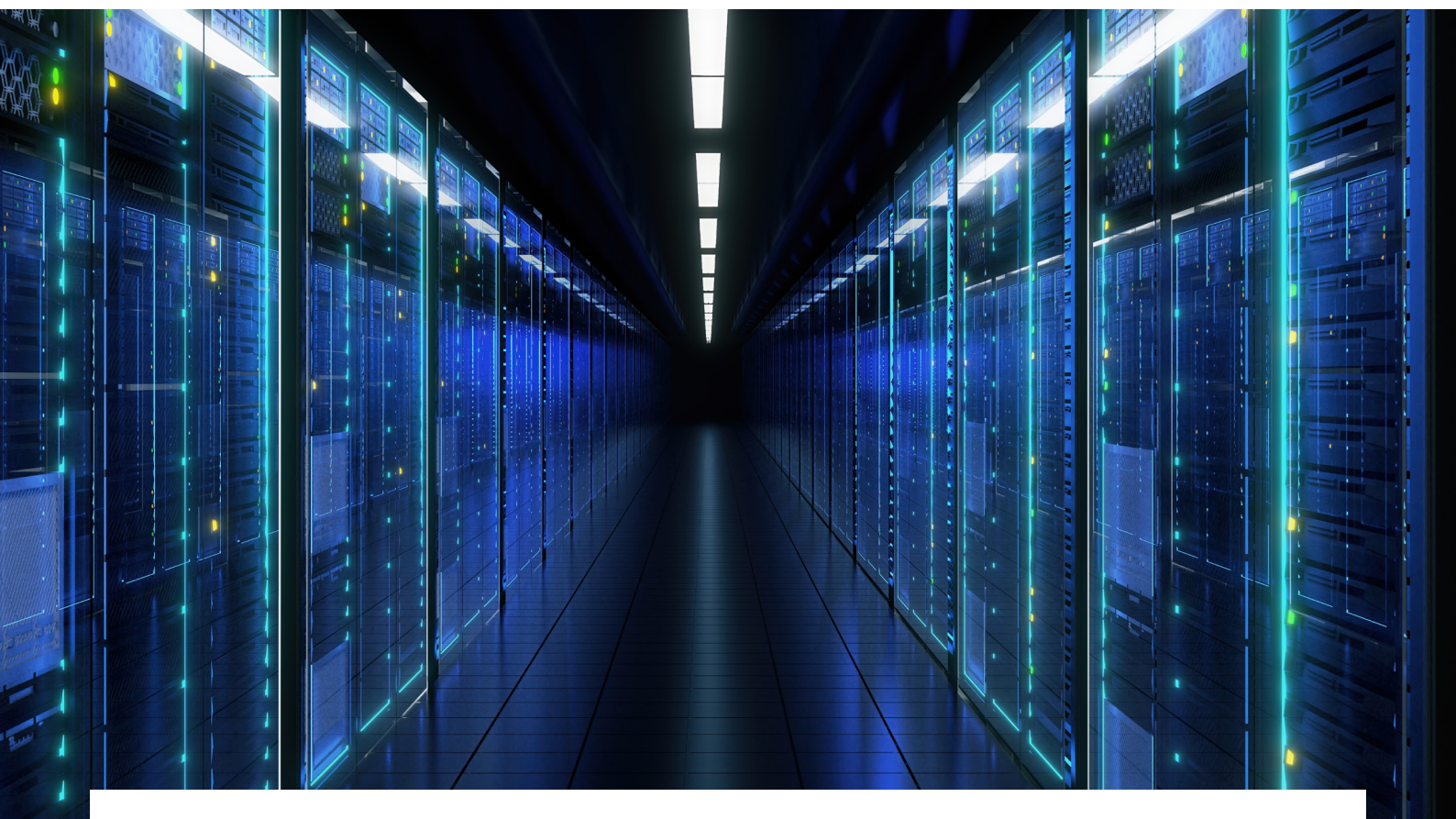


**SUCCESS STORY**

Selbstüberwachung: proaktives Sicherheits- Management

IT-Verantwortliche in Behördenorganisationen sind darauf angewiesen, dass innerhalb von selbstüberwachenden Systemen der Transfer von relevanten Meta-Informationen aus komplett isolierten oder teil-isolierten Zonen nach aussen möglich ist, ohne die Sicherheit der schützenswerten Daten zu kompromittieren. Denn nur wenn auch die Elemente in einer isolierten Zone überwacht werden, können allfällige Probleme entdeckt und behoben werden.

Die CyOne Security ist auf den Trade-Off zwischen der Informationsdichte, die aus der isolierten Zone nach aussen transferiert wird, und den Kerninformationen mit höchstem Schutzbedarf spezialisiert und bietet im Behördenumfeld massgeschneiderte Lösungen für den sicheren Zonentransfer von Informationen an.

Projektspezifikation

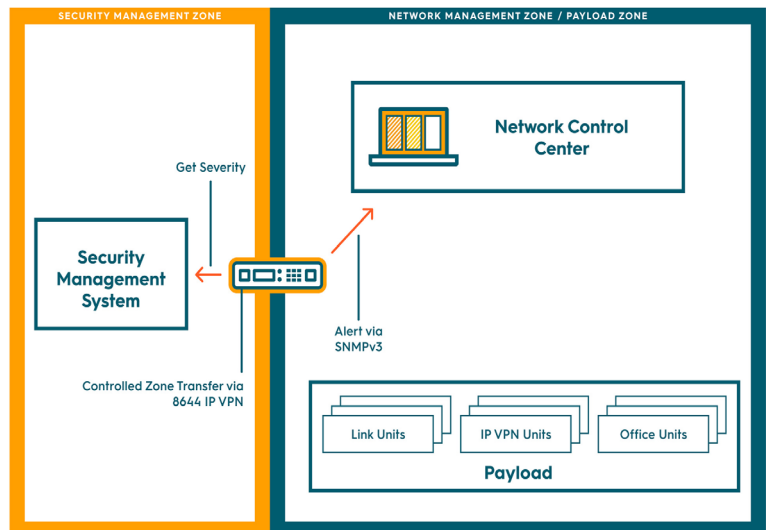
Sensible Informationen dürfen ihre Sicherheitszone im Netzwerk keinesfalls verlassen, wohingegen Informationen zu Cyber Security-relevanten Ereignisse die Zonengrenzen passieren sollten.

Implementation

Die CyOne Security unterstützt ihre Kunden bei der Konzeption und Implementierung von notwendigen Überwachungsfunktionen.

- Aufteilung des Netzwerks in speziell gesicherte, isolierte oder teil-isolierte Zonen, die Daten mit ähnlichen Compliance-Anforderungen enthalten
- Erarbeitung eines kundenspezifischen Severity-Konzepts und Definition der alarmauslösenden Cyber Security-relevanten Ereignisse
- Integration in das Network Operation Center (NOC), sodass darin der aktuelle Zustand des betreffenden Teilsystems übersichtlich auf einem Dashboard dargestellt wird
- Bei einem sicherheitsrelevanten Vorfall in der isolierten Zone werden relevante Meta-Daten über eine definierte Schnittstelle nach aussen transferiert.
- Es gelangen nur Notifications zum bestehenden Problem nach aussen, nicht aber schützenswerte Informationen. Im NOC fliessen sie mit anderen relevanten Netzwerkdaten zusammen.

Selbstüberwachung des Security Managements



Höchste Sicherheit

Für Kerninformationen mit höchstem Schutzbedarf ist durchgängige Sicherheit und Vertraulichkeit sichergestellt.

Ständige Verfügbarkeit

Im NOC werden die Probleme auch innerhalb der isolierten Zone erkannt, unter anderem durch Selbstüberwachung. Damit wird die ständige Verfügbarkeit und Ausfallsicherheit der Security Management-Zone gewährleistet.

Hohe Benutzerfreundlichkeit

Via Remote Management wird das System zentral verwaltet und der Systemzustand übersichtlich auf einem Dashboard dargestellt.