



Success Story

MDR Managed Service

Keine Datenlecks bei schweizerischem Gesundheitsdienstleister

Omicron AG
Industriestrasse 50b
Postfach
8304 Wallisellen
Schweiz

Telefon +41 44 839 11 11
Fax +41 44 839 11 00
E-Mail mail@omicron.ch
Web <https://www.omicron.ch>



Moderne IT-Sicherheit, proaktiv geschützt – rund um die Uhr

Mit der Einführung von Managed Detection & Response (MDR) Services, basierend auf einer marktführenden Lösung für Endpunktschutz, konnte ein schweizerischer Gesundheitsdienstleister bessere Transparenz seiner IT-Infrastruktur und schnellere Reaktionszeiten erzielen. Dank der 24/7-Überwachung konnte ein potenzieller Sicherheitsvorfall eines damaligen Mitarbeiters frühzeitig erkannt, analysiert und gestoppt werden – ohne Auswirkungen auf Patienten oder Betrieb.

Zunehmende Risiken zwingen zum ständigen Schritt halten

Der regionale mittelständische Dienstleister ist seit knapp einem Jahrhundert eine feste Grösse in der schweizerischen Gesundheitsversorgung. Neben dem Wohl seiner Patienten hat er zugleich einen hohen Anspruch an die Sicherheit seiner digitalen Infrastruktur sowie der sensiblen Patienten- und Unternehmensdaten. Zusammen entschieden Geschäftsleitung und IT-Abteilung, dass es aufgrund der sich wandelnden und zunehmenden Cyberrisiken notwendig sei, die bestehenden Sicherheitsmassnahmen weiterzuentwickeln und die IT-Security neu auszurichten.

Wie bei vielen vergleichbaren Einrichtungen war beispielsweise die Endpunktsicherheit über die Jahre hinweg funktional aufgebaut worden, jedoch nicht zentralisiert. Eine ganzheitliche Sicht auf Endgeräte und Netzwerkdaten war so nur eingeschränkt möglich. Auch die Prozesse zur Bearbeitung von sicherheitsrelevanten Ereignissen erfolgten bislang manuell. Mit Blick auf heutige Anforderungen an Geschwindigkeit, Automatisierung und Rund-um-die-Uhr-Verfügbarkeit war dieser Ansatz jedoch nicht mehr ausreichend.

Es sollte unter anderem neu eingeführt werden:

- ein durchgängiges 24/7-Monitoring für Endpunkte und Netzwerkdaten
- direkte komplette Incident-Analyse mit Triage und Kundenalarmierung bei Verdacht auf echten Angriff
- automatisierte Prozesse für raschere Reaktionsgeschwindigkeit
- sichere Integration von Netzwerk-, Benutzer- und Cloud-Datenquellen wie Firewalls, Active Directory und M365
- eine Anpassung der Netzwerksegmentierung zum Minimieren potenzieller Angriffsflächen
- vereinheitlichtes und automatisiertes Patch- und Update-Management



Der IT-Verantwortliche beim Gesundheitsdienstleister begrüsst die Zusammenarbeit:

«Mit den Managed Services von der Omicron AG haben wir unsere Sicherheitsprozesse gestärkt, mit einem Partner, der nicht nur technologisch, sondern auch menschlich überzeugt. Heute sehen wir Sicherheitsvorfälle, bevor sie zum Problem werden.»



Eine Lösung wurde gesucht, welche sowohl Sichtbarkeit als auch Reaktionszeit verbesserte. Ohne zusätzliches Personal aufbauen und ausbilden zu müssen, war dies nur mit Automatisierung, Machine Learning Kapazitäten und Managed Services möglich.

Die Lösung: MDR – Managed Detection & Response

Die Entscheidung fiel daher auf eine leistungsstarke MDR-Lösung eines führenden Sicherheitsanbieters, professionell betreut durch die Omicron AG. Mit diesem Modell profitiert der Anbieter aus dem Gesundheitswesen von durchgehender Transparenz, ressourcensparender Automation und aktivem Schutz.

Im Juni 2023 startete der Gesundheitsdienstleister mit dem gemanagten MDR-Service. Das Ziel war klar definiert: ganzheitlicher Schutz der Endgeräte, zentrale Sichtbarkeit über das Netzwerk sowie sofortige Reaktionsmöglichkeit bei Sicherheitsvorfällen.

Das Projekt startete mit einem Kickoff-Workshop und dem Baselineing-Prozess, in dem die Infrastruktur konfiguriert, angepasst und optimiert wurde. Dabei wurden in der Einrichtungsphase beispielsweise Best-Practices-Regeln aktiviert, Detection Rules eingerichtet und False Positives systematisch reduziert.

Zusätzlich erfolgte die Anbindung folgender kritischer Datenquellen:

- Microsoft Active Directory
- Palo Alto Networks Firewall
- Microsoft 365
- DHCP

Die Omicron AG konnte diese unterschiedlichen Quellen in einen zentralen Speicher integrieren, um vollständige Erkennungsmuster zu generieren.

Für den laufenden Betrieb übernahm die Omicron AG die komplette Incident-Triage, inklusive:

- Incident Analyse
- Eskalation an definierte Kontakte
- Endgeräte-Isolation bei True Positives
- Regelpflege und kontinuierliche Verbesserung der Detection Logic (Erkennungslogik)

Der Gesundheitsdienstleister erhielt Vollzugriff auf das Web-Interface der MDR-Plattform sowie wöchentliche Reports. Updates und Health Checks wurden laufend im Rahmen des Managed Service übernommen.



Zum Jahresende 2024 zeigte sich die Wirksamkeit des MDR-Services deutlich:

Ein ungewöhnlicher 1 GB Upload eines gekündigten Mitarbeiters wurde rechtzeitig erkannt – obwohl der Vorfall nur als Low-Severity (geringer Schweregrad) eingestuft war. Der Fall wurde schnell analysiert, gemeldet und intern eskaliert. Es wurden geeignete firmeninterne Massnahmen ergriffen, wodurch ein potenzieller Schaden – sowohl für das Image als auch wirtschaftlich – rechtzeitig verhindert werden konnte.

Proaktive Abwehr – mit weniger Aufwand und mehr Kontrolle

Mit den Cyber Care Services - managed by Omicron konnte der Gesundheitsdienstleister ein ganzheitliches und proaktives Rund-um-die-Uhr-Monitoring für die zahlreichen Endpunkte und Netzwerkdaten einführen – ohne zusätzlich intern Personal aufbauen zu müssen.

Ein weiterer wesentlicher Vorteil liegt in der durchgängigen Transparenz: Sämtliche sicherheitsrelevanten Aktivitäten auf Endpunkten und in verbundenen Netzwerkquellen werden in einer gemeinsamen Plattform zusammengeführt und analysiert. Dadurch entsteht ein ganzheitliches Lagebild, das es ermöglicht, potenzielle Risiken und deren Quellen frühzeitig zu erkennen und gezielt zu handeln.

Dank automatisierter Analyse- und Reaktionsmechanismen ist die Reaktionszeit auf Vorfälle erheblich gesunken. Auffälliges Verhalten kann rechtzeitig identifiziert, eingeordnet und - falls notwendig - eingedämmt werden. Die manuelle Bearbeitung von Incidents (Vorfällen) reduziert sich auf ein Minimum.

Die wichtigsten Vorteile auf einen Blick:

- 24/7-Überwachung & automatische Reaktion bei Bedrohungen
- Minimierung von False Positives durch präzises Baselining
- Konsolidierung von Datenquellen: Integration von Firewall-, AD- und O365-Daten in ein zentrales System
- Transparente Reports für IT und Management
- Kontinuierliche Verbesserung durch laufende Regelpflege und Empfehlungen zur Systemoptimierung
- Schweizer Hosting für höchste Datenschutzerfordernungen
- Gleichzeitiger Kundenzugriff für volle Transparenz



Die Kombination von marktführender Technologie, erprobten Prozessen und professionellem persönlichem Support ermöglicht eine erstklassige, leistungsfähige Sicherheitsarchitektur mit maximaler Kontrolle und minimalem Aufwand für die interne IT des Gesundheitsdienstleisters. So kann sich dieser vollumfänglich und ohne Unterbruch um die Gesundheit und das Wohlbefinden seiner Patienten kümmern.

Über Omicron AG

Seit 1995 ist die Omicron AG, mit Sitz in Wallisellen, Bern und Appenzell, auf IT-Sicherheits- und Netzwerklösungen für Unternehmen spezialisiert und deckt alle Bedürfnisse von A bis Z ab. Das erfahrene Team bietet bedarfsgerechte Lösungen in Bereichen wie Endpunkt- und Netzwerksicherheit, Intrusion Prevention, Sandboxing, NAC, Pentesting und Network Monitoring – auch als Managed Cyber Care Services.

Zu den Kunden zählen führende Banken, Versicherungen, Industriebetriebe, Energiedienstleister, Transportunternehmen, Hochschulen, Krankenhäuser und Behörden.

Dank Fachkompetenz, modernsten Sicherheitsprodukten und starken Partnerschaften profitieren Omicron AG Kunden von maximalem Schutz, langfristigen Lösungen, fairen Konditionen und massgeschneiderten Services.

Omicron AG
Industriestrasse 50b
Postfach
8304 Wallisellen
Schweiz

Telefon +41 44 839 11 11
Fax +41 44 839 11 00
E-Mail mail@omicron.ch
Web <https://www.omicron.ch>