

Kunde: **Telekommunikationsanbieter**

## Sicherheitslösungen auf Basis von Microsoft-Produkten für Telekommunikationsanbieter

Verbesserung der Sicherheitslandschaft für asiatische Telekommunikationsanbieter

Branche: **Telekommunikation**

Ort: **Asien**

Mitarbeiter: **3.500+**



## Über den Kunden

Unser Kunde ist einer der führenden Telekommunikationsanbieter in der Region Zentralasien. Das Unternehmen bietet Drahtlos-, Festnetz- und Breitbanddienste sowie Telekommunikationslösungen für Privat- und Geschäftskunden an.

## Anforderung

Der Kunde kam auf Infopulse mit einer Reihe von Herausforderungen im Bereich der Informationssicherheit zu. Sicherheitsschwachstellen in verschiedenen Unternehmensbereichen machten es für unseren Kunden schwierig, die Ursachen für seine IT-Sicherheitslücken zu ermitteln.

Die Liste der zu behebenden Probleme unseres Kunden umfasste folgende Punkte:

- Häufige Verstöße durch interne Ressourcen (vor allem durch E-Mail und Benutzerkonten)
- Weniger effiziente und verzögerte Aktualisierungen von Sicherheitsrichtlinien durch die Arbeit von zu Hause aus
- Hohe Kosten für VPN-Lizenzen, um alle Benutzer abzudecken
- Die Benutzer benötigten nicht für alle ihre Aufgaben ein VPN, aber dennoch mussten sie auf einige Dienste zugreifen, die nur über das interne Netzwerk verfügbar waren
- Mangel an Endpunktsicherheit



## Lösung

In enger Zusammenarbeit mit dem Kunden führten wir eine eingehende Prüfung der IT-Infrastruktur und der Sicherheitsperimeter durch. Wir systematisierten alle Lücken in der Informationssicherheit und identifizierten die wichtigsten Problembereiche.

Daraufhin implementierten wir ein POC-Projekt (Proof of Concept) mit einer Microsoft 365 E5-Lizenz und fortschrittlichen Sicherheitsprodukten. Außerdem haben wir die Architektur und die Einstellungen so aufgebaut und integriert, dass sie entsprechend den wachsenden Anforderungen des Kunden skaliert und weiterentwickelt werden können.

Um die Sicherheitsstrategie des Unternehmens zu stärken, **setzten wir die folgenden Tools und Ansätze ein:**

**Microsoft Endpoint Manager** – für sichere Geräteanmeldung, Verwaltung und Richtlinienbereitstellung für einen modernen Arbeitsplatz.

**Microsoft Defender for Endpoint** – für ein breites Spektrum an Informationssicherheitsdiensten für Endpunktgeräte. Es ermöglicht eine gründliche Bestandsüberwachung und Datenerfassung.

- Erkennung von Betriebssystemen, Konten, Anwendungen und Netzwerkfehlfunktionen
- Risikobewertung
- Automatisierte Abhilfemaßnahmen
- Systemhärtung

**Microsoft Cloud App Security** – für die Analyse der Nutzung riskanter Online-Dienste durch Benutzer. Wir haben eine Sicherheitsrichtlinie entwickelt, die eine Grundlage für das Unternehmen schafft:

- Einschränkung der Nutzung von Apps mit niedrigem Risikowert
- Nutzungsbeschränkung für persönliche Cloud-Dateispeicher (OneDrive und Google Drive)
- Analyse der Nutzung sozialer Medien und hoher Zugriffszahlen

**Azure AD Identity Protection + Microsoft Defender for Identities** – zum Schutz von Unternehmensbenutzerkonten vor Sicherheitsverletzungen. Wir haben die Analyse des Benutzerverhaltens implementiert, um eine maßgeschneiderte Schutzrichtlinie zu erstellen.

- Überwachen und profilieren des Benutzerverhaltens und der Benutzeraktivitäten
- Schutz der Benutzeridentitäten und Verringerung der Angriffsfläche
- Identifizierung verdächtiger Aktivitäten und fortgeschrittener Angriffe über die gesamte Kill-Chain von Cyberangriffen
- Prüfen von Warnungen und Benutzeraktivitäten

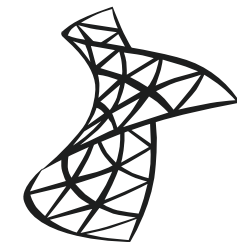
**Microsoft Defender für Office 365** – für die Sicherheit von geschäftlichen E-Mails und Anmeldeinformationen.

- Anti-Phishing-Tests
- Testen von sicheren Links
- Testen von sicheren Anhängen

## Technologien



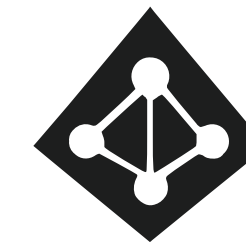
**Microsoft Defender  
für Endpoint**



**Microsoft Endpoint  
Manager**



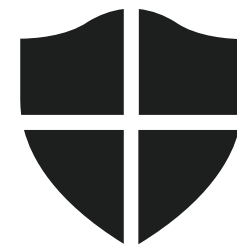
**Microsoft Cloud App  
Security**



**Azure AD  
Identitätsschutz**



**Microsoft Defender  
für Identitäten**



**Microsoft Defender  
für Office 365**





## Ergebnis

Als Ergebnis des dreimonatigen Projekts erhielt unser Kunde eine vollständige Sichtbarkeit seiner IT-Infrastruktur und deren Sicherheitsschwachstellen mit einer Reihe von skalierbaren Tools für seine Sicherheitsstrategie. Zu den greifbaren Vorteilen der implementierten Lösung gehören:

- Sicherheit des Unternehmenswertes
- Verringerung von Datenschutzverletzungen und Cyber-Bedrohungen
- Sicherer Zugriff auf die Unternehmensressourcen außerhalb des Büros
- Einwandfreie Integration in das Ökosystem der Microsoft-Produkte des Kunden
- Automatisierung von Sicherheitsprodukten, die eine automatische Reaktion auf Sicherheitsbedrohungen ermöglicht
- Geringere Gemeinkosten im Zusammenhang mit der Sicherheit der Betriebsumgebung

Der von Infopulse entwickelte Sicherheitsansatz wurde zu einer großartigen Erweiterung für das SOC-Team (Security Operation Center) und ermöglichte eine:

- Verbesserte Sicherheitstransparenz durch Erfassung von mehr Sicherheitsdaten
- Verbesserte Untersuchung und Reaktion auf Vorfälle mit umfangreichen integrierten Playbooks
- Durchsetzung der gleichen Richtlinien für Benutzer innerhalb und außerhalb des Unternehmensgeländes
- Differenziertere und flexiblere Durchsetzung von Richtlinien für den Zugriff auf Cloud-Dienste





## 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](http://www.infopulse.com/de)

## Kontaktieren sie uns

**DE** +49 (69) 505-060-4719

**UA** +38 (044) 585-25-00

**US** +1 (888) 339-75-56

**UK** +44 (8455) 280-080

**PL** +48 (221) 032-442

**BG** +359 (876) 92-30-90

**BR** +55 (21) 99298-3389

 [info@infopulse.com](mailto:info@infopulse.com)

