

www.neox-networks.com

WHITEPAPER

NETZWERK-TAPS IM KRITIS-BEREICH

PROFESSIONELLE DATENAUSLEITUNG
FÜR MONITORING-, ANALYSE- UND SECURITY-TOOLS
IN KRITISCHEN INFRASTRUKTUREN



1. Einleitung

Laut der NIS2-Richtlinie müssen Betreiber von kritischen Infrastrukturen (KRITIS), wie Unternehmen aus den Bereichen Gesundheitswesen, Digitale Infrastruktur, Verkehrswesen, Wasserversorgung, Digitale Dienstleistungen, Infrastruktur der Banken und Finanzdienstleister, Energie und außerdem nun auch Anbieter öffentlicher elektronischer Kommunikationsnetze oder -dienste, Abwasser- und Abfallwirtschaft, Hersteller bestimmter kritischer Produkte (z. B. Pharmazeutika, medizinische Geräte und Chemikalien), Hersteller von Lebensmitteln, Anbieter von digitalen Diensten wie Plattformen für soziale Netzwerke und Data-Center-Services, Luft- und Raumfahrt, Post- und Kurierdienste und die öffentliche Verwaltung in allen 27 Mitgliedsstaaten der EU, sowie Liechtenstein, Island und Norwegen bis zum 18.10.2024 umfassende Maßnahmen für die Sicherheit ihrer Netzwerk- und Informationssysteme ergreifen.



Dazu gehören unter anderem die Implementierung von geeigneten Tools, die das Unternehmensnetzwerk, egal, ob es sich um ein IT- oder OT-Netzwerk handelt, kontinuierlich überwachen und schützen. Doch alle diese Tools haben eines gemeinsam: Sie benötigen eine zuverlässige Quelle, aus der sie die Netzwerkdaten, also den Datenverkehr, erhalten.

Auf die mannigfaltigen Gründe, warum es keine gute Idee ist, dafür den SPAN/Mirror-Port von Switches zu verwenden, sind wir bereits in unserem Whitepaper „Netzwerk-TAP gegen SPAN/Mirror-Port – Professionelle Datenausleitung der Netzwerkdaten für Monitoring-, Analyse- und Security-Tools“ eingegangen.



Dazu gehören unter anderem die Implementierung von geeigneten Tools, die das Unternehmensnetzwerk, egal, ob es sich um ein IT- oder OT-Netzwerk handelt, kontinuierlich überwachen und schützen. Doch alle diese Tools haben eines gemeinsam: Sie benötigen eine zuverlässige Quelle, aus der sie die Netzwerkdaten, also den Datenverkehr, erhalten. Auf die mannigfaltigen Gründe, warum es keine gute Idee ist, dafür den SPAN/Mirror-Port von Switches zu verwenden, sind wir bereits in unserem Whitepaper „Netzwerk-TAP

gegen SPAN/Mirror-Port – Professionelle Datenausleitung der Netzwerkdaten für Monitoring-, Analyse- und Security-Tools“ eingegangen.

Wenn man sich diese Gründe, zum Beispiel die Gefahr einer Kompromittierung der Switches, vergegenwärtigt hat und der SPAN/Mirror-Port als Datenquelle folglich ausscheidet, dann wird ziemlich schnell klar, dass man als Datenquelle am besten Netzwerk-TAPs einsetzt. Doch auch hier ist Vorsicht geboten, denn der Begriff „Netzwerk-TAP“ ist rechtlich nicht geschützt. So verkaufen beispielsweise einige Hersteller einfach billige Switches mit einer permanent eingerichteten SPAN/Mirror-Session als Netzwerk-TAP.

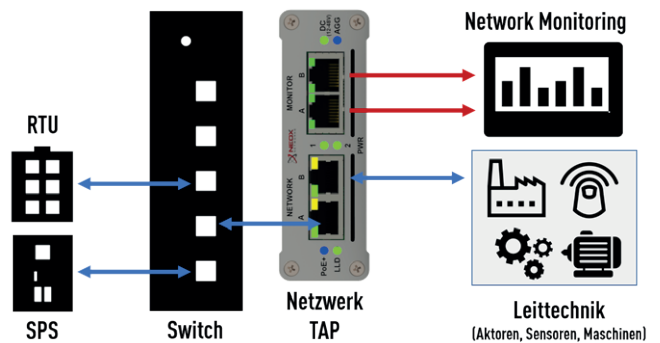
Daher sollte man bei der Auswahl auf bestimmte Kriterien achten.

2. Merkmale von echten Netzwerk-TAPs

Echte Netzwerk-TAPs implementieren die Logik für die Ausleitung einer Kopie der Netzwerkdaten in Hardware, und nicht mittels Software, wie im Fall von Switch-Hardware mit permanenter SPAN/Mirror-Session!

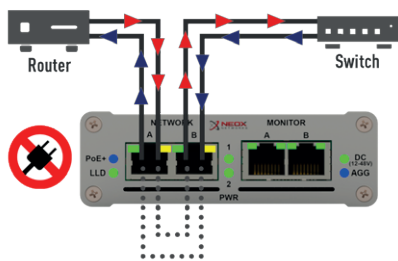
Sehr wichtig ist, dass Netzwerk-TAPs 100% des Datenverkehrs spiegeln und somit nicht nur FCS/CRC-fehlerbehaftete Datenpakete, sondern auch übergroße Pakete und Pakete, die kleiner sind als die per Standard definierte Mindestgröße, sauber ausleiten.

Weiterhin dürfen beim Spiegeln der Datenpakete durch Netzwerk-TAPs keinesfalls Paketverluste auftreten.



Beispiel-Platzierung eines Netzwerk-TAPs im KRITIS-Netzwerk

Die Stromversorgung von Netzwerk-TAPs sollte aus Gründen einer verlässlichen Verfügbarkeit auf jeden Fall redundant sein. Für Standorte, an denen nur Gleichspannung verfügbar ist, sollte ein Netzwerk-TAP zudem über eine integrierte DC-Stromversorgung (z. B. 12V – 48V) verfügen.



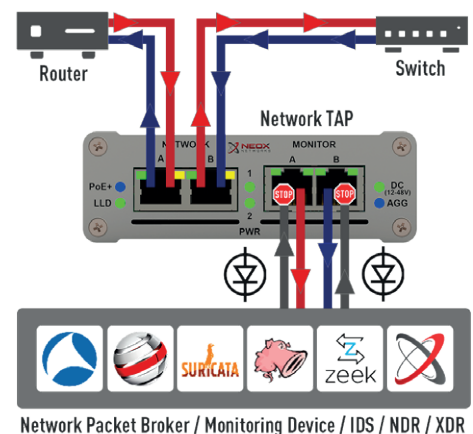
Failsafe-Funktion eines Netzwerk-TAPs

Für den Fall, dass dennoch ein Stromausfall auftritt, sollten Netzwerk-TAPs unbedingt über eine Failsafe-Funktion verfügen, die sicherstellt, dass die aktive Netzwerkverbindung, in die der Netzwerk-TAP eingeschleift ist, auch bei fehlender Stromversorgung ohne Fremdeinwirken wieder aufgebaut wird.

Für eine professionelle Montage sollten Montage-Optionen wie Rack-Einbau und Montage auf einer DIN-Hutschiene für die Netzwerk-TAPs verfügbar sein.

Außerdem sollten Netzwerk-TAPs nach Möglichkeit unbedingt über eine Datendiode-Funktion verfügen, die sicherstellt, dass über die Monitoring-Ports des Netzwerk-TAPs keine Daten in das Primärnetzwerk, das an den Netzwerk-Ports angeschlossen ist, gelangen können, ob nun beabsichtigt oder unbeabsichtigt.

Ein Netzwerk-TAP, der eine solche Funktion besitzt, ist somit rückwirkungsfrei.



Datendiode-Funktion eines Netzwerk-TAPs

3. Der Cybersecurity-Standard IEC 62443

IEC 62443 ist eine Normenreihe, die einen internationalen Cybersecurity-Standard darstellt und sich an Betreiber, Hersteller und Integratoren von OT-Systemen und -Netzwerken richtet. OT steht für Operational Technology, also industrielle Steuerungssysteme und -Netzwerke. Auch in der IT (Information Technology) findet der Standard IEC 62443 zunehmend Beachtung.



Der Standard deckt auch die Sicherheit von kritischen Infrastrukturen ab. Die enthaltenen Normen beschreiben Maßnahmen und Methoden, um eventuelle Schwachstellen von Netzen und Systemen identifizieren und vermeiden zu können, die bei Angriffen auf diese ausgenutzt werden könnten.

Daher ist es für KRITIS-Betreiber sehr empfehlenswert, Netzwerk-TAPs zu verwenden, die den technischen Anforderungen aus IEC 62443 entsprechen.

4. Nach IEC 62443 gehärtete Netzwerk-TAPs

Aus IEC 62443 ergeben sich einige Anforderungen, die auf Netzwerk-TAPs zutreffen und nach denen Netzwerk-TAPs für Compliance mit dem Standard gehärtet werden müssen.

Im Folgenden geben wir Ihnen einen Überblick über einige dieser für Netzwerk-TAPs relevanten Anforderungen und zeigen, wie gehärtete Netzwerk-TAPs diese Anforderungen erfüllen können:



Anforderung aus der IEC 62443: Die Komponente muss ein segmentiertes Netz unterstützen.

Netzwerk-TAPs sollten sich, was die Netzaufteilung angeht, transparent verhalten und jegliche Art von Protokollen unterstützen. VLAN oder auch andere Segmentierungen sollten 1:1 durchgereicht werden, Netzwerk-TAPs sollten auf der physikalischen Ebene arbeiten und alle Netzwerkübertragungen, inklusive aller Ethernet-Pakete auf sämtlichen OSI-Schichten, protokollunabhängig und transparent weiterreichen.

Anforderung aus der IEC 62443: Die Komponente muss über eine Möglichkeit verfügen, die Nutzung unnötiger Funktionen, Ports, Protokolle und/oder Dienste gezielt zu verbieten und/oder einzuschränken.

Um diese Anforderung zu erfüllen, sollten Netzwerk-TAPs keine Management-Schnittstelle haben, über die man Funktionen aktivieren bzw. deaktivieren kann. Die Netzwerk-TAPs sollten mit nur der Funktionalität gemäß Anforderung des jeweiligen Kunden geliefert werden. DIP-Schalter, über die man die Funktionalität einstellen könnte, könnten in diesem Fall deaktiviert werden, so dass eine andere als die gewünschte Konfiguration keinesfalls vornehmbar ist.

Anforderung aus der IEC 62443: Das Netzwerkgerät muss gegen die unbefugte Nutzung der physikalischen Werksdiagnose- und Testschnittstellen geschützt sein.

Netzwerk-TAPs sollten keine Diagnose- und Testschnittstelle aufweisen. Ferner sollten Netzwerk-TAPs gemäß dieser Anforderung ohne jegliche interne Schnittstelle geliefert werden. Ein unautorisierter Zugriff für eine mögliche Manipulation der Firmware ist dann technisch nicht möglich.

Anforderung aus der IEC 62443: Das Netzwerkgerät muss entweder direkt oder über eine kompensierende Steuerung einen Schutz vor böartigem Code bieten.

Dies kann sichergestellt werden, indem Netzwerk-TAPs nicht über eine Protokollschicht, eine MAC-Adresse oder IP-Adresse verfügen und somit auch keine Angriffsfläche für die Ausführung von nicht autorisierter Software, beispielsweise über die Netzwerk-Ports, bieten. Ferner sollten Netzwerk-TAPs keine Management-Schnittstelle für eine mögliche Installation von fremder Software besitzen. Des Weiteren sollten Netzwerk-TAPs im Auslieferungszustand auch nicht über eine interne Schnittstelle verfügen.

Anforderung aus der IEC 62443: Netzwerkgeräte müssen manipulationssicher sein und über einen Erkennungsmechanismus verfügen.

Netzwerk-TAPs sollten ein sicheres, stabiles und robustes Gehäuse haben, womit ein physikalischer Zugriff erschwert wird. Des Weiteren sollten Netzwerk-TAPs mit nicht rückstandsfrei ablösbaren Sicherheitssiegeln ausgestattet werden, womit ein unautorisierte Zugriff erkannt werden kann.

Zusätzlich sollten Netzwerk-TAPs mit Sicherheitsschrauben assembliert werden. Gewöhnliche Schrauben besitzen einen Kopf, der mit handelsüblichen Werkzeugen gelöst oder festgezogen werden kann. Sicherheitsschrauben hingegen haben einen Schraubenkopf, bei dem dies nur mit speziellen Werkzeugen möglich ist.

Anforderung aus der IEC 62443: Fähigkeit zur Bereitstellung und zum Schutz der Vertraulichkeit, Integrität und Authentizität von Schlüsseln und Daten des Produktlieferanten, die als eine oder mehrere „Roots of Trust“ zum Zeitpunkt der Herstellung des Geräts zu verwenden sind.

Um diese Anforderung zu erfüllen, sollten Netzwerk-TAPs über einen Mechanismus verfügen, anhand dessen verifiziert werden kann, dass die Firmware die originale, vom Hersteller aufgespielte Firmware ist.

Anforderung aus der IEC 62443: Die Netzwerkgeräte müssen die Integrität der Firmware, der Software und der Konfigurationsdaten, die für den Boot- und Laufzeitprozess der Komponente benötigt werden, vor der Verwendung überprüfen.

Um diese Anforderung zu erfüllen, sollten Netzwerk-TAPs über einen speziellen Chip verfügen, der eine Funktion besitzt, welche vor dem Hochfahren der Netzwerk-TAPs die Echtheit der aufgespielten Firmware prüft (Secure-Boot-Funktion). Die Netzwerk-TAPs starten dann nur im Falle eines positiven Prüfergebnisses die aufgespielte Firmware und verhindern die Ausführung einer manipulierten Version.

5. Fazit

Sind Sie KRITIS-Betreiber oder ein anderer Betreiber eines OT- oder IT-Netzwerkes und wollen compliant mit dem IEC 62443 Cybersecurity-Standard sein? Dann gehen Sie auf Nummer Sicher und verwenden für die Ausleitung Ihrer Netzwerkdaten gehärtete Netzwerk-TAPs!



Gerne beraten wir Sie zu unseren verschiedenen PacketRaven Netzwerk-TAPs und deren Eigenschaften, sowie zu Ihren individuellen Anforderungen. Unsere Kontaktdaten finden Sie untenstehend!



PACKETRAVEN

Modulare, portable und virtuelle **NETZWERK-TAPS** für bis zu 400G



PACKETLION

High-End **NETWORK PACKET BROKER** für bis zu 400G



PACKETTIGER

Kosteneffiziente Next-Gen **NETWORK PACKET BROKER**
als Appliance oder virtuell



PACKETWOLF

Advanced **PACKET PROCESSING** bis zu 400Gbps



PACKETFALCON

Portable und kompakte **PACKET CAPTURE**-Appliances



PACKETGRIZZLY

Modulare & skalierbare **NETZWERK-FORENSIK**-Lösung

