BlackBerry | CYLANCE

CASE STUDY

Gemeinde Sylt Cybersicherheit: Mit Mathe gegen Malware und neuartige Bedrohungen

Das Unternehmen

Sylt ist - so ist es auf der Homepage der Gemeinde nachzulesen - viel mehr als ein Urlaubsparadies. Sylt ist ein lebendiger Ort zum Leben und Wohlfühlen mit einer hervorragenden Infrastruktur und einer zeitgemäßen serviceorientierten Verwaltung. Die hauptamtlich verwaltete Gemeinde Sylt führt die Geschäfte des Amtes Landschaft Sylt mit den Gemeinden Hörnum (Sylt), Kampen (Sylt), List auf Sylt und Wenningstedt-Braderup (Sylt). Die Gemeindeverwaltung verfolgt in jeder Hinsicht einen modernen Dienstleistungsansatz und informiert über ihre Internetseiten sowie den Kurznachrichtendienst Twitter zeitnah über wichtige Angelegenheiten. Ziel ist es, Fragen zu Angeboten, Dienstleistungen und Behördengängen “rund um die Uhr” zu beantworten.

Die Situation

Die Gemeinde Sylt setzt in vielen Belangen auf eine elektronisch gestützte Verwaltung und Kommunikation mit den Bürgerinnen und Bürgern. Bei Ämtern, Behörden und in der Verwaltung im Allgemeinen gibt es eine Reihe von Prozessen, die sich von denen in der freien Wirtschaft unterscheiden. Das wirkt sich auch auf die innerhalb der IT-Sicherheit eingesetzten Methoden und Technologien aus. Ein Beispiel war die bestehende Antivirenlösung der Gemeinde Sylt. Die Administration gestaltete sich sehr aufwendig, und die Mitarbeiter bemängelten, dass sich Art und Umfang der durchzuführenden Scans negativ auf ihre Produktivität auswirkten.

Thomas Ranke, Inselverwaltung der Gemeinde Sylt und des Amtes Landschaft Sylt Amt für Inneres und Bildung, SB IT, Zentrale Dienste, wird noch deutlicher: „Die Admin-Systeme unserer bestehenden Lösung waren im alltäglichen Gebrauch schlicht gruselig. Hier bestand, drücken wir es ein Mal vorsichtig aus, dringender Veränderungsbedarf. Im Grunde war unser Anforderungsprofil gar nicht so komplex. Wir suchten nach einem verlässlichen Endpunkt-Schutz für unsere Clients und Server, einfach zu verwalten und mit einem Werkzeugkasten ausgestattet in dem man die notwendigen Tools bei Bedarf schnell findet.“

Um die Endpunkte abzusichern hatte man sich bei Gemeindeverwaltung Sylt bisher auf eine traditionelle, also Signatur-basierte AV-Lösung verlassen. Die Verwaltung stellte sich in der Folge als ausgesprochen aufwändig heraus, und um die Lösung jederzeit auf dem neuesten Stand zu halten, brauchte man erhebliche personelle Ressourcen.

Branche:

- Verwaltung

Umgebung:

- CylancePROTECT® für insgesamt 175 Clients, davon 110 virtuell, 30 virtuelle Server auf 6 realen Server-Blechen, 3 davon für die VMware View – Umgebung

Herausforderungen:

- Die Administration der bestehenden Antivirenlösung (AV) gestaltete sich ausgesprochen mühsam und schränkte zudem bei speziellen Verwaltungsprozessen die Produktivität ein
- Die bisherige Lösung beanspruchte erhebliche Systemressourcen
- Der traditionelle Ansatz entsprach nicht den aktuellen Bedürfnissen bei der Abwehr von Bedrohungen

Lösung:

- Implementierung von CylancePROTECT um sowohl bereits bekannte Bedrohungen abzuwehren als auch vor bis dato unbekannten zu schützen, und das bei minimalen Auswirkungen auf das System

Etliche der gängigen Lösungen beanspruchen zudem einen großen Teil der CPU-Last für sich. So auch hier. Die AV-Lösung beeinträchtigte in nicht unerheblichem Maß die den Endbenutzern gebotene Systemleistung. Dadurch verlangsamten sich die operativen Abläufe, die sich in der Verwaltung zum Teil erheblich von denen in Unternehmen der freien Wirtschaft unterscheiden.

Thomas Ranke: „Ein Beispiel ist das kommunale Haushalts-, Kassen- und Rechnungswesen, ein Herzstück der öffentlichen Verwaltung. Hier öffnet ein Benutzer unter Umständen bis zu 300 Dateien gleichzeitig. Diese Dateien werden in kurzer Folge immer wieder geöffnet und geschlossen, entsprechend dem Rhythmus der Buchungen. Die notwendigen Scans der ursprünglichen Antivirenlösung haben sich teilweise massiv auf die Bearbeitungsgeschwindigkeit ausgewirkt. Dadurch waren wir gezwungen über 10 Prozent dieser Dateien aus den regelmäßigen Scans ausschließen. Das hat unsere Angriffsfläche deutlich erhöht. Dazu kam dann noch das kontinuierlich notwendige und zeitaufwändige Einspielen der Signatur-Updates."

„Wir setzen insgesamt 175 Clients ein, davon 110 virtuelle sowie 30 virtuelle Server. Systeme auf denen Daten höchster Schutzgüte vorgehalten werden. Dazu gehören Einwohnermeldedaten, Personendaten, die teilweise mit Auskunftssperren versehen sind, Liegenschaftsdaten und weitere mehr. Man kann sich leicht vorstellen, was es heißen würde, wenn diese Informationen bei einem Datenschutzvorfall offen gelegt werden."

Behördliche Verwaltungsprozesse werden zunehmend digitalisiert. Durch die steigende Zahl von Datenschutzverletzungen und Cyberangriffen steht die öffentliche Verwaltung hier vor einer nicht zu unterschätzenden Herausforderung. Damit die öffentliche Verwaltung in der Lage ist weiterhin auf entsprechend stabile und sichere Verwaltungsprozesse zu vertrauen, muss sie den Datenschutz in ein umfassendes IT-Sicherheitskonzept einbinden und bestehende Methoden und Technologien dahingehend überprüfen. Dazu kommt: auch im behördlichen Sektor wird die IT-Infrastruktur immer komplexer. Nicht selten gibt es eine eigene IT, IT im nahen behördlichen Umfeld, die zentrale IT im Rechenzentrum und vielleicht externe Dritte als IT-Dienstleister. Hier erhöht neben einer Vielzahl von bereits geltenden Richtlinien die am 25. Mai 2018 in Kraft tretende EU-Datenschutz-Grundverordnung den Druck zusätzlich. Einerseits was die konkreten Anforderungen zum Schutz personenbezogener Daten anbelangt andererseits was den Umgang mit Daten und Informationen innerhalb einer Behörde insgesamt betrifft.

Der Prozess

„Wir waren mit der bestehenden Situation alles andere als glücklich. Wie es der Zufall wollte wurden wir just zu diesem Zeitpunkt vom Systemhaus-Partner Communication Systems GmbH angesprochen. Und ich muss zugeben, dass ich als an Mathematik interessierter Mensch den vorgetragenen Ansatz bestechend fand.

Allerdings waren wir zunächst trotzdem skeptisch, denn inzwischen werden die beiden Begriffe künstliche Intelligenz (für die es keine einheitliche Definition gibt) und maschinelles Lernen gleichermaßen inflationär gebraucht. Nur selten wird dann erklärt wie ein Produkt genau arbeitet, welche Modelle maschinellen Lernens zugrunde gelegt werden, wie die Code-Analyse vonstatten geht und so weiter. Zum Glück konnte ein Referenzkunde des Unternehmens unsere Bedenken komplett entkräften. Beim eigentlichen Test waren wir von der schnellen Implementierung und der Performance des Systems angemessen beeindruckt. CylancePROTECT als Endpunkt-Sicherheitslösung nutzt die mathematischen Grundlagen sehr, sehr überzeugend. Das Ergebnis unseres Tests: Es funktioniert."

Die Ergebnisse

Thomas Ranke: „Wir setzen CylancePROTECT auf (und auf) insgesamt 175 Clients, davon 110 virtuelle und 30 virtuellen Servern ein. Natürlich hat die Lösung in der Anfangsphase etliche Dateien „angemeckert". Das verwundert aber nicht bei 50 verschiedenen Fachverfahren aus dem Spezialsegment öffentliche Verwaltung. In den ersten Tagen hatte ich das Portal permanent offen, um zu entscheiden, ob die betreffenden Dateien freigegeben oder blockiert werden, respektive in die Quarantäne wandern sollten. Das musste ich aber nur ein einziges Mal tun, was sich schnell und einfach erledigen ließ. Eine ein Mal freigegebene Datei bleibt freigegeben, es sei denn sie verhält sich anders als sonst üblich. Was das schon angesprochene Haushalts-, Kassen- und Rechnungswesen anbelangt, bemerken die Benutzer jetzt nicht ein Mal mehr, dass im Hintergrund eine hochkarätige Sicherheitslösung ununterbrochen ihren Dienst tut. Die Code-Analyse bringt in der Verwaltung viele Vorteile mit sich. Bandbreiten sind heute zwar nicht mehr so das Thema, trotzdem spart man auch an dieser Stelle Ressourcen. Da wir jetzt darauf verzichten können in schöner Regelmäßigkeit Updates einzuspielen, haben wir sogar den anfallenenden Daten-Traffic reduziert."

Cybersicherheit ist als Anwendungsfeld für maschinelles Lernen eine verhältnismäßig junge Entwicklung. Ab etwa 2013 konnte man erste Versuche beobachten. Man wird vermutlich noch einiges an Weiterentwicklung hinsichtlich Laufzeit, Eigenschaften, Datensätzen, Mensch-Modell-

Interaktion und Anpassungsgüte erleben. Maschinelles Lernen hat seine Einsatzfähigkeit in unterschiedlichen Feldern bereits unter Beweis gestellt. Die Anwendung in der IT-Sicherheit ist allerdings vergleichsweise jung. Hier gilt es vor allem das Potenzial maschinellen Lernens für bisher noch ungelöste Cybersicherheitsprobleme auszuloten; es geht nicht nur darum verhältnismäßig simple Modelle an Cyberdatensätzen zu trainieren. Jede einzelne Generation maschinellen Lernens steht für einen qualitativen Sprung. Indem sie sich verbessern werden die Modelle nicht nur erwachsen, sie sind damit besonders wertvoll für Anwendungsfelder wie die Cybersicherheit. Dabei geht es nicht um marginale Effizienzverbesserungen. Vielmehr handelt es sich um die fundamentale Fähigkeit Angriffe sehr viel besser zu erkennen als zuvor sie (und sie) zu verhindern. Maschinelles Lernen zeigt, welcher Wert darin liegt. Das volle Potenzial für Anwendungen in der Cybersicherheit wird sich noch weiter entfalten.

Fazit

„Ich gehe jetzt mit einem deutlich ruhigeren Gewissen nach Hause, wenn ich an den Schutz unserer Clients denke. Die neue Lösung braucht deutlich weniger Rechenzeit, was sich wiederrum positiv auf die Reaktionszeiten auswirkt, sie ist einfach zu verwalten und läuft quasi geräuschlos im Hintergrund. CylancePROTECT ist für mich die erste Wahl auch wenn ich an die Administration in größeren Organisationen denke.“

Über BlackBerry Cylance

BlackBerry Cylance entwickelt künstliche Intelligenz, um präventionsorientierte, prädiktive Sicherheitsprodukte und intelligente, einfache und sichere Lösungen zu bieten, die Unternehmen einen völlig neuen Ansatz für die Endpunktsicherheit bieten. BlackBerry Cylance bietet ein umfassendes Spektrum an prädiktiver Bedrohungsabwehr und unternehmensweiter Transparenz, um die berüchtigtsten und komplexesten Cybersicherheitsangriffe abzuwehren und Endpunkte abzusichern und so Sicherheitshygiene im Sicherheitszentrum, in globalen Netzwerken und sogar in den Heimnetzen von Mitarbeitern zu fördern. Mit KI-basierter Verhinderung von Malware, Bedrohungssuche, einer automatisierten Erkennung und Bekämpfung von Bedrohungen und spezialisierten Sicherheitsdiensten schützt BlackBerry Cylance Endpunkte, ohne den Arbeitsaufwand für Mitarbeiter oder die Kosten zu erhöhen.

BlackBerry
CYLANCE

+49-89-244455571
sales@cylance.com
www.cylance.com

MKTG 18-0264-20191113