, signifikant länger dauert.
- System-Anmeldedaten sind nur schwer nach Kunden aufzuschlüsseln.

Werden Sie ein Zero-Compromise Unternehmen

Clearswift bietet eine umfassendere Lösung mit höherer Sicherheit als Microsoft 365 alleine. Für IT-Sicherheits-Fachkräfte ist das ein wichtiger Faktor zum Schutz und zur Überwachung sensibler und kritischer Daten in zunehmend Cloud-zentrierten Infrastrukturen.

Führen Sie das Clearswift Secure Email Gateway zusammen mit Microsoft 365 ein: Dann verfügen Sie über die fehlenden Elemente für eine robuste und umfassende Sicherheit. Wenn Sie außerdem die zusätzlichen Vorteile der Adaptiven Redaktion nutzen, kann Ihr Unternehmen sicher sein, dass seine sensiblen und kritischen Daten im Rahmen von Microsoft 365 sicher sind. Dabei ist es nicht notwendig, die Zusammenarbeit aus Sicherheitsgründen einzuschränken, denn dieser Ansatz bietet das Beste in beiderlei Hinsicht.
Das Clearswift Secure Email Gateway deckt alle Basiselemente ab. Es umfasst die Deep Content Inspection, ein Programm zur tiefgreifenden Inhaltsuntersuchung. Es analysiert Mitteilungstitel, Betreffzeilen, die Mitteilungen selbst und ihren Inhalt gründlich, einschließlich der Anhänge, Abbildungen und Dokument-Kopfzeilen und Fußzeilen, sowie auch eventuell in Dokumenten vorhandene Metadaten. Dieses Vorgehen maximiert die Chancen, sensible Inhalte aufzuspüren, wie etwa Kreditkartennummern, Bankcodes, Vertraulichkeitsklauseln, unangemessene Sprache, vom Kunden festgelegte oder reguläre Ausrücke sowie boolesche oder auf Positionsoperatoren basierende Ausrücke.

Darüber hinaus kontrollieren und überwachen Sie mit diesem Gateway Ihre **internen E-Mails**. Diese granulare Überwachung und der fortschrittliche Schutz vor Datenverlust verhindern den unbefugten Zugriff. Während Unternehmen den Zugriff auf Dateiserver und andere Kollaborationsdienste auf der Basis der Tatsache kontrollieren, dass nicht alle Informationen für alle Personen zugänglich sein sollten, fehlen bei internen E-Mails traditionell diese Einschränkungen. Das bedeutet: Jeder Firmenangestellte kann und darf jedem Kollegen innerhalb des Unternehmens senden, was er/sie möchte. Das Secure Email Gateway mindert Gefahren dieser Art.

Adaptive Redaktion auf einen Blick:

Diese einzigartige Clearswift-Technologie schützt Ihre E-Mails, ohne die Produktivität zu beeinträchtigen. Sie entfernt in Echtzeit ausschließlich jene Informationen, die zu Datenschutz-Verletzungen führen oder Cyber-Angriffe ermöglichen könnten, lässt aber die sonstigen Mitteilungen ungestört an ihre Zielorte durch. Um zukünftige Auswahlprozesse zu erleichtern, erhält der betreffende Sender eine Mitteilung über eine eingetretene Datenschutz-Verletzung. Die Adaptive Redaktion umfasst folgende Hauptfunktionen:

- **Die „Redaktion" (Bearbeitung)** von Dateien der Formate Word, Excel, PowerPoint und PDF und von E-Mails zur Beseitigung sensibler Daten (Personal- und Kreditkartendaten etc.).
- **Document Sanitization** , einschließlich des Löschens von markierten Änderungen und Eigenschaftsangaben.
- **Structural Sanitization** entfernt aktive Inhalte und sonstige potenziell bösartige Elemente wie fortgeschrittene Bedrohungen (Advance Persistent Threats, APTs, Ransomware usw.) aus Dokumenten.

Sie können diese Funktionen auf eingehenden, ausgehenden und internen Datenverkehr anwenden.

Schließen von Sicherheitslücken in Microsoft 365

Mit Clearswift-Technologie bringt sich Ihr Unternehmen in eine starke Position gegen Datenverluste und Cyberangriffe. Das ist möglich, da leistungsstarke Funktionen und Kontrollelemente jene Lücken schließen, die Cyberkriminellen – und auch böswilligen oder nur achtlosen Firmenangestellten – Angriffsflächen bieten.

- **Flexible und granulare Kontrolle des Regelwerks zum Schutz vor Datenverlusten:** Geben Sie je nach Sender, Empfänger, Domäne oder Abteilung unterschiedliche Regeln vor. Sie verfügen über einsatzbereite Regelwerke gemäß Vorschriften wie DSGVO, individuelle Token-Wörterbücher und über 200 vorkonfigurierte Token.
- Eine **optische Zeichenerkennung (OCR)** spürt sensible Daten (z. B. Personal- und Kreditkartendaten) in Bildern und gescannten Dokumenten auf.
- Darüber hinaus verhindert die **Anti-Steganografie**-Funktion das Herausschleusen sensibler Angaben aus Bilddateien und entfernt ankommende eingebettete Bedrohungen.
- **Structural Santization** bietet zusätzlichen Schutz vor APTs und Ransomware.
- Nötigenfalls werden E-Mails in Quarantäne überstellt. Dort lassen sie sich bearbeiten, bereinigen oder im Detail untersuchen. Je nach Art der Datenschutz-Verletzung können Administratoren, Linienmanager oder Endbenutzer diese Abläufe verwalten.
- Die Schutzfunktionen erkennen ausführbare Dateien, Bilddateien, Dokumente und Multimedia-Dateien nach ihrem Format.
- Anpassbare **Missing Manager**-Regeln ermöglichen es einem Administrator, für jeden Benutzer einen Manager/Compliance Officer zu definieren und die CC- und TO-Felder für dessen E-Mail-Adresse zu überprüfen. E-Mails werden zur Freigabe durch den Manager/Compliance Officer geprüft
- Einfaches Verwalten von Richtlinien mit wiederverwendbaren Richtlinienobjekten, ohne dass zusätzliche Overhead-Kosten anfallen
- Die Möglichkeit, eine benutzerdefinierte Dateityperkennung zu definieren, um Dateien zu blockieren, die zu sensibel sind, um sich auf erweiterungsbasierte Kontrollen zu verlassen
- **Umfassende Berichterstattung** mit vollständigem Track und Trace
- **Echtzeit-Verfolgung von Mitteilungen** ohne spürbare Verzögerungen
- Sie erhalten Zugriff auf alle Aufzeichnungsdaten, denn Sie sind der exklusive Benutzer (tenant).

Integration von Microsoft 365 und Clearswift Secure Email Gateway

Sie können die E-Mail Security-Lösung von Clearswift gemeinsam mit Microsoft 365 einsetzen. So gewährleisten Sie die Sicherheit Ihrer sensiblen Unternehmensdaten – ganz gleich, ob diese vor Ort, in der Cloud oder in einer Hybrid-Umgebung gespeichert sind.

Zusätzliche Betrachtungen gemäß Abbildung 1:

- **Scannen des E-Mail-Verkehrs:** Das Clearswift Secure Email Gateway analysiert eingehende, ausgehende und intern übermittelte E-Mails und bietet so einen umfassenden Schutz.
- **Hybrid-Einführungen:** Die Clearswift-Lösung kann als Hybrid-Konfiguration eingesetzt werden, wenn Ihr Unternehmen sowohl Microsoft 365 als auch eine On-Premise-E-Mail-Lösung verwendet.
- **Ein adaptiver Ansatz:** Microsoft 365 bietet eine umfassende gehostete E-Mail und SharePoint-Lösung mit unterschiedlichen Sicherheitsebenen. Wenn Sie wirklich auf die Sicherheit Ihrer sensiblen und kritischen Daten vertrauen möchten, müssen Sie die genannten Sicherheitsfunktionen mit einem adaptiven Ansatz ergänzen.

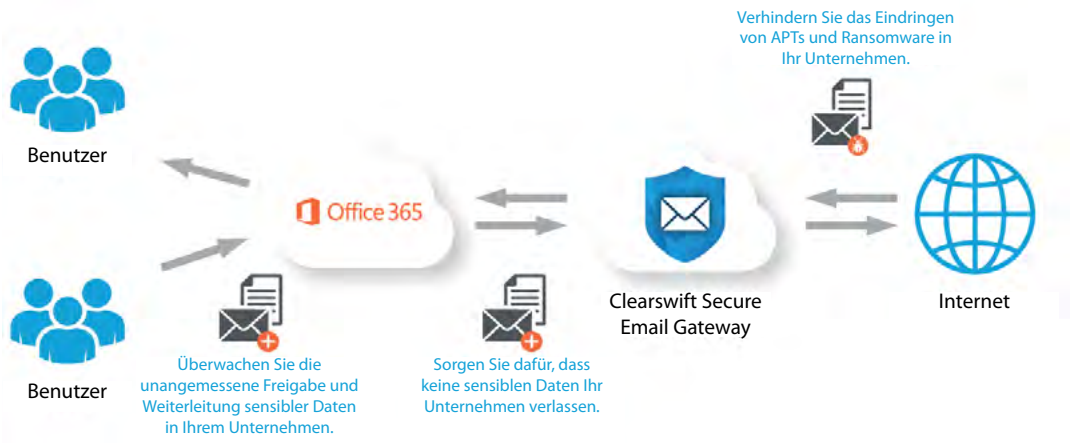

Abbildung 1: Clearswift Secure Email Gateway integriert sich in Microsoft 365, um Lücken in der Informationssicherheit zu schließen

Zusammenfassung

Mit wachsender Kreativität erzeugen Cyberkriminelle immer ausgefeiltere Bedrohungen – und die gesetzlichen Vorgaben zum Datenschutz werden strenger. Daher sollten Unternehmen, die ihre sensiblen und kritischen Informationen in Microsoft 365 speichern, die Vorteile dieses Systems und die damit verbundenen Gefahren abwägen. Auch in der am weitesten fortgeschrittenen Variante hat die Microsoft-Plattform noch Mängel, die es zu beheben gilt.

Clearswift bietet die bewährte Sicherheitslösung, die Sie für eine nahtlose Integration in Microsoft 365 benötigen, um einen erweiterten Schutz vor Bedrohungen und Daten zu ermöglichen. Die leistungsstarke Kombination der Technologien von Clearswift und Microsoft 365 schließt Sicherheitslücken und senkt die Risiken für Ihr Unternehmen.

Weitere Informationen zur Cloud-gestützten Sicherheit finden Sie unter www.clearswift.com/solutions/cloud-security. Möchten Sie tiefer ins Thema einsteigen? Dann sehen Sie sich unser auf Anfrage verfügbares Webinar an oder fordern Sie bei unserem Team eine Demo an.

clearswift
by HelpSystems

www.clearswift.com

Über HelpSystems

HelpSystems ist ein „People-First"-Software-Anbieter und unterstützt Unternehmen bei Verbesserungen ihrer Informationstechnologie (Build a Better IT™). Unsere ganzheitliche Suite aus Sicherheits- und Automatisierungs-Lösungen schafft eine einfache, intelligente und leistungsstarke IT. Kunden in über 100 Ländern und in allen Branchen vertrauen auf die Ruhe und Sicherheit, die HelpSystems bietet. Erfahren Sie mehr unter www.helpsystems.com.