



«Durch die Zusammenarbeit mit ITRIS One und Artic Wolf können wir uns auf unser Kerngeschäft konzentrieren.»

René Rickenbach, Wirtschaftsinformatiker, KSU



Cybersicherheit im Fokus:

Wie das Kantonsspital Uri seine digitale Infrastruktur besser schützt

Cyberangriffe bedrohen zunehmend die Sicherheit im Gesundheitswesen – mit potenziell gravierenden Folgen für Patientinnen und Patienten sowie den Spitalbetrieb. Das Kantonsspital Uri hat deshalb den Schritt von einer reaktiven zu einer proaktiven IT-Sicherheitsstrategie vollzogen. Mit der langjährigen Partnerin ITRIS One und dem Security-Spezialisten Arctic Wolf setzt das Spital neu auf ein Managed Security Operations Center – für eine rund um die Uhr überwachte, widerstandsfähige IT-Landschaft.

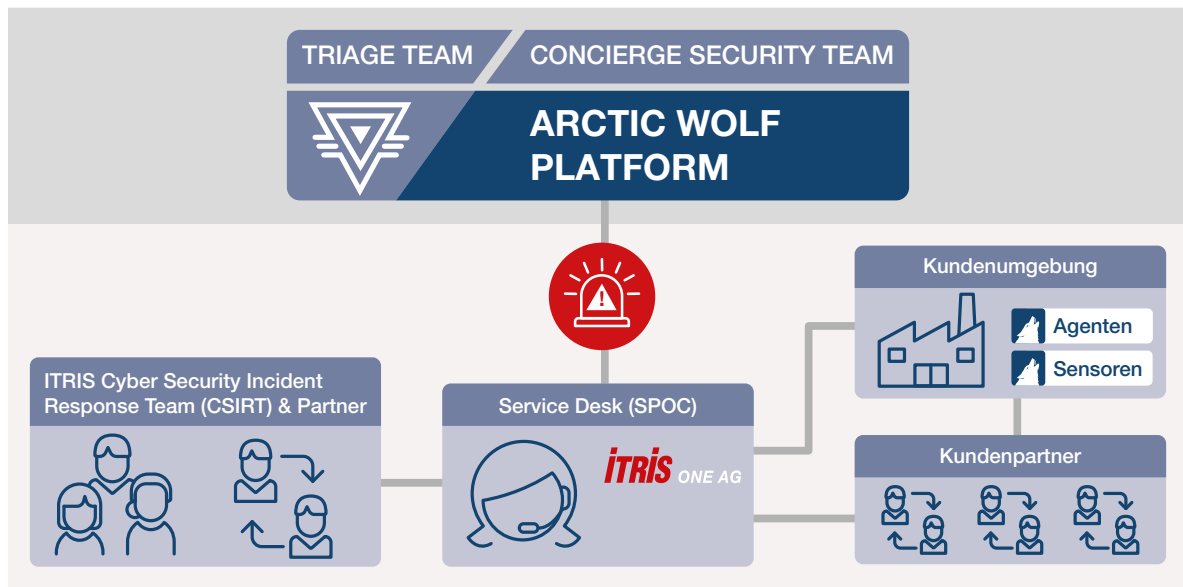
Cyberangriffe stellen im Gesundheitswesen eine besonders ernst zu nehmende Bedrohung dar. Nicht nur wegen der sensiblen Patientendaten, sondern auch aufgrund der Vielzahl vernetzter medizinischer Geräte. Kommt es zu einem Angriff, sind die Folgen oft weitreichend: Neben erheblichen wirtschaftlichen Schäden kann vor allem die Patientenversorgung direkt beeinträchtigt werden. Ein Ausfall kritischer IT-Systeme, etwa durch Ransomware, kann dazu führen, dass lebenswichtige Informationen und Geräte nicht mehr verfügbar sind, was die medizinische Versorgung erheblich beeinträchtigt. Zudem ist der Diebstahl sensibler Gesundheitsdaten mit allen Mitteln zu vermeiden. Eine

robuste IT-Sicherheitsstrategie mit präventiven Massnahmen, schneller Reaktionsfähigkeit und regelmässigen Schulungen des Personals sind unerlässlich.

Ausgangssituation

Das Kantonsspital Uri (KSU) setzte lange Zeit auf eine klassische Firewall sowie eine Antivirenlösung auf den Endgeräten. Die IT-Abteilung reagierte auf auftretende Warnmeldungen und Alerts und verfolgte diese gezielt. Ergänzend wurden regelmässig Empfehlungen vom Cyber Security Hub des Bundes berücksichtigt und entsprechende Anpassungen, etwa auf der Firewall, umgesetzt. Bereits zu diesem Zeitpunkt wurde das KSU

MANAGED SECURITY OPERATION CENTER



Das Managed Security Operation Center (SOC) überwacht die IT-Umgebung des KSU permanent.

bei der Konfiguration von Firewall und Netzwerk durch externe Partner unterstützt, während die Betriebsverantwortung stets beim Spital selbst lag. Den steigenden Anforderungen zur Erhöhung der Sicherheit gerecht zu werden, erfordert nicht nur zusätzliche Ressourcen, sondern auch spezialisiertes Fachwissen. Dies konnte mit dem internen IT-Team allein nicht mehr effizient und effektiv bewältigt werden. Es brauchte eine Veränderung. Um der wachsenden Bedrohungslage angemessen zu begegnen, wurden mehrere Möglichkeiten evaluiert. Ein Wechsel von einer reaktiven zu einer proaktiven Sicherheitsstrategie war nötig. Gerade im Bereich Cybersecurity ist es wichtig, mit Expertinnen und Experten zu arbeiten, die sich täglich mit neuen Bedrohungen auseinandersetzen. Das Team des KSU hat sich daher bewusst entschieden, mit einem externen Partner zusammenzuarbeiten.

Vertrauen durch Erfahrung: Warum sich das KSU erneut für ITRIS One entschieden hat

Nach der Evaluation mehrerer Möglichkeiten entschied sich das KSU für die Zusammenarbeit mit ITRIS One und Arctic Wolf. «ITRIS One ist seit über 20 Jahren unser verlässlicher Partner – eine Zusammenarbeit, die auf Vertrauen, positiven Erfahrungen und bewährten Lösungen basiert. In all den Jahren hatten wir stets einen guten Draht zum Team und die Lösungen haben unsere Erwartungen immer erfüllt», sagt René Rickenbach, Wirtschaftsinformatiker beim KSU. Diese langjährige Zuverlässigkeit war ein wichtiger Faktor für die Entscheidung, auch diesmal wieder auf ITRIS One zu setzen. «Gleichzeitig war die Zusammenarbeit mit Arctic Wolf eine spannende Ergänzung, die zusätzliche Perspektiven in unsere Sicherheitsstrategie eingebracht hat», so René Rickenbach.

DER KUNDE: DAS KANTONSSPITAL URI

Das Kantonsspital Uri (KSU) in Altdorf ist das Akutspital des Kantons Uri und bietet rund 37 000 Einwohnerinnen und Einwohnern die erweiterte medizinische Grundversorgung. Mit etwa 650 Mitarbeitenden, davon 80 Auszubildende, spielt das KSU eine bedeutende Rolle als Arbeitgeber und Ausbildungs-

stätte in der Region. Das KSU verfügt über ein umfassendes ambulantes und stationäres Leistungsangebot.

IT-Security ist zentral

Als medizinisches Kompetenzzentrum in Uri setzt das KSU auf eine patientenorientierte Spitalinfrastruktur, persönliche

Betreuung und eine enge interdisziplinäre Zusammenarbeit. Damit diese hochwertige Versorgung auch in Zukunft gesichert bleibt, spielt der Schutz der digitalen Infrastruktur eine immer zentralere Rolle.

Die Umsetzung:

Managed Security Operations Center

Im Zentrum der neuen Lösung steht das Managed Security Operations Center (SOC), welches das KSU mit modernster Technologie und einem umfassenden Servicepaket absichert. Die Plattform überwacht die IT-Umgebung rund um die Uhr, erkennt auffällige Aktivitäten frühzeitig, analysiert sie und schlägt bei Bedarf Alarm (siehe Grafik).

Die Kernkomponenten der Lösung sind:

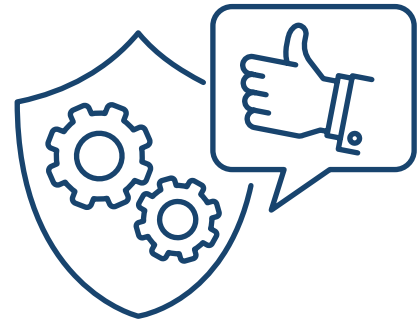
Triage Team: Das Triage Team im Security Operations Center übernimmt die taktische Umsetzung: 24/7-Überwachung, schnelle Reaktion auf Vorfälle und aktive Unterstützung bei der Behebung. Ziel ist es, Fehlalarme zu minimieren und dem KSU nur relevante, verständlich aufbereitete Informationen und klare Handlungsempfehlungen zu liefern.

Concierge Security Team: Der Service wird durch ein Concierge Security Team (CST) ergänzt. Hierbei handelt es sich um explizit zugewiesene, mit dem KSU vertraute Experten. Das CST unterstützt das KSU strategisch in ihrer Cybersicherheitsentwicklung. Der Sicherheitsstatus wird regelmässig analysiert, verbessert und an aktuelle Bedrohungen angepasst – individuell abgestimmt und im engen Austausch mit dem IT-Team des KSU.

Koordination und Reaktion bei Vorfällen: Im Falle eines Incidents wird der Service Desk von ITRIS One als zentraler Anlaufpunkt (Single Point of Contact) aktiv. Er koordiniert die Kommunikation und erste Analysen gemeinsam mit dem CSIRT (Cyber Security Incident Response Team). Sofortmassnahmen werden eingeleitet, um beispielsweise die Ausbreitung von Schadsoftware zu stoppen.

Aktivitäten, die über bestehende Partner des KSU laufen (z. B. für Netzwerk oder Firewalls), werden ebenfalls durch ITRIS One koordiniert und ausgeführt, um möglichst schnell reagieren zu können.

Je nach Schadensausmass müssen gewisse oder sogar alle Aktivitäten vor Ort im Kundenumfeld erfolgen.



DIE GRÖSSTEN VORTEILE DER MANAGED-SOC-LÖSUNG FÜR DAS KSU

Zentrale und automatisierte Analyse

Alle relevanten Systemdaten und Logfiles werden direkt an Arctic Wolf übermittelt. Das ermöglicht eine effiziente Auswertung. Das KSU wird sofort informiert, wenn Handlungsbedarf besteht – inklusive einer klar strukturierten Ticket-Benachrichtigung.

Starke Unterstützung und unkomplizierte Zusammenarbeit

Besonders der gute und direkte Draht zu ITRIS One als SPOC (Single Point of Contact) erleichtert die Zusammenarbeit und sorgt für schnelle, praxisnahe Lösungen. ITRIS One verfügt über ein sehr breites Know-how zur gesamten Infrastruktur und kann bei einem Incident in allen Disziplinen unterstützen.

Mehr Sicherheit, weniger Aufwand

Das IT-Team des KSU muss sich nicht mehr fragen, ob alle relevanten Logfiles richtig interpretiert oder kritische Details übersehen wurden. Stattdessen werden jetzt diese Daten professionell überwacht und analysiert, wodurch das IT-Team des KSU spürbar entlastet wird und sich auf das Wesentliche konzentrieren kann.

Kontinuierliche Optimierung der Sicherheitsstrategie

Das KSU profitiert von fortlaufenden Verbesserungen der Sicherheitsprozesse und -massnahmen, indem Sicherheitspläne, -kontrollen und -indikatoren regelmässig überprüft und angepasst werden.

Prävention durch Dokumentation und Handlungsempfehlungen

Das KSU erhält nach Sicherheitsvorfällen umfassende Auswertungen sowie konkrete Hinweise, wie ähnliche Situationen in Zukunft vermieden werden können – als wertvolle Grundlage für die kontinuierliche Weiterentwicklung der Sicherheitsstrategie.



Moderne Infrastruktur und IT – das KSU in Altdorf.

Durch die lokale Präsenz der ITRIS One in der ganzen Schweiz kann unter Abstimmung mit Arctic Wolf und dem KSU direkt im Kundenumfeld agiert werden. Dies hat sich in der Vergangenheit schon oft als sehr wertvoll erwiesen.

Nachbereitung und kontinuierliche Verbesserung

Nach einem Sicherheitsvorfall folgt eine detaillierte Analyse – inklusive Ursachenforschung, forensischer Bewertung und klarer Dokumentation. Ziel ist es, die Angriffsfläche nachhaltig zu verringern und ähnliche Vorfälle künftig zu verhindern. Dafür arbeitet ITRIS One bei Bedarf mit spezialisierten Partnern für digitale Forensik zusammen.

Fazit

Durch die kontinuierliche Anpassung und Verbesserung der Sicherheitsmassnahmen können Spitäler wie das KSU die Risiken von Cyberangriffen minimieren und die Sicherheit der Patientendaten gewährleisten. Mit der Einführung des Managed Security Operations Center und der Zusammenarbeit mit erfahrenen Partnern wie ITRIS One und Arctic Wolf hat das KSU einen entscheidenden Schritt in Richtung zukunftsfähige IT-Sicherheit gemacht. Dank der proaktiven Cybersicherheitsstrategie, die aus einer Kombination aus modernster Technologie, kontinuierlicher Überwachung und strategischer Beratung besteht, ist das Spital heute deutlich besser gegen Cyberbedrohungen gewappnet – zum Schutz seiner Patientinnen und Patienten, der Mitarbeitenden und der medizinischen Versorgung im Kanton Uri.



«Die Experten ITRIS One und Arctic Wolf bringen nicht nur das notwendige Know-how, sondern auch die Erfahrung mit, um uns optimal zu unterstützen.»

René Rickenbach, Wirtschaftsinformatiker, KSU



DARUM ITRIS ONE

Als einer der führenden Schweizer ICT-Serviceprovider unterstützt ITRIS One AG Ihr Unternehmen bei der Entwicklung und Umsetzung modernster IT-Lösungen und Services. Egal, ob leistungsfähiges Datacenter, zeitsparende Kommunikationslösungen, zuverlässige Netzwerke, moderne Workplaces oder wirksame Sicherheitskonzepte: Profitieren Sie von unseren agilen und leistungsfähigen IT-Infrastruktur-Lösungen und unserem breiten, massgeschneiderten Service-Portfolio. Dank jahrzehntelanger Erfahrung sind wir Ihr Partner für Healthcare und Business Aligned IT – ob mit einer On-Premises-, Managed-, Cloud- oder Hybrid-Cloud-Lösung.

ITRIS ONE AG

ITRIS One AG

Hauptsitz
Industriestrasse 169
CH-8957 Spreitenbach

Tel. +41 58 855 51 51
Mail one@itris.ch
Web www.one.itris.ch

Für Sie vor Ort sind wir ausserdem in weiteren Niederlassungen in Chur, Gland, Gossau, Lamone, Reinach, Tagelswangen, Urtenen-Schönbühl.

