Advertorial

Prävention statt Reaktion

Bisherige Endpoint-Schutzlösungen – von klassischen Antiviruslösungen bis zur EDR/XDR-Plattform – setzen bei der Abwehr **unbekannter** Angriffe primär auf ein reaktives Verhalten. Deep Instinct geht einen anderen Weg und stellt die Prävention in den Vordergrund: Dabei blockt ein schlanker Agent mit einer speziell entwickelten Deep-Learning-Engine selbst fortschrittlichste Angriffe ab, bevor sie Schaden anrichten können.

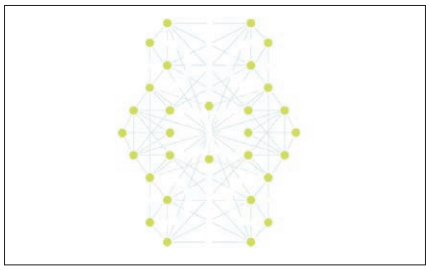
Traditionelle Endpoint-Schutzlösungen auf der Basis von Signaturen, Regeln und Heuristik wehren bekannten Schadcode zuverlässig ab, versagen jedoch oft bei den immer häufiger auftretenden unbekannten Schädlingen, Zero-Day-Attacken und fortgeschrittenen Angriffsmethoden. Vor allem die horrende Geschwindigkeit, mit der etwa Ransomware-Angriffe die Daten verschlüsseln, ruft nach neuen Lösungen.

«Extended Detection and Response»-Lösungen (EDR/XDR) liefern zwar einen erhöhten Schutz, bieten aber noch nicht den erforderlichen Speed für die Abwehr neuer Gefahren in Echtzeit. Denn im Kern solcher Lösungen steht die Post-Analyse verdächtiger Vorgänge «after the fact», also dann, wenn der Schadcode häufig bereits ausgeführt ist. Zum Schutz des Unternehmensnetzwerks und zur Eingrenzung des Schadens werden infizierte Endpunkte häufig automatisch isoliert. Dies hat zur Folge, dass jemand den möglichen Schaden analysieren muss. Dazu kommt das entsprechende Wiederherstellen des ursprünglichen Stands.

Prävention durch Deep Learning

Der Cybersecurity-Spezialist Deep Instinct verfolgt einen anderen, neuartigen und vielversprechenden Ansatz. «Deep Instinct for Endpoints» setzt ganz auf eine schlanke, agentenbasierte Technologie auf der Basis von Deep Learning, einer fortgeschrittenen Form von Machine Learning. Das neurale Netzwerk von Deep Instinct lernt aus Hunderten Millionen Dateien und Dateitypen (darunter schädliche und unschädliche Files), versteht die «DNA» der Bedrohungen, passt die Algorithmen selbsttätig an und verhindert Angriffe in weniger als 20 Millisekunden – also deutlich bevor sich die Malware entfalten kann.

Ransomware benötigt typischerweise bis zu 15 Sekunden, bis die böswillige Verschlüsselung der Daten beginnt – weit mehr



also als die maximal 20 Millisekunden von Deep Instinct für deren Erkennung und Abwehr. Darüber hinaus verspricht Deep Instinct eine Erkennungsrate von 99 Prozent bei **unbekannter** Malware und garantiert, dass mit weniger als 0,1 Prozent falsch positiven Warnungen zu rechnen ist.

Deep Learning an sich ist nichts Neues – es kommt zum Beispiel für autonomes Fahren, bei der Gesichtserkennung oder in der Medizin zum Einsatz. Im Gegensatz zum klassischen Machine Learning arbeitet Deep Learning automatisch und kommt ohne Training von Modellen durch menschliche Akteure aus. Deep Instinct nutzt für seine Endpoint-Schutzlösung ein eigens entwickeltes, speziell auf Cybersecurity zugeschnittenes Deep-Learning-Framework und kann so eine End-to-End-Lösung aus einer Hand anbieten, Es handelt sich um das erste und bisher einzige Deep-Learning-Framework für Cybersecurity.

Intelligenz im Agenten

Bei «Deep Instinct for Endpoints» steckt die fertig ausgebildete künstliche Intelligenz, gewissermassen das «Hirn» der Lösung, direkt im Agenten auf dem Endpoint, der die Systemressourcen dennoch kaum belastet. Für die Voraussage und Prävention von Angriffen über bekannte und unbekannte Malware, Zero-Day-Exploits, Ransomware und gängige Scripts benötigt der Agent keinerlei Cloud-Zugriff. Die Lösung unterstützt dabei eine Vielzahl von Dateitypen – inklusive PDF, Office, Fonts, TIFF, JAR und Makros.

Gegen weitere Angriffsarten wie dateilose und mehrstufige Attacken, Remote Code Injection, Spyware oder Credential Theft/Dumping kommen zusätzliche, mehrschichtige Schutzmechanismen wie verhaltensbasierte Analyse zum Einsatz. Ein spezielles Modul kümmert sich um die Abwehr von Angriffen via Windows PowerShell.

«Deep Instinct for Endpoints» ist für Windows, MacOS und Linux sowie Chrome OS und Android erhältlich. In manchen KMU-Szenarien erfüllt die Lösung die Endpoint-Schutzbedürfnisse komplett. Deep Instinct lässt sich auch ergänzend zu EDR/XDR-Lösungen und zum Microsoft-365-Dienst Defender ATP einsetzen, um die Abwehr am Endpoint gegen unbekannte Malware und Ransomware deutlich zu erhöhen. Deep Instinct reduziert zudem die Anzahl falsch positiver Meldungen in XDR-, SIEM- und SOAR-Lösungen massiv, was das Security-Team beim Endkunden oder beim Security-Partner stark entlastet.

Deep Instinct for Endpoints

- Wehrt Cyberangriffe in unter 20 Millisekunden ab
- Stoppt auch mehrstufige, komplexe Ransomware-Attacken
- Erkennt 99 Prozent aller **unbekannten** Malware
- Maximal 0,1 Prozent falsch positive Resultate
- Basiert auf speziell für Cybersecurity zugeschnittener Deep-Learning-Technologie
- Arbeitet mit schlanken, systemfreundlichen Agenten auf den Endpoints

Kontakt:

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch, www.boll.ch