01.02.2023

Leistungsbeschreibung
Advanced Threat Protection (ATP)

1. Hornetsecurity ATP schützt den E-Mail-Verkehr von Unternehmen vor gezielten und individuellen Angriffen, wie Spearphishing, Blended Attacks, Advanced Persistent Threats, Ransomware und CEO-Fraud.
2. Zur Erkennung von Angriffen werden als verdächtig eingestufte E-Mails des Auftraggebers durch folgende Filtertechniken untersucht:
    a. Sandboxing: Verdächtige E-Mail-Anhänge werden in mehreren separaten, geschützten Umgebungen geöffnet oder ausgeführt und ihr Verhalten auf mögliche Schadwirkung untersucht. Als verdächtig werden insbesondere Anhänge eingestuft, in denen ausführbarer Code gefunden wird.
    b. Secure Links: In E-Mails oder in E-Mail-Anhängen enthaltende URLs werden aktiviert und das resultierende Verhalten analysiert.
    c. Secure Links: URLs in E-Mails werden durch andere URLs ersetzt, die die entsprechenden Inhalte bei Aktivierung über Hornetsecurity Web Filter abrufen. Ggf. werden heruntergeladene Daten per Sandboxing auf ihr Verhalten untersucht. Durch den Web Filter als potentiell gefährliche erkannte Inhalte werden gesperrt. URLs ohne erkennbare Bedrohung nach einem Scan und URL Einträge auf einer Whitelist werden nicht ersetzt.
    d. Targeted Fraud Forensics: Heuristische Filter zur Erkennung gezielter Angriffe, mit Prüfung von Authentizität und Integrität von Metadaten und E-Mail-Inhalten, Erkennung und Blockierung gefälschter Absender-Identitäten, Erkennung gefälschter Inhalte, Erkennung von Angriffen auf besonders schützenswerte Daten, insbesondere Daten, die Zahlungsflüsse betreffen (z.B. Kreditkartendaten, Rechnungen, Zahlungsanweisungen), Erkennung gezielter Angriffe auf besonders exponierte Personen des Auftraggebers (z.B. Buchhaltung, CFO, CEO, Controlling).
    e. Freezing: Zeitweiliges “Einfrieren” verdächtiger E-Mails. Eingefrorene E-Mails werden nach einigen Minuten erneut mit aktualisierten Filtern verarbeitet.
    f. Malicious Document Decryption: Verschlüsselte E-Mail-Anhänge in Form von Office-Dateien, Archiven und PDF-Dateien werden vor dem Eintreffen beim Empfänger entschlüsselt, sofern das Passwort aus der E-Mail rekonstruiert werden kann, und die Inhalte nach einer möglicher Schadsoftware untersucht.
    g. Ex-Post-Alarmierung: Stellt sich im Nachhinein heraus, dass eine bereits zugestellte E-Mail doch als potentiell schädlich eingestuft werden muss, erhält das IT-Sicherheitsteam eines Unternehmens nach Bekanntwerden eine Alarmierung.

   h. QR Code Analyzer: In E-Mails enthaltende QR Codes sowie Bilder mit integrierten QR Codes werden bedarfsorientiert und automatisch im Hintergrund beim E-Mail-Verarbeitungsprozess auf potenziell gefährliche Links überprüft.

3. E-Mails können durch die zusätzliche aufwändige Filterung zeitlich verzögert zugestellt werden. Die Verzögerung beträgt im Einzelfall maximal 15 Minuten.
4. Als potenziell schädlich identifizierte E-Mails werden von Hornetsecurity in Quarantäne gestellt.
5. Auf quarantinierte E-Mails kann der Auftraggeber über das Hornetsecurity Control Panel zugreifen.
6. E-Mails mit geeigneten Anhängen in der Quarantäne können von Administratoren des Auftraggebers aus dem Control Panel heraus per Sandboxing geprüft werden. Detaillierte Ergebnisse der Prüfung werden über das Control Panel zur Verfügung gestellt.
7. Sicherheitsverantwortliche des Auftraggebers werden bei erkannten Bedrohungen unmittelbar per E-Mail über die Bedrohung informiert (Real-Time Alerts).
8. Für den ATP-Dienst wird eine Verfügbarkeit von 99,9% garantiert, ausgenommen sind angekündigte Wartungszeiten.
9. Fair Use Limits (Einschränkungen zur angemessenen Nutzung)
   a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Soft-ware erforderlich sind und die wir in diesem Zusammenhang zur Verfügung stellen, werden von allen unseren Kunden gemeinsam genutzt. Daher haben wir das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.
   b. Wir haben uns dazu entschlossen, keine Richtwerte vorab festzulegen, die eine exzessive oder unangemessene Nutzung bestimmen, da wir nach unserem Ermessen entscheiden können, unsere normalen Service-Levels aufrechtzuerhalten, indem wir anderen Nutzern reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zuweisen oder Ressourcen anderweitig skalieren. Sie verstehen, dass wir, wenn wir uns entscheiden, unsere Richtlinie zur angemessenen Nutzung nicht aktiv durchsetzen, nicht davon ausgehen, dass wir auf unser Recht, dies zu tun, verzichtet haben, noch haben wir zugestimmt, dass Sie unsere Dienste weiterhin auf demselben Niveau nutzen, wie Sie es zu einem bestimmten Zeitpunkt tun.
   c. Um unsere Dienste nutzen zu können, müssen Sie abrechenbare Einheiten erwerben. Die Anzahl der abrechenbaren Einheiten, die Sie benötigen, hängt von einer Reihe von Kriterien ab, wie z. B. der Größe Ihres Unternehmens, der Anzahl der Nutzer und der Speichergröße der jeweiligen Datenquellen. Sie können die Anzahl der abrechenbaren Einheiten, die Sie benötigen, anhand unserer Leitfäden, die

wir auf unserer Webseite für Gebühren und Abrechnungen hochgeladen haben, oder durch die Unterstützung unseres Vertriebsteams ermitteln.

d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienstleistungen zweckmäßig nutzen, und zwar in einer Weise, die es nicht erforderlich macht, dass wir unverhältnismäßig viele Ressourcen zuweisen müssen. Um dies festzustellen, werden wir Ihre Nutzung unserer Ressourcen und Ihren Speicherbedarf mit dem eines durchschnittlichen Kunden vergleichen. Den Durchschnittskunden ermitteln wir, indem wir die 5% höchsten und die 5% niedrigsten Kunden der jeweiligen Ressource unberücksichtigt lassen und den Mittelwert über alle unsere aktiven Kunden bilden.

e. Spezifische Merkmale, die sich auf die Branche beziehen, in der Sie tätig sind, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.

f. Wenn wir nach vernünftigem Ermessen und in gutem Glauben davon ausgehen, dass die Nutzung unserer Lösung durch Sie nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen.
    i. Ihnen erlauben, unsere Lösungen weiterhin zu nutzen, jedoch vorbehaltlich unter der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.
    ii. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieses Zeitraums werden die Backups ausgesetzt.

g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
    i. werden Ihre Sicherungsdaten am Ende des von uns in der diesbezüglichen Benachrichtigung festgelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.
    ii. erhalten Sie eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums.