
+
E-Book
Neue Erkenntnisse für den Bedrohungs- und Datenschutz
Was Anbieter veralteter Lösungen verbergen wollen
netskope

Inhaltsverzeichnis

Einleitung

Veraltete Praktiken im Bedrohungs- und Datenschutz können mehr schaden als nutzen. Außerdem ermöglichen es diese uralten Praktiken den Anbietern von Sicherheitslösungen auch, Probleme zu verbergen, die sie lieber im Dunkeln lassen wollen. Die Pandemie hat die Einführung von SaaS und der Cloud beschleunigt, sodass sich nun immer mehr Benutzer und Daten außerhalb des schwindenden Perimeters und außerhalb des Wirkungsbereichs herkömmlicher Sicherheitslösungen bewegen. Durch die Zusammenarbeit mit großen und multinationalen Unternehmen bei der Bereitstellung von Security Service Edge (SSE) haben wir zehn Erkenntnisse über Richtlinienkontrollen, Best Practices und die Aufdeckung blinder Flecken zusammengestellt. Wenn Sie eine SSE- oder SASE-Lösung (Secure Access Service Edge) in Erwägung ziehen, empfehlen wir Ihnen, auf der Grundlage dieser Erkenntnisse aus der Praxis Ihre RFI-Anforderungen (Request for Information; Informationsanfrage) zu aktualisieren.

Für wen sind diese Erkenntnisse relevant?

Sicherheits- und Netzwerkarchitekten, Geschäftsführer und Manager.

Wann sollten Sie diese Erkenntnisse studieren?

Bevor Sie ein SSE/SASE-Projekt starten und eine RFI herausgeben.

Warum sollten Sie diese Erkenntnisse studieren?

Um bedeutende Veränderungen in der Schutzlandschaft zu verstehen.

Erkenntnis 1

Umgehung der Inspektion des Microsoft 365-Datenverkehrs schafft blinde Flecken

Mit den erstklassigen SSE-Lösungen gehören Kompromisse hinsichtlich Leistung und Sicherheit, die mit der Inspektion des Datenverkehrs von Microsoft 365 (M365) einhergehen, der Vergangenheit an. Abgesehen davon, ist dieser blinde Fleck im Rahmen des Bedrohungs- und Datenschutzes zu groß geworden, um ihn zu ignorieren. Stellen Sie jede Inline-Sicherheitslösung infrage, die den M365-Datenverkehr in Ihrer Umgebung umgeht.

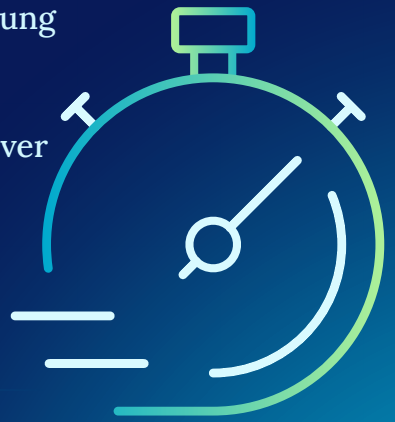
Kernpunkte

- **Mehr als ein Drittel der Bedrohungen aus der Cloud gehen von OneDrive und SharePoint aus.** Diesen Trend gibt es schon seit einigen Jahren, wie im Netskope Threat Labs 2024 Report beschrieben, In diesem Bericht stehen diese beiden Anwendungen an erster bzw. dritter Stelle in Sachen Beliebtheit.
- **Mehr als die Hälfte des verschlüsselten Webdatenverkehrs ist Cloud-bezogen, und M365 kann den größten Anteil davon ausmachen.** Wir haben einen Punkt überschritten, an dem der SaaS- und Cloud-Dienst-Datenverkehr größer ist als der herkömmliche Webdatenverkehr. M365-Anwendungen können 35–40 % des Cloud-bezogenen SaaS-Datenverkehrs ausmachen, da IT-Benutzer ihren Arbeitstag mit der Erstellung und Verwaltung von Inhalten in diesen Anwendungen verbringen.
- **Die Inspektion des M365-Datenverkehrs mit älteren Sicherheitslösungen beeinträchtigt die Benutzerfreundlichkeit.** Das Backhauling des Datenverkehrs von remote und hybrid arbeitenden Benutzern zu Sicherheits-Appliances im Rechenzentrum kann die Benutzerfreundlichkeit einschränken. Der direkte Zugriff von Benutzern unter Umgehung dieser Sicherheitsgateways wiederum resultiert in blinden Flecken beim Bedrohungs- und Datenschutz. SSE-Lösungen ersetzen diese Sicherheits-Appliances und älteren VPNs und ermöglichen so eine sicherere, granulare und schnellere Benutzererfahrung.
- **Microsoft-Partnerzertifizierungen erfordern eine Umgehung der Inspektion mit der Voreinstellung „keine Inspektion“.** Rückblickend betrachtet, hatte die Zertifizierung ihre Berechtigung, wenn man bedenkt, dass ältere Sicherheitslösungen die Benutzerfreundlichkeit beeinträchtigen. Heutzutage bieten SSE-Lösungen jedoch eine Reihe von globalen On-Ramps mit einer leistungsstarken Benutzererfahrung, ganz ohne Kompromisse in Sachen Sicherheit und Leistung. Der M365-Datenverkehr sollte im Gegensatz zu früher standardmäßig überprüft werden, da er eine Hauptquelle für Bedrohungen aus der Cloud und für potenziellen Datendiebstahl darstellt.
- **Sehen Sie sich das Zertifikat der gesicherten Verbindung Ihres Webbrowsers an, um die Inspektion zu bestätigen.** Wenn Sie in einer M365-Anwendung arbeiten, klicken Sie auf das Symbol vor der URL, um die gesicherte Verbindung des Webbrowsers und ihr Zertifikat anzeigen zu lassen. Wenn Sie ein Microsoft-Zertifikat für TLS Tunnel sehen, dann umgehen Sie die Inspektion und haben einen blinden Fleck. Eine SSE-Lösung ermöglicht die Inspektion und verwendet ihr eigenes Zertifikat (oder ein von einer Kunden-CA signiertes Zertifikat) für den sicheren TLS Tunnel vom Benutzer zur SSE-Cloud-Plattform. Sie sollten also das Zertifikat für die gesicherte Verbindung der SSE-Lösung sehen, nicht das Microsoft-Zertifikat.

Erkenntnis 2

Die Frontlinie beim Bedrohungsschutz liegt im Vergleich zur Herde jetzt bei T+0 in Echtzeit

Bedrohungsschutz in Echtzeit bei T+0 Stunden – das ist die neue Frontlinie. Lassen Sie sich nicht von höheren Erkennungsraten täuschen, die Stunden oder Tage später durch in der Herde ausgetauschte Informationen über die Bedrohung erzielt werden. Hier müssen Sie darauf bestehen, dass Anbieter von Inline-Sicherheitslösungen bei der Bedrohungserkennung Wirksamkeitsraten von T+0 mit einem niedrigen Prozentsatz falscher positiver Ergebnisse anbieten.



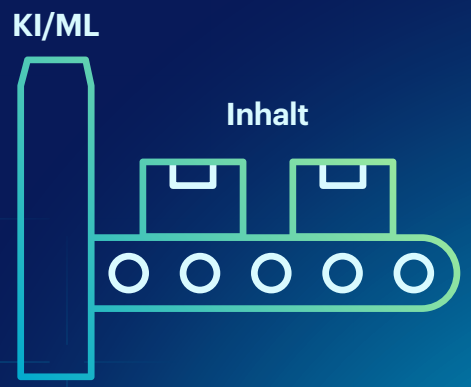
Kernpunkte

- **Angriffe haben schnellere Lebenszyklen, können gezielt erfolgen und verwenden vertrauenswürdige Anwendungen/Domains.** „Patient null“ ist die erste Person, die von einer neuen Bedrohung infiziert wird, und bei gezielten Angriffen ist es möglich, dass der Angriff auf diese eine Person beschränkt ist. Da die Angriffe vertrauenswürdige Anwendungen und Cloud-Dienste für das Hosting und die Bereitstellung nutzen, sind diese Domains oft zugelassen und werden, wie oben erwähnt, oft umgangen.
- **Validieren Sie die Wirksamkeit des Schutzes vor Bedrohungen in Echtzeit (T+0) statt in T+4 Stunden oder länger.** Wenn Sie Analyseberichte zur Wirksamkeit des Inline-Bedrohungsschutzes lesen, prüfen Sie die Echtzeitergebnisse bei T+0. Falls sie Ihnen nicht vorgelegt wurden, fordern Sie die Ergebnisse an. Viele Berichte melden die höchsten Wirksamkeitsraten Stunden oder Tage nach der Bedrohung, wenn gemeinsame Bedrohungsdaten aus der Herde jeden gut dastehen lassen.
- **Achten Sie in den Testberichten auf die Falsch-positiv-Rate (FP); je niedriger der Prozentsatz desto besser.** Ein bekannter Trick bei Tests in Sachen Bedrohungsschutz besteht darin, die Bedrohungserkennung durch falsche positive Ergebnisse zu verbessern. Auch wenn eine Lösung in mehrstündigen Wiederholungstests eine Wirksamkeit von 98 % und 99 % erzielt, sollten Sie prüfen, ob die FP-Rate 2,0 % oder mehr beträgt. Es ist unwahrscheinlich, dass Sie die gleichen hohen Erkennungsergebnisse erzielen, wenn Sie den Bedrohungsschutz herunterfahren, um die FP-Rate auf ein für Kunden akzeptables Niveau von unter 1,0 % zu senken.
- **Verlangen Sie einen aktuellen Testbericht über die Wirksamkeit von Inline-Abwehrsystemen.** Die Angriffe ändern sich und nicht jede Bedrohung ist eine ausführbare Datei: Dateilose Angriffe nehmen zu und gefälschte Formulare sowie Phishing-Angriffe zielen auf das Hacking von Zugangsdaten ab. Gehostete gefälschte Anmeldeformulare in vertrauenswürdigen Cloud-Diensten für Anwendungen, auf die Benutzer täglich bei der Arbeit zugreifen, erfordern einen Echtzeitschutz, um den „Patienten null“ und andere Personen mit Erstkontakt zu schützen. Die Testberichte sollten PE-Dateien (ausführbare Dateien), Nicht-PE-Angriffe (dateilos) und Phishing-Angriffe abdecken. Die meisten Endpunkttests decken nicht alle drei Bereiche ab, daher sollten Sie diese Lücken mit SSE-Lösungen schließen. Wenn kein Testbericht vorgelegt werden kann, ziehen Sie optional die besten Penetrationstest-Tools in Betracht.
- **Echtzeit (T+0) ist die neue Frontlinie; wenn Bedrohungsdaten nach mehreren Stunden in der Herde geteilt wurden, ist es einfach, mit einem guten Ergebnis dazustehen.** Es reicht nicht aus, nur einen kurzen Blick auf die Testberichte des Bedrohungsschutzlabors zu werfen oder diese schnell zu überfliegen: Sie müssen die Details für Echtzeitergebnisse bei T+0 verstehen und mit den Ergebnissen nach mehreren Stunden oder Tagen vergleichen. Vergewissern Sie sich auch, dass die FP-Rate bei dem Test akzeptabel ist und Ihren Erwartungen entspricht. Entscheidend sind der Schutz vor Bedrohungen in Echtzeit bei T+0 und die Geschwindigkeit, mit der Lösungen neue Angriffe innerhalb einer Stunde erkennen lernen können.

Erkenntnis 3

Transparenz von Inhalten ermöglicht Echtzeitschutz mit KI/ML-gestützten Abwehrsystemen

Generative KI ist inzwischen weit verbreitet und es wird erwartet, dass sie viele Bereiche unseres täglichen Lebens komplett verändern wird, auch bei der Arbeit und zu Hause. Damit KI und maschinelles Lernen (ML) in Echtzeit arbeiten können, sind Inhalte erforderlich, und hier unterscheiden sich die SSE-Lösungen beim Bedrohungs- und Datenschutz.



Kernpunkte

- **KI/ML-Echtzeit-Abwehrsysteme funktionieren nur, wenn sie den Inhalt sehen.** Die Annahme, dass Angriffe dateibasiert sind, lässt die gefälschten Anmeldeformulare und andere Taktiken außer Acht, die in Cloud-Diensten gehostet werden und bei Angriffen zum Einsatz kommen. Hier ist eine Phishing-Erkennung in Echtzeit mit KI/ML-Abwehrmechanismen möglich, da der Inhalt während der Geschäftstransaktion zum Schutz des Benutzers inline offengelegt werden kann. KI/ML-Abwehrmechanismen, die nur im Hintergrund eingesetzt werden, schützen nicht in Echtzeit.
- **Die Inline-Abwehr muss die Inhalte von SaaS-Anwendungen sichtbar machen.** Nicht jede Inline-SSE-Sicherheitslösung kann Inhalte für verwaltete und nicht verwaltete SaaS-Anwendungen und Cloud-Dienste aufdecken, also machen Sie eine Aufstellung der Inhalte, die untersucht werden können. Bedenken Sie auch, dass die meisten Bedrohungen von unternehmensfremden Tenants und privaten Instanzen beliebter SaaS-Anwendungen ausgehen, bei denen die Inline-Inspektion Ihre erste Verteidigungslinie ist, weil Endpunkte und E-Mail-Sicherheit nicht in der Lage sind, SaaS-Anwendungsinhalte in Echtzeit für die KI/ML-Analyse zu decodieren.
- **Sowohl der Daten- als auch der Bedrohungsschutz nutzen KI/ML-basierte Abwehrmechanismen inline.** PE-Dateien (Portable Executable) können inline mit ML-Klassifikatoren erkannt werden, wobei laut der Netskope-Bedrohungsforschung 6 von 10 bösartigen PE-Dateien zum Zeitpunkt der Erkennung keine bekannte Signatur haben. Auch Phishing-Angriffe können erkannt werden: Gefälschte Formulare werden für den Echtzeitschutz durch KI/ML analysiert, lange bevor Phishing-URLs in Bedrohungsdatenfeeds ausgetauscht werden. Hier finden Sie einige **Beispiele für Phishing-Angriffe**, die mithilfe von KI/ML-Abwehrsystemen in Echtzeit erkannt wurden.
- **Der am häufigsten verwendete Inhalt in ChatGPT ist Quellcode.** Als die bisher beliebteste Anwendung generativer KI, wird ChatGPT vor allem zur Optimierung von Quellcode verwendet. Die KI/ML-Datenklassifikatoren von Netskope können mehr als 20 Arten von Quellcode inline erkennen, und zwar ohne die bisherige Datenklassifizierung, Registrierung oder Datenkennungen der DLP. So können SSE-Lösungen mit GenAI-App-Anbindung sofort den Datenschutz für den Quellcode des Unternehmens gewährleisten und die Benutzer in Echtzeit bei der Nutzung der vom Unternehmen genehmigten GenAI-Anwendungen und -Tenants anleiten.
- **Die KI/ML-Abwehr muss inline erfolgen, nicht nur im Hintergrund.** KI/ML-Funktionen werden seit Jahren im Hintergrund zur Erkennung, Optimierung, Klassifizierung und sogar für Prozesse eingesetzt. Das explosionsartig angestiegene Interesse für GenAI-Apps hat zu einem übermäßigen Einsatz von KI in Marketingbotschaften und -inhalten geführt. Achten Sie darauf, was SSE-Lösungen mit KI/ML-Funktionen in Echtzeit bieten, wenn sie nicht nur im Hintergrund ausgeführt werden.

Erkenntnis 4

Phishing betrifft nicht mehr nur E-Mails, sondern die gesamte Kommunikation

Die weit verbreiteten Kommunikationskanäle zu den Benutzern begünstigen Phishing, Betrugsversuche und die Gefährdung von Unternehmen und haben herkömmliche E-Mails als Einfalltor für Angriffe längst abgelöst. Durch die Nutzung von SaaS- und Cloud-Hosting-Diensten können Phishing-Angriffe über diese beliebten Domains eingeschleust werden und so der Erkennung durch veraltete Sicherheitsmechanismen entgehen. Diese sind nämlich nicht in der Lage, SaaS-Inhalte zu decodieren und mit Echtzeit-Abwehrsystemen zu analysieren. Die Transparenz von Inhalten ist eine wichtige Voraussetzung für SSE-Lösungen, um in Zukunft Bedrohungen in Echtzeit abwehren zu können.

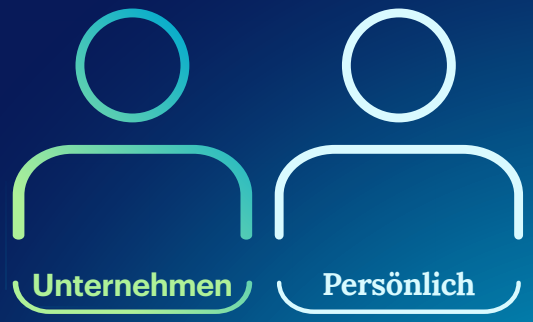
Kernpunkte

- **Ein Haupteinfallstor für Ransomware ist Phishing.** Jede Woche wird in den Nachrichten über die Folgen von Ransomware berichtet und in Forschungsberichten auf die wichtigsten Einfallstore für Phishing hingewiesen, darunter Softwarepakete und -patches, gehackte Anmeldedaten, Drive-by-Downloads, Malvertising und dateilose Angriffe. Entlang der gesamten Kill-Chain von Ransomware-Angriffen ermöglichen transparente Einblicke in Inhalte den Bedrohungs- und Datenschutz, einschließlich der Erkennung von Anomalien, dem Hacking von Anmeldedaten und Datenexfiltration.
- **Phishing nimmt soziale Netzwerke, IM, Chats und die private Kommunikation ins Visier.** Das Hauptziel von Phishing-Angriffen waren bisher zwar Finanzinstitute, aber aus den neuesten Trends geht hervor, dass die sozialen Medien fast gleichauf liegen und mit nur einem Prozentpunkt Abstand den zweiten Platz belegen, gefolgt von SaaS/Webmail auf dem dritten Platz.
- **Benutzer wünschen sich eine ausgeglichene Work-Life-Balance und Zugang zu privaten Anwendungen.** Hybrid- und Remote-Arbeit stellen neue Anforderungen an verwaltete Geräte für den Zugriff auf private Kommunikation. Auch ffür die phasenweise Arbeit im Büro wünschen sich Benutzer einen unkomplizierten Zugang. Versuchen Sie, den Zugriff auf risikoreiche Anwendungen einzuschränken; App-Aktivitäten zu kontrollieren, um Daten zu schützen, und die Remote Browser Isolation (RBI) von privaten SaaS-Anwendungen und Webmail in Betracht zu ziehen, um verwaltete Geräte zu schützen. Wenn Sie den Zugriff komplett sperren, frustrieren Sie nur Ihre Benutzer. Und da hochqualifizierte IT-Kräfte einen Wettbewerbsvorteil darstellen, sollten Sie sie nicht verschrecken.
- **SaaS-Anwendungen hosten gefälschte Anmeldeformulare in vertrauenswürdigen Domains und zeigen sie Benutzern.** Die Nutzung von SaaS nimmt von Jahr zu Jahr mit einer Wachstumsrate von mehr als 20 % zu, wobei mehr als 98 % der neuen SaaS-Anwendungen von den Geschäftseinheiten und Benutzern und nicht von der IT-Verwaltung eingeführt werden. Schauen Sie nicht nur auf verwaltete SaaS-Anwendungen, sondern auch auf nicht verwaltete Tenants und private Instanzen von Anwendungen, die für Phishing-Angriffe mit gefälschten Anmeldeformularen blinde Flecken darstellen können.
- **Angriffe werden nicht mehr ausschließlich über E-Mails gestartet, deshalb müssen Ihre SaaS-Anwendungen inline inspiziert werden.** Die heimliche Wunderwaffe zwischen den herkömmlichen SWG- (Secure Web Gateway) und CASB-Lösungen (Cloud Access Security Broker) ist die Inline-Überprüfung von SaaS-Anwendungen und Cloud-Diensten, die bei vielen Unternehmen und Organisationen in die Tausende gehen. Vermeiden Sie bei verwalteten SaaS-Anwendungen und veralteten SWG-Lösungen für das Web und die Cloud die Fallstricke im Zusammenhang mit CASB als DLP.

Erkenntnis 5

Konzentration auf private Anwendungsinstanzen im Kampf gegen Bedrohungen und Datenexfiltration

Die neue Hochrisikozone für Bedrohungen und Datendiebstahl ist bedingt durch die blinden Flecke von privaten SaaS-Instanzen (und nicht in Unternehmensinstanzen). Sie können Ihren Benutzern zwar verwaltete SaaS-Anwendungen für die Produktivität im Büro zur Verfügung stellen, aber sie können auch ihre eigenen privaten Instanzversionen haben. Dies ermöglicht nur allzu leicht die Exfiltration von Daten von Unternehmensinstanzen in private Instanzen von Anwendungen, und zwar unter der gleichen Domain, die von Ihnen zugelassen ist und die Sie daher möglicherweise nicht inline überprüfen.



Kernpunkte

- **In den letzten 30 Tagen von Mitarbeitern, die aus dem Unternehmen ausscheiden, steigt der Datendiebstahl um 300 %.** In den ersten zwei Jahren der Pandemie haben die Untersuchungen von Netskope über die Datenverschiebung und -ausbreitung etwas Interessantes zutage gefördert. Forscher haben bei der Betrachtung der Datenaktivitäten von scheidenden Mitarbeitern festgestellt, dass sie während ihrer letzten 30 Tage mehr als 300 % mehr Daten exfiltrieren als aktive Benutzer. Wochen vor ihrem Ausscheiden sammelten Benutzer im Homeoffice Daten und Informationen, die sie für ihre nächste Stelle als wertvoll erachteten.
- **In diesen 30 Tagen fließen 74 % der gestohlenen Daten in private Cloud-Speicher-Anwendungen.** Es ist keine Überraschung, dass die Benutzer die Daten in den letzten 30 Tagen ihrer Beschäftigung in einem privaten Cloud-Speicher – hauptsächlich Google Drive – gesammelt haben. Anwendungen und Cloud-Dienste, die kostenlose Dateispeicherung anbieten, werden aufgrund ihrer einfachen Nutzung und des einfachen Zugriffs gern für die Datenexfiltration und die Verbreitung von Bedrohungen genutzt.
- **Überwachen und kontrollieren Sie Datenverschiebungen zwischen unternehmenseigenen und privaten Instanzen.** Weit über 480 Anwendungen haben sowohl unternehmenseigene als auch private Instanzen, bei denen Datenverschiebungen und -aktivitäten überwacht, kontrolliert und auf Verhaltensanomalien untersucht werden sollten. Und bei Anwendungen ohne Instanzerkennung sollte Ihre SSE-Lösung in der Lage sein, jedem einzelnen Anwendungs-Tenant Benutzeridentitäten für Anmeldungen für Richtlinienkontrollen zuzuordnen.
- **Die überwältigende Mehrheit der Bedrohungen aus der Cloud geht von privaten Instanzen aus.** Der erste Kernpunkt in diesem E-Book hat aufgezeigt, dass OneDrive und SharePoint für mehr als ein Drittel der über die Cloud verbreiteten Malware verantwortlich sind. Bei diesem Kernpunkt wird differenziert, ob die Bedrohungen hauptsächlich von privaten und nicht autorisierten Instanzen ausgehen, und nicht von den von Ihrem Unternehmen verwalteten Instanzen. Angreifer erstellen und verwenden mühelos kostenlose, nicht autorisierte öffentliche Anwendungen oder kompromittierte Konten, um Bedrohungen zu verbreiten und Daten zu exfiltrieren. Daher muss der SaaS-Datenverkehrs inline mit Echtzeit-Abwehrsystemen untersucht werden.
- **Vermeiden Sie Sperrungen und Tenant-Beschränkungen und ermöglichen Sie Instanzerkennung für SaaS-Anwendungen**. SSE-Lösungen ohne Instanzerkennung für Hunderte von Anwendungen leiten Sie an, nicht verwaltete Tenants zu sperren und somit nur den Inline-Zugriff auf verwaltete SaaS-Instanzen zu erlauben. Das frustriert Unternehmen und Benutzer, da mehr als 98 % der genutzten Anwendungen nicht von der IT verwaltet werden und Sie so eine praktikable Ausfallsicherung entfernen, falls Ihre verwalteten Anwendungen aus irgendeinem Grund offline gehen.

Erkenntnis 6

Benutzer brauchen Echtzeit-Coaching und -Anleitung, keine Transparenz

Sicherheitsschulungsprogramme dienen vielleicht einmal im Jahr der Erfüllung von Compliance-Vorschriften, aber das Wissen gerät schnell in Vergessenheit, und Benutzer verfallen wieder in alte Praktiken. Die bisherige Sicherheitspraxis der Transparenz spielt zwar nach wie vor eine wichtige Rolle bei der Bedrohungsabwehr, aber wir haben es nun mit einer wachsenden SaaS- und Cloud-Dienst-Umgebung zu tun, in der Benutzer bei Geschäftsvorgängen Anweisungen in Echtzeit benötigen, damit Daten geschützt bleiben. Stellen Sie sich vor, Sie müssten im Dunkeln und ohne GPS-Navigation in eine neue Stadt fahren und Ihr Ziel finden ...

Kernpunkte

- **Echtzeit-Coaching und -Anweisungen helfen Benutzern bei Geschäftsvorgängen.** Unterstützen Sie Benutzer bei Geschäftsvorgängen. Informieren Sie sie über riskante Anwendungen und empfehlen Sie sicherere Alternativen. Oder warnen Sie vor riskanten Aktivitäten innerhalb von Anwendungen, wenn Sie Daten außerhalb des Unternehmens austauschen. Echtzeit-Coaching, wie die GPS-Navigation beim Autofahren, ist jetzt verfügbar und sollte bei neuen SSE-Implementierungen schnell und effektiv genutzt werden, um Benutzer zu unterstützen.
- **Wenn Benutzer angeleitet werden, tun sie in mehr als 95 % der Fälle das Richtige und vermeiden Risiken.** Wenn Benutzer während eines Geschäftsvorgangs eine Echtzeit-Warnung über eine riskante Anwendung oder Aktivität erhalten, brechen sie nach unseren Erkenntnissen und dem Kundenfeedback in mehr als 95 % der Fälle den Vorgang ab und gehen das Risiko nicht ein.
- **Sammeln Sie bei den restlichen 5 % Begründungen, um zu erfahren, wie Ihre Zugriffsrichtlinienkontrollen aussehen müssen und wie Sie sie optimieren können**. Bei Benutzern, die mit Echtzeit-Coaching vor einer riskanten Aktivität gewarnt wurden und den Vorgang fortgesetzt haben, können Sie die Begründung dafür erfassen. So können Sie Ihre granularen Richtlinienkontrollen mit einem besseren Verständnis der weiteren Anwendungsfälle und -szenarien weiter verfeinern.
- **Die Blockierung von Aktivitäten frustriert Benutzer, erhöht die Anzahl der Helpdesk-Tickets und verringert die Agilität des Unternehmens**. Grobe Richtlinienkontrollen, die Geschäftsvorgänge blockieren, sollten durch Echtzeit-Coaching und das Sammeln von Begründungen ersetzt werden. Das schafft ein Win-Win-Win-Szenario: Die meisten Benutzer brechen hierbei den riskanten Vorgang ab; von den wenigen, die den Vorgang trotzdem durchführen müssen, werden Sie über die genauen Gründe für diese Notwendigkeit informiert. Zusätzlich steigern Sie die Agilität Ihres Unternehmens.
- **Blockieren Sie Aktivitäten nicht pauschal, wenn Echtzeit-Coaching eine Option ist, und klären Sie über riskante Vorgänge auf.** Rückmeldungen von CIOs und CISOs unserer Kunden zeigen, dass der Einsatz von Echtzeit-Coaching auch zu weniger Helpdesk-Tickets im Zusammenhang mit Blockierrichtlinien führt. Benutzerfreundlichkeit, schneller Zugriff und Transparenz sind nach wie vor wichtig, aber wie bei der GPS-Navigation schätzen es die Benutzer, wenn sie angeleitet werden und dadurch Daten und das Unternehmen schützen können.

Erkenntnis 7

Datenschutz versus formale DLP – den Unterschied müssen Sie kennen

Wenn Sie in der Netzwerk- oder Sicherheitsbranche arbeiten und die Verhinderung von Datenverlust (DLP) in einem Meeting zur Sprache kommt, denken Sie wahrscheinlich, dass Sie jetzt den Raum verlassen oder Ihre E-Mails abrufen sollten. Die Reduzierung der Angriffsfläche durch Datenschutzmaßnahmen vor der formalen DLP ist für Netzwerk- und Sicherheitsteams von großem Nutzen. Beim Datenschutz funktionieren Richtlinienkontrollen und Zugriff wie ein Trichter, sodass die effizientesten und gezieltesten Richtlinien greifen, sobald die DLP aktiv wird.

Kernpunkte

- **Eine formale DLP erfordert oft eine Datenklassifizierung und -registrierung, die viel Zeit kostet.** Für strukturierte Daten, wie für alle Datenaktivitätskanäle im Web und in SaaS-, Cloud- und E-Mail-Anwendungen sowie in Endpunkten, ist die formale DLP eine gute Lösung. Ja, es kostet Zeit, die Quellen sensibler Daten zu entdecken, Daten zu klassifizieren und die Daten für einen exakten Datenabgleich oder Fingerprinting zu registrieren, wenn Leistung und Skalierung für Millionen oder sogar Milliarden von Datensätzen entscheidend sind.
- **Zum Datenschutz werden die Datenverschiebungen nach Anwendung und Instanz überwacht und kontrolliert.** Vor der formalen DLP sollten Sie Datenschutzrichtlinien implementieren, die den Zugriff auf riskante Anwendungen, Anwendungsaktivitäten und Datenverschiebungen nach Anwendung und Instanz kontrollieren. Errichten Sie mit der SSE-Netzwerksicherheit Leitplanken rund um die Datenverschiebungen seitens der Benutzer, um die Angriffsfläche und die Risiken für Datenoffenlegungen zu verringern.
- **Empfehlen Sie sicherere Alternativen für riskante Anwendungen und Aktivitäten und bieten Sie Echtzeit-Coaching**. Ein Teil der Datenschutzmaßnahmen vor der DLP ist der Einsatz von Echtzeit-Coaching bei Geschäftsvorgängen. Ähnlich einem GPS-Navigationssystem, das den Fahrer anleitet und auf einen Verkehrsunfall auf der Strecke aufmerksam macht, können Sie sicherere Alternativen anbieten, um Benutzer, Daten und Ihr Unternehmen zu schützen.
- **Sammeln Sie Begründungen für die Weiterentwicklung und Verbesserung der Richtlinienkontrollen für Datenverschiebungen.** Lernen Sie anhand der Begründungen von Benutzern neue Anwendungsfälle und -szenarien kennen, um die Richtlinienkontrollen für den Datenschutz zu optimieren, die eventuell formale DLP-Richtlinien und -Regeln erfordern könnten. Eine SSE-Lösung bietet Transparenz und Kontrolle für Inhalte und geht damit weit über die Möglichkeiten herkömmlicher Sicherheitslösungen hinaus. Nehmen Sie sich die Zeit, diese neuen Funktionen kennenzulernen.
- **Reduzieren Sie die Angriffsfläche mit einem Trichteransatz für Datenschutzkontrollen.** Wenn Sie an Ihren RFI-Anforderungen und am Konzeptnachweis arbeiten, sollten Sie Ihre Richtlinienkontrollen entsprechend einer Trichterstruktur gestalten, die die Angriffsfläche immer weiter reduziert, lange bevor DLP-Richtlinien und -Regeln greifen. Eine ganze Reihe von Richtlinienkontrollen sollte sich auf Datenverschiebungen und Aktivitäten, Coaching, Begründungen und sicherere Alternativen konzentrieren.

Erkenntnis 8

Verwaltete vs. nicht verwaltete Anwendungen – diese Problematik definiert Inline-Abwehrsysteme neu

Es gibt kaum mehr reine Sicherheitsabteilungen. IT-Beauftragte schauen über den Tellerrand hinaus und sehen ihre Rolle nicht mehr nur im Verwalten der von ihnen selbst eingeführten Anwendungen. Die digitale Transformation schreitet voran und veranlasst Geschäftseinheiten und Benutzer, SaaS-Anwendungen und Cloud-Dienste zu nutzen, ohne die IT-Abteilung hinzuzuziehen. Während eine IT-Abteilung etwa 40–60 SaaS-Anwendungen und Cloud-Dienste verwaltet, sind in einem Unternehmen oder einer Organisation wahrscheinlich Tausende von Anwendungen im Einsatz. Sollte dies unbekannt sein, wird als erster Schritt eine Cloud-Risikobewertung empfohlen.

Verwaltet Nicht verwaltet

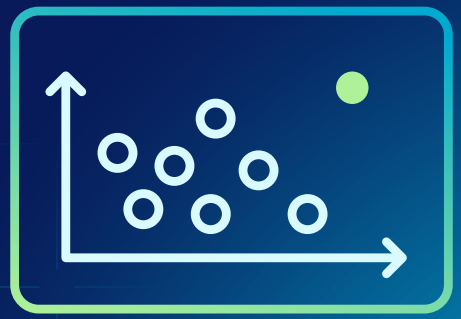
Kernpunkte

- **Mehr als 97 % der genutzten Anwendungen wurden von der IT weder eingeführt noch verwaltet.** Das zeigt, wie schnell die Einführung von SaaS voranschreitet: mit einem jährlichen Wachstum von mehr als 20 %. Da Unternehmen eine Cloud-First-Strategie verfolgen, suchen sie nach SaaS-Anwendungen, welche die in ihren Rechenzentren verwendeten Anwendungen ersetzen. Sogar einige Länder verfolgen eine Cloud-First-Strategie, wie z. B. Australien.
- **Eingeführt werden nicht verwaltete Anwendungen hauptsächlich von Geschäftseinheiten und Benutzern.** Diese haben Ziele und Zeitpläne und arbeiten auf die digitale Transformation hin. Für einige Unternehmen ist das eine Frage des Überlebens. Geschäftseinheiten und Benutzer sind Hauptnutzer von nicht verwalteten SaaS-Anwendungen und Cloud-Diensten, die sich der Kontrolle der IT entziehen. Eine SSE-Lösung kann nicht verwaltete Tenants und private Instanzen mit Inline-Richtlinienkontrollen und Coaching sicher zulassen.
- **Die API-Überprüfung wird nur bei verwalteten Anwendungen und Cloud-Diensten angewendet.** Die Devise lautet „am besten beides“, da die API-Überprüfung auf verwaltete Anwendungen und Cloud-Dienste beschränkt ist und die bereits erwähnte heimliche Wunderwaffe Inline-Inspektion verwaltete, nicht verwaltete und private Anwendungsinstanzen abdeckt. Sie wollen das Teilen von Dateien kontrollieren? Dann heißt die Antwort API-Überprüfung! Sie wollen riskante Apps einschränken und Benutzer anleiten? Dann setzen Sie auf die Inline-Überprüfung mit Richtlinienkontrollen in Echtzeit.
- **Ihr Cloud-Speicher ist wahrscheinlich sauber, der Rest hostet aber bösartige Bedrohungen.** Das ist kein Problem, denn Ihr vom Unternehmen verwalteter Cloud-Speicher ist wahrscheinlich sauber und gut geschützt. Aus diesem Grund nutzen Angreifer kostenloses Cloud-Hosting mit nicht autorisierten Konten und kompromittierten privaten Instanzen, um in der Cloud gehostete Bedrohungen zu verbreiten und Phishing-Angriffe durchzuführen. Hier kommt wieder unsere heimliche Wunderwaffe ins Spiel, die alles abdeckt, was über verwaltete Tenants und Instanzen hinausgeht.
- **Überprüfen Sie nicht verwaltete Anwendungen und private Instanzen inline.** Ihre RFI sollte auch eine Inline-Überprüfung von Tausenden von nicht verwalteten Anwendungen und Hunderten von Anwendungen ermöglichen und Instanzerkennung bieten. Die Fähigkeit, diese Inhalte inline zu prüfen, ist der Schlüssel für den Bedrohungs- und Datenschutz, die Erkennung von Verhaltensanomalien und die Nutzung von Analysen, um unbekannte Risiken und Datenverschiebungen aufzudecken.

Erkenntnis 9

Die Erkennung von Verhaltensanomalien ist nicht mehr optional

Jahrelang hatte die Analyse des Benutzerverhaltens (UEBA) zur Anomalieerkennung Probleme, die optimalen Ereignisse und Protokolle für die gewünschten Anwendungsfälle bereitzustellen, wie Insider, Kompromittierung von Anmeldedaten und Datenexfiltration. Zusätzliche SSE-Protokolle und -Ereignisse, die einen Einblick in Benutzer, Anwendungen und Datenaktivitäten bieten, haben es schließlich möglich gemacht, diese Anwendungsfälle mit hoher Effizienz zu unterstützen.



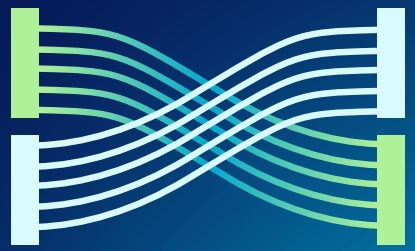
Kernpunkte

- **Benutzer, die remote oder hybrid arbeiten, gehen selbstbewusster mit Daten um.** Wenige Monate nach Beginn der Pandemie zeichnete sich deutlich ab, dass Remote-Benutzer beim Aufrufen von Websites und Inhalten sowie bei der gemeinsamen Nutzung von verwalteten Geräten mehr Risiken eingehen. Wenn Benutzer remote mit mehreren SaaS-Anwendungen und Cloud-Diensten arbeiten, darunter auch ihren eigenen privaten Instanzen, fanden sie auch Wege, außerhalb der bekannten Kanäle Daten zu teilen und gemeinsame Aktivitäten durchzuführen. Mit dem Fortschreiten der Pandemie steigerte sich auch die Produktivität der Benutzer – vielleicht lag das an den fehlenden Gesprächen in der Kaffeeküche und dem Ausbleiben der typischen Ablenkungen, wie sie in Großraumbüros üblich sind.
- **Kompromittierte Anmeldedaten stellen eine eigenständige sogenannte Underground Economy dar.** Die zunehmende Nutzung von SaaS mit direktem Zugriff von remote und hybriden Arbeitsplätzen aus, hat nicht nur Tür und Tor für Angriffe geöffnet, die auf die Kompromittierung von Anmeldedaten abzielen, sondern auch für eine Underground Economy, in der diese Daten verkauft werden. Um dagegen vorzugehen, sollte Ihre SSE-Lösung separate Egress-IP-Adressen für den verwalteten SaaS-Zugang bereitstellen, die nur für Ihr Unternehmen oder Ihre Organisation gelten. Dies verhindert die Verwendung kompromittierter Anmeldeinformationen und beugt Reputationsproblemen mit gemeinsam genutzten IP-Adresspools vor.
- **Verwenden Sie die Inline-Inspektion, um Baselines für Benutzer- und Peer-Gruppen-Aktivitäten zu erstellen.** SSE-Lösungen, die Tausende von SaaS-Anwendungen und Hunderte von Instanzen untersuchen, liefern hervorragende Ereignis- und Protokolldaten. Dies ermöglicht die Erstellung der gewünschten UEBA-Baselines für Benutzer- und Peer-Gruppen-Aktivitäten zur Erkennung von Anomalien, die über das hinausgehen, was sequenzielle Anomalie-Regeln und Abfragen mit Genauigkeit erkennen können. Außerdem werden durch Peer-Gruppen alle bereits vorhandenen anomalen Verhaltensweisen innerhalb der Baseline für einen einzelnen Benutzer aufgedeckt.
- **Nutzen Sie die auf maschinellem Lernen (ML) basierende UEBA, um Anomalien zu erkennen.** Angesichts der granularen Richtlinienkontrollen einer SSE-Lösung, ermöglichen die Warnmeldungen, Protokolle und Ereignisse mehrere maschinelle Lernmodelle (ML) und einzigartige Detektoren. Eine SSE-Lösung sollte über mehr als 50 ML-Modelle und 100 Detektoren für die Erkennung von Anomalien verfügen, um den gewünschten Reife- und Erfahrungsgrad zu erreichen.
- **Bewerten Sie Benutzer und überwachen Sie sie auf risikoreiche Verhaltensweisen und Datenexfiltration hin.** SSE-Lösungen öffnen die Tür für eine Bewertung mithilfe des Benutzervertrauensindex für adaptive Zugriffsrichtlinienkontrollen und zur Veranlassung von Untersuchungen von Ereigniskorrelationszeitlinien für risikoreiche Aktivitäten und Datenverschiebungen. Für weitere Details lesen Sie unseren Blogbeitrag über die Umsetzung von UEBA.

Erkenntnis 10

Überwachung von Aktivitäten, um unbekannte Anomalien in Analysen und Visualisierungen aufzudecken

Die Verwendung von erweiterten Analysen und Visualisierungen, um Anwendungstrends, Verhaltensweisen sowie bekannte oder unbekannte Anomalien nachzuvollziehen, ist vergleichbar mit dem Einsatz von KI/ML in Abwehrsystemen. Mit einer Cloud-Risikobewertung können Sie eine Baseline ermitteln, um dann mit der Implementierung von Richtlinienkontrollen zu beginnen, Änderungen im Verhalten und in den Aktivitäten zu überwachen und so die gewünschten Ergebnisse zu erzielen. Echtzeit-Coaching und das Sammeln von Begründungen können als grafische Visualisierungen sowie als Wortwolken dargestellt werden. Denken Sie über die alten SWG- und Webfilter-Berichte hinaus und nutzen Sie die neue SSE-Transparenz für Anwendungen, Benutzer und Datenaktivitäten.



Kernpunkte

- **Um Unbekanntes zu finden, sind transparente Einblicke in Benutzer, Anwendungen und Datenaktivitäten entscheidend.** Wie viele Cloud-Speicheranwendungen sind in Ihrem Unternehmen und Ihrer Organisation im Einsatz? Wie viele davon werden verwaltet, wie viele nicht und gibt es einen Datenaustausch mit Dritten, Partnern und Beratern? Das Gleiche gilt für GenAI-Apps sowie für eine breite Palette an Anwendungen, die in Marketing-, Vertriebs- und Personalabteilungen eingesetzt werden, wo mit sensiblen Daten gearbeitet wird.
- **Eliminieren Sie blinde Flecken in M365, Instanzen und nicht verwalteten Anwendungen.** SSE-Lösungen beseitigen den blinden Fleck, der durch die fehlende Inspektion des M365-Datenverkehrs entsteht, und deckt die versteckten privaten Instanzen oder nicht verwalteten Partner-Tenants auf, die häufig mit der Einschleusung von Bedrohungen und der Datenexfiltration in Verbindung stehen. Die Zeiten, in denen die am häufigsten genutzten Anwendungen und Cloud-Dienste nach Domain- und Webkategorie gefiltert wurden, sind vorbei. Die Details sind jetzt aus den Instanzen, Aktivitäten und Datenverschiebungen ersichtlich.
- **Nutzen Sie Dashboards und grafische Visualisierungen (z. B. Sankey-Diagramme).** Visualisierungen sind äußerst hilfreich, um Anomalien und verdächtige Bereiche zu erkennen, um weitere Details zu erhalten und näher zu untersuchen. SSE-Lösungen sollten diverse Dashboards und Visualisierungen bieten, die über herkömmliche Berichtfunktionen hinausgehen. Außerdem sollten sie Ereignisse und Protokolle für 3, 6 oder 13 Monate speichern können und so eine Analyse über das Jahr hinweg ermöglichen. Das Streaming von Protokollen in nahezu Echtzeit von SSE-Plattformen aus wird ebenfalls bevorzugt. Hierbei kann es jedoch vorkommen, dass am Zielort keine erweiterten Analysefunktionen und Dashboards zur Verfügung stehen.
- **Überwachen Sie Datenexfiltrationsströme bei Benutzern, Anwendungen und Instanzen.** Daten sind die Zero-Trust-Komponente, die Benutzer, Geräte, Anwendungen und Netzwerke miteinander verbindet. Daten fließen zwischen diesen Komponenten und sind das Herzstück dessen, was es zu schützen gilt. SSE-Lösungen mit granularer Transparenz und Kontrolle ermöglichen den Zugriff mit den geringsten Rechten und eine kontinuierliche Überwachung zur weiteren Verfeinerung und Ausreifung der Richtlinienkontrollen, um die Zero-Trust-Prinzipien zu unterstützen. Die Bereitstellung eines Zero-Trust-Zugangs, der blinde Flecken hinsichtlich Benutzern, Anwendungen und Datenaktivitäten aufweist, unterwandert die Strategie und die Ziele von Zero Trust.
- **Entdecken Sie Unbekanntes mit Analysen des Kontexts und Visualisierungen.** Benutzer finden und nutzen täglich neue Wege für unbekannte und nicht genehmigte Datenverschiebungen. Die Analytik kann diese unbekannten Verschiebungen in grafischen Visualisierungen schnell und effizient aufdecken. Wenn die neue Datenaktivität keine Warnungen auslöst, könnte sie für Insider, mutwillig böse Benutzer oder einen ausscheidenden Mitarbeiter, der sensible Informationen für seine nächste Stelle sammelt, verborgen bleiben.

Zusammenfassung

Diese 10 Erkenntnisse bringen neue Funktionen und Anforderungen für eine SSE- oder SASE-RFI und zukünftige Projekte ans Licht. Anhand der Erkenntnisse, die wir unseren Kunden zu verdanken haben, empfiehlt sich als erster Schritt eine SSE-Transformation, die von den bestehenden Funktionen älterer Sicherheitslösungen ausgeht. Mit der Umstellung auf SSE entwickeln sich neue Fähigkeiten. Es kommen neue Abwehrmechanismen wie separate Egress-IP-Adressen hinzu, Benutzer werden durch Echtzeit-Coaching unterstützt, blinde Flecken und Konflikte werden beseitigt, Leitplanken und Datenschutzmaßnahmen werden vor der DLP hinzugefügt, Echtzeit-Abwehrsysteme (T+0), einschließlich KI-/ML-basierter Erkennung, genutzt und Verhaltensanomalien unter Verwendung von Analysen überwacht, um das Unbekannte grafisch offenzulegen.

- **Erfahren Sie mehr über Netskope Security Service Edge**
- **Kunden-Fallstudien**
- **Analysten-Bericht von Gartner – Kritische Funktionen für Security Service Edge**