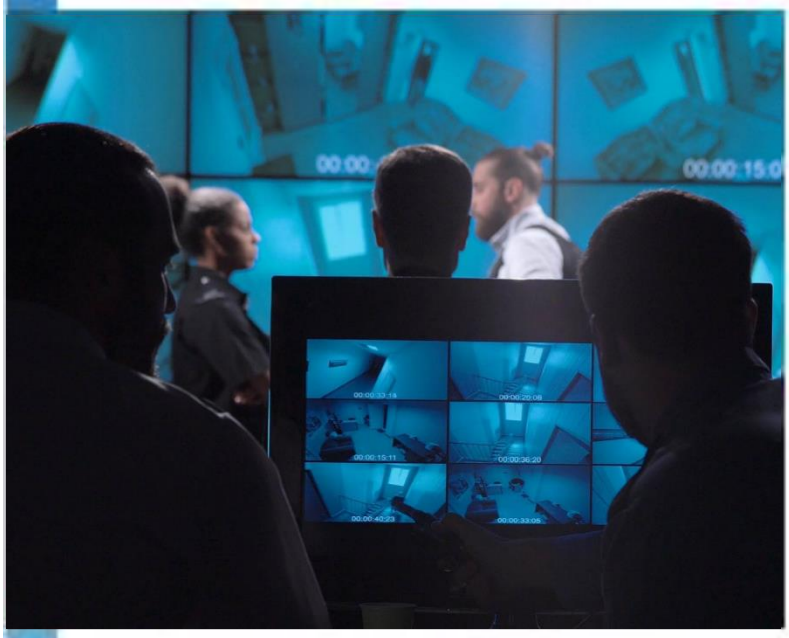
APPGUARD

Die Malware-Defensive

AppGuard wehrt polymorphe Malware-Angriffe ab, verhindert die Ausdehnung auf andere Systeme und schützt vor zukünftigen Zero-Day-Angriffen

FALLSTUDIE: BÜRO DES SHERIFFS VON MAHNOMEN COUNTY



Über das Büro:

Das Büro des Sheriffs von Mahnomen County bietet öffentliche Sicherheitsdienstleistungen für 16 Gemeinden in Minnesota an und deckt 576 Meilen innerhalb des Indianerreservats White Earth ab. Das Büro besteht aus 14 Vollzeit-Deputies, die auf eine Vielzahl von Notfällen reagieren, eingehende 9-1-1-Anrufe bearbeiten und kriminelle Aktivitäten untersuchen.

Situation:

Im Jahre 2019 war das Büro des Sheriffs von einem Malware-Angriff betroffen, der von einer anderen Bundesbehörde ausging. Nachdem er in das Netzwerk des Sheriffs gelangt war, bewegte er sich schnell, behinderte Aktivitäten und sprang schnell von einem Computer zum nächsten. Als anfängliche Versuche, die Malware zu entfernen, fehlschlugen, suchte das Büro des Sheriffs von Mahnomen County eine Cybersecurity-Lösung, mit der die Systeme schnell wieder hergestellt werden könnten und das Netzwerk gleichzeitig vor zukünftigen Angriffen geschützt würde.

HERAUSFORDERUNGEN:

- Schutz vor fortschrittlichen Cyber-Angriffen
- Gewährleisten, dass kritische Systeme effektiv arbeiten, um die Bürger zu schützen

ERGEBNISSE:

- Malware, die das Antivirus-Tool umgehen konnte, wurde eingegrenzt und die Ausbreitung verhindert
- Kosteneinsparungen aufgrund des Rückgangs der IT-Serviceanforderungen und der Säuberungsmaßnahmen
- Mehr Sicherheit mit weniger Aufwand
- Schutz vor zukünftigen fortschrittlichen Angriffen, einschließlich Zero Day

Herkömmliche Antivirus-Tools konnten den Angriff nicht vereiteln

Als mehr über das Ausmaß des Malware-Angriffs bekannt wurde, war klar, dass die vom Büro des Sheriffs verwendete herkömmliche, signaturbasierte Antivirus-Software auf ganzer Linie versagt hatte. Das ist nicht überraschend, da herkömmliche Antivirus-Lösungen typischerweise von einer zuvor verbreiteten Datenbank mit bekannten Angriffsvektoren abhängen. Diese Datenbanken sind häufig nicht auf dem neuesten Stand und wenn sie das sind, sind sie nicht in der Lage, sich gegen nie dagewesene Zero-Day-Angriffe zu wehren. Dadurch sind sie weitgehend ineffektiv und nicht gut als Schutz vor den heutigen, sich schnell entwickelnden Cyber-Bedrohungen geeignet.

Unglücklicherweise traf das auf das Büro des Sheriffs von Mahnomen Country zu. Die Malware verfügte über eine nicht erkannte Signatur, die nicht in der Datenbank der Antivirus-Lösung existierte. Dadurch wurde das Büro des Sheriffs

> *Als AppGuard installiert war, konnten wir sagen, dass die Computer isoliert und geschützt waren, denn wir konnten beobachten, dass die Malware erfolglos versuchte, wieder in die Maschine zu gelangen.*
>
> *-- Josh Guenther, Sheriff in Mahnomen County*

in einen hochgradig reaktiven Modus gezwungen, als sich die Malware ihren destruktiven Pfad bahnte und sogar versuchte, auf Bankdaten und andere private Informationen zuzugreifen. Das IT-Team des Büros des Sheriffs wurde aktiv, führte fortlaufend Scans durch und säuberte infizierte Maschinen. Jedoch erwies es sich als unmöglich, die Malware in Schach zu halten und diese nahm auf ihrem Weg durch das Netzwerk verschiedene Formen an.

Ein zum Scheitern verurteiltes Katz-und-Maus-Spiel

Ein erster Scan ergab, dass vier Maschinen infiziert waren, was dem Büro des Sheriffs Hoffnung machte, dass das Virus schnell zu stoppen sei. Die IT-Mitarbeiter säuberten alle Maschinen in der Abteilung, in der Sorge, dass sich das Virus auf kritische Server ausbreiten könnte, die öffentliche Dienstleistungen und Sicherheit unterstützen, darunter auch 9-1-1-Ausstattung. Trotz dieser Anstrengungen wurde ein sauberes System jedes Mal, wenn es an das Netzwerk angeschlossen wurde, schnell neu infiziert, wobei das Virus auf neue Endpunkte übersprang. Dieses Katz-und-Maus-Spiel dauerte länger als drei Wochen an und die Maschinen wurden nur Stunden nach der Säuberung neu infiziert. „Wir haben die Maschinen ständig neu aufgesetzt, aber die Malware sprang immer wieder hervor und von einer Maschine zur nächsten," sagte Josh Guenther, Sheriff in Mahnomen County.

Malware behinderte die County-Aktivitäten

Von der Annahme eingehender Anrufe bis hin zur Reaktion auf Notfälle vor Ort - viele der alltäglichen Aktivitäten des Büros des Sheriffs hängen von computerbasierten Anwendungen ab. Die Auswirkungen des Virus waren weitreichend und behinderten die Möglichkeiten der Mitarbeiter, mit anderen staatlichen und benachbarten Behörden zu kommunizieren und verhinderten, dass kritische Informationen wie Haftbefehle in der Datenbank der Behörde erfasst werden konnten. Um die kritischen Dienste aufrechtzuhalten, musste das Büro des Sheriffs die 9-1-1-Einsatzaktivitäten in einen benachbarten Bezirk auslagern.

Lösung

Um den Betrieb wiederherzustellen und zukünftigen Schaden zu verhindern, entschied sich das Büro des Sheriffs von Mahnomen County für die fortschrittliche Cybersecurity-Lösung von AppGuard, die vor der Kompromittierung eingreift und vor neu aufkommenden und einzigartigen Angriffen schützt, die von herkömmlichen, erkennungsbasierten Cybersecurity-Methoden häufig übersehen werden. Die patentierte „Zero-Trust"-Isolierungstechnologie von AppGuard geht davon aus, dass Endpunkte unbekannte Sicherheitslücken aufweisen könnten, die missbraucht werden können, oder sogar zuvor unerkannte fortgeschrittene residente Infektionen enthalten. Die Technologie verhindert alle nicht regelkonformen Aktionen auf Prozessebene, um das System vor allen Arten von Angriffen zu schützen. Da AppGuard sich nicht auf das Scannen nach bekannten Signaturen oder Mustern verlässt, um gute von schlechten Dateien zu unterscheiden, bietet die Lösung Schutz, ohne dass ständig gepatcht werden muss.

AppGuard erkannte die Malware sofort und grenzte sie ein

Da AppGuard Netzwerke isoliert und schützt, sogar solche mit bereits infizierten Systemen, installierte das Büro des Sheriffs die Lösung umgehend auf allen Systemen. Innerhalb der ersten fünf Stunden isolierte AppGuard die Malware und hielt sie machtlos im Inneren einer jeden infizierten Workstation fest. Somit wurde das Virus davon abgehalten, sich auszubreiten oder schädliche Prozesse auszuführen. „Als AppGuard installiert war, konnten wir sagen, dass die Computer isoliert und geschützt waren, denn wir konnten beobachten, dass die Malware erfolglos versuchte, wieder in die Maschine zu gelangen," sagte Guenther. „Die Malware war, nachdem sie von AppGuard unter Quarantäne gestellt und isoliert worden war, nutzlos und von dem Ökosystem abgeschnitten, das sie zum Ausführen ihrer Aktivitäten brauchte." Durch AppGuard konnte das Büro des Sheriffs die Arbeit wieder aufnehmen, während die Malware davon abgehalten wurde, ihr Vorhaben auszuführen. AppGuard sorgt für die Sicherheit des Bezirks in dem Wissen, dass die Endpunkte nicht mehr kompromittiert werden können.

Über AppGuard

AppGuard ist ein Cybersecurity-Unternehmen, das es sich zur Aufgabe gemacht hat, einen neuen Standard zu setzen: echter Cyber-Schutz für alle. Die patentierte Technologie von AppGuard verhindert Kompromittierungen, bevor sie geschehen, indem sie Malware-Aktivitäten daran hindert, Schaden anzurichten, ohne sie wiederkennen zu müssen. Im Gegensatz zu erkennungsbasierten Lösungen überlistet AppGuard böswillige Akteure, damit Unternehmen ihren Aufgaben nachgehen können und die Schadsoftware nicht machen kann, was sie will.

APPGUARD

Die Malware-Defensive

www.appguard.us | software@ingrammicro.ch