ENTERPRISE THREAT PROTECTOR

Schutz vor gezielten Bedrohungen in der Cloud

Die Bedrohungslandschaft für Unternehmen entwickelt sich schnell weiter. Die Anzahl gezielter Bedrohungen, wie z. B. Malware, Ransomware, Datenextraktion und Phishing, nimmt ständig zu, und Cyberkriminelle werden immer besser darin, Sicherheitsansätze zu umgehen. Gleichzeitig bietet der zunehmende Einsatz von SaaS, Cloud und IoT in Unternehmen Angreifern neue Vektoren. Zusammen schaffen diese Aspekte völlig neue Herausforderungen in den Bereichen Transparenz, Kontrolle und Sicherheit. Dank der einzigartigen weltweiten Einblicke in den Internet- und DNS-Traffic (Domain Name System) von Akamai können Sicherheitsteams mithilfe von Enterprise Threat Protector gezielte Bedrohungen blockieren bzw. abwehren und darüber hinaus Nutzungsrichtlinien einrichten, die über das gesamte Unternehmen hinweg Gültigkeit finden.

ENTERPRISE THREAT PROTECTOR

Bei Enterprise Threat Protector (ETP), das auf der Akamai Intelligent Platform™ sowie unserem Carrier-Grade-DNS AnswerX™ basiert, handelt es sich um eine Cloudlösung, die sich schnell und einfach konfigurieren und bereitstellen lässt – ohne dass hierfür Hard- oder Software installiert oder gewartet werden müsste.

Enterprise Threat Protector nutzt in Echtzeit die Akamai Cloud Security Intelligence und die bewährte globale rekursive DNS-Plattform von Akamai, um proaktiv gezielte Bedrohungen, wie z. B. Malware, Ransomware, DNS-Datenextraktion und Phishing, zu erkennen. Mit dem Akamai-Cloudportal können Sicherheitsteams die Sicherheit zentral managen und in Minutenschnelle einheitliche Nutzungsrichtlinien für alle Mitarbeiter festlegen.

FUNKTIONSWEISE

Das Domain Name System (DNS) bildet die Grundlage für sämtliche Services im Internet. Allerdings nutzen auch viele schädliche Domänen, einschließlich Sites, auf denen Malware und Ransomware gehostet wird, und ihre zugehörigen CnC-Server (Command and Control), rekursives DNS für Angriffe.

Wenn der ausgehende DNS-Traffic eines Unternehmens an Enterprise Threat Protector umgeleitet wird, werden die angeforderten Domänen mithilfe der Echtzeit-Risikobewertung überprüft, sodass Unternehmen Mitarbeiter am Zugriff auf schädliche Domänen und Services hindern können. Diese Überprüfung geschieht, bevor die IP-Verbindung hergestellt wird. So werden Bedrohungen bereits in frühen Phasen der Kill Chain – und somit noch weit von Ihrem Netzwerk entfernt – aufgehalten. Darüber hinaus ist das DNS über alle Ports und Protokolle hinweg aktiv, sodass Sie auch vor Malware geschützt sind, die sich nicht auf standardmäßige Webports und -protokolle verlässt.

Domänen können auch auf ihren Inhalt hin überprüft werden, um Mitarbeiter am Zugriff auf gemäß der Nutzungsrichtlinien ungeeignete Inhalte zu hindern.

Enterprise Threat Protector lässt sich einfach in andere Sicherheitsprodukte und Reporting-Tools integrieren, einschließlich Secure Web Gateways, Next-Generation Firewalls, SIEM-Systeme sowie externe Bedrohungsfeeds. So können Unternehmen sämtliche Investitionen in die Sicherheit optimal nutzen.

VORTEILE

- **Deutlich erhöhte Sicherheit:** dank proaktiver Blockierung von DNS-Anfragen für Websites, auf denen Malware und Ransomware gehostet wird, CnC-Server (Command and Control) sowie DNS-Datenextraktions- und Phishing-Domänen – basierend auf unseren umfassenden und topaktuellen Bedrohungsinformationen.
- **Verbesserter Schutz ohne zusätzliche Komplexität oder Hardware** mit einer zu 100 Prozent cloudbasierten Lösung, die in Minutenschnelle und ohne Unterbrechungen für Nutzer konfiguriert und bereitgestellt werden kann und sich blitzschnell skalieren lässt.
- **Einfache Reduzierung des Verwaltungsaufwands** durch die Möglichkeit, Sicherheitsrichtlinien und -updates von überall aus und in Sekundenschnelle zu managen und so alle Standorte gleichzeitig zu schützen.
- **Schnelle und einheitliche Gewährleistung der Compliance** dank Nutzungsrichtlinien, die den Zugriff auf ungeeignete oder unzulässige Domänen und Inhaltskategorien blockieren.
- **Sofortige Steigerung der DNS-Ausfallsicherheit und -Zuverlässigkeit** dank der globalen Carrier-Grade Intelligent Platform von Akamai.

ENTERPRISE THREAT PROTECTOR

AKAMAI CLOUD SECURITY INTELLIGENCE (CSI)

Enterprise Threat Protector wird durch Akamai Cloud Security Intelligence unterstützt. Dieser Service stellt Echtzeitdaten zu schädlichen Domänen sowie zu den Risiken bereit, die diese Domänen für Unternehmen darstellen.

Diese Informationen basieren auf den Daten, die die Akamai Intelligent Platform – die 30 Prozent des globalen Traffics bereitstellt und bis zu 150 Milliarden DNS-Abfragen am Tag beantwortet – täglich erfasst. Die gewonnenen Daten werden durch externe Bedrohungsfeeds weiter optimiert. Die kombinierten Datensätze werden dann für fortschrittliche Verhaltensanalysen genutzt, deren Ergebnisse im Anschluss von einem speziellen Forschungsteam weiter verbessert werden. Werden hierbei neue Bedrohungen gefunden, werden diese umgehend zum ETP-Service hinzugefügt, um Unternehmen und ihre Mitarbeiter in Echtzeit zu schützen.

AKAMAI INTELLIGENT PLATFORM

Enterprise Threat Protector basiert auf der Akamai Intelligent Platform, eine Carrier-Grade-Plattform, die sicher, zuverlässig und schnell agiert. Dank ihrer globalen Verteilung erreicht die Plattform eine Verfügbarkeit von 100 Prozent, die auch durch unsere Service Level Agreements garantiert wird, und bietet Unternehmen optimale Zuverlässigkeit für ihren rekursiven DNS-Service.

CLOUDBASIERTES MANAGEMENTPORTAL

Sämtliche Konfiguration und Verwaltung von Enterprise Threat Protector erfolgt über das cloudbasierte Luna-Portal von Akamai. So können Sie den Service von überall aus und zu jeder Zeit problemlos managen.

Auch Richtlinien lassen sich schnell und einfach verwalten. Änderungen können in Minutenschnelle global verteilt werden, um zu gewährleisten, dass alle Unternehmensstandorte und Mitarbeiter geschützt sind. Sie können E-Mail-Benachrichtigungen konfigurieren, um Sicherheitsteams über kritische Richtlinienereignisse zu informieren, damit sie umgehend reagieren und potenzielle Bedrohungen schnell erkennen und aufhalten können. Ein Echtzeit-Dashboard bietet eine Übersicht über DNS-Traffic, Bedrohungsereignisse und Richtlinienverletzungen. Ausführliche Informationen zu sämtlichen Aktivitäten können über detaillierte Ansichten oder individuelle Dashboard-Elemente angezeigt werden. Diese detaillierten Informationen stellen wertvolle Ressourcen für die Analyse und Behebung von Sicherheitsvorfällen dar.

Sämtliche Portalfunktionen sind per API verfügbar, und die DNS-Datenprotokolle können an ein SIEM-System exportiert werden. So lässt sich Enterprise Threat Protector einfach und effektiv in Ihre vorhandenen Sicherheitslösungen und Reporting-Tools integrieren.

WICHTIGE FUNKTIONEN

- **Bedrohungskategorisierung durch Akamai:** Topaktuelle Bedrohungsinformationen, die auf den unvergleichlichen Einblicken von Akamai in 15 bis 30 Prozent des Webtraffics sowie den ca. 150 Milliarden täglichen Anfragen an unsere rekursive DNS-Cloud basieren.
- **Bedrohungskategorisierung durch Kunden:** Sicherheitsteams können die verfügbaren Feeds mit Bedrohungsinformationen schnell integrieren und somit den Wert vorhandener Sicherheitsinvestitionen steigern.
- **Nutzungsrichtlinien:** Setzen Sie Nutzungsrichtlinien durch, und gewährleisten Sie Compliance durch Beschränkung der zulässigen bzw. unzulässigen Inhaltskategorien.
- **Analyse und Reporting:** Dashboards bieten Echtzeiteinblicke in sämtlichen ausgehenden DNS-Traffic sowie in Bedrohungen und Verstöße gegen die Nutzungsrichtlinien.
- **Protokollierung:** DNS-Protokolle werden sieben Tage lang gespeichert und können einfach in eine CSV-Datei exportiert oder zur weiteren Analyse in ein SIEM-System integriert werden.
- **DNSSEC:** Für sämtliche an Enterprise Threat Protector gesendeten DNS-Anfragen ist DNSSEC aktiviert.

DIE AKAMAI-UMGEBUNG

Akamai macht das Internet schnell, zuverlässig und sicher. Unsere umfassenden Lösungen bauen auf der global verteilten Akamai Intelligent Platform™ auf. Sie wird durch das vereinheitlichte, individuell anpassbare Luna Control Center verwaltet, das für Transparenz und Kontrolle sorgt, und von Professional-Services-Experten unterstützt, die Ihnen bei der Einrichtung helfen und zu Innovationen während Ihrer fortlaufenden Strategieentwicklung inspirieren.

Über Akamai

Als weltweit größte und renommierteste Plattform für die Cloudbereitstellung unterstützt Akamai seine Kunden dabei, ein optimales und sicheres digitales Erlebnis bereitzustellen – auf jedem Gerät, an jedem Ort und zu jeder Zeit. Die stark verteilte Plattform von Akamai weist mit über 200.000 Servern in 130 Ländern eine beispiellose Skalierbarkeit auf und bietet Kunden somit eine überragende Performance sowie einen umfassenden Bedrohungsschutz. Das Akamai-Portfolio für Website- und App-Performance, Cloudsicherheit sowie Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice und Rund-um-die-Uhr-Überwachung begleitet. Warum führende Finanzinstitute, E-Commerce-Unternehmen, Medien- und Unterhaltungsanbieter sowie Behörden auf Akamai vertrauen, erfahren Sie unter www.akamai.de, im Blog blogs.akamai.com/de oder auf Twitter unter @AkamaiDACH sowie @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.de/locations. Sie können uns zudem unter der Telefonnummer +49 89 94006 308 erreichen. Veröffentlicht: Juni 2017