LANline

13,– €
Januar/Februar 2023
2. Februar

IT ■ Network ■ Datacenter www.lanline.de

Security

Neuer Angriffsvektor: Missbrauch von ChatGPT

Confidential Computing

Incident Response sinnvoll planen

Energieverbrauch im RZ senken
DCIM leistet signifikanten Beitrag

Security-Trends, Teil 2: Von NDR bis WAAP
Bedrohte Netzwerke und Kritis-Umgebungen

Schwerpunkt Kupfer- und LWL-Verkabelung
Power over Ethernet sichert Cu-Marktanteile

Network TAPs mit Datendiode

Daten aus kritischen Netzen sicher weiterleiten

Wie lassen sich kritische IT/OT-Infrastrukturen vor Hackerangriffen schützen? Eine Frage, die in instabilen Zeiten wie diesen immer mehr an Brisanz gewinnt. Hinzu kommt, dass für Energieversorger & Co. das Thema Netzwerksicherheit nicht immer ganz oben auf der Agenda steht und zudem die Erfahrung fehlt. So kommt es, dass zur Überwachung des Netzwerkverkehrs häufig SPAN-Ports (Switch Port Analyzer) im Einsatz sind, die einfachste und kostengünstigste Lösung zur Weiterleitung von Datenpaketen an IDS-Systeme (Intrusion Detection System). Die bessere Alternative sind Netzwerk-TAPs (Test Access Points) mit Datendioden-Technik.

Der Gesetzgeber hat auf die zunehmende Bedrohung bereits reagiert: Mit Inkrafttreten des IT-Sicherheitsgesetzes 2.0 am 28. Mai 2021 hat man auch die Kritis-Regelung für kritische Infrastrukturen signifikant erweitert. Diese beinhaltet nun deutlich mehr Pflichten für die Betreiber und mehr Befugnisse für den Staat. So müssen Kritis-Betreiber bis spätestens 1. Mai 2023 auch Systeme und Prozesse zur kontinuierlichen Angriffserkennung etablieren. Dazu gehört die Einrichtung eines SOCs (Security Operation Center) und eines SIEMs (Security-Information- and Event-Management).

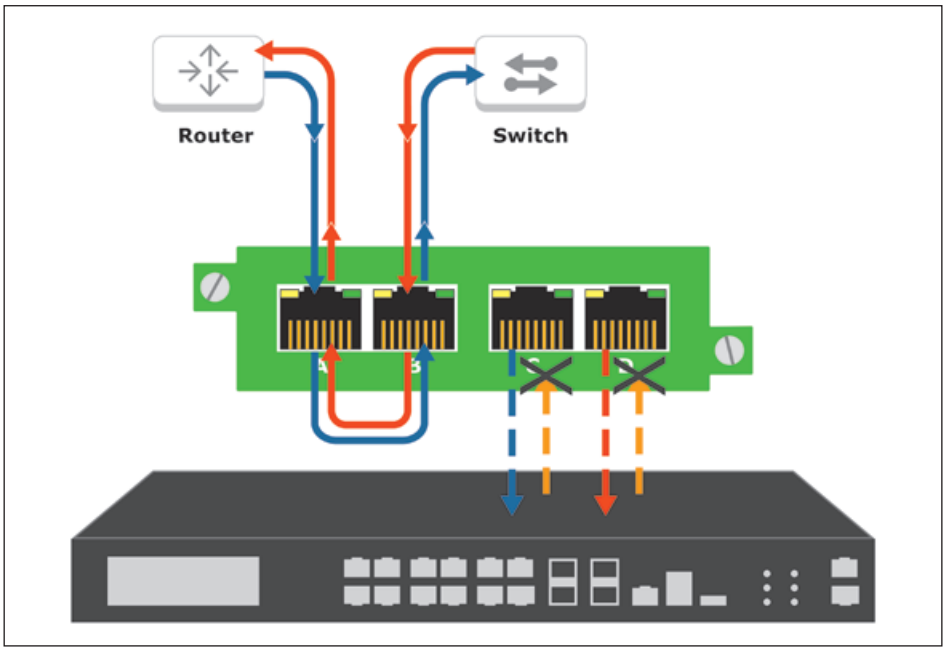

Bild 1. In diesem Szenario ist das Netzwerksignal aus beiden Richtungen gespiegelt und unidirektional als Duplikat auf dedizierte Ports ausgegeben. Es kann dabei keine Packet Injection zurück ins Netzwerk erfolgen. Bild: Netcor

Eine Security-Monitoring-Lösung muss dauerhaft Datenpakete aus dem IT/OT-Netz analysieren, um eventuelle Bedrohungen zu erkennen. Diese Pakete stehen meist als Datenkopie über sogenannte SPAN-Ports zur Verfügung. Häufig keine Berücksichtigung findet die Tatsache, dass bei der Verwendung von SPAN-Ports ein Rückfluss von Daten nicht gänzlich auszuschließen ist. Denn der SPAN-Port ist ein physischer Switch-Port und verfügt daher sowohl über eine Sende- als auch über eine Empfangsfunktion. Somit kann der Switch anfällig für Angriffe von Hackern sein und die einst isolierte OT-Umgebung ist indirekt einer Bedrohung von außen ausgesetzt. Jede SPAN-Verbindung ist letztlich eine Hintertür in das Live-Netzwerk und damit ein potenzielles Sicherheitsrisiko.

SPAN-Ports sind aber auch in anderer Hinsicht problematisch. Zum einen ist die Konfiguration fehleranfällig, denn sie ist keine einfache Aufgabe (vor allem, wenn auch VLANs beteiligt sind). Administratoren können Fehler unterlaufen oder es ergeben sich Probleme durch unbekannte Eigenschaften eines Geräts. Ist ein Port am Switch als SPAN konfiguriert, gibt es Einschränkungen hinsichtlich der maximal zur Verfügung stehenden Bandbreite, die sich an ein Überwachungssystem schicken lässt. Die Verbindung, die zu überwachen ist, tauscht Daten Fullduplex aus – es steht also in beide Richtungen beispielsweise jeweils eine Bandbreite von 1 GBit/s zur Verfügung. Diese Daten aggregiert der Switch und leitet sie an den SPAN-Port. Dieser kann jedoch wie jeder andere Port lediglich mit 1 GBit/s Daten verschicken. Liegt die Auslastung einer Verbindung über 50 Prozent – dauerhaft oder temporär – gehen zwangsläufig Pakete verloren.

Eine weitere Einschränkung, die zu Paketverlust führen kann: Die Pakete der SPAN-Session haben bei hoher Netzwerkauslastung eine geringere Priorität innerhalb des Switches. Die Live-Netzwerk-Ports haben Vorrang. Im Ergebnis verwerfen SPAN-Ports Pakete. Während die Auslastung des

Live-Netzwerks unter normalen Umständen niedrig sein kann, steigt das Verkehrsaufkommen bei einer Sicherheits-Kompromittierung oft erheblich an, was zu einem Verlust der Sichtbarkeit führt. Es besteht also das Risiko, dass man dann am wenigsten Transparenz erhält, wenn man sie am meisten benötigt.

All diese Gefahren lassen sich durch den Einsatz von TAPs mit Datendioden-Technik ausräumen. Bei Datendioden-TAPs handelt es sich um speziell entwickelte Hardware, mit der sich Datenpakete ausschließlich in eine Richtung übertragen lassen. Diese TAPs erstellen eine exakte, kontinuierliche Kopie des Verkehrsflusses. Für Hinweg und Rückweg gibt es jeweils dedizierte Ports, die Daten an das IDS ausgeben, wobei keine Veränderung oder Verzögerung der Pakete erfolgt. Es gibt keinen Rückkanal zwischen den TAPs und dem Netzwerk, was ein Einschleusen von Schadsoftware ausschließt. Zudem sind die TAPs passiv und ausfallsicher, was bedeutet, dass der Datenverkehr weiter fließt, falls die Stromversorgung ausfällt. Netzwerk-TAPs muss man nur einmal zwischen zwei Netzwerkkomponenten einschleifen und bedürfen keinerlei Konfiguration, die Auswirkungen auf die Sicherheit haben könnten. Wichtig ist, dass es sich um Netzwerk-TAPs mit einer Datendioden-Technik handelt.

Passive vs. aktive TAPs

Ein passives Netzwerk-TAP ist ein Gerät, das keine physische Trennung zwischen seinen Netzwerkanschlüssen aufweist. Das bedeutet, dass bei einem Stromausfall des Geräts der Datenverkehr zwischen den Netzwerkanschlüssen weiter fließen kann und die Verbindung aufrechterhalten bleibt. Dies gilt sowohl für Glasfaser-TAPs als auch für Netzwerk-TAPs als Kupferschnittstelle mit 10/100 MBit/s. Glasfaser-TAPs teilen das ankommende Licht in zwei oder mehr Pfade auf und benötigen zunächst einmal keinen Strom. 10- oder 100-MBit/s-Kupfer-TAPs benötigen bei ihrer Verwendung Strom, aber da es keine physische Trennung zwischen den Netzwerkanschlüssen gibt, sind sie auch vollständig passiv. In ihrem Fall bleibt die Verbindung bei einem Stromausfall ohne Failover-Zeit oder Verzögerung bei der Wiederherstellung der Verbindung bestehen. Aus Sicherheitsgründen ist bei passiven TAPs zu beachten, dass eingehendes Licht im Monitorausgang ausreichend gedämpft ist. Indem das von den Monitoranschlüssen kommende Licht blockiert ist, lassen sich mögliche Angriffe oder Störungen verhindern.

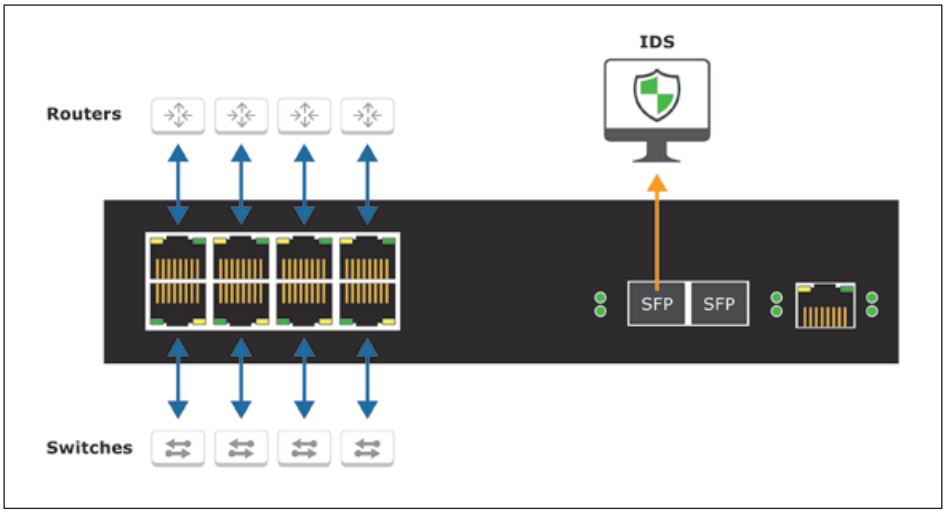

Bild 2. Dieses Vierfach-Network-TAP mit integrierter Datendiode leitet die Paketkopien aggregiert auf einen oder zwei Ports zum IDS weiter. Auch hier kann keine Packet Injection zurück ins Netzwerk erfolgen. Bild: Netcor

Im Gegensatz zu passiven TAPs verfügen aktive TAPs typischerweise über 1-GBit/s-Kupfer-Ports. Die Netzwerk-Ports sind physisch getrennt, was auf die im TAP verwendeten elektrischen Komponenten zurückzuführen ist. Daher benötigen sie einen ausfallsicheren Mechanismus, der sicherstellt, dass das Netz bei einem Stromausfall des TAPs betriebsbereit bleibt. Die Technik basiert auf einer Reihe von Relais, die offen gehalten werden, wenn das Gerät mit Strom versorgt ist. Bei Stromausfall überbrücken diese Relais die elektronischen Komponenten, sodass das Netz betriebsbereit bleibt.

Es gibt jedoch Situationen, zum Beispiel Platzgründe oder eine zu große Anzahl an TAPs, in denen die Verwendung von SPAN-Ports weiterhin erforderlich ist. In diesen Fällen ist es ratsam, die SPAN-Ports mit einem Datendioden-TAP zu verbinden, das gleichzeitig Daten aggregieren kann. So lassen sich die gespiegelten Daten sicher, aggregiert und ohne großen Platzbedarf im Schaltschrank an die Überwachungstools weiterleiten. Wenn ein Unternehmen mehrere TAP- oder SPAN-Ports nutzt, kann das kostspielig sein, denn Intrusion-Detection-Systeme sind nach Leistungsfähigkeit lizenziert. In diesem Fall sollte die Wahl auf Datendioden-Aggregations-TAPs fallen. Sie nutzen ein bewährtes Hardwaredesign und ermöglichen eine verlustfreie Datenverkehrsaggregation. Es lassen sich beispielsweise vier Network-TAPs oder bis zu acht SPAN-Ports zu einem oder zwei Monitorausgängen zusammenführen. Somit reduzieren sich auch die Kosten für die IDS-Lösung.

SPAN-Ports sind ursprünglich für eine temporäre Netzwerkanalyse konzipiert und nicht für einen Dauerbetrieb. Datendioden-TAPs hingegen erlauben es, IT/OT-Sicherheitslösungen rund um die Uhr sämtliche Datenpakete zur Verfügung zu stellen. Nur so ist zu gewährleisten, dass sich das Netzwerk ordnungsgemäß analysieren und schützen lässt, ohne dabei zusätzliche Schwachstellen durch eingehenden Datenverkehr zu schaffen. Aus diesem Grund sind Datendioden-TAPs die ideale Lösung für Hochsicherheitsumgebungen und können in kritischen Infrastrukturen als Verbindungen zwischen zwei oder mehr Netzen unterschiedlicher Sicherheitseinstufung dienen. Die Technik bewährt sich in Kraftwerken ebenso wie in anderen sicherheitskritischen Umgebungen. Jos Op ‘t Root/am

Jos Op ‘t Root ist Geschäftsführer von Netcor.