CYLANCE

FALLSTUDIE WOHLFAHRTSVERBÄNDE

Cybersecurity

bei der Caritas: KI-getriebene Lösung bietet sofort erkennbaren Mehrwert

BRANCHE
Wohlfahrtsverbände

UMGEBUNG
CylancePROTECT schützt zirka 400 Endpunkte und 110 Server

HERAUSFORDERUNGEN

- Vorausschauendes Erkennen und Abwehren auch von noch unbekannter Malware; zukunftsfähige Lösung
- Ressourcenschonende, leicht zu implementierende, benutzerfreundliche und kosteneffiziente Lösung

LÖSUNGEN

- Implementierung von CylancePROTECT um selbst Zero-Day-Angriffe vorausschauend zu erkennen und abzuwehren
- Zukunftsfähige Lösung, die nur minimale Ressourcen beansprucht, leicht zu verwalten ist
- Sofortiger Schutz und unmittelbar ersichtlicher Mehrwert bereits in der Scanphase

caritas frankfurt

Das Unternehmen

„Menschen stärken. Wege finden" unter diesem Leitwort steht die Arbeit des Caritasverband Frankfurt e. V, dem Wohlfahrtsverband der katholischen Kirche in Frankfurt am Main.

Mit rund 100 Einrichtungen und Diensten in den verschiedenen Feldern der sozialen Arbeit gehört der Caritasverband Frankfurt e. V. zu den großen Trägern der freien Wohlfahrtspflege in Frankfurt am Main. Als kompetenter und moderner Dienstleister, dessen Handeln auf christlichen Werten aufbaut, bieten wir gemeinsam mit katholischen Kirchengemeinden in Frankfurt, ein einzigartiges Netzwerk sozialer Angebote und Hilfen.

Mehr als 1.600 Beschäftigte sowie rund 1.400 Ehrenamtliche und Helfer/-innen setzen sich bei uns täglich für die Beteiligung aller Bürger/-innen an einer solidarischen und sozialen Stadtgesellschaft ein und bieten Menschen Unterstützung für ein selbstbestimmtes und selbstverantwortetes Leben.

Die Situation

Der Caritasverband Frankfurt e.V. beschäftigt zirka 1.600 Mitarbeiterinnen und Mitarbeiter in vielfältigen Aufgabenfeldern. Darunter die Allgemeine Sozialberatung als Erstkontaktstelle, die Bahnhofsmission, Kindertagesstätten und Horte, aber auch spezielle Beratungsstellen zu Themen wie Frauen, Behinderung, Pflege und Wohnen.

Steffen Lantzsch ist in seiner Funktion als Leiter der IT für die rund 100 Standorte des Verbandes verantwortlich. Das informationstechnische Rückgrat bilden 110 Server mit zirka 400 Endpunkten und 1.000 aktiven

Nutzern. Unternehmen und Organisationen müssen heute mit vielfältigen neuartigen Bedrohungen umgehen und haben gelernt wie wichtig es ist, möglichst schnell zu reagieren. Zwar stellen Anbieter von Sicherheitslösungen Signatur-Updates in schneller Folge zur Verfügung. Die helfen aber nur, wenn die Malware bekannt ist und es bereits Betroffene gegeben hat.

Das war genau das Problem mit dem auch Steffen Lantzsch in seiner täglichen Arbeit zu kämpfen hatte. Traditionelle Antivirenlösungen wie die installierte greifen zu spät beziehungsweise funktionieren rein reaktiv. Das heißt, sie werden erst tätig, wenn die Malware als solche erkannt ist und potenziell bereits Schaden angerichtet hat. Eine wenig zufriedenstellende Lösung, wenn man sich das Tempo vor Augen hält mit dem neuartige Malware - gepaart mit wechselnden Angriffsvektoren - heutzutage auftritt.

Als Verband in kirchlicher Trägerschaft gehört der Caritasverband Frankfurt zu den Einrichtungen, die unter das Gesetz zum besonderen Schutz von kritischen Infrastrukturen fallen. Neben den Anforderungen, die mit dem BSI-Grundschutz, dem IT-Sicherheitsgesetz und insbesondere mit der ab Mai 2018 in Kraft tretenden EU-Datenschutz-Grundverordnung (DSGVO) einhergehen.

Steffen Lantzsch: „Wir arbeiten in einem sensiblen Umfeld und gehen mit einer Unmenge von schützenswerten Daten um, die besonderen gesetzlichen Anforderungen unterliegen. Unsere Antivirenlösung war einfach nicht mehr zeitgemäß, weil sie mit moderner Malware nicht Schritt halten kann. Schon gar nicht mit Malware, die erstmals in Erscheinung tritt. Das gilt übrigens meiner Ansicht nach für praktisch alle traditionellen Antivirenlösungen. Deshalb haben wir uns aktiv nach Alternativen umgesehen.“

Der Prozess

Klassische IT-Security-Lösungen stoßen zunehmend an ihre Grenzen. Die aktuellen Ransomware-Angriffe, aber auch hochentwickelte und weitgehend unsichtbar arbeitende Malware wie Petya/NotPetya, GoldenEye oder WannaCry, haben ausreichend bewiesen, dass trotz des hohen technischen Aufwands viele Angriffe dennoch erfolgreich sind. Offenbar lassen sich diese Systeme recht einfach umgehen, sobald der Schadcode zur Ausführung kommt. Aus der KI-Forschung (Künstliche Intelligenz) kommen nun völlig neue Ansätze auch bislang unbekannte Gefahren mithilfe von intelligenten, mathematischen Algorithmen abzuwehren.

Der Caritasverband steht innovativen Ansätzen grundsätzlich offen gegenüber und so stieß IT-Experte Lantzsch bei der Recherche schnell auf die KI-getriebenen Produkte von Cylance.

Steffen Lantzsch: „Wir haben intensiv nach einer neuartigen Lösung gesucht. Cylance bietet als einziges mir bekanntes Unternehmen eine Lösung an, die Malware vorausschauend erkennt und abwehrt, bevor sie überhaupt ausgeführt werden kann. Dazu kommt, dass die Lösung vergleichsweise einfach zu implementieren ist. Für die Basiskonfiguration haben wir lediglich einen halben Tag gebraucht, und die komplette Installation hat uns rückblickend betrachtet nicht mehr als drei Manntage gekostet. Das System hat schnell bewiesen, dass wir uns richtig entschieden haben: Jede Malware wird zuverlässig vorausschauend erkannt und abgewehrt. Das ist genau das, wonach wir gesucht haben, nämlich eine zukunftsfähige Lösung, die nur minimale Ressourcen beansprucht. Auch dadurch hat sich die Lösung von anderen positiv abgehoben. “

Die Ergebnisse

Steffen Lantzsch: „Um traditionelle Lösungen richtig zu nutzen braucht man umfassende Kenntnisse, denn das Management ist komplex. Ohne Support geht letzten Endes gar nichts. Das ist hier anders. Nach Ende des halbtägigen Workshops wussten wir, wie die betroffenen Dateien zu bewerten sind. Der Schutz ist sofort aktiv und der Mehrwert schon in der Scanphase eindeutig zu erkennen.“

Die Einstellungen sind einsichtig und die Richtlinien gut nachvollziehbar. Für individuelle Anforderungen kann die IT aber auch selbst Dashboards erstellen.

Lantzsch weiter: „Früher haben wir sehr viel mehr Manpower gebraucht. Die bisherige Lösung zu verwalten war aber nicht nur zeitaufwendig, sondern auch komplex. Sprich: das

1,600
BESCHÄFTIGTE

1,400
EHRENAMTLICHE
UND HELFER/INNEN

400
GESCHÜTZTE
ENDPUNKTE

110
GESCHÜTZTE
SERVER

haben hochbezahlte Fachleute übernommen, die sich zudem stetig weiterbilden mussten. Im Gegensatz zu signatur-basierten Sicherheitslösungen entfällt das zeitaufwendige und fehleranfällige Verteilen von Updates. Spezialisierte Fachleute kann ich jetzt für andere wichtige Aufgaben einsetzen, und trotzdem haben wir einen hundertprozentigen Schutz. Inzwischen sind bereits über 10 Millionen Dateien überprüft worden. CylancePROTECT hat zudem etliche Malware- und Adware-Varianten erkannt, die unsere alte Lösung übersehen hatte."

Der Caritasverband Frankfurt setzt die folgenden Module ein:

- Skriptkontrolle: Wie viele und welche Skripte laufen im Hintergrund (Gerätesteuerung, Anwendungskontrolle, Auto-Quarantäne)
- Ausführungskontrolle ist aktiv, inklusive Hintergrundbeobachtung
- Speicherschutz
- Applikationskontrolle
- Vollumfängliche Device-Kontrolle

CylancePROTECT ist Bestandteil der KI-Plattform des Unternehmens. Sie fungiert als wissenschaftliche Daten-Engine, die spezialisierte Modelle maschinellen Lernens generiert. Statt auf der Reaktion liegt das Augenmerk erstmals auf der Prävention. Dazu werden komplett neue Wege beschritten, weg vom massenhaften Erstellen von Signaturen hin zu vorhersagenden statistischen Methoden. Diese nutzen maschinelles Lernen und selbsttrainierende KI-Modelle, um das Schadrisiko von ausführbarem Code zu berechnen. Auf dieser Basis entscheidet man, ob eine Datei sicher ist und ausgeführt werden kann oder in Quarantäne gestellt werden muss. Die Trefferquote ist zum Teil doppelt so hoch wie bei traditionellen Verfahren bei einem gleichzeitig niedrigen Falsch-Positiv-Anteil. Sicherheitsteams profitieren aus zwei Gründen von der KI-basierten Plattform: Zum einen senkt sie das Volumen der zu analysierenden Bedrohungen und zum anderen reduziert sie den für die Analyse notwendigen Zeitaufwand.

Steffen Lantzsch abschließend: „In Summe haben wir drei Tage gebraucht um die Lösung zu installieren, anzupassen, den Workshop durchzuführen und die Revisionen umzusetzen. Und das sogar noch innerhalb der Testlaufzeit. Vom Proof-of-Concept, mit dem wir Ende Februar begonnen haben, bis zum abgeschlossenen Rollout Ende März, haben wir insgesamt nicht mehr als drei Manntage aufgewendet. Innerhalb der Serverumgebung und der Windows-Clients hat Cylance als Standalone-Variante die bestehende Lösung bereits abgelöst. Eine deutliche Erleichterung war und ist, dass wir uns auf einen erfahrenen Cylance-Partner wie Com-Sys verlassen können."

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

CYLANCE

20170920-1717