NEXIO
OPERATIONAL IT-SERVICES

PRODUKTDATENBLATT · STAND 03.2017

Advanced Threat Protection

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

Schützen Sie Ihr Unternehmen mit ATP 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

Ransomware nimmt seit Anfang 2016 stark zu: Dabei handelt es sich um Viren, die den Rechner oder ein ganzes Netzwerk durch Verschlüsselung der lokal gespeicherten Dateien lahmlegen. Nur durch Zahlung eines Lösegeldes - daher der Name - haben Nutzer eine Chance, wieder auf ihre Daten zugreifen zu können. Locky, Tesla, Petya und 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 und die Mail bei positivem Fund herauszufiltern. Zudem werden verdächtige E-Mails "eingefrohren" ("Freezing"), um sie nach wenigen Minuten, wenn sich die Signaturen der Filter aktualisiert haben, erneut zu scannen.

Schutz vor Blended Attacks

Blended Attacks kombinieren verschiedene Angriffswege, um erfolgreich zu sein. Die E-Mail kann zum Beispiel ein Dokument enthalten, in dem sich wiederum ein Link zu einer Downloadseite mit Malware verstecken kann. ATP bekämpft diese Art von Angriffen mittels URL-Scans und URL-Rewriting, es kommen darüber hinaus aber auch Sandboxing und Freezing zum Einsatz.

Schutz vor Targeted Attacks

Oftmals sind hochrangige Mitarbeiter von Unternehmen Ziel individueller Angriffe, dem sogenannten Spearphishing, Whaling oder auch CEO Fraud. Dabei versuchen die Angreifer, an Passwörter oder Kreditkartendaten zu gelangen, oder die Mitarbeiter dazu zu bringen, Gelder auf ein bestimmtes Konto zu überweisen. Diese Attacken sind auf herkömmlichem Wege quasi nicht zu entdecken. Mit ATP wird die interne Kommunikation zwischen bestimmten Personen des Unternehmens gezielt auf solche Angriffe untersucht und so ein Missbrauch etwa per Identity Spoofing unterbunden.

Schutz vor digitaler Spionage

Über die Hälfte der deutschen Unternehmen war laut Umfrage des IT-Branchenverbands Bitkom bereits von Datendiebstahl, Sabotage oder Spionage betroffen. Das Spy-Out Forensiksystem erkennt sowohl bekannte als auch komplett neue Muster zum Ausspähen von Informationen. Das System reagiert sofort und alarmiert Sie, bevor schützenswerte Informationen das Unternehmen verlassen.

Benachrichtigung bei Angriffen

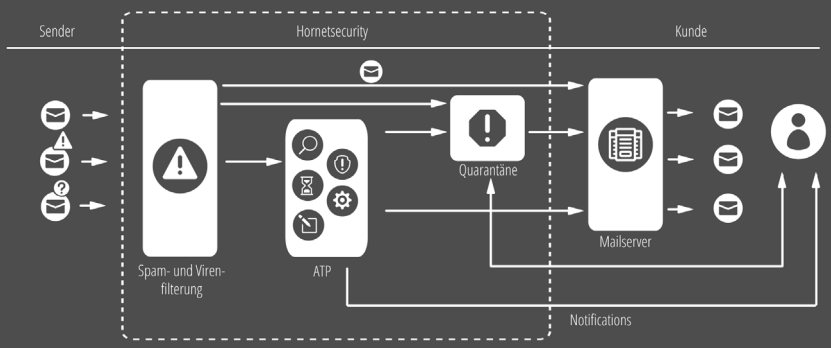
Die Real Time Alerts benachrichtigen in Echtzeit über akute Angriffe auf Unternehmen und ermöglichen eine schnelle Einleitung weiterer interner Maßnahmen und juristischer Vorgehensweisen. Hierfür liefert das Benachrichtigungssystem detaillierte Analyseergebnisse. Zudem kann das Sicherheitsteam der Kunden die Mitarbeiter sensibilisieren, um weitere Angriffswege zum Beispiel per Telefon zu erkennen. Falls bereits zugestellte E-Mails nachträglich als potentiell schädlich erkannt werden, ermöglicht die Ex-Post-Alarmierung dem IT-Sicherheitsteam eine Untersuchung der betroffenen Konten oder Systeme.

+49 6131 90799 60
www.nexio.de
vertrieb@nexio.de

Einbindung von ATP in das Mail Security Management.

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

Abb.: Ablauf des Spam- und Virenfilters mit ATP



HORNETSECURITY®

Hornetsecurity Advanced Threat Protection - Real Time Alert

The Hornetsecurity Advanced Threat Protection Service has just detected the following email attack:

Classification:

User:	accounting@hornetsecurity.com
Date:	08/19/2016 06:38 PM CEST
Sender:	phisher@hackeddomain.com, phisher@hackeddomain.com
Server Address:	123.123.123.123, relay42.hackerserver.com
Reason:	Hornet-ATP02
URL:	http://bit.ly/axJoQXLn

Benachrichtigungen in Echtzeit

Sobald ATP einen Angriff entdeckt, wird eine Benachrichtigung an das IT-Sicherheitsteam des Unernehmens 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-Alert

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 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 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

+49 6131 90799 60
www.nexio.de
vertrieb@nexio.de