CYLANCE

FALLSTUDIE ÖFFENTLICHE VERWALTUNG

Cybersecurity

Zukunftsfähige Sicherheitslösung für die öffentliche Verwaltung

BRANCHE
Öffentliche Verwaltung

PARTNER
Schoeller Network Control

UMGEBUNG
CylancePROTECT schützt 3.000 Endpunkte, Clients und Server, mit File Actions, Memory Protection, Script Control – Alert und Auto Quarantine

HERAUSFORDERUNGEN
- Vorausschauendes Erkennen und Abwehren auch von noch unbekannter Malware;
- Leicht zu implementierende, benutzerfreundliche und zukunftsfähige Lösung

LÖSUNGEN
- Implementierung von CylancePROTECT um Angriffe vorausschauend zu verhindern

LAND SALZBURG

Das Unternehmen

Im Land Salzburg arbeiten das Amt der Salzburger Landesregierung, die Bezirksverwaltungen sowie weitere Sonderverwaltungsbehörden, betriebsähnliche Einrichtungen, wirtschaftliche Unternehmungen, Bildungseinrichtungen, nichtbehördliche Einrichtungen und sonstige Einrichtungen des Landes im Dienst der Öffentlichkeit. In Summe sind rund 3.000 Landesbedienstete in der Landeshauptstadt und in allen Bezirken tätig.

Die Situation

Moderne Verwaltung ist inzwischen stark durch IT-Prozesse geprägt. Datenverarbeitungssysteme sind gerade in den letzten Jahren modernisiert, ausgebaut und vernetzt worden. Dazu kommen verstärkt elektronisch angebotene Service-Leistungen für Bürger und Bürgerinnen. IT-Sicherheit ist somit zu einem unverzichtbaren Bestandteil der IT geworden, denn auch Behörden und öffentliche Verwaltung sind zunehmend ins Visier von Angreifern gerückt. Neben der Umsetzung von national und international anerkannten Sicherheitsstandards kommt dem Schutz vor Malware, Ransomware und anderen neuartigen Bedrohungen ein besonderer Stellenwert zu. Der vorwiegend reaktive Ansatz beim Bekämpfen von Malware hat allerdings gravierende Nachteile. Denn erst, wenn eine neue Malware-Variante bereits erfolgreich war, kann man sie erkennen, analysieren, Signaturen generieren und einen entsprechenden Patch bereitstellen. Das allein kostet viel Zeit und Aufwand.

Diplomingenieur (FH) Bernhard Glanzer, IT-Architekt und beim Land Salzburg verantwortlich für die IT-Sicherheit: „Traditionelle Antiviren-Lösungen arbeiten rein Pattern-basiert. Bei der aktuellen Malware-Flut entstehen aber durch dieses Verfahren massive Sicherheitslücken. Erst recht, wenn wir von bisher noch unbekannter Malware oder neuen Varianten sprechen. Einen zuverlässigen Schutz für unsere Systeme und die komplette Infrastruktur einer öffentlichen Verwaltung konnten wir so nicht mehr gewährleisten. Deshalb haben wir uns nach einer zukunftsfähigen Lösung und einer anderen als der traditionellen Herangehensweise umgeschaut. Durch unseren Partner, die schoeller network control, sind wir auf Cylance und CylancePROTECT aufmerksam geworden."

Traditionelle Anti-Malware-Lösungen werden von der immensen Zahl aktuell kursierender Malware praktisch überflutet. Die rein reaktive Methodik ist neu auftretenden Malware-Varianten kaum gewachsen. Aktuelle Statistiken sprechen von durchschnittlich 300.000 bis zu einer 1 Million Malwaresamples, die täglich dazu kommen. Diese Entwicklung hat dazu geführt, dass Firmen aktiv nach alternativen Methoden suchen, um Sicherheitsherausforderungen anders als bisher zu begegnen. Einer dieser Ansätze ist es, künstliche Intelligenz und maschinelles Lernen in der IT-Sicherheit zu benutzen. Dabei geht es weniger um ein weiteres Tool, eine weitere Technologie oder einen weiteren Layer. Genauso wie es nicht mehr ausreicht, sich ausschließlich auf allgemein empfohlene Best Practices zu verlassen. Künstliche Intelligenz (KI) und im Speziellen das maschinelle Lernen sind angetreten die „alte Welt" der Cybersecurity zu revolutionieren. Erklärtes Ziel, natürlich, der Bedrohungsentwicklung einen Schritt weit voraus zu sein. Maschinelles Lernen benutzt Algorithmen, die Eigenschaften und Zusammenhänge erkennen und sich kontinuierlich lernend weiterentwickeln.

Der Fokus liegt auf Prävention und Prognose statt nur zu reagieren, wenn eine Infektion bereits erfolgreich war. Maschinelles Lernens hilft Unternehmen und Institutionen bessere Entscheidungen zu treffen als Menschen es könnten, und das vor allem deutlich schneller. Dafür sorgen nicht zuletzt die angesprochenen „Prognosequalitäten". Sie basieren auf dem, was die Lösung bereits aus der Vergangenheit „weiß", gelernt und korreliert hat.

Der Prozess

Will man eine IT-Sicherheit und insbesondere die Malware-Abwehr zukunftsfähig machen, braucht es ein grundsätzliches Umdenken. Neue Ansätze konzentrieren sich auf die Prävention mithilfe statistischer Methoden. Sie nutzen maschinelles Lernen und selbsttrainierende KI-Module, um das Schadrisiko eines ausführbaren Codes zu berechnen, der ureigenen DNA jeder Malware. Danach entscheidet der Algorithmus, ob die Datei sicher ist und ausgeführt werden kann oder ob sie in die Quarantäne verschoben werden muss.

Bernhard Glanzer: „Bereits im Proof of Concept hat sich die KI-basierte Lösung von Cylance als performante Alternative zu den üblichen Antiviren-Lösungen erwiesen. Neben der besseren Leistung haben wir in unserer Testumgebung vor allem eine sehr viel höhere Erkennungsrate erzielt, als mit herkömmlichen Methoden und Tools. Wir haben uns nach einem temporären Parallelbetrieb mit der bestehenden Lösung zügig entschieden CylancePROTECT in der Standard-Windows 7-Umgebung als alleinigen Malware-Schutz zu implementieren. Also für sämtliche Clients und Server, insgesamt für 3.000 Endpunkte. Der Dienstleister unseres Vertrauens, die schoeller network control, hat uns bei der Auswahl und Implementierung unterstützt."

Das Produkt wurde in einem gemeinsamen Gespräch mit dem Partner schoeller network control genau geprüft und daraufhin in einem POC evaluiert.

„Vor allem durch den ausgesprochen schnell umgesetzten Proof of Concept war es möglich, das System innerhalb kürzester Zeit auf 150 Clients auszurollen und zu evaluieren. In dieser Phase haben uns beide, Hersteller und Partner, optimal unterstützt, so dass wir die Vorteile der Lösung rasch nachvollziehen und zielsicher überprüfen konnten", so Glanzer weiter.

3.000
BESCHÄFTIGTE

3.000
ENDPUNKTE

Die Ergebnisse

CylancePROTECT überwacht sämtliche der 3.000 Endpunkte beim Land Salzburg. Durch einen hohen Standardisierungsgrad war es ohne großen zusätzlichen Aufwand möglich, das Whitelisting von Falsch-Positiv-Meldungen an die Bedürfnisse des Kunden anzupassen. Dadurch ist es jetzt nicht nur möglich bekannte und neuartige Schadsoftware zu erkennen und abzuwehren, sondern auch sogenannte „Potentially Unwanted Software" zu finden und ebenfalls zu blockieren. Solche unerwünschte Software wird meistens innerhalb der jeweiligen Benutzerprofile ausgeführt.

„Besonders hervorzuheben ist, wie einfach wir die Lösung nach dem erfolgreichen POC in den laufenden Betrieb überführen konnten. Das hat alles in allem nicht mehr als vier Wochen in Anspruch genommen. Der Pilot war problemlos in den Produktionsbetrieb zu übernehmen, so dass wir den flächendeckenden Rollout tatsächlich in der kürzest möglichen Zeit abgeschlossen haben. Im Zuge des geplanten flächendeckenden Rollouts von Windows 10 werden wir CylancePROTECT dann parallel zu Windows Defender einsetzen."

Jede Malware besitzt ihre ureigene DNA. Sammelt man nun sozusagen diese DNA ein und analysiert sie, findet man sowohl gutartige wie bösartige Muster. WannaCry ist ein gutes Beispiel, dafür was man mithilfe von lernenden maschinellen Algorithmen bewirken kann. Als die Ransomware auftauchte war sie vollkommen neu. Allerdings war die WannaCry zugrunde liegende Code-Basis durchaus bekannt und somit prognostizierbar. Ein Algorithmus, der auf der Basis von maschinellem Lernen fungiert, hätte die Ransomware demnach sofort identifiziert und gestoppt. Und zwar noch bevor der Schadcode tatsächlich ausgeführt wird und Schaden anrichten kann.

Solche lernenden Algorithmen installiert man am Besten an den Endpunkten. Dort führen sie statistische Analysen durch, die eine Ausführung potenziellen Schadcodes verhindern. Diese Technik ist schnell in der Lage zu entscheiden, ob es sich um eine harmlose Datei handelt oder um Schadcode. Anders als bei Cloud-basierten Analysen, sitzt eine solche Sicherheitslösung direkt am Endpunkt und braucht bei ihrer Analyse keine Internetverbindung. Signatur-basierende Lösungen sind auf eine regelmäßige Internetverbindung angewiesen um die heutzutage schon fast im Minutentakt ausgebrachten Updates zu beziehen oder Einzelbewertungen abzufragen. Algorithmen auf Basis maschinellen Lernens arbeiten über Monate autark, auch dann, wenn Systeme Offline geschaltet sind. Dabei sind sie effizienter als signatur-basierte Lösungen, selbst wenn diese immer auf dem aktuellen Stand sind.

Bernhard Glanzer bilanziert: „Durch den effizient abgewickelten POC konnten wir schnell die Stärken des Produktes verifizieren. Das Ergebnis hat uns in unserer Annahme bestätigt, dass wir mit einem flächendeckenden Rollout der Lösung das Sicherheitsniveau insgesamt wesentlich erhöhen. Und gleichzeitig, dass wir mit der neuen Technologie absolut am Puls der Zeit sind."

+49-89-244455571
sales@cylance.com
www.cylance.com
Second Floor, 89/90 South Mall, Cork City, Ireland T12 RPP0

CYLANCE

20171115-1955