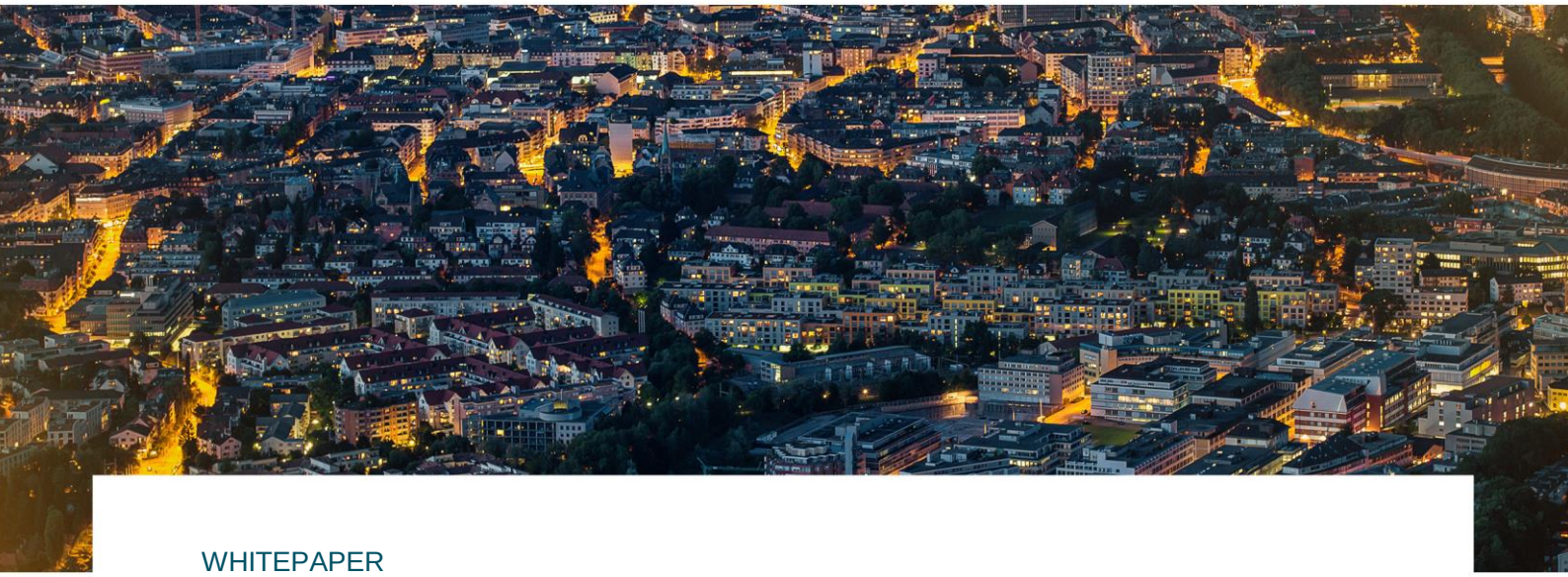
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WHITEPAPER

Selbstüberwachung: proaktives Sicherheits-Management statt reaktives Troubleshooting

CyOne Security | Steinhausen, 23. August 2022

Hochsichere Zonen dienen dem Schutz sensibler Informationen. Sie sind vom restlichen Netzwerk und der Payload isoliert. Das wird dann zum Problem, wenn Informationen über sicherheitsrelevante Ereignisse übermittelt werden müssten. Abhilfe schafft ein selbstüberwachendes System, das via definierte Zonenübergänge vorausschauend Alarm schlagen kann.

Die Komponenten eines Netzwerks haben unterschiedliche Ansprüche an die Cyber Security. Während beispielsweise gewisse Servicesysteme externe Zugriffe erlauben müssen, dürfen sensible Daten keinesfalls abfliessen und in falsche Hände gelangen. Standorte, kryptografische Schlüssel, IP-Adressen oder Netzwerk-Topologien müssen vor dem Zugriff Dritter geschützt werden. Darum ist es sinnvoll, ein Netzwerk zu zonieren: Besonders sensitive Bestandteile werden dabei in speziell gesicherte, isolierte oder teil-isolierte Zonen ausgelagert. Der Zugriff wird auf die nötigsten Schnittstellen beschränkt.

Die Vorteile von zonierten Netzwerken im Überblick:

1. Es teilt das Netzwerk in Zonen auf, die Daten mit ähnlichen Compliance-Anforderungen enthalten.
2. Innerhalb einer Zone reduziert sich der Compliance-Umfang, und die Sicherheitsrichtlinien können innerhalb der Zone einheitlich umgesetzt werden.
3. Ein zoniertes Netzwerk erschwert bei einer allfälligen erfolgreichen Infektion die ungehinderte Weiterverbreitung der Malware(s) (Lateral Movement).

Zonierung: Herausforderung für das Security Monitoring

Die Zonen und Zonenübergänge stellen allerdings eine Herausforderung dar, wenn es um das Security Monitoring des Gesamtsystems geht. Um die Sicherheit zu gewährleisten, müssen Aufzeichnungen (Logs), Notifications (Alarme) und Echtzeitdaten (Metadaten zu Traffic Flow, Storage, CPU-Last oder Backup-Stati) zonenübergreifend gesammelt und aufbereitet werden – und zwar ohne, dass die Sicherheitsvorgaben der einzelnen Zonen verletzt werden.

Weil sich die Bedürfnisse jeder Behörden- und Verwaltungsorganisation unterscheiden, kann eine Standard-Sicherheitsarchitektur das nicht leisten. Es braucht massgeschneiderte Lösungen, die den Transfer von relevanten Meta-Informationen aus komplett isolierten oder teil-isolierten Zonen nach aussen ermöglichen, 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. Das erhöht die Verfügbarkeit des Gesamtsystems und kommt der Organisation zugute: Denn das System ist so besser vor unvorhergesehenen und somit kostspieligen Ausfällen geschützt.

Geo-Redundanz und Remote-Management

Infrastrukturen, welche der Bearbeitung von klassifizieren Daten dienen, sind oftmals redundant in räumlich getrennten Datacenters untergebracht. Diese Geo-Redundanz sorgt für zusätzliche Betriebssicherheit. Einerseits kann die Archivierung innerhalb des Systems erreicht werden, andererseits sind die Systeme auch im Krisenfall und während Wartungsarbeiten unterbruchfrei verfügbar. Um auch dem physischen Schutz gerecht zu werden, wird der Zugang zu den Datacenters streng überwacht und wenn immer möglich vermieden. Aus diesem Grund werden die Komponenten falls möglich via Remote-Management verwaltet. Auch dieser Zugriff erfolgt auf definierten, speziell gehärteten Systemen.

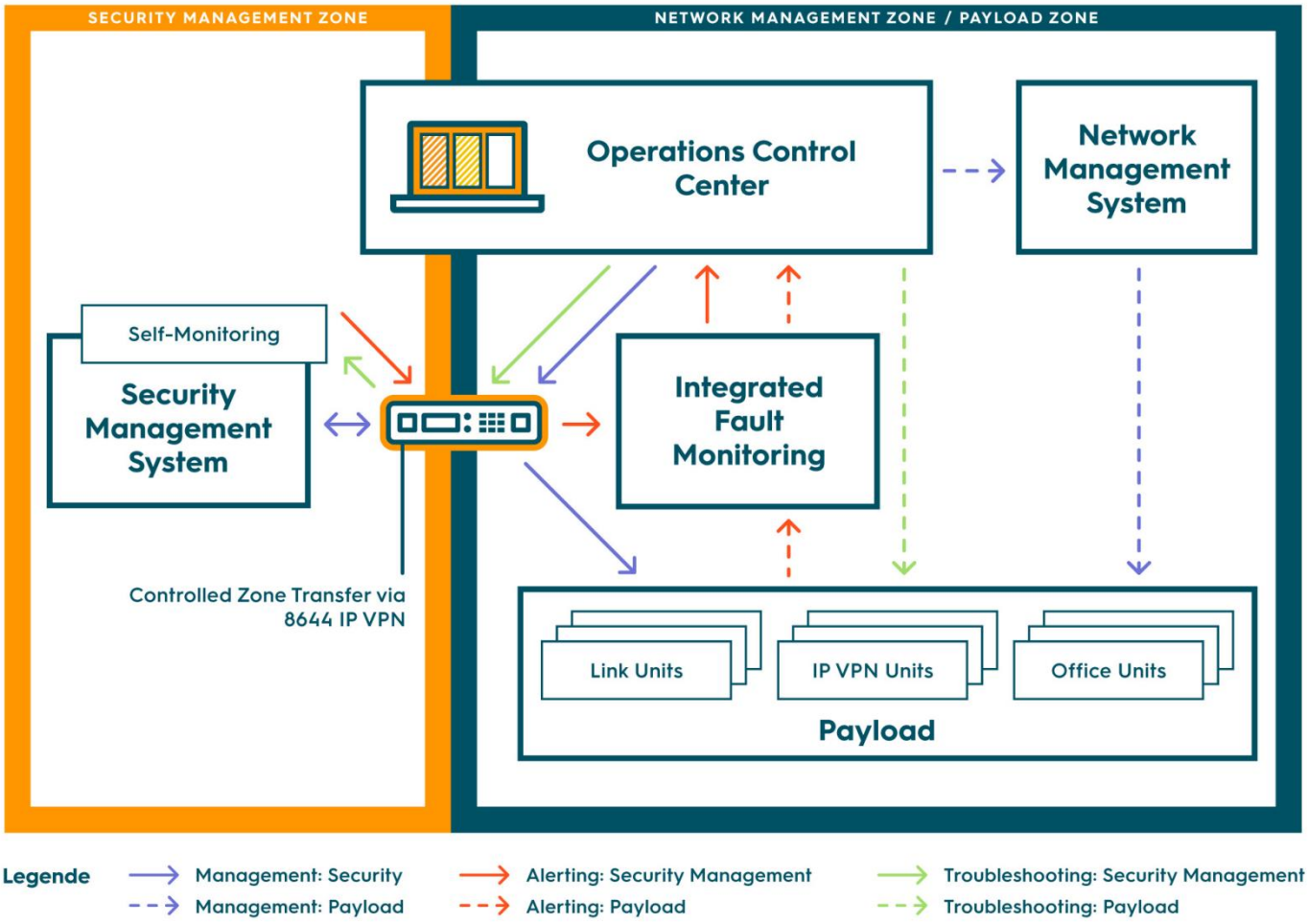
Hier zeichnet sich ein Paradigmenwechsel ab: Reaktives Troubleshooting wird nach und nach durch ein proaktives Sicherheits-Management ersetzt. Probleme werden im Idealfall durch vorausschauende Interventionen behoben. Systemtechnisch ist dafür eine Überwachung und Alarmierung notwendig. Eine weiterführende Ausbaustufe ist das automatische Einleiten von ersten Schritten basierend auf definierten Abläufen, um Problemfälle eigenständig beheben zu können (Self-Healing). Dadurch können lokale Wartungsaufwände und Remote-Zugänge minimiert und schliesslich Unterhaltskosten reduziert werden.

So funktionieren selbstüberwachende Systeme

Das selbstüberwachende Referenzsystem der CyOne Security stellt den aktuellen Zustand des betreffenden Teilsystems übersichtlich in Form eines Dashboards dar. Administratoren können sich dabei je nach Bedürfnis auch Werte der untersten Hierarchieebene anzeigen lassen, bis hin zu einzelnen Sensordaten. Wenn Probleme auftauchen, etwa wenn ein Backup nicht durchgeführt werden kann, die Replizierung gestört oder die Stromversorgung kritisch ist, kommuniziert das System dies über das Value Mapping via einen definierten Zonenübergang nach aussen. Empfänger dieser Notification kann beispielsweise ein Integrated Fault Monitoring (IFM) sein. Dabei wird streng darauf geachtet, dass ausschliesslich definierte Statusinformationen zum bestehenden Problem den Zonenübergang passieren; generelle, schützenswerte Informationen aber nicht aus der isolierten Zone abfliessen.

Der Vorteil dieses selbstüberwachenden Systems: Hardware-Probleme im betreffenden Teilsystem werden frühzeitig erkannt und können rechtzeitig behoben werden. Die Daten lassen sich nicht nur separat erfassen, sondern können zentral in einem Network Operation Center (NOC) oder Security Operation Center (SOC) zusammengeführt werden. Dort können sie gemeinsam mit weiteren

relevanten Daten aus anderen Netzwerkkomponenten und Zonen analysiert werden. So lässt sich der Zustand der gesamten Netzwerkinfrastruktur überwachen. Allfällige Ereignisse, welche die Cyber Defence betreffen, werden so sicher erkannt.



Bei einem sicherheitsrelevanten Vorfall in einer isolierten Zone werden relevante Meta-Daten über eine definierte Schnittstelle nach aussen transferiert (rote Pfeile). Wichtig ist: Es dürfen nur Notifications zum bestehenden Problem nach aussen gelangen, nicht aber schützenswerte Informationen. Im Operations Control Center fliessen sie mit anderen relevanten Netzwerkdaten zusammen.

So viele Informationen wie nötig, so wenig wie möglich

Die CyOne Security unterstützt Kunden bei der Konzeption, der Implementierung von notwendigen Überwachungsfunktionen und bei einer allfälligen Integration in ein NOC / SOC / Cyber Defence Center (CDC). Das beginnt mit der Erarbeitung eines kundenspezifischen Severity-Konzepts. Diese Grundlage für die Selbstüberwachung dient der:

- Definition der alarmauslösenden Cyber Security-relevanten Incidents.
- nachfolgenden Aufbereitung bzw. Weiterverarbeitung innerhalb des kundenspezifischen Operation Centers (NOC / SOC / CDC).

Bei der Umsetzung legt die CyOne Security grossen Wert darauf, dass sich Sicherheit und Durchlässigkeit die Waage halten. Kerninformationen mit höchstem Schutzbedarf sind sicher, während relevante Meta-Informationen die Zonengrenzen passieren können. Das heisst schlussendlich: Beim Transfer von Daten aus einer isolierten Zone sollen so wenige Informationen wie möglich fliessen – aber so viele wie nötig.

Beginnen Sie heute, Ihre Netzwerke und Informationen vor Cyber-Risiken zu schützen.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.