Zukünftige Netze sind verschlüsselt

Viele Datenverbindungen sind heute angreifbar

Klaus Pollak

Geht es um Cybersecurity steht vor allem die Absicherung der internen Netze im Fokus. Weitverkehrsverbindungen oder Verteilnetze sind dagegen häufig ungeschützt. So lassen sich z.B. Glasfaserkabel mit sehr einfachen Mitteln abhören. Ein wirksamer Schutz erfordert deshalb sichere Verschlüsselungslösungen. Sie unterscheiden sich aber je nach Anforderung und Netzebene.

„Erfolgreicher Hackerangriff auf kommunale Versorgungsunternehmen", „Hacker dringen ins IT-Netz des Verbands Europäischer Übertragungsnetzbetreiber ENTSO-E ein" oder „Verschlüsselungstrojaner zwingt Pipelinebetreiber zur Abschaltung", so lauten einige Meldungen der letzten Monate. Eine der offenen Sicherheitslücken besteht im mangelnden Schutz der Datenverbindungen. So lassen sich Glasfaserverbindungen im laufenden Betrieb sehr einfach abhören. Ein handelsüblicher Biegekoppler für ca. 1.000 € ermöglicht das unbemerkte Überwachen der Daten, da die Kommunikation durch den Zugriff nicht gestört wird. Auch die Einspeisung von Daten durch einen Man-in-the-Middle-Angriff ist über diesen Weg möglich.

Sicherheitslücken bei Kritis-Unternehmen

Weitverkehrsverbindungen, Verteil- und Fernwirknetze gehören zu den kritischen Infrastrukturen (Kritis) mit hohem Schutzbedarf. Hier kommen unterschiedliche Verschlüsselungslösungen zum Einsatz:

Glasfaser-Weitverkehrsverbindungen
Für die Absicherung von Weitverkehrsverbindungen sind Verschlüsselungslösungen auf Layer-1- und Layer-2-Ebene sinnvoll (siehe Textkasten auf S. 38). Sie arbeiten ohne bzw. mit geringem Overhead, minimalen Performance-Verlusten sowie geringen Latenzen und sind deshalb auch für große Datenraten über große Entfernungen geeignet.

Verteil- und Fernwirknetze
Verteil- und Fernwirknetze zur Anbindung von entfernten Standorten und zur Anlagensteuerung werden immer häufiger über das Internetprotokoll (IP) betrieben. Sie lassen sich im Vergleich mit bisherigen SDH-/PDH-Netzen allerdings viel leichter überwachen und manipulieren. Für die sichere Kommunikation z.B. zu Transformatorstationen oder Umspannwerken können Security Gateways eingesetzt werden, die den Datentransfer per IPsec (Layer 3) verschlüsseln.

Kritis-Verschlüsselungslösungen
Die Kritis-Verschlüsselungslösungen müssen die Vorgaben der BSI-Krypto-Richtlinie BSI TR-02102 erfüllen. Sie beschreibt, welche Verschlüsselungsverfahren und Schlüssellängen eingesetzt werden dürfen. Neben der Verschlüsselung sind die Lösungen auch speziell auf die Bedürfnisse (Redundanz, Zuverlässigkeit, Managementsystem) der Kritis-Unternehmen angepasst. Zum Portfolio von Corning Services speziell für Kritis-Unternehmen gehören Verschlüsselungen auf allen Netz-Layern, Secure Gateways und Anomalieerkennung.

Carrier setzen standardmäßig keine Verschlüsselungen ein

Die meisten Carrier setzen in den Netzen derzeit keine generelle Verschlüsselung von Daten ein. Um Verbindungen abzusichern, sind bisher vor allem Geschäftskunden auf eigene Lösungen angewiesen. Die Verschlüsselung von Diensten und Leitungen ist für Carrier daher ein Ansatzpunkt für zusätzliche Angebote und Mehrwertdienste:

- Mehrwertdienste für Geschäftskunden: Mit der Network Function Virtualisation (NFV) können auf der Applikationsebene Netzfunktionen virtualisiert werden. So kann z.B. eine SD-WAN-Applikation in eine Mikro-CPE-Box geladen und als virtuelles Image mit anderen Funktionen wie Verschlüsselungen oder Firewalls unterschiedlicher Hersteller ausgeführt werden.

Klaus Pollak ist Product Care Manager bei Corning Services in Hannover

- Verbindungen zu Cloud-Rechenzentren: Ein typischer Mehrwertdienst ist die Verschlüsselung von Verbindungen zu Cloud-Rechenzentren. Um eine hohe Datenrate zu gewährleisten, sind hier Layer-2- oder Layer-1-Verschlüsselungen sinnvoll.
- Lawful Interception (LI): Carrier ab 10.000 Teilnehmern sind gesetzlich verpflichtet, den überwachenden Behörden LI-Dienste zur strafrechtlichen Auswertung abzubilden, den Transport der angeforderten Daten zu verschlüsseln und bereitzustellen. Die Verschlüsselungsgeräte müssen für den LI-Dienst von dem BSI (VS-NFD) zugelassen sein. Corning Services hat hier im Auftrag von zahlreichen Carriern LI-Dienste zum Ausleiten der Daten übernommen.

Verschlüsselung von VS-NFD-Daten

Behörden klassifizieren vertrauliche Daten und Verschlusssachen je nach ihrer Schutzbedürftigkeit in Geheimhaltungsstufen wie „VS-Nur für den Dienstgebrauch“ (VS-NFD).
Die elektronische Übermittlung geschützter Daten innerhalb einer Behörde über öffentliche Leitungen muss verschlüsselt werden. Dies gilt generell auch für den Transport von personenbezogenen Daten. Dafür dürfen nur Verschlüsselungsboxen mit BSI-Zulassung eingesetzt werden.
Corning Services setzt insbesondere bei dem Transport zwischen Behördenstandorten BSI-zugelassene Verschlüsselungssysteme mit einer Transportverschlüsselung im Layer-2-Bereich ein. Sie benötigt nur einen geringen Overhead mit minimalen Datendurchsatz- und Performance-Verlusten. Die Verschlüsselungsboxen ermöglichen hohe Datenraten zu geringen Kosten und umfassen zusätzliche Carrier-Ethernet-Funktionen und -Services (z.B. OAM, Zertifizierung nach MEF CE-2.0). Ein weiterer Vorteil für die Layer-2-Verschlüsselung in diesem Umfeld besteht auch darin, dass Standard-Ethernet-Mietleitungen verwendet werden können.

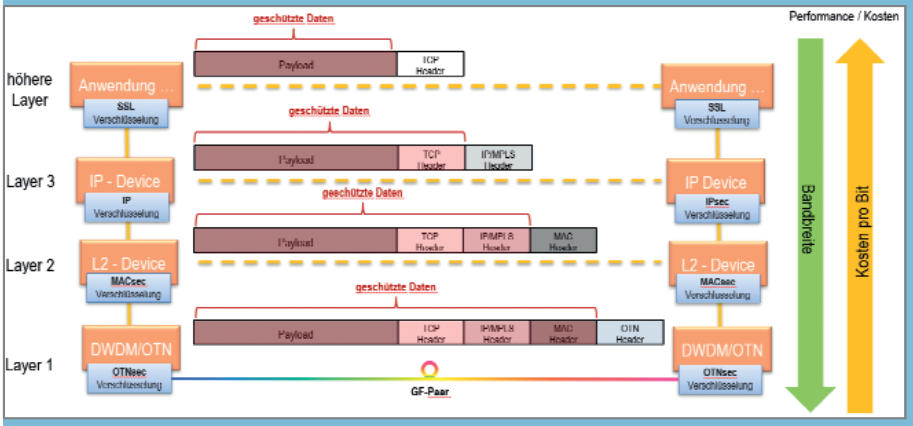
Sichere Vernetzung redundanter Rechenzentren

Laut BSI soll die Entfernung zwischen redundanten Rechenzentren mindestens 200 km betragen. Da die Laufzeitverzögerung mit der Entfernung zunimmt, darf die notwendige Datenverschlüsselung zu keinen zusätzlichen Latenzproblemen führen. Deshalb wird für das Backup und die Kopplung von Ausweichrechenzentren die Layer-1-Verschlüsselung eingesetzt. Sie führt zu keinem zusätzlichen Overhead, keiner nennenswerten Verzögerung der Laufzeit und zu keinerlei Verlusten beim Datendurchsatz.
Corning Services liefert speziell für die Kopplung von Rechenzentren Lösungen mit Layer-1-Verschlüsselung und rechenzentrenspezifischen Schnittstellen wie beispielsweise Fiber Channel. *(bk)*

Verschlüsselungslösungen von Layer 1 bis Layer 3

Layer-1-Verschlüsselung (OTNsec)
Die Verschlüsselung im OTN-Header erfolgt direkt auf der Ebene der Glasfaser (Layer-1-Ebene) und umfasst die komplette Wellenlänge oder die ganze Faser. Es entstehen kein Overhead, kein Verlust beim Datendurchsatz und nur eine sehr geringe Erhöhung der Laufzeit. Der Schlüsselaustausch wird im OTN-Overhead durchgeführt. Die Layer-1-Verschlüsselung eignet sich für alle Transportwege mit hoher Datenrate und zum Beispiel zur Kopplung von Rechenzentren.

Layer-2-Verschlüsselung (MACsec)
Die Verschlüsselung des Ethernet-Frames erfolgt durch Einfügen eines Secure Headers auf dem MAC-Layer (Layer-2-Ebene). Der geringe Overhead führt im Vergleich zur Layer-3-Verschlüsselung nur zu geringen Datendurchsatz- und Performance-Verlusten, insbesondere wenn die Verschlüsselung hardewarebasiert durchgeführt wird. Die Verschlüsselung wird für lokale und Metronetze mit hohem Datenvolumen genutzt und kann aufgrund der niedrigen Latenzen für alle Applikationen eingesetzt werden. Die Verschlüsselung ist standardisiert, der Schlüsselaustausch allerdings herstellerspezifisch und die verschiedenen Lösungen sind daher untereinander nicht kompatibel.



Verschlüsselung versus OSI-Layer

Layer-3-Verschlüsselung (IPsec)
Die Verschlüsselung im IP-Header auf Layer-3-Ebene z.B. per IPsec wird als Applikationsverschlüsselung für einzelne Datenströme verwendet. Sie ist hoch skalierbar und die Lösungen unterschiedlicher Hersteller sind untereinander kompatibel. Die Layer-3-Verschlüsselung hat allerdings auch etliche Nachteile. Der Daten-Overhead für die Verschlüsselung ist relativ hoch, der Datendurchsatz wird stark vermindert und die Laufzeit der Verbindung (Latenz) deutlich vergrößert.