infopulse

EDR-Implementierung des Microsoft Defender for Endpoint für ATB-Market_

Kunde: **ATB-Market** Branche: **Einzelhandel** Ort: **Ukraine**

Mitarbeiter: **60,000+** Website: **www.atbmarket.com/en**

Über den Kunden

ATB-Market ist das größte Einzelhandelsunternehmen in der Ukraine und ist auf die Produktion und den Verkauf von Lebensmitteln und anderen wichtigen Gütern spezialisiert. Die Einzelhandelskette unseres Kunden umfasst mehr als 1200 Lebensmittelläden in 24 Regionen der Ukraine, die täglich von mehr als 4 Millionen Kunden besucht werden. Das Unternehmen sichert sich mit seinem Konzept für Logistik, Qualitätskontrolle und Kundenservice seine Position als führender Einzelhändler der Ukraine hinsichtlich des Lagerumschlags, der gezahlten Einkommenssteuer und der Anzahl der Kunden.

Anforderung

Infopulse blickt auf eine langjährige Zusammenarbeit mit dem ATB-Markt zurück, zu der auch eine vorangegangene Pilotimplementierung von Microsoft Sentinel und andere gemeinschaftliche IT-Projekte gehören. In diesem Fall hat sich der Kunde entschieden, eine Endpoint Detection & Response (EDR)-Lösung zu implementieren und damit eine zuverlässige Sicherheit sowohl für unternehmenseigene als auch für private Mitarbeitergeräte zu gewährleisten, die außerhalb des Unternehmensnetzwerks genutzt werden.

ATB-Market hat Infopulse um eine Sicherheitsberatung gebeten, um die perfekte EDR-Lösung auszuwählen, die für verschiedene Betriebssysteme geeignet ist und verschiedene grundlegende geschäftliche Herausforderungen bewältigen kann, wie z. B:

- die allgemeine Sicherheitslage des Unternehmens zu stärken, indem tote Winkel beseitigt und die Angriffsfläche deutlich reduziert werden
- das proaktive Aufspüren und Verhindern von hochentwickelten Cyberbedrohungen, die von Antivirenprogrammen und Firewalls nicht erkannt werden können
- den effektiven Schutz einer großen Anzahl von Unternehmens- und BYOD-Endpunkten für Mitarbeiter, die von verschiedenen Standorten in der Ukraine und im Ausland aus arbeiten

Lösung

Mit der Erkenntnis, dass EDR zwar wichtig ist, aber für einen umfassenden Schutz vor den sich entwickelnden Cyberbedrohungen nicht ausreicht, ermutigte Infopulse ATB-Market, die Implementierung einer Extended Detection & Response (XDR) Lösung in Betracht zu ziehen. Unser Team schlug vor, Microsoft Defender for Endpoint zu testen. Diese integrierte Sicherheitsplattform für Endpunkte bietet fortschrittliche ML-gesteuerte Verhaltensanalysen, leistungsstarke digitale Forensik und intelligente Automatisierung.

Das Projekt begann mit einem Einführungsworkshop, im Rahmen dessen Infopulse den Kunden mit Microsoft Defender for Endpoint und dessen wichtigsten Funktionen vertraut machte. Daraufhin führten unsere Experten einen kurzen PoC auf ihren Laptops durch, um zu demonstrieren, wie die Lösung funktioniert und um zu gewährleisten, dass sie den Geschäftsanforderungen des Kunden entspricht.

Die nächste Phase umfasste eine Reihe von Testfällen, um zu prüfen, ob Microsoft Defender für Endpoint die erwarteten technischen Anforderungen erfüllte. In enger Zusammenarbeit mit ATB-Market hat Infopulse eine Versuchsgruppe von Benutzern mit Firmengeräten zusammengestellt und zahlreiche Testfälle entwickelt, um die Leistung der Lösung unter Windows 10/11, macOS und Linux zu bewerten. Außerdem entwarf unser

Team einen Testfall für die automatische Bereitstellung der Lösung auf Microsoft Intune - einem Cloud-basierten Dienst für die Verwaltung mobiler Geräte (MDM).

Infopulse führte nicht nur herkömmliche Testfälle durch, sondern auch eine Reihe von simulierten Cyberangriffen, um das etablierte Endpunkt-Verteidigungssystem zu bewerten, den vollen Umfang der XDR-Funktionen in der Praxis zu demonstrieren und dem Kunden zu helfen, potenzielle Cyberrisiken zu vermeiden, indem reale Angriffsszenarien demonstriert wurden.

Nach dem erfolgreichen Durchlaufen aller Testaktivitäten bestand für ATB-Market kein Zweifel mehr daran, dass Microsoft Defender for Endpoint die beste Lösung für das Unternehmen war. Deshalb begann Infopulse mit der umfassenden Implementierung der Lösung für die Einzelhandelskette. Das Ergebnis war eine hochmoderne XDR-Plattform mit einem breiten Spektrum an wertvollen Funktionen:

- Zwei mögliche Betriebsmodi für Laptops, Tablets und Smartphones - ohne Agent für Windows 10/11 und mit Agent für macOS, Linux, iOS und Android
- Eine umfassende Analyse des Benutzerverhaltens, die anomale Aktivitäten wie unbefugte Zugriffsversuche, versteckte Skripts oder beschädigte Dateien schnell aufdeckt
- Digitale Forensik, die komplexe schädliche Muster sammelt, verarbeitet und untersucht, inklusive dateiloser Bedrohungen, die im Random Access Memory (RAM) gestartet werden
- Eine vollständige Automatisierung verschiedener Sicherheitsabläufe, darunter Threat Intelligence, Dateiprüfungen, Übertragung in die Quarantäne, Blockierung kompromittierter Kommunikationskanäle usw.
- Ein halbautomatischer Modus, bei dem die Lösung automatisch Sicherheitsanalysen durchführt und die Ergebnisse an die jeweiligen Experten meldet, bevor eine Datei oder ein Prozess blockiert wird
- Das Herausfiltern und Kontrollieren von Webinhalten durch Kategorie-basierte URL-Sperrung
- Funktionen zur Netzwerkabsicherung und ein integrierter Scanner für Sicherheitslücken im Netzwerk - Qualys
- Die Bewertung von Schwachstellen der auf den Endpunkten installierten Software, einschließlich Benachrichtigungen über wichtige Sicherheitspatches/Aktualisierungen.

Zur weiteren Verstärkung der Sicherheitsmaßnahmen des Kunden boten unsere Spezialisten an, Microsoft Defender for Endpoint in das SIEM-Tool des Kunden, IBM QRadar, zu integrieren. Die Kombination von XDR und SIEM ermöglichte ATB-Market eine zentralisierte Echtzeit-Bedrohungserkennung über alle Angriffsvektoren hinweg.

Um die Lernkurve für die Sicherheitsexperten des Kunden abzuflachen, veranstaltete Infopulse mehrere Schulungen, um sie bei der Konfiguration und Beherrschung der digitalen Forensik, der Berichterstattung und anderer Funktionen zu unterstützen.

Technologien

Microsoft Defender für Endpoint

Qualys

Ergebnis

Fazit: Die Implementierung von Microsoft Defender for Endpoint zusammen mit den zusätzlichen maßgeschneiderten Leistungen hat ATB-Market geholfen, bestehende Kompetenzlücken zu schließen, die Widerstandsfähigkeit im Netz zu erhöhen und die folgenden Vorteile für die Einzelhandelskette zu erzielen:

- Zuverlässiger Rund-um-die-Uhr-Schutz von mehr als 1.500 Unternehmens- und BYOD-Endpunkten gegen alle Arten von Cyberrisiken
- ML-gestützte Analyse des Nutzerverhaltens, die jegliche Anomalien präzise erkennt und so potenzielle Cyberangriffe oder Insider-Bedrohungen verhindert
- Eine automatisierte Untersuchung von Vorfällen und eine Reaktion darauf, welche die Ausrichtung auf komplexere Bedrohungen oder andere wichtige strategische Aufgaben ermöglicht
- Eine minimale Lernkurve und eine verbesserte Bereitschaft, anspruchsvolle Sicherheitslücken zu entschärfen und zu bekämpfen
- Dank der detaillierten Analyse der Bedrohungsdaten kann das Sicherheitsteam des Kunden die bestmöglichen Maßnahmen zur Behebung der Bedrohung festlegen und Fehlalarme reduzieren.

Über Infopulse

Infopulse, Teil des führenden nordischen, digitalen Dienstleistungs-Unternehmens Tietoevry, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Software-F&E, Anwendungsmanagement, Cloud- und IT-Betrieb sowie Cybersicherheit für KMUs und Fortune 100 Unternehmen auf der ganzen Welt. Das in 1991 gegründete Unternehmen verfügt über ein Team von über 2,300 Fachleuten und ist weltweit in 7 Ländern - in Europa sowie in Nord-, Mittel- und Südamerika - vertreten.

Infopulse genießt das Vertrauen vieler etablierter Marken wie BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Norwegian Oil and Gas Association, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group und vieler anderer.

Für weitere Informationen besuchen Sie bitte **www.infopulse.com/de**

Kontaktieren sie uns:

PL +48 (221) 032-442

DE +49 (69) 505-060-4719

US +1 (888) 339-75-56

UK +44 (8455) 280-080

UA +38 (044) 585-25-00

BG +359 (876) 92-30-90

BR +55 (21) 99298-3389

info@infopulse.com