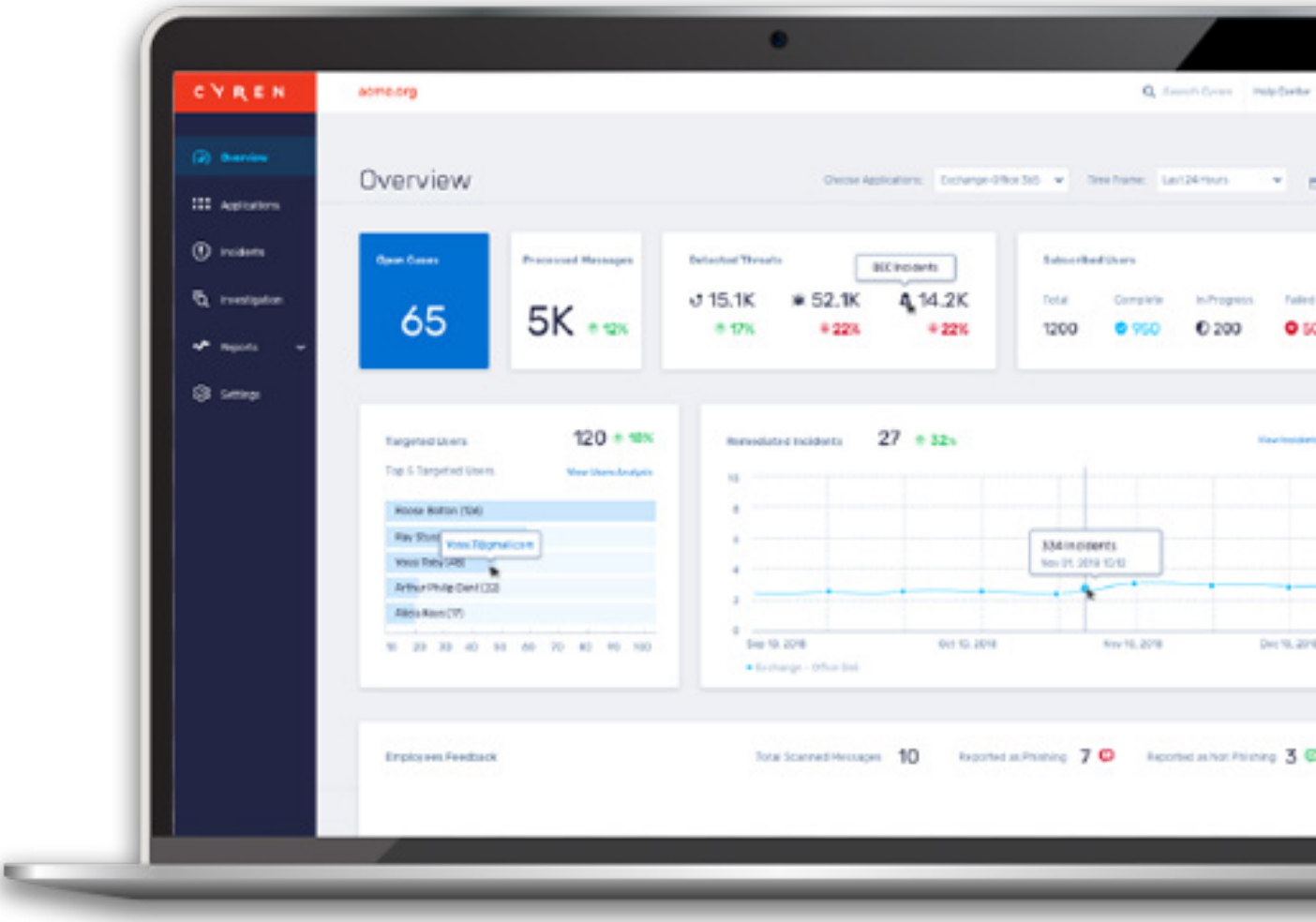
CYREN

SICHERHEITSLEITFADEN

Wie man Evasive Phishing-Angriffe auf Microsoft 365 Konten stoppt



Inhalt

Kurzversion

Cybersecurity-Profis wissen, dass ein einzelner Schutzmechanismus nicht alle Cyberbedrohungen abfangen kann. Gartner empfiehlt eine mehrstufige, adaptive Sicherheitsarchitektur, die einen kontinuierlichen Abwehrzyklus nach dem Prinzip „Verhindern-Erfassen-Reagieren-Prognostizieren" ermöglicht. Diese Architektur wird zwar bei Cybersicherheitsanbietern großflächig eingesetzt, glänzt jedoch im Rahmen der Mailsicherheit vieler Firmen sichtlich durch Abwesenheit – insbesondere bei Nutzern von Microsoft 365. Die meisten Organisationen setzen nach wie vor in erster Linie auf Prävention, die in Form eines sicheren E-Mail-Gateways (SEG) an den Netzwerkgrenzen erfolgt.

Das sichere E-Mail-Gateway hat einen Zweck: das Eindringen von Cyberangriffen in E-Mail-Form in das Unternehmensnetzwerk zu verhindern. Aber je ausgefeilter und häufiger diese Bedrohungen werden, desto öfter versagt das SEG. Obwohl die Anbieter ihre SEGs mit immer höherer Leistung und immer besseren Filtern ausstatten, gelangen noch immer zu viele Phishing-Attacken, Business Compromised Emails (BEC) und betrügerische Angriffe am SEG vorbei in die E-Mail-Postfächer von Unternehmen, was das Geschäftsrisiko erheblich steigert.

Phishing-E-Mails sind ein großes Problem, das Organisationen jeder Größenordnung betrifft. 78 % aller Microsoft-365-Administratoren geben Phishing als führende Ursache von Sicherheitsverletzungen an. Experten erwarten, dass Phishing-Angriffe immer häufiger werden, schließlich schlafen Phisher nie. Die Investition ist gering, zahlt sich aber umso mehr aus. Und es braucht nur ein Opfer, um in die Organisation einzudringen.

Der Anstieg der erfolgreichen Cyberangriffe in E-Mail-Form fußt auf drei wesentlichen Faktoren:

1. **Erstens** bietet Microsoft 365 eine neue, attraktive Angriffsmöglichkeit in Form gehosteter E-Mail-Plattformen in der Cloud. Die Nutzung von Microsoft 365 wird immer allgegenwärtiger, was es zur attraktiven Zielscheibe für Cyberkriminelle macht.

2. **Zweitens** werden Phishing-Attacken, BEC und betrügerische Angriffe immer ausgefeilter und entwickeln sich ständig weiter. Mittels Umgehungstechniken verhindern sie die Erkennung durch Cybersicherheitssysteme und mit Social Engineering sollen Menschen dazu gedrängt werden, auf einen Link zu klicken oder Anweisungen zu befolgen.

3. **Drittens** haben IT-Administratoren und Sicherheitsteams mit extremer Arbeitsbelastung zu kämpfen. Fähigkeiten im Bereich Cybersicherheit sind ein knappes Gut. Unterbesetzte IT-Teams werden täglich mit Warnmeldungen bombardiert und kommen mit der Arbeit kaum hinterher.

Organisationen müssen ihren Perimeteransatz für E-Mail-Sicherheit bei Microsoft 365 verstärken. Inbox Detection and Response, kurz IDR, schafft eine kritische Sicherheitsebene im Posteingang direkt im Cloud-Postfach und schließt dort die Lücke bei der Erkennung und Remediation, die das SEG zurücklässt. Das SEG bleibt als erste Sicherheitsebene bestehen und entfernt Spam und Malware aus dem E-Mail-Eingang. Die IDR-Ebene ist im Postfach aktiv, wo sie alle Phishing-E-Mails einfängt, die nicht im Netz hängengeblieben sind.

In diesem Whitepaper wird die Thematik der E-Mail-Sicherheit in Unternehmen detailliert untersucht, um darzulegen:

- Warum Microsoft-365-E-Mails in der Cloud besonders anfällig für Cyberbedrohungen bleiben
- Wie sich diese Schwachstellen mit Inbox Detection and Response (IDR) angehen lassen
- Bewährte Verfahren der IDR-Umsetzung

Das E-Mail-Programm von Microsoft 365 ist besonders anfällig für Cyberbedrohungen

Das Gartner-Modell der adaptiven Sicherheitsarchitektur wurde bereits auf viele Einfallstore für Cyberangriffe angewendet, einschließlich E-Mail-Sicherheit. Auf internen E-Mail-Servern sind oftmals Anti-Malware- und Anti-Phishing-Programme installiert, die regelmäßig Scans durchführen und neuartige Bedrohungen im Postfach erkennen. Wenn Organisationen auf Cloud-gehostete Postfächer umsteigen, ist dies nicht mehr möglich. Daher existiert bei E-Mails heute eine kritische Sicherheitslücke.

Cloud-Lücken

Unternehmen, die eine Microsoft-365-E-Mail-Plattform in der Cloud nutzen, verzeichnen im Durchschnitt mehr erfolgreiche Phishing-Angriffe als während der Nutzung interner E-Mail-Plattformen. Nutzer geben außerdem an, dass die nativen Microsoft-365-Add-ons Exchange Online Protection (EOP) und Advanced Threat Protection (ATP) Bedrohungen häufig nicht erkennen oder isolieren. Infolgedessen landen allzu oft Phishing-E-Mails beim Nutzer im Postfach. Dort ist es dann das Problem des Nutzers.

Phishing lohnt sich

Erfolgreiches Phishing von Microsoft-365-Anmeldedaten eines Mitarbeiters ist lukrativ. Mit echten Zugangsdaten in der Hand kann ein Cyberkrimineller E-Mails von einem echten und erkannten Unternehmenskonto versenden und damit die Tür zu Daten und Anlagen des Unternehmens öffnen. Mit einem Angriff per BEC lassen sich Informationen abgreifen, mit denen ein weiteres Eindringen in die Organisation ermöglicht, aber auch weitaus direktere Schäden verursacht werden können. Verschärft wird das Geschäftsrisiko noch, wenn das kompromittierte Konto Admin-Rechte hat. Es ist viel schwieriger, sich vor einer Gefahr von innen zu schützen, als vor einer E-Mail eines externen Absenders, der sich als interner Absender ausgibt.

Keine Erfahrungen nötig

Heute braucht es keine besonderen Kenntnisse, um einen ausgefeilten Phishing-Angriff zu starten. Es ist einfach. Im Dark Web machen erfahrene und neue Cyberkriminelle lukrative Geschäfte mit kostengünstigen, hochwertigen und benutzerfreundlichen Phishing-Kampagnen, erhältlich als Service oder als Selbstbausatz, die alles Notwendige für eine Phishing-Kampagne enthalten. Um unerkannt zu bleiben und ihre Erfolgschancen zu erhöhen, nutzen ausgefeilte Phishing-Kampagnen eine ganze Reihe von Umgehungstechniken. Je mehr der Kriminelle im Dark Web für ein Phishing-Kit oder einen Phishing-Service bezahlt, desto mehr Umgehungstaktiken sind im Preis enthalten.

Durch den Wegfall der Zugangshindernisse sind die Menge und Häufigkeit von Phishing-Angriffen förmlich explodiert und herkömmliche SEGs sind nicht in der Lage, sie zu erkennen. Wie können sichere E-Mail-Gateways versagen? Üblicherweise entnimmt das SEG URLs aus E-Mail-Nachrichten und Anhängen. Handelsübliche SEGs gleichen die URL mit einer Liste bekannter Phishing-Seiten ab. Moderne SEGs arbeiten mit fortgeschrittenen Detektionsfähigkeiten wie „Time-of-Click“. Erwartungsgemäß haben diese verbesserten Erkennungstechniken den Nährboden für neue Umgehungstaktiken bereitet, was die Wirksamkeit des SEG mindert.

Ausweichangriffe verhindern Erkennung

Moderne sichere E-Mail-Gateways beinhalten auch Erkennungsfunktionen wie In-Line-Sandboxing und unterstützen Authentifizierungsprotokolle wie SPF, DKIM und DMARC[3]. Leider haben selbst die modernsten SEGs ein kritisches Manko, weshalb sie Kontoübernahme-Angriffe, Spear-Phishing, Cousin-Domain-Spoofing und unbekannte Bedrohungen nicht erkennen können. Ihr unüberwindbares Manko ist, dass sie die E-Mail nur einmal zu Gesicht bekommen und daher auch nur einen Versuch haben, um einen Angriff zu erkennen. Erkennt das SEG eine Bedrohung nicht, wird die E-Mail an das E-Mail-Postfach weitergeleitet und ist für das SEG nicht mehr zugänglich. Wird eine neue Bedrohung erst nach dem Anklicken oder nach der Zustellung entdeckt, ist es zu spät. Die E-Mail kann nicht aufgerufen werden und das SEG kann nicht mehr eingreifen.

Sehen wir uns einmal genauer an, wie Phishing- und Betrugs-E-Mails das SEG mittels Umgehungstaktiken durchdringen und den Nutzer dazu bewegen, den Köder zu schlucken.

Umgehungstaktiken

Umgehungstaktiken ermöglichen es böswilligen Akteuren, unerkannt zu bleiben, sodass ihre Angriffe eine größere Erfolgschance haben. Sie müssen das SEG, den Nutzer und weitere Cybersicherheitslösungen, die im Web Jagd auf sie machen, in die Irre führen.

Das SEG austricksen

Bösartige Inhalte erst nach Prüfung der E-Mail zu aktivieren oder auf die Zielseite hochzuladen, ist keine neue Taktik. Moderne SEGs begegnen dieser Taktik mit „Klickzeit-Erkennung“, die eine E-Mail automatisch erneut prüft, wenn der Nutzer den Link anklickt. Dies gibt dem SEG eine letzte Chance, eine bösartige URL zu erkennen. Jedoch enthalten Spear-Phishing- und BEC-Angriffe keine URLs oder Anhänge, sodass sie dem SEG harmlos erscheinen. Sobald die infizierte E-Mail das SEG umgangen hat, ist der Nutzer die letzte Verteidigungslinie.

Ein Beispiel:

Angenommen, ein Angriff vom Typ Business Email Compromise durchdringt das SEG und kann sich Zugang zu den Login- und Passwortdaten eines Nutzers verschaffen. Der Angreifer muss einfach nur den E-Mail-Verkehr seines Opfers über einen gewissen Zeitraum beobachten und dann damit beginnen, Nachrichten an strategisch platzierte Mitarbeiter zu verschicken, um Zugang zu sensiblen Daten zu erhalten und mittels Überweisungsbetrug Geldmittel zu stehlen. Das SEG erkennt solche Aktivitäten nicht.

Den Nutzer austricksen

Umgehungstaktiken tricksen auch die Nutzer aus. 50 % aller Nutzer klicken auf Links, weil sie mittels Social Engineering dazu gedrängt werden. Mit ähnlichen Domains werden URLs verschleiert und Websites mit identischem Design erstellt. Bei Punycode-Angriffen kommen Buchstaben aus anderen Sprachen zum Einsatz, die deutschen Buchstaben ähneln. Nach dem gleichen Prinzip erstellen die Angreifer lokale Versionen einer gefakten Website, sodass die Domain zwar echt aussieht, es aber nicht ist.

Ein Beispiel:

Angenommen, ein Mitarbeiter bekommt eine E-Mail von einer seiner Schattenanwendungen, in der steht, dass eine Anfälligkeit soeben behoben wurde, also klicken Sie bitte hier, um das Update zu installieren. Die gefälschte E-Mail/Seite sieht nicht nur echt aus und verhält sich echt, sie hat außerdem alle erwarteten Sicherheitsfunktionen. Selbst die aufmerksamsten, in Sicherheit geschulten Nutzer fallen auf diese Tricks herein.

Austricksen von Cybersicherheitsprogrammen

Böswillige Akteure müssen außerdem verhindern, dass sie von Cybersicherheitsanbietern entdeckt werden. Sie lernen die IP-Adressen dieser Unternehmen auswendig und blockieren den Verbindungsversuch. Oder sie ändern einige Pixel bei einem Fingerabdruckbild, damit die Manipulation nicht erkannt wird. Der HTML-Code der Zielseite wird oft verschleiert und verschlüsselt. Dies sind nur einige der Techniken, um unerkannt zu bleiben. Es gibt noch viele weitere.

Höchste Zeit für eine IDR-Ebene zur Sicherung von Unternehmens-E-Mails

Gartner rechnet damit, dass im Jahr 2021 70 % aller öffentlichen und privaten Unternehmen Cloud-E-Mail-Dienste nutzen werden. Weitere Erkenntnisse von Gartner:

1 von 5

Beschäftigte nutzen aktuell den Cloud-Dienst von Microsoft 365.

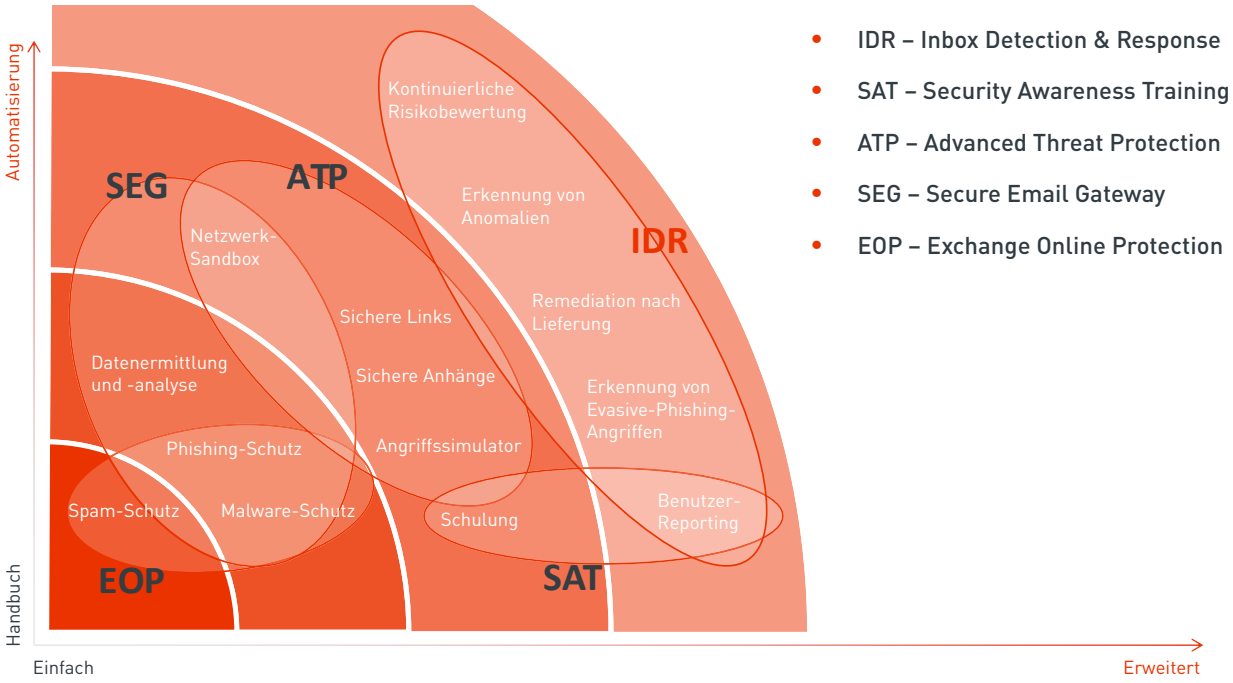
Microsoft 365

ist der am weitesten verbreitete Cloud-Dienst nach Nutzerzahl.

In der Cloud gehostete Unternehmensanwendungen haben einen Bedarf für eine innere E-Mail-Sicherheitsebene geschaffen. Das SEG bleibt zwar ein wichtiges Perimeterschutzsystem, bei ausgefeilteren Bedrohungen wird es hingegen durchlässig. Mit Inbox Detection and Response (IDR) können Unternehmen diese Sicherheitslücke bei E-Mails schließen, indem sie eine zusätzliche Schutzebene gegen intelligente und anpassungsfähige Bedrohungen schaffen, und zwar dort, wo sie am meisten gebraucht wird – im Posteingang.

Die IDR-Ebene der E-Mail-Sicherheit ist einfach in der Cloud umsetz- und skalierbar und konzentriert sich auf das Postfach des Nutzers, anstatt auf die Wege des Netzwerks zum und vom Microsoft-365-Server.

E-Mail-Sicherheit – Reifemodell



- IDR – Inbox Detection & Response
- SAT – Security Awareness Training
- ATP – Advanced Threat Protection
- SEG – Secure Email Gateway
- EOP – Exchange Online Protection

Microsoft 365 ist eine ausgereifte Anwendung, die eine ausgereifte Cybersicherheitslösung erfordert

IDR – modernes, automatisiertes und anpassungsfähiges Sicherheitswerkzeug für Firmenmails

Inbox Detection and Response (IDR) erkennt, dass das SEG eine wesentliche erste Stufe der präventiven Sicherheitskontrolle bleiben sollte. Sie hält die Internetleitung sauber, indem sie Spam, Malware und bekannte Bedrohungen aus eingehenden E-Mails entfernt.

Die IDR-Ebene ergänzt und verstärkt die Aufstellung der Cybersicherheit, indem sie die Lücken schließt, die das SEG und die nativen Microsoft-365-Add-ons EOP und ATP hinterlassen.

Konzipiert ist die IDR-Ebene so, dass sie jederzeit Zugriff auf alle E-Mails im Microsoft-365-Postfach hat. Daher kann sie eine laufende Überwachung und Erkennung gewährleisten, anstatt der einmaligen Erkennung des SEG und seiner Add-ons. Außerdem ermöglicht das permanente Rescanning von E-Mails eine ausgefeiltere Erkennungs- und Remediationskontrolle unter Zuhilfenahme von Machine Learning und Closed-Loop-Automatisierung. Auf der IDR-Ebene können Organisationen beispielsweise

- das Verhalten und die Interaktionen der Nutzer im Postfach überwachen, um Anomalien festzustellen.
- Daten aus verschiedenen Quellen erheben und korrelieren, um festzustellen, ob eine E-Mail bösartig ist und Aktionen erforderlich sind.
- die automatische Remediation im betroffenen sowie in allen anderen Postfächern ermöglichen
- Nutzer mit Erkennungstechnologien interagieren lassen und sie um Feedback bitten
- Nutzerfeedback automatisch einbauen
- Feedback-Schleifen nutzen, um Machine-Learning-Algorithmen (ML) zu verbessern und die Beschaffenheit der nächsten Bedrohung vorherzusagen.
- SEGs und andere Sicherheitseinrichtungen intelligenter machen und dadurch die Sicherheitsaufstellung der gesamten Organisation stärken.

IDR – Verringerung von Geschäftsrisiken

Der Anstieg von Evasive-Phishing-Angriffen stellt ein Risiko für Ihr Unternehmen dar. Erstens überwältigt er das SOC- und IT-Personal, das für die Analyse und Remediation dieser verdächtigen/böswilligen E-Mails zuständig ist. Sicherheitsteams haben weder die Zeit noch die Mittel, um sich um alle Bedrohungen zu kümmern. Zweitens, selbst wenn nur ein einziger Mitarbeiter eine infizierte E-Mail öffnet und auf Phishing oder Betrug hereinfällt, können Eigentum, Daten und Ruf Ihres Unternehmens dennoch erheblichen Schaden nehmen.

Sicherheitsschulungen legen zwar den Schwerpunkt auf Bewusstsein und Verhaltensanpassung, führen jedoch selten dazu, dass der Mitarbeiter Phishing erkennt. Durch die Schutzebene direkt im Postfach machen es IDR-Lösungen den Mitarbeitern leichter, aufmerksam auf die E-Mail-Sicherheit zu achten, ohne dass viel Zeit verloren geht oder die Produktivität beeinträchtigt wird.

Bewährte Praktiken bei der Umsetzung von IDR

Organisationen, die von den Vorteilen einer IDR-Lösung profitieren möchten, sollten auf vier Funktionen bestehen: nahtlose Einrichtung, Automatisierung, adaptiver Bedrohungsschutz und effektive Nutzereinbindung.

Einfache Einrichtung

Die Installation einer Schutzebene im Microsoft-365-Postfach muss sowohl für IT-Administratoren als auch für die Nutzer reibungslos verlaufen. IDR-Lösungen sollten am besten als Cloud-Dienst geliefert werden, der direkt an Cloud-Postfächer anschließt, indem er die nativen APIs von Microsoft 365 nutzt. Plug-and-Play-Lösungen verkürzen die Amortisierungszeit und reduzieren die Einführungskosten.

Die Bereitstellung sollte Minuten statt Tage dauern und ohne jegliche Veränderung der bestehenden E-Mail-Sicherheitsinfrastruktur der Organisation auskommen. Hierbei bleibt das SEG unberührt, sodass die versunkenen Kosten erhalten bleiben. Außerdem können Organisationen mit einer Lizenz für die nativen SEG-Fähigkeiten von Microsoft 365 damit ihre laufenden Investitionen schützen.

Automatisierte Reaktion und Abhilfe

Die kontinuierliche Überprüfung, Erkennung, Analyse und Remediation der IDR-Ebene sollten vollautomatisch erfolgen. Die IDR-Ebene sollte in der Lage sein, alle E-Mails bei Eingang im Postfach zu überprüfen und anschließend das Postfach immer wieder erneut zu überprüfen, wenn neue Bedrohungen erkannt werden, oder in regelmäßigen Abständen.

Die berührungslose Automatisierung ist der Schlüssel zur Beschleunigung von Reaktion und Remediation. Automatisierung erhöht die Produktivität der IT-Administratoren und Sicherheitsteams. Achten Sie auf automatisierte Remediationsaktionen wie:

- verdächtige E-Mails markieren und senden, damit Nutzer den Kreislauf schließen können
- erkannte Bedrohungen in separate Ordner verschieben und Warnmeldungen versenden
- erkannte Bedrohungen aus jedem Postfach in der gesamten Organisation entfernen – gemäß der Sicherheitsrichtlinie. Das allein erspart dem Sicherheitsteam Stunden der manuellen Remediation.

Adaptiver Bedrohungsschutz

Um mit evasiven Angriffen Schritt zu halten, müssen IDR-Lösungen einen echten adaptiven Bedrohungsschutz bieten. Setzen Sie auf Lösungen mit hochwertigen nativen Erkennungsfähigkeiten, ergänzt durch Machine-Learning-Algorithmen. Die IDR-Ebene muss sich ständig weiterentwickeln und anpassen, da auch die Angreifer flexibel sind und verschiedene Methoden ausprobieren. Idealerweise sollten IDR-Lösungen mehrere Analysen durchführen, darunter:

Analyse des Absenderverhaltens: erkennt betrügerische oder gefälschte E-Mails anhand der Analyse der Betreffzeile, der Erkennung ähnlicher Domains sowie der Verarbeitung natürlicher Sprachen, um zu bestimmen, ob die Sprache einer E-Mail auf Social Engineering hindeuten könnte.

Effektive Nutzereinbindung

Die besten IDR-Lösungen haben ein Rahmenkonzept für E-Mail-Erkennung, Analyse und Remediation, das es den Mitarbeitern ermöglicht, auf produktive Weise zu den Sicherheitszielen des Unternehmens beizutragen. Nutzer sollten klar und deutlich vor Bedrohungen gewarnt werden und in der Lage sein, verdächtige E-Mails in ihrem Postfach automatisch zu prüfen, zu melden und zu entfernen. Ebenso sollte das Feedback der Nutzer beim Schließen des Remediationskreislaufs ins System eingepflegt werden, damit es mit der Zeit effektiver wird.

Idealerweise sollten IDR-Lösungen mehrere Analysen durchführen, darunter:

URL-Verhaltensanalyse: schützt die Nutzer vor Identitätsdiebstahl, indem URLs aus E-Mails entnommen werden und die Zielseite auf Hinweise überprüft wird, die sie als Phishing-Seite enttarnen könnte. Die zugrundeliegenden Technologien sollten speziell so konzipiert werden, dass Phishing-Ausweichtaktiken erkannt werden. Zum Beispiel sollten sie über IP-Adressen aus mehreren Quellen automatisch auf verdächtige Seiten zugreifen und verschiedene Browser nachahmen können, um zu beobachten, wie die Seite in verschiedenen Umgebungen wiedergegeben wird.

Analyse des Postfachverhaltens: erstellt ein Aktivitätenprofil des Postfachs, um eine Ausgangsbasis vertrauenswürdiger Verhaltensweisen und Beziehungen zu schaffen. Wer schickt wem zu welcher Tageszeit E-Mails? In welchen Mengen? Wie sehen die Inhalte aus? Und viele andere. Postfächer werden dann kontinuierlich auf abnormales Verhalten überwacht. Mithilfe von prädiktiven Analysen werden Bedrohungen erfasst. Schickt eine Führungskraft bspw. nie E-Mails an eine Finanzcloud und tut dies dann an einem späten Freitagabend plötzlich doch einmal mit der Bitte um eine Geldüberweisung, wird dieses Verhalten als Abweichung eingestuft, die auf einen möglichen BEC-Angriff hindeutet.

Vorfallanalyse: ermöglicht bei Bedrohungen eine rasche Untersuchung, Eindämmung, Reaktion und Remediation. Vorfälle treten immer dann auf, wenn eine E-Mail gegen Sicherheitsrichtlinien verstößt oder vom Nutzer gemeldet wird. Setzen Sie auch hier auf Automatisierung. Dazu gehören auch eine klare Darstellung der detaillierten forensischen Daten zu jedem Vorfall und eine Zusammenführung ähnlicher Vorfälle zu einem einzigen Fall, sodass die Remediation in einem Rutsch erledigt werden kann. Die Automatisierung der Vorfallanalyse und der Workflows bedeutet, dass Sicherheitsteams mit weniger qualifiziertem Personal auskommen und schneller auf Bedrohungen reagieren können.

Zusammenfassung

Die übliche E-Mail-Sicherheitsarchitektur in den meisten Organisationen hat nicht mit den Herausforderungen Schritt gehalten, die Microsoft 365 und evasive Angriffe mit sich bringen. Phishing-E-Mails, BEC und Betrugsversuche bleiben nach wie vor unentdeckt und landen in den Postfächern der Nutzer. Egal, wie gut die Mitarbeiter geschult sind, sie fallen dennoch diesen betrügerischen Angriffen zum Opfer, was das Risiko einer Datenschutzverletzung erhöht.

Inbox Detection and Response bietet eine automatisierte und anpassungsfähige Cybersicherheitsebene, und zwar dort, wo sie am meisten gebraucht wird – direkt im Postfach von Microsoft 365. Unternehmen wird empfohlen, eine IDR-Lösung zu wählen, die nicht invasiv ist und für IT-Administratoren und Nutzer nahtlos bereitgestellt wird.

Lösungen nach dem Prinzip Inbox Detection and Response können die Lücken, die durch sichere E-Mail-Gateways hinterlassen werden, erfolgreich schließen. Das Geschäftsrisiko und die Überlastung der SOCs gehen dramatisch zurück, wenn eine schnelle Eindämmung von Phishing-Bedrohungen mittels kontinuierlicher Überwachung und Erkennung, automatisierter Reaktion und Remediation sowie effektiver Mitarbeitereinbindung erfolgt.

CYREN

Cyren ist ein Messaging-Security-Unternehmen, das Enterprise-E-Mail-Benutzer von heute vor schwer erkennbaren Bedrohungen schützt und Sicherheitssoftware-Integratoren, Hardware-OEMs und großen Dienstanbietern Bedrohungsintelligenz-Lösungen bereitstellt. Das GlobalViewTM Bedrohungsintelligenz-Netzwerk von Cyren analysiert Milliarden von E-Mail- und Internet-Transaktionen täglich. Unternehmen wie Microsoft, Google und Check Point, die APIs und SDKs von Cyren nutzen, um die Bedrohungsintelligenz für ihre Kunden zu operationalisieren, verlassen sich darauf.

HAUPTSITZ

Virginia, USA

1430 Spring Hill Road Suite 330

McLean, Virginia 22102

Tel.: 703-760-3320

Fax: 703-760-3321

VERTRIEB UND MARKETING

Austin, USA

10801-1 North Mopac Expressway Suite 250

Austin, Texas 78759

Bracknell, UK

Maxis 1, 43 Western Road

Bracknell Berkshire RG12 1RT

Silicon Valley, USA

1230 Midas Way Suite 110

Sunnyvale, CA 94085

Tel.: 650-864-2000

Fax: 650-864-2002

F&E-LABORE

Deutschland

Hardenbergplatz ,2 10623 Berlin,
Tel.: +49 (30) 52 00 56- 0

Fax: +49 (30) 52 00 56- 299

Island

Dalshraun 3 IS-220,
Hafnarfjordur

Tel.: +354-540-740

Israel

1 Sapir Rd. 5th Floor, Beit Ampa
P.O. Box 4014, Herzliya, 46140,
Tel.: +972-9-8636 888

Fax: +972-9-8948 214

Cyren.com

@CyrenInc

linkedin.com/company/cyren

©2020. Cyren Ltd. Alle Rechte vorbehalten. Eigentumsrechtlich geschützt und vertraulich. Dieses Dokument und seine Inhalte sind alleiniges Eigentum von Cyren und dürfen ohne die ausdrückliche schriftliche Zustimmung von Cyren weder übertragen noch vervielfältigt werden. Alle anderen Marken, Produkt- und Unternehmensnamen sowie Logos, die in diesem Dokument vorkommen, sind Eigentum ihrer jeweiligen Rechtsinhaber. [20200218]