ACP

Freiwillige Feuerwehr Wels

IT for innovators.

Die Expert:innen von ACP unterstützen die Freiwillige Feuerwehr Wels nach einem schwerwiegenden Cyber-Security-Vorfall mit einem strukturierten Incident-Response-Einsatz. Durch die rasche technische Analyse, den koordinierten Neuaufbau der IT-Infrastruktur und die Implementierung nachhaltiger Sicherheitsmaßnahmen konnte der IT-Betrieb in kurzer Zeit wiederhergestellt und das Sicherheitsniveau langfristig erhöht werden.

Freiwillige Feuerwehr Wels

Facts

Sitz: **Wels**
Feuerwachen: **4**
Mitglieder: **146**
Gründung: **1867**
Branche: **Feuerwehr & Katastrophenschutz**

Unsere Lösung

Security Incident Response Service

Die Herausforderung

m August 2025 wurde die IT-Infrastruktur der Freiwilligen Feuerwehr Wels Ziel eines Cyberangriffs. Zentrale Server- und Verwaltungssysteme waren verschlüsselt und nicht mehr verfügbar, auch bestehende Backups konnten nicht ohne weiteres für eine Wiederherstellung genutzt werden. Durch die Beeinträchtigung der Domänen- und Vertrauensstellung war eine rasche Rücksicherung ausgeschlossen.

Als Organisation mit kritischen Aufgaben im Bereich Einsatz- und Katastrophenschutz ist die Feuerwehr auf eine hochverfügbare und sichere IT angewiesen. Ziel war es daher, den Betrieb schnellstmöglich wiederherzustellen, die Ursache des Vorfalls vollständig zu analysieren und gleichzeitig die IT-Umgebung nachhaltig gegen zukünftige Bedrohungen abzusichern.

Die Lösung

Unmittelbar nach der Meldung des Vorfalls stellte ACP ein interdisziplinäres Incident-Response-Team aus IT-Forensik, Netzwerk- und Serverexpert:innen sowie Kommunikation zusammen. In Abstimmung mit dem Kunden wurde zunächst eine forensische Analyse durchgeführt, um das Ausmaß des Angriffs sowie die betroffenen Systeme einzugrenzen. Auf Basis dieser Analyse empfahl ACP einen kontrollierten Neuaufbau der betroffenen Infrastruktur in einer bereinigten Umgebung.

Parallel dazu wurde die E-Mail-Kommunikation rasch und sicher durch die Umstellung auf Exchange Online wiederhergestellt. Während des gesamten Prozesses blieb der Kunde eingebunden und wurde laufend über den Status informiert. Zusätzlich übernahm ACP die Koordination mit externen Softwarepartnern, um alle Fachapplikationen ohne Datenverlust wieder in Betrieb zu nehmen. Bereits nach kurzer Zeit konnten erste Systeme produktiv genutzt werden, nach wenigen Wochen stand die IT-Landschaft wieder vollständig zur Verfügung.

Die Vorteile

Der strukturierte Incident-Response-Einsatz von ACP ermöglichte nicht nur eine rasche Wiederherstellung des IT-Betriebs, sondern auch eine nachhaltige Modernisierung der gesamten Sicherheitsarchitektur. Im Anschluss an den Vorfall wurden unter anderem Multi-Faktor-Authentifizierung, ein Zero-Trust-Ansatz sowie ein 24x7 Security Operations Center (SOC) implementiert.

Das SOC von ACP überwacht und korreliert sicherheitsrelevante Ereignisse kontinuierlich, erkennt Auffälligkeiten frühzeitig und liefert konkrete Handlungsempfehlungen zur laufenden Verbesserung des Security-Niveaus. Die Freiwillige Feuerwehr Wels verfügt damit heute über eine deutlich widerstandsfähigere IT-Infrastruktur und ist optimal auf zukünftige Cyberbedrohungen vorbereitet.