Acronis Der Einsatz von maschinellem Lernen zur Absicherung von Daten

Acronis Active Protection wurde im Januar 2017 eingeführt und ist eine fortschrittliche Technologie, die Systeme mithilfe ausgeklügelter Analysen auf Ransomware-typische Verhaltensmuster hin untersucht und auf entsprechend erkannte Ransomware-Angriffe umgehend stoppen kann. Trotz hervorragender Ergebnisse bei unabhängigen Tests und Auszeichnungen durch Medien wollte Acronis die Lösung noch robuster machen. Durch die Implementierung von maschinellem Lernen und KI-Technologien (Künstliche Intelligenz) ist dies auch erfolgreich gelungen.

WIE MASCHINELLES LERNEN HILFT

Der Begriff „maschinelles Lernen" wird häufig mit dem Begriff „Big Data" assoziiert – die Analyse besonders große Datenmengen zur Gewinnung umsetzbarer Ergebnisse. Da maschinelles Lernen auf der Menge der Daten und den gewählten Algorithmen beruht, sind die Ergebnisse umso besser, je größer die Datenprobe ist.

Wie wird diese Technologie von Acronis eingesetzt? Der erste Schritt besteht in der Durchführung einer sogenannten Stacktrace-Analyse, die über Programm-Subroutinen berichtet. Diese Technik wird häufig für bestimmte Arten von Debugging verwendet, mit denen Software-Entwicklern herausfinden können, wo ein Problem liegt oder wie verschiedene Programm-Subroutinen während einer Ausführung zusammenarbeiten.

Acronis wendet diesen Ansatz auf Ransomware-Angriffe an, um mithilfe von maschinellem Lernen bösartige „Code-Injections" (Einschleusung von Software-Code in andere Programme) zu erkennen.

WIE MASCHINELLES LERNEN FUNKTIONIERT

Acronis hat sehr große Mengen an „sauberen" Daten auf Windows-Systemen analysiert, auf denen eine Vielzahl von zulässigen Prozessen ausgeführt wurden. Dabei wurden Millionen von legitimen „Stacktraces" (Stapelüberwachungsdaten) von diesen Prozessen gewonnen und daraus mithilfe von Entscheidungsbaum-Lernen unterschiedliche Modelle über „gutes" Verhalten entwickelt. Zusätzlich wurden „bösartige" Stacktraces aus verschiedenen Quellen gesammelt, um Gegenbeispiele zu erhalten.

Basierend auf diesen millionenfachen Lernproben wurden dann entsprechende Verhaltensmuster identifiziert.

Dank Entscheidungsbaum-Lernen konnten wir von der Beobachtung eines Elements zu einer Schlussfolgerung über dessen Zielwert gelangen, um damit wiederum ein Modell zu erstellen, welches den Wert eines neuen Elements auf Basis identifizierbarer Faktoren genau vorhersagen kann. Diese Modelle ermöglichten es Acronis, angemessene Reaktionen auf Sollwerte direkt in die Data Protection-Lösung zu integrieren. Statt eine Client-Maschine dadurch zu verlangsamen, dass Daten gesammelt und zur Analyse versendet werden, bieten diese On-Board-Modelle das gleiche Schutzniveau, aber mit höherer Effizienz.

WANN WIRD DAS MASCHINELLE LERNEN AKTIVIERT?

Wie bereits oben erwähnt, basiert Acronis Active Protection auf heuristischer Verhaltenserkennung. In Version 2.0 unserer Schutztechnologie haben wir mehrere neue Heuristiken hinzugefügt, die nach zulässigen Prozessen suchen. Wenn Acronis Active Protection in einem Prozess ein seltsames Verhalten entdeckt, erfasst es einen Stacktrace und übermittelt diesen an das „Machine-Learning-Modul" von Acronis. Von diesem wird das Verhalten mit bestehenden Modellen von korrekten und infizierten Stacktraces verglichen, um zu bestimmen, ob eine Bedrohung vorliegt oder nicht.

Wenn das Verhalten als bösartig eingestuft wird, wird der Anwender mit einer Warnung darauf hingewiesen, dass der Prozess blockiert werden sollte.

EINE NEUE STUFE DER RANSOMWARE-ABWEHR

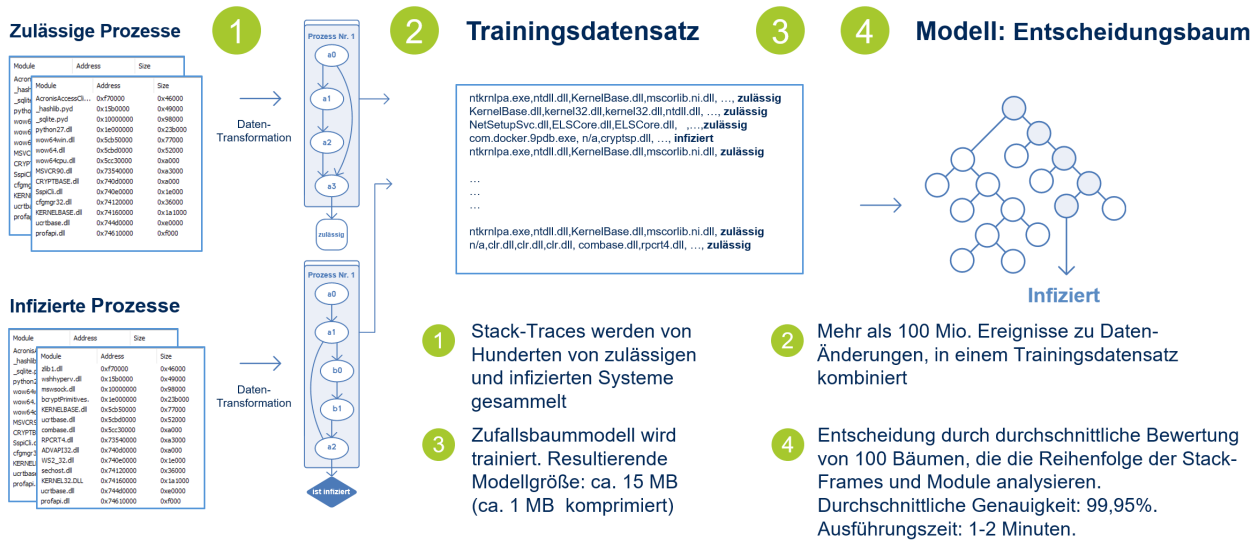
All diese Technologien, die letztendlich auf maschinellem Lernen beruhen, heben Acronis Active Protection auf eine ganz neues Leistungsniveau – insbesondere bei der Bekämpfung von Zero-Day-Bedrohungen. Es erstellt ein Modell über zulässige Prozesse, sodass auch neue, bisher unbekannte Ransomware-Varianten (die z.B. neue Software-Schwachstellen ausnutzen oder andere, neue Infiltrationsmethoden verwenden) erkannt und gestoppt werden können.

Die „Machine Learning"-Infrastruktur von Acronis ist so aufgebaut, dass neue, anonymisierte Programmdaten regelmäßig zur Analyse hochgeladen werden. Diese Infrastruktur kann Millionen von Anfragen gleichzeitig verwalten – und dank des ständigen Informationsflusses sind neue Verhaltensmodelle viel schneller verfügbar. Zudem wird die Sicherheit durch regelmäßige Updates der Produkt-Heuristiken fortlaufend verbessert. Keine dieser in Sekunden-bruchteilen durchgeführten Hintergrundarbeiten sind für den Anwender spürbar – vielmehr kann er Acronis Active Protection einfach einschalten und dann quasi vergessen.

WAS KOMMT ALS NÄCHSTES?

Acronis wird den Einsatz dieser Technologie weiter ausbauen und das maschinelle Lernen auch für statische Code-Analyse einsetzen. Eine solche Analyse kann noch vor der Ausführung einer Software erfolgen. Wenn Sie also eine Datei herunterladen oder auf eine Festplatte kopieren, wird diese Datei direkt auf abweichende, bösartige Programmcodes überprüft werden können. Wenn etwas Verdächtiges gefunden wird, kann der entsprechende Prozess noch vor seiner Ausführung (durch den Anwender oder ein automatisiertes Skript) blockiert werden.

Außerdem können maschinelle Lernmodelle auch zur Analyse von Skripten verwendet werden – und Acronis arbeitet bereits in diese Richtung. Tatsächlich haben Tests des Sicherheitsunternehmens „NioGuard Security Lab" gezeigt, dass die meisten aktuellen Antivirus-Lösungen skriptbasierte Angriffe nicht erkennen können – Acronis Active Protection dabei aber eine gute Performance bietet. Trotz all dieser bisherigen Erfolge werden wir unsere Anti-Ransomware-Technologien auch zukünftig noch weiter verbessern.



Weitere Informationen finden Sie unter **www.acronis.com**