Prädiktive Endpoint Security, die aus Erfahrung lernt: Sophos Intercept X mit Deep Learning

Neuronales Trainingsmodell mit weniger als 20 MB erkennt bekannte und unbekannte Malware sowie PUAs, bevor sie ausgeführt werden können – ohne dabei auf Signaturen zurückzugreifen

Wiesbaden, 30. Januar 2018 – Sophos stellt seine jüngste Version von Intercept X vor und treibt damit die Integration modernster Abwehr und Präventionstechnologien für Malware weiter voran. Neben einer neuen Active-Hacker-Abwehr, einem fortschrittlichen Anwendungs-Lockdown und nochmal erweitertem Ransomware-Schutz basiert die Malware-Erkennung dieser neuesten Version der Next-Gen-Endpoint Security auf den neuronalen Netzen des Advanced Deep Learning.

Deep Learning ist die jüngste Weiterentwicklung des Machine Learning mit einem hoch skalierbaren Erkennungsmodell, das die gesamte erkennbare Bedrohungslandschaft erlernen kann. Weil dabei Milliarden von Stichproben verarbeitet werden können, sind mit Deep Learning im Vergleich zum herkömmlichen Machine Learning noch einmal genauere Vorhersagen möglich – und das schneller und mit weit weniger Fehlalarmen.

Auch in Sachen Anti-Ransomware und Exploit-Prävention sowie Active-Hacker-Abwehr wie z.B. Schutz vor Identitätsdiebstahl hält die neue Version von Sophos Intercept X Innovationen parat. Seit Anti-Malware-Software besser geworden ist, haben sich die Angriffe vorwiegend auf Identitätsdiebstahl verlagert, damit Hacker sich als legitime Nutzer in Systemen und Netzwerken bewegen können. Intercept X erkennt und verhindert dies. Die Software wird über die cloudbasierte Managementplattform Sophos Central bereitgestellt und kann neben bestehenden Endpoint-Security-Programmen beliebiger Hersteller installiert werden. So erhöht Intercept X sofort den Endpoint-Schutz der Nutzer. In Verbindung mit der Sophos XG Firewall erweitert Intercept X den Schutz zudem um Synchronized Security, den synchronisierten Schutz von miteinander kommunizierenden Endpunkten und Netzwerk.

„Die Zukunft der IT-Sicherheit liegt im prädiktiven Schutz. Mit der Erweiterung des Exploit- und Ransomware-Schutzes von Intercept X um neuronale Deep-Learning-Netze hat Sophos einen großen Schritt getan“, erklärt Dan Schiappa, Senior Vice President und General Manager of Products bei Sophos. „Auch für zukünftige, unbekannte Angriffe gewappnet zu sein, diese nicht mehr abwarten zu müssen – das eröffnet den IT-Abteilungen in Unternehmen ganz andere Möglichkeiten, ihre Anwender und Ressourcen zu schützen. Mit Intercept X läßt sich modernster Next-Gen-Schutz unabhängig von der aktuellen Strategie für jede Organisation und jedes Unternehmen umsetzen.“ Herkömmliche Machine-Learning-Ansätze führen zu riesigen Modellgrößen und beanspruchen viele Gigabytes auf der Festplatte. Der Sophos Deep-Learning-Ansatz hingegen generiert stark komprimierte Modelle mit weniger als 20 MB auf dem Endpoint, sodass die Performance praktisch nicht beeinträchtigt wird.“

Das neuronale Deep-Learning-Netz von Intercept X lernt aus Erfahrung

„Bei den ursprünglichen Machine-Learning-Modellen müssen Analyseexperten die Attribute vorgeben, mit denen das Modell trainiert wird, wodurch ein subjektives menschliches Element vorhanden bleibt. Mit zunehmendem Dateninput werden diese Modelle zudem immer

komplexer und erreichen Gigabyte-Größe, was sie behäbig und langsam macht. Außerdem weisen sie erhebliche Fehlalarmraten auf, die die Produktivität der IT bremsen. Administratoren müssen mühsam herausfinden, was nun wirklich Malware ist und was legitime Software“, erklärt Tony Palmer, Senior Validation Analyst bei der Enterprise Strategy Group (ESG). „Dagegen lernt das neuronale Deep-Learning-Netz von Intercept X aus Erfahrung und stellt Korrelationen zwischen beobachtetem Verhalten und Malware her. Diese Korrelationen sind der Grund, weshalb sowohl für bekannte als auch für Zero-Day-Malware so eine hohe Genauigkeit und ein geringerer Anteil an Fehlalarmen erreicht wird. Untersuchungen des ESG-Lab haben ergeben, dass dieses neuronale Netzmodell gut skalierbar ist und umso schlauer wird, je mehr Daten es bekommt. Das ermöglicht eine aggressive Erkennung ohne Abstriche bei der Administrations- oder Systemperformance.“

Die neuen Funktionen von Intercept X in der Übersicht:

Malware-Erkennung mit Deep Learning

- Das Deep-Learning-Modell erkennt bekannte und unbekannte Malware und potenziell unerwünschte Anwendungen (PUAs), bevor sie ausgeführt werden können – ohne dabei auf Signaturen zurückzugreifen
- Das Trainingsmodell ist kleiner als 20 MB und benötigt nur selten Updates

Abwehr aktiver Angreifer

- Schutz vor Identitätsdiebstahl – verhindert den Diebstahl von Authentifizierungspasswörtern und Hash-Informationen aus Arbeitsspeicher, Registry und persistentem Speicher, wie zum Beispiel bei Angriffen wie „Mimikatz“
- CodeCave-Ausnutzung – erkennt, ob Code in eine andere Anwendung eingeschleust wurde (geschieht oft aus Persistenzgründen und um Antivirus-Software zu umgehen)
- APC-Schutz – identifiziert den Missbrauch von APCs (Asynchronous Procedure Calls), welche oft im Rahmen der AtomBombing-Code-Injizierungstechnik zur Anwendung kommen. In der jüngeren Vergangenheit wurde diese Methode genutzt, um den WannaCry-Wurm und den NotPetya-Wiper via EternalBlue und DoublePulsar zu verbreiten (mithilfe dieser Aufrufe können Angreifer einen anderen Prozess dazu missbrauchen, bösartigen Code auszuführen)

Neue und verbesserte Exploit-Präventionstechniken

- Bösartige Prozessmigration – erkennt remote durchgeführte reflektive DLL-Injektion, durch die Angreifer sich zwischen den auf dem System laufenden Prozessen bewegen können
- Prozessberechtigungsausweitung – verhindert, dass ein Prozess mit niedriger Berechtigung auf eine höhere Berechtigungsstufe eskaliert wird, um erweiterten Systemzugriff zu erhalten

Erweiterter Anwendungs-Lockdown

- Lockdown des Browserverhaltens – Intercept X verhindert den Missbrauch von PowerShell aus dem Browser heraus als grundlegende Verhaltenssperre
- HTA-Lockdown – auf vom Browser geladene HTML-Anwendungen wird die Lockdown-Maßnahme angewendet, als wären sie ein Browser

Alle Infos zu Deep Learning und Intercept X unter www.sophos.de/interceptx.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de