Omicron Seit 1995

Success Story

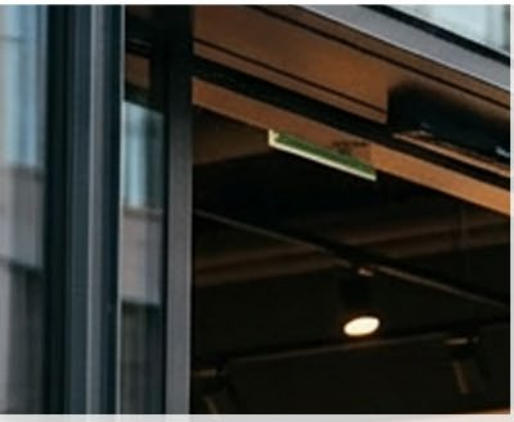
Managed IT-Security Services

Mehr Sicherheit, weniger Aufwand: Die **mobilezone ag** stärkt ihre Cyber-Defense

mobilezone

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



Von Sicherheits-Silos zur ganzheitlich gemanagten Sicherheitslösung

Die Schweizer Telekommunikationsspezialistin **mobilezone ag** ersetzte ihre eigenständigen Sicherheitslösungen durch einen umfassend betreuten Service, welcher Firewall, Managed Detection and Response (MDR) sowie die automatisierte Sicherheitsvalidierung adressiert. Dank der Zusammenarbeit mit der Omicron AG verfügt das Unternehmen heute über eine rund um die Uhr überwachte IT-Landschaft, ein deutlich entlastetes Team, kürzere Reaktionszeiten und eine bessere Bedrohungserkennung.

Komplexe Bedrohungslage trifft begrenzte Ressourcen

Die mobilezone ag ist die führende unabhängige Telekommunikationsspezialistin der Schweiz. Über 125 Filialen und der hauseigene Webshop bieten Privat- und Geschäftskunden ein umfassendes Produkt- und Service-Sortiment. Dieses reicht von Mobilgeräten über TV und Internet bis zu Enterprise-Lösungen wie Device as a Service sowie Reparatur- und Buyback-Programmen. Insgesamt beschäftigt das Unternehmen knapp 1'000 Mitarbeiter und ist an der Schweizer Börse SIX kotiert.

Obwohl bereits eine Reihe von leistungsfähigen Security-Werkzeugen wie eine Extended Detection and Response (XDR) Lösung zum Endpunktschutz im Einsatz waren, blieben zentrale Herausforderungen bestehen:

- **Zunehmende Bedrohungsszenarien:** Entwicklungen wie Large Language Models (LLMs) und Malware as a Service senkten die Einstiegshürden für Cyberangriffe und machten diese zugleich raffinierter. Dadurch rückten auch mittelständische Unternehmen zunehmend ins Visier.
- **Fragmentierte Sicherheitsarchitektur:** Verschiedene Sicherheitstools ohne durchgängige Integration verhinderten eine vollständige und rasche Sicht auf mögliche Bedrohungslagen.
- **Personelle Ressourcen:** Immer komplexere Sicherheitsprodukte und ständig neue Angriffsmuster erforderten zunehmend spezialisiertes Fachwissen für wirksames Incident Management. Die bestehende IT sah sich durch das Tagesgeschäft stark gefordert. Dadurch waren die Möglichkeiten für laufenden Wissensaufbau wie auch für umfassende Reaktionen auf neue Bedrohungen zunehmend begrenzt.

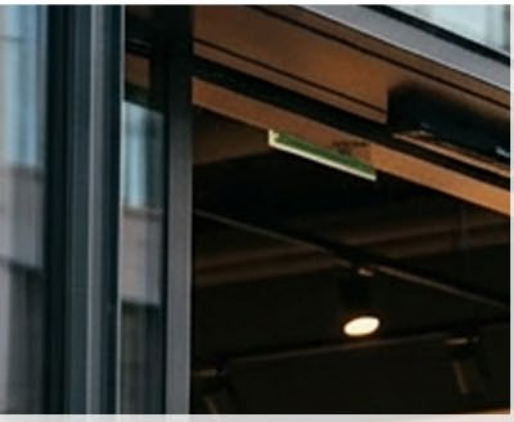
Das mobilezone Security-Team stand vor der Aufgabe, den Geschäftsbetrieb zielführend und verlässlich sicherzustellen – ohne dabei personelle Kapazitäten aufzustocken. Zur gleichen Zeit erlaubten die Umstände keinen intensiven spezialisierten Know-how-Aufbau im bestehenden Team. mobilezone suchte daher eine Lösung, die nicht nur Technologien bereitstellt, sondern aktive Unterstützung, tiefes Expertenwissen und echte Entlastung im Betrieb bietet.

Managed Services – mehr als nur Softwarelizenzen

Die Entscheidung fiel auf die Cyber Care Services der Omicron AG: umfassende gemanagte Services, die weit über die reine Beschaffung von Technologie hinausgehen. Durch die Kombination und den abgestimmten Einsatz von

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



«Mit der Omicron AG haben wir unsere Security nicht nur technisch optimiert, sie betreibt den Service auch mit grosser Fachkompetenz. Für uns bedeutet das: weniger Aufwand, mehr Schutz und mehr Ruhe im Tagesgeschäft.»

Fritz Hauser, Director IT Security & Governance, mobilezone ag

branchenführenden Security-Produkten konnte die Omicron den laufenden Betrieb wie folgt unterstützen:

Leistungsstarke Bedrohungserkennung mit MDR Managed Service

mobilezone setzte bereits eine gute Extended Detection & Response (XDR) Lösung ein, stellte jedoch fest, dass zunehmend komplexere Bedrohungsszenarien auch zusätzliche personelle Ressourcen für die Detailanalyse erforderten. Ziel war es, die Visibilität zu erhöhen, Analysen zu beschleunigen und damit die Reaktionsfähigkeit für sicherheitsrelevante Ereignisse zu verbessern.

Um sich für die wichtigen Themen im Tagesgeschäft freizuspielen, übertrug mobilezone die routinemässige Betreuung, die Wartung und Optimierung an die Omicron. Als Managed Security Service Provider (MSSP) übernahm die Omicron den vollständigen operativen Betrieb der XDR-Lösung inklusive 24/7 Monitoring aller angebundenen Endpunkte, Triage und Analyse verdächtiger Aktivitäten. Damit erhält die mobilezone IT-Abteilung nur noch sicherheitsrelevante, vorqualifizierte Alerts. Bei Bedarf und nach Abstimmung isoliert die Omicron betroffene Systeme, übernimmt das Änderungsmanagement und sorgt für regelmässige Updates.

Trotz ausgelagerter Betriebsverantwortung behält das interne mobilezone Team vollen Zugriff auf die Plattform – mit allen Funktionen und Daten. Die Aufgabenteilung schont Budget und Ressourcen.

Firewall-Upgrade und -Betrieb: alles aus einer Hand

Im Zuge wachsender Anforderungen an den Datendurchsatz entschied sich mobilezone zudem für ein Firewall-Upgrade auf eine leistungsfähigere Lösung. Dieses Umsetzungsprojekt wurde reibungslos und unterbrechungsfrei mit der Omicron durchgeführt.

Da das mobilezone Team im täglichen Betrieb für zahlreiche Aufgaben zuständig war, wurde entschieden, die internen Ressourcen strategisch gezielt einzusetzen und das Firewall Management in die Hände eines erfahrenen Partners zu legen.

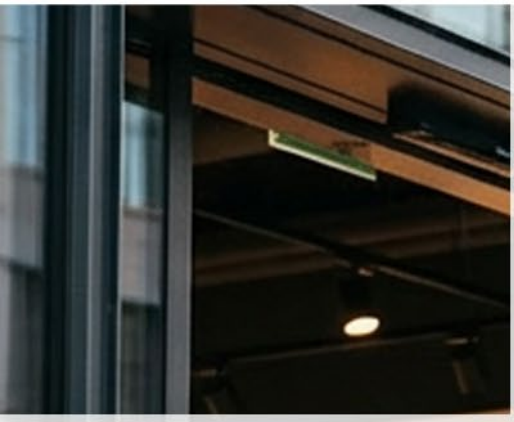
Zu Beginn der Betriebsübernahme wurde die Firewall zunächst gemeinsam und systematisch überarbeitet. Dazu zählten die Vereinheitlichung von Namenskonventionen, eine Analyse und Optimierung der Sicherheitsrichtlinien sowie eine gründliche Überarbeitung bestehender Konfigurationen.

Heute betreut die Omicron die gesamte Firewall-Infrastruktur: von der Systemhärtung über den regulären Betrieb, das Umsetzen von Changes, Analysen und Updates bis hin zum Incident-Handling. Weitere proaktive Massnahmen wie das Einspielen von Emergency-Patches, das Monitoring von Systemgesundheit, Zertifikaten und IT-Assets sowie das RMA-Handling und die Subscription-Verwaltung gehören ebenfalls zum Leistungsumfang.

Da neben den Managed Firewall Services auch der MDR-Service über die Omicron läuft, kann das eingespielte und erfahrene Team die gesamte Incident Response aus einer Hand abdecken – schnell, korreliert, koordiniert und mit hoher Präzision.

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



Pentesting und laufende Betreuung der Sicherheitsvalidierung

Um das eigene Sicherheitssetup einer kritischen Prüfung zu unterziehen und den aktuellen Status Quo zu ermitteln, beauftragte mobilezone die Omicron zunächst damit, mit einer branchenführenden Plattform den initialen Penetrationstest durchzuführen. Ziel war es herauszufinden, welche Angriffsmöglichkeiten ein externer Angreifer in der aktuellen Infrastruktur aktiv nutzen könnte. Die Durchführung erfolgte agentenlos, vollständig On-Premise und mit realen, ethischen Angriffstechniken – im Gegensatz zu rein hypothetischen Szenarien.

Die Ergebnisse bestätigten ein insgesamt hohes Schutzniveau, zeigten jedoch auch Optimierungspotenziale auf. Basierend auf den Empfehlungen wurden gezielte Massnahmen zur Schliessung der identifizierten Schwachstellen abgeleitet.

Im Anschluss entschied sich mobilezone, das Testing in den regulären Betrieb zu überführen und künftig regelmässig automatisierte Penetrationstests einzusetzen. Die Omicron übernahm nicht nur das technische Onboarding, sondern wurde darüber hinaus auch mit dem operativen Betrieb der Pentestinglösung betraut. Zu den laufenden Leistungen zählen unter anderem die Wartung der Plattform, regelmässige Updates, die Einführung neuer Funktionen sowie die halbjährliche Überprüfung der aktuellen Angriffsszenarien.

mobilezone erhält regelmässig strukturierte Berichte und wird auch im Rahmen von Review-Meetings über aktuelle Sicherheitsbewertungen und -empfehlungen informiert. Zusätzlich unterstützt die Omicron bei der Analyse von Testergebnissen sowie bei der Umsetzung empfohlener Massnahmen.

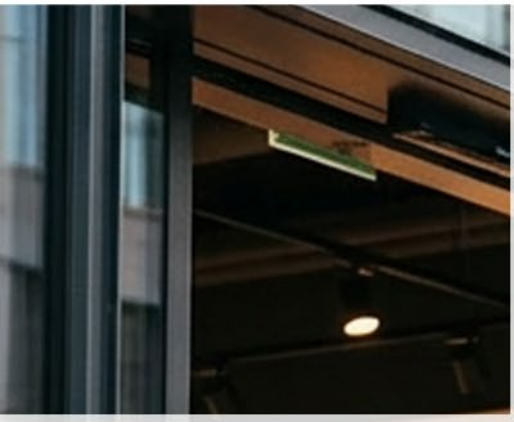
Mehr Schutz und schnellere Reaktion bei weniger internem Aufwand

Durch den Wechsel zu den *Cyber Care Services – managed by Omicron* profitiert mobilezone gleich mehrfach:

- ✓ **Gestärkte Security Posture** deckt Schwachstellen auf, bevor sie ausgenutzt werden können.
- ✓ **Mehr Sichtbarkeit und schnellere Angriffserkennung** dank Integration verschiedener Security-Tools und enger, fachübergreifender Zusammenarbeit beim MSSP.
- ✓ **Angriffsflächen** werden **laufend minimiert**, dank kontinuierlicher Optimierung und Best-Practice.
- ✓ **Erhebliche Zeitersparnis**: Zeitintensive Routineaufgaben und tägliche Analysen sind ausgelagert. Es werden nur relevante Alerts an den Kunden gemeldet, die nicht durch den MSSP selbst gelöst werden können.
- ✓ **Kein interner Mehraufwand** für Rekrutierung, Einsatzplanung und Weiterbildung eigener Mitarbeiter für spezialisierte Anwendungen. Erfahrene MSSP-Experten der Omicron mit kontinuierlicher Weiterbildung konfigurieren und betreiben aktuellste Security-Tools optimal und zuverlässig.

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



- ✓ **Jederzeit überprüfbar**: Zusätzlich zu regelmässigen Leistungsreports verbleibt der Lese- oder Vollzugriff auf alle Security-Tools beim Kunden.
- ✓ **Messbare Wirksamkeit** erleichtert den transparenten Leistungsnachweis ans Management mit regelmässigen Reports und unbeschränktem Einblick in forensische Daten.
- ✓ **Relevante Verbesserungen** werden aus den Findings proaktiv erarbeitet und in Abstimmung mit dem Kunden umgesetzt.
- ✓ **Planbare Kosten** dank transparentem, fairem und flexiblem Security as a Service (SECaaS) Subscription-Modell.

Starke Sicherheit mit einem starken Partner

Durch die Zusammenarbeit mit der Omicron konnte mobilezone die Weiterentwicklung ihrer Sicherheitsstrategie gezielt und zeitgerecht umsetzen. Die Einführung der *Cyber Care Services – managed by Omicron* brachte nicht nur eine deutlich höhere Transparenz über die gesamte IT-Landschaft, sondern auch spürbare Entlastung im Tagesgeschäft. Dank professioneller operativer Unterstützung kann mobilezone Angriffe nun noch schneller erkennen und gezielt eindämmen, bevor Schaden entsteht. Statt Insellösungen gibt es heute übergreifende, intelligent vernetzte Security-Plattformen mit umfassendem MSSP-Service. Ein klarer Gewinn für effizienten Mitteleinsatz und grösstmögliche Sicherheit.

Über die 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 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