ATP

Hochkomplexe und ausgeklügelte Attacken erkennen und verhindern - effektiv und in Echtzeit.

Schützen Sie Ihr Unternehmen mit Skyfillers Advanced Threat Protection vor gezielten und individuellen Angriffen ab der ersten Schad-Mail. Hochinnovative forensische Analyse-Engines sorgen dafür, dass die Attacken sofort unterbunden werden. Gleichzeitig liefert die Lösung detaillierte Informationen über die Angriffe auf das Unternehmen.

SCHUTZ VOR RANSOMWARE

Seit 2016 nehmen Angriffe durch Viren, die Netzwerke durch Verschlüsselung lokaler Dateien lahmlegen, stark zu. Locky, Tesla, WannaCry & Co. sind polymorphe Viren, die sich nur sehr schwer entdecken lassen. ATP nutzt hierfür unter anderem eine Sandbox Engine, um das Verhalten von Dateianhängen beim Öffnen zu analysieren. Zudem werden verdächtige E-Mails „eingefroren", um sie nach wenigen Minuten, wenn sich die Signaturen der Filter aktualisiert haben, erneut zu scannen.

BENACHRICHTIGUNG BEI ANGRIFFEN

Die ATP Real Time Alerts benachrichtigen in Echtzeit über akute Angriffe auf Unternehmen und ermöglichen eine schnelle Einleitung weiterer interner Maßnahmen und juristischer Vorgehensweisen. Hierfür liefert das Benachrichtigungssystem detaillierte Analyseergebnisse. Zudem kann Ihr Sicherheitsteam Ihre Mitarbeiter sensibilisieren, um weitere Angriffswege zum Beispiel per Telefon zu erkennen.

ABGESICHERT GEGEN TARGETED ATTACKS & DIGITALE SPIONAGE

Spearphishing, Whaling oder CEO Fraud – gezielte Angriffe auf hochrangige Mitarbeiter in Unternehmen sind mittlerweile ein globales Problem. Auf herkömmlichen Wege sind diese Attacken kaum zu entdecken. Deshalb untersucht ATP laufend die interne Kommunikation zwischen bestimmten Personen auf solche Angriffe, um z.B. Angriffe per Identity Spoofing zu unterbinden. Zudem erkennt das Spy-Out Forensiksystem bekannte und neue Muster zur Ausspähung von Informationen, damit Sie sofort reagieren können.

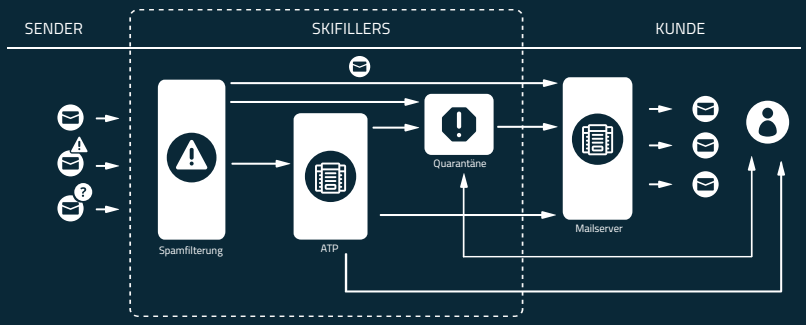
Unsere Cloud Vorteile auf einen Blick

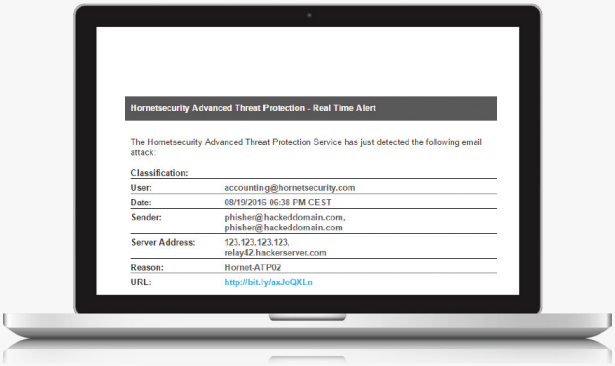
+ Erweiterung des Spam- & Virenfilters
+ Schnelle & einfache Einrichtung
+ Erfordert keine zusätzliche Hardware oder Software
+ Einfache Administration über web-basierte Verwaltungsoberfläche
+ Schadhafte E-Mails werden vor der Auslieferung an die eigene IT-Struktur abgefangen

EINBINDUNG VON ATP IN DIE E-MAIL STRUKTUR

Skyfillers ATP integriert sich nahtlos in den Spam- und Virenfilter. E-Mails, die diese erste Prüfung passiert haben, werden von Skyfillers ATP weitergehenden Analysen unterzogen. Dabei führt der Service unter anderem Attachments aus und betrachtet deren Verhalten detailliert.

Abb.: Ablauf des Spam- und Virenfilters mit Skyfillers ATP





BENACHRICHTIGUNGEN IN ECHTZEIT

Sobald Skyfillers ATP einen Angriff entdeckt, wird eine Benachrichtigung das IT-Sicherheitsteam des Unternehmens versendet, um es unmittelbar über eine mögliche Bedrohung zu informieren. Dabei erhält die zuständige Person verschiedene Details zu der Art und dem Ziel des Angriffes, dem Absender und dem Grund, weshalb die E-Mail abgefangen wurde.

Abb.: Real-Time-Notification

SKYFILLERS ATP ENGINES	FUNKTIONSWEISE UND VORTEILE
Sandbox Engine	Dateianhänge werden in einer Vielzahl verschiedener Systemumgebungen ausgeführt und ihr Verhalten analysiert. Stellt sich heraus, dass es sich um Malware handelt, werden Sie benachrichtigt. Schützt vor Ransomware und Blended Attacks.
URL Rewriting	Die URL Rewriting Engine sichert alle Internet-Aufrufe aus E-Mails heraus über die Hornetsecurity Webfilter ab. Dabei werden auch Downloads über die Sandbox Engine analysiert.
URL Scanning	An eine E-Mail angehängte Dokumente (z.B. PDF, Microsoft Office) können Links enthalten. Diese lassen sich jedoch nicht ersetzen, da dies die Integrität des Dokumentes verletzen würde. Die Hornetsecurity URL Scanning Engine belässt das Dokument in seiner Originalform und prüft ausschließlich das Ziel dieser Links.
Freezing	Nicht sofort eindeutig klassifizierbare, aber verdächtige E-Mails werden per Freezing über einen kurzen Zeitraum zurückgehalten. Anschließend erfolgt eine weitere Prüfung mit aktualisierten Signaturen. Schützt vor Ransomware, Blended Attacks und Phishing-Angriffen.
Ex-Post-Alarmierung (ab 2017)	Stellt sich im Nachhinein heraus, dass eine bereits zugestellte E-Mail doch als potentiell schädlich eingestuft werden muss, erhält das IT-Sicherheitsteam eines Unternehmen sofort nach Bekanntwerden eine Benachrichtigung über Ausmaß und mögliche Gegenmaßnahmen. Dadurch ist eine rasche Eindämmung einer Gefahrenlage möglich.
Targeted Fraud Forensics	Die Targeted Fraud Forensics erkennt gezielte personalisierte Angriffe ohne Malware oder Links. Dabei kommen folgende Erkennungsmechanismen zum Einsatz: + Intention Recognition System: Alarmierung bei Inhaltsmustern, die auf bösartige Absichten schließen lassen + Fraud Attempt Analysis: Prüft die Authentizität und Integrität von Metadaten und Mailinhalten + Identity Spoofing Recognition: Erkennung und Blockierung gefälschter Absender-Identitäten + Spy-Out Detection: Spionageabwehr von Attacken zur Erlangung schützenswerter Informationen + Feign Facts Identification: Inhaltsanalyse von Nachrichten auf Basis von Vorspiegelung fingierter Tatsachen + Targeted Attack Detection: Erkennung gezielter Angriffe auf einzelne Personen