CYREN

Inbox-Schutz als Schlüssel zu mehr Sicherheit bei Microsoft 365

Kommerzielle IT-Publikation

Inbox-Schutz als Schlüssel zu mehr Sicherheit bei Microsoft 365 – Inbox Detection & Response

Inhaltsverzeichnis

Einleitung: Inbox-Schutz als Schlüssel zu mehr Sicherheit bei Microsoft 365

Die von Gartner empfohlene adaptive Sicherheitsarchitektur, die das Konzept Verhindern-Erfassen-Reagieren-Prognostizieren beschreibt, wird in der Cybersicherheit seit Jahren umfassend angewendet. Bis jetzt wurde dieses Rahmenwerk aber nicht ganzheitlich auf die E-Mail-Sicherheit bei Microsoft 365 angewendet, die sich traditionell auf den Präventionsaspekt durch ein sicheres E-Mail-Gateway am Netzwerkperimeter konzentrierte.

Forschungsdaten zeigen aber, dass dieses herkömmliche E-Mail-Gateway-Sicherheitsmodell selbst bei dieser einzelnen Aufgabe, dem Schutz vor den Angriffen von heute, bei Nutzern von Microsoft 365 zunehmend versagt. In jüngsten Umfragen von Osterman Research gaben 70 Prozent der IT-Sicherheitsmanager allgemein und 78 Prozent der E-Mail-Administratoren von Microsoft 365 an, 2018 Datenverletzungen erlitten zu haben, wobei E-Mail-Phishing-Angriffe als Hauptursache genannt wurden. Ein Hauptgrund dafür, dass diese Phishing-Angriffe bestehende Verteidigungslinien überwinden konnten, ist, dass sie immer ausgefeilter werden und zunehmend Methoden zur Detektionsumgehung einsetzen. Der Einsatz solcher Methoden wird durch ihre Eingliederung in die Angebote eines immer robusteren Phishing-as-a-Service-Ökosystems, das zu niedrigen Kosten qualitativ hochwertige und einfach zu verwendende Phishing-Kampagnen-Tools und Services im Dark Web bietet, immer häufiger.

Prozentsatz der Organisationen, die Microsoft 365 nutzen und 2019 mindestens einen IT-Sicherheitsverstoß gemeldet haben:

78 %

Um die Sicherheit angesichts solcher Phishing-Bedrohungen zu erhöhen, müssen Unternehmen, die Microsoft 365 nutzen, von einem Gateway-basierten Einzeldurchlauf-Inspektionsmodell zu einem neuen, geschichteten Sicherheitsmodell wechseln, das kontinuierliche E-Mail-Überwachung und Detektion umfasst. Bei diesem neuen Ansatz wird jede Nachricht nach der Zustellung auf Bedrohungen und anomales Verhalten untersucht. Wird eine Bedrohung identifiziert, können verdächtige Nachrichten automatisch aus allen betroffenen Posteingängen entfernt werden. Dadurch wird ein zweiter Mangel des aktuellen E-Mail-Sicherheitsmodells angesprochen: der arbeitsintensive Prozess der Untersuchung, des Containment, der Reaktion auf und Remediation von bösartigen E-Mails im gesamten Unternehmen.

Indem im Posteingang Verteidigungsfunktionen hinzugefügt werden, entsteht auch eine neue Gelegenheit, die „Schwarmintelligenz" auf automatisierte, strukturierte Weise besser zu nutzen. Beim alten E-Mail-Sicherheitsmodell hatten Nutzer trotz der in Sicherheitsschulungen geflossenen Mittel keine wirksame Möglichkeit, verdächtige Mails den Sicherheitsteams zu melden. Dieses neue E-Mail-Sicherheitsmodell unterstützt die Integration eines einfachen Add-ins für den E-Mail-Client, das Benutzern eine Möglichkeit gibt, alle verdächtigen E-Mails (nicht nur Spam) für ein bedarfsgesteuertes, automatisiertes Scanning zu kennzeichnen. Durch den Scan wird die Bedrohungsintelligenz mit forensischen Daten angereichert, und die Informationen werden sofort mit den Benutzern geteilt, die dann aus mehreren nächsten Schritten wählen können.

Schließlich sollten die Schutzmaßnahmen Algorithmen für das maschinelle Lernen mithilfe der erfassten Outputs durch kontinuierliches Scannen von E-Mails, Überwachen des Benutzerverhaltens und Verfolgung von URLs stärken. Durch die Analyse dieser Daten können sie Anomalien besser erfassen und prognostizieren, wie die nächste Bedrohung aussehen könnte.

Ausweich-Phishing umgeht übliche Verteidigungsmaßnahmen von MICROSOFT 365

Der Posteingang ist ein Ziel, und kein sicheres E-Mail-Gateway (SEG) kann völlig vor den E-Mail-Bedrohungen von heute schützen, die immer ausgefeilter und schwieriger zu erkennen sind. Phishing ist ein industrieweites Problem. Dies liegt an der zunehmenden Geschwindigkeit von Phishing-Angriffen, immer ausgefeilteren Phishing-Methoden und dem Aufstieg der „Phishing-as-a-Service"-Branche.

Forscher bei Cyren beobachten eine Vielzahl schlauer Phishing-Angriffe, die Geschäfts-E-Mail-, App- und Systemanmeldedaten ins Visier nehmen. Wenn Angreifer auf einen Satz legitimer Anmeldedaten zugegriffen haben, können sie einen mehrphasigen Unternehmens-E-Mail-Kompromittierungsangriff starten, der die eigenen internen Kommunikationssysteme des Unternehmens nutzt, um zu lauschen, zu lernen und den finalen Angriff zu planen. Ein Angreifer kann z. B. den Posteingang eines Benutzers an einer guten Stelle anvisieren und dann beobachten, um zu erfahren, wann eine Führungskraft in den Urlaub geht, welche Zahlungen fällig werden und wer für Zuliefererzahlungen zuständig ist. All diese Informationen können vom Angreifer zur Planung eines überzeugenden Überweisungsbetrugs eingesetzt werden.

Prozentsatz der im Dark Web zum Verkauf angebotenen Phishing-Bausätze, bei denen mindestens eine Ausweichtechnik genutzt wird, um das Erkennen zu erschweren:

87 %

Cyren Security Lab

Prozentsatz der Phishing-Bausätze, mit denen Anmeldedaten für Microsoft 365 anvisiert werden:

25 %

Cyren Security Lab

Zunehmend häufige Taktiken, die eine Detektion schwieriger machen, sind z. B. verzögerte Aktivierung, URL-Kodierung, um Phishing-Crawler zu täuschen, HTML-Verschlüsselung (d. h. Verschlüsseln der Phishing-Website mit AES-Verschlüsselung), Host- und IP-Blockaden, Missbrauch legitimer Cloud-Dienste sowie Maßnahmen, die verhindern, dass Sicherheitssysteme die wahre Natur einer Phishing-Website evaluieren und erkennen.

Darüber hinaus stellen technisch versierte Phishing-as-a-Service-Anbieter schlüsselfertige Phishing-Kampagnen, die schwer zu erkennende Methoden umfassen, einer breiten Zielgruppe nicht technisch versierter Krimineller zur Verfügung.

Phishing folgt der Malware-Kurve

„Evasive Malware“ gibt es schon lange, und auch der Begriff wird bereits seit Jahrzehnten benutzt. Das Konzept des „Evasive Phishing“ ist relativ neu, folgt aber eindeutig einem ähnlichen Entwicklungspfad wie Malware. Der Einsatz schwer zu erkennender Methoden wird immer häufiger. Analysen des Cyren Security Lab an Malware, die an die Cloud-Sandbox von Cyren geschickt wurde, ergaben, dass 99 % der Malware mindestens eine Methode zur Detektionsumgehung nutzten. Eine Aufschlüsselung einer einzigen Malware ergab, dass sie sogar 29 unterschiedliche Umgehungstechniken nutzte.

Während Cyren-Forscher noch keine Phishing-Versuche entdeckt haben, die technische Täuschungsmethoden dieses Grades umfassten, stellten sie in einer jüngsten Studie fest, dass 87 % der im Dark Web zum Kauf angebotenen Phishing-Kits mindestens eine Methode zur Reduzierung der Erkennungswahrscheinlichkeit umfassten.

Die Einschränkungen aktueller E-Mail-Sicherheitsarchitekturen

Sichere E-Mail-Gateways (SEGs) wurden ursprünglich mit dem Ziel entwickelt, Spam und Malware zu stoppen, bevor sie den Mailserver einer Organisation erreichen. Sie können das recht gut, vor allem, wenn sie fortgeschrittene Detektionsfunktionen wie Inline-Sandboxing umfassen und Sicherheitsprotokolle wie SPF, DKIM und DMARC unterstützen. Zweifelsohne sind SEGs wichtige Bestandteile einer Defense-in-Depth-Strategie.

Selbst die besten SEGs stellen aber keine umfassende E-Mail-Sicherheit bereit und können nicht jede bösartige E-Mail abwehren. Angesichts des riesigen Volumens an E-Mails, die Unternehmen heutzutage erhalten, können selbst niedrige Prozentsätze nicht abgeblockter bösartiger E-Mails monatlich Hunderttausend zugestellte Nachrichten bedeuten.

Eine SEG hat nur eine Chance zu bestimmen, ob eine E-Mail sauber ist, bevor diese zugestellt, gelöscht oder unter Quarantäne gestellt wird. Wenn das SEG eine E-Mail zustellt, die eine Bedrohung enthält, ist es schon zu spät. Es ist egal, ob das SEG aktualisiert wird, um in Zukunft vor dieser jeweiligen Bedrohung zu schützen: Die Bedrohung ist bereits im Netzwerk aktiv.

Manche Arten von SEGs sind schwierig und zeitaufwändig zu konfigurieren. Das stellt in sich schon ein Sicherheitsrisiko dar, weil kritische Funktionen übersehen oder falsch konfiguriert werden könnten, wodurch Sicherheitslücken entstehen, die erst nach einem erfolgreichen Angriff zu Tage treten.

Klickzeit-Schutz ist kein Allheilmittel

Time-of-Click-Schutz bietet dem SEG eine letzte Chance, eine Phishing-E-Mail mit einer URL zu erfassen, und zwar zu einem einzigen Zeitpunkt.

Bei der üblichen Implementierung gilt: Klickt ein Benutzer auf die URL, sucht die SEG in einer Datenbank bekannter Phishing-Sites dann nach dieser URL. Sie führt in der Regel keine Echtzeitanalyse der Inhalte auf dem Zielserver durch.

Benutzern wird beigebracht, auf verdächtige URLs zu achten. Time-of-Click-Schutz schreibt die URLs aber oft um, sodass alle geschützten URLs für den Durchschnittsbenutzer verdächtig aussehen. Das Endergebnis ist eine Flut falscher Alarme, durch die Produktivität beeinträchtigt und das Supportteam überlastet wird.

Als Perimetersicherheit haben SEGs durchaus ihre Berechtigung. Jeder Sicherheitsexperte weiß aber auch, dass keine Verteidigung alle Bedrohungen abwehrt. Selbst SEGs mit fortgeschrittenen Detektionsfähigkeiten stoßen bei der Exponierung von Kontoübernahme-Angriffen, Spear-Phishing, Cousin-Domain-Spoofing und vielen unbekannten Bedrohungen an ihre Grenzen. Phishing-E-Mails werden die Sicherheitsvorkehrungen überwinden. In diesem Fall kann das SEG die erforderlichen nächsten Schritte „Erfassen, Reagieren, Prognostizieren“ nicht durchführen. Daher kann sich die betroffene Organisation nicht gegen Angriffe wehren, von denen sie nicht einmal weiß, dass sie gerade stattfinden.

Phishing-Verteidigung im Detail

Eine neue Kategorie der E-Mail-Sicherheit entsteht gerade: Inbox Detection and Response (IDR). Mithilfe der nativen, von Cloud-Plattformen wie Microsoft 365 bereitgestellten APIs kann IDR den Kreis der von Gartner beschriebenen adaptiven Sicherheitsarchitektur schließen. IDR bietet kontinuierliche Überwachung, Detektion und Vorfallmanagement für alle E-Mails im Postfach von Microsoft 365, wodurch die „Prävention" eines SEG beim ersten Scan um Phishing-Defense-in-Depth und die anderen Elemente des Sicherheitsmodells ergänzt wird, wie nachstehend angegeben.

IDR schafft eine Feedback-Schleife basierend auf den von kontinuierlichen E-Mail-Scans, Überwachung des Benutzerverhaltens und Verfolgung von URLs erfassten Outputs, um Algorithmen für das maschinelle Lernen zu stärken. Durch die Analyse dieser Daten können Organisationen Anomalien besser erfassen und prognostizieren, wie die nächste Bedrohung aussehen könnte. Zudem lassen sich mit IDR Informationen zu SEGs und anderen Sicherheitskomponenten forcieren und so das Sicherheitsprofil der Organisation insgesamt stärken.

Das SEG ist weiterhin die erste Schutzschicht, stellt möglichst saubere Verbindungen her und schützt vor bekannten und vielen unbekannten Bedrohungen.

Mithilfe des Rahmenwerks erfasste Daten werden in Korrelation gebracht, um zu bestimmen, ob eine E-Mail bösartig ist und Abhilfemaßnahmen ergriffen werden sollten. Mit Vorfall- und Fallverwaltungsabläufen können E-Mail-Admins und Sicherheitsanalysten falsch positive Ergebnisse entfernen sowie Bedrohungen untersuchen und eindämmen, als auch entsprechende Reaktions- und Abhilfemaßnahmen treffen.

IDR schützt vor neuen Bedrohungen, indem jede E-Mail im Postfach jedes Nutzers geprüft und bei Entdeckung einer neuen Bedrohung abermals geprüft wird. Die Lösung überwacht Verhalten und Benutzerinteraktionen in der Mailbox und identifiziert Anomalien. IDR bildet zudem das Rahmenwerk für die Benutzerinteraktion mit Detektionstechnologien und integriert Benutzer-Feedback schnell und automatisch, um Phishing-Angriffe zu identifizieren und vor ihnen zu schützen.

IDR kann schnell und einfach bereitgestellt werden und verwendet die von E-Mail-Plattformen bereitgestellten nativen APIs. Es müssen keine MX-Records geändert oder ein bestehendes SEG ersetzt werden. Die IDR-Plattform sollte erweiterbar sein, um die Bereitstellung mehrerer Sicherheitstechnologien zu unterstützen. Zunächst wird sie sich darauf konzentrieren, die vom SEG zurückgelassenen Lücken zu stopfen. Im Verlauf der Zeit eignet sie sich wegen ihrer Erweiterbarkeit aber hervorragend zur Integration von oft an anderer Stelle eingesetzten Technologien wie z. B. Sandboxing, Anti-Malware und DLP. Das bedeutet, dass Unternehmen und Organisationen alle Vorteile der kontinuierlichen Überwachung, Detektion und Reaktion auf alle Bedrohungen nutzen können. IDR entlastet außerdem Sicherheitsanalysten und E-Mail-Administratoren, indem der Remediationsprozess automatisiert wird und die für eine tiefgehende forensische Analyse erforderlichen Tools bereitgestellt werden, um eine schnelle Reaktion beim Auftreten neuer Bedrohungen zu ermöglichen.

Grundlegende Merkmale eines IDR-Service

Grundlegende IDR-Funktionen umfassen:

FORTLAUFENDE ÜBERPRÜFUNG – *FÄNGT MÖGLICHE PHISHING-NACHRICHTEN NACH DER SEG-VERARBEITUNG AB*

E-Mails in allen Ordnern von Microsoft 365 sollten beim Empfang und danach kontinuierlich gescannt werden, wann immer eine neue Bedrohung festgestellt wird.

LAUFENDER SCHUTZ VOR NEUEN UND SICH WEITERENTWICKELNDEN BEDROHUNGEN – *FÄNGT NEUE AUSWEICH-PHISHING-BEDROHUNGEN IN SEKUNDEN AB*

Die Geschwindigkeit der Detektion und Zeit bis zum Schutz ist ausschlaggebend, doch können manche Phishing-Bedrohungen anfangs unerkannt bleiben. Durch die Kombination von kontinuierlicher Überwachung mit schneller Detektion und automatisierter Remediation kann eine IDR-Lösung in Sekundenschnelle vor neuen Evasive-Phishing-Bedrohungen schützen. Falls sich eine zuvor als sauber eingestufte E-Mail später als Bedrohung herausstellt, sollte das IDR-System die E-Mail im Nachhinein zurückrufen („Claw Back“) und aus jeder Mailbox bei Microsoft 365 im gesamten Unternehmen entfernen.

ABSENDERVERHALTENSANALYSE – *VERHINDERT GEZIELTE ANGRIFFE WIE BEC*

Es müssen viele verschiedene Methoden angewendet werden, um Betrüger- oder Spoof-E-Mails im Posteingang zu erkennen. Hierzu sollten folgende Methoden gehören: umfassende Kopfzeilenanalyse; Cousin- oder Lookalike-Domain-Detektion; lexikalische Analyse zur Suche nach Wörtern und Ausdrücken, die auf Social-Engineering-Angriffe hinweisen, sowie versuchte Verkörperung von Führungskräften, Kunden oder Geschäftspartnern.

POSTFACHVERHALTENSANALYSE – *DECKT VERDÄCHTIGE AKTIVITÄTEN UND KONTOÜBERNAHMEANGRIFFE AUF*

Mailbox-Verhaltensanalyse sollte Mailboxen profilieren, um eine Baseline vertrauenswürdiger Verhaltensweisen und Beziehungen zu schaffen, indem historische Daten wie etwa vertrauenswürdige Absender und Domains, Anzahl der gesendeten und empfangenen E-Mails in einem bestimmten Zeitraum, wie oft in der Regel E-Mails gesendet und empfangen werden, usw. in Modelle für maschinelles Lernen integriert werden. Mailboxen sollten dann kontinuierlich auf anormale Verhaltensweisen überwacht und Bedrohungen mithilfe prädiktiver Analytik erfasst werden. Benutzeraktionen sollten ebenfalls analysiert und mit anderen im Unternehmen verglichen werden, um Verhaltensweisen zu entdecken, die in Echtzeit darauf hinweisen, dass ein Angriff stattfinden könnte.

URL-VERHALTENSANALYSE – *VERHINDERT DIEBSTAHL VON ANMELDEDATEN*

URL-Verhaltensanalyse sollte Benutzer vor Phishing-Websites schützen, die Anmeldedaten stehlen. Dies ist oft die erste Phase eines Kontoübernahme-Angriffs. Durch eine solche Funktion werden aus E-Mails extrahierte URLs auf Verdachtshinweise hin analysiert, sie werden bis zum endgültigen Ziel verfolgt und die Zielwebseite wird auf Hinweise einer Phishing-Site untersucht.

CROWD-SOURCING-BENUTZERDETEKTION – *BIETET NUTZERN SELBSTBEDIENUNGSWERKZEUGE ZUM SCHUTZ IHRER POSTEINGÄNGE*

Ein großer Vorteil einer IDR-Lösung besteht darin, Benutzern von Microsoft 365 ein einfach zu verwendendes Rahmenwerk bereitzustellen, damit sie Phishing-E-Mails entdecken und informierte Entscheidungen zur Reaktion auf fragwürdige Nachrichten treffen können. Dieses Selbstbedienungstool ist direkt in den Mailclient integriert und ist so besonders benutzerfreundlich. Reicht ein Benutzer eine Nachricht zur Untersuchung ein, kann diese automatisch gescannt und klassifiziert werden, wodurch das IT-Team beim Benutzersupport entlastet wird.

VORFALLMANAGEMENT – *ERMÖGLICHT BEI BEDROHUNGEN EINE RASCHE UNTERSUCHUNG, EINDÄMMUNG, REAKTION UND REMEDIATION*

Immer wenn eine E-Mail einer Richtlinie nicht entspricht oder von einem Benutzer gemeldet wird, der einen On-Demand-Scan fordert, sollte ein Vorfall erstellt werden. Ein Posteingangssicherheitsadministrationsportal muss Vorfall- und Fallmanagement sowie Workflow und umfassende IOC- und Forensikinformationen bieten, die an ein SIEM exportiert werden können.

Fazit: Postfachsicherheit als neue Verteidigungslinie

Sichere E-Mail-Gateways wurden nicht dafür entwickelt, vor den ausgefeilten, schwer zu erkennenden Phishing-Angriffen von heute zu schützen, und es kann nicht verhindert werden, dass manche Angriffe Benutzer erreichen. Die Perimeter-E-Mail-Sicherheit eines SEGs reicht nicht mehr aus. Es ist an der Zeit, kontinuierliche Sicherheit in den Posteingang von Microsoft 365 zu integrieren, der als neuer Perimeter aufgefasst werden kann.

Die Herausforderung für Unternehmen besteht darin zu bestimmen, welche Bedrohungen am gefährlichsten sind. Die Angriffe, auf die es ankommt, sind die am stärksten zielgerichteten. Diese nutzen oft Detektionsumgehungstechniken, und die Angreifer sind fähig, schnell auf einen neuen Ansatz umzusteigen, wenn der vorherige fehlgeschlagen ist.

Der sich entwickelnde Technologiebereich IDR bietet eine neue Gelegenheit, Unternehmen vor Evasive-Phishing-Angriffen zu schützen, indem kontinuierliche E-Mail-Überwachung, Detektion und Reaktion eingesetzt werden, um wirkliche Defense-in-Depth für E-Mail zu bieten und dadurch die erste vom SEG gebotene Verteidigungslinie zu ergänzen, während gleichzeitig eine schnelle Remediation automatisiert und dadurch das Sicherheitsteam eines Unternehmens entlastet wird. Microsoft-365-Administratoren und Sicherheitspersonal erhalten dadurch außerdem Vorfallmanagement-Workflows und eine echte Integration der „Schwarmintelligenz" von den Benutzern, ohne dass sich dies auf die Benutzerproduktivität auswirken würde.

Über Cyren

Mehr als 1,3 Milliarden Benutzer weltweit verlassen sich täglich auf die zu 100 % cloudbasierten Sicherheitslösungen von Cyren für den Schutz vor Cyberangriffen und Datenverlusten. Auf Basis der weltweit größten Sicherheits-Cloud schützt Cyren (NASDAQ: CYRN) Unternehmen schnell mit mehrfach ausgezeichneter E-Mail-Sicherheit, Cloud-Sandboxing- und DNS-Filterdiensten für Unternehmen sowie Threat-Intelligence-Lösungen für Sicherheits- und Dienstanbieter wie Microsoft, Google und Check Point.