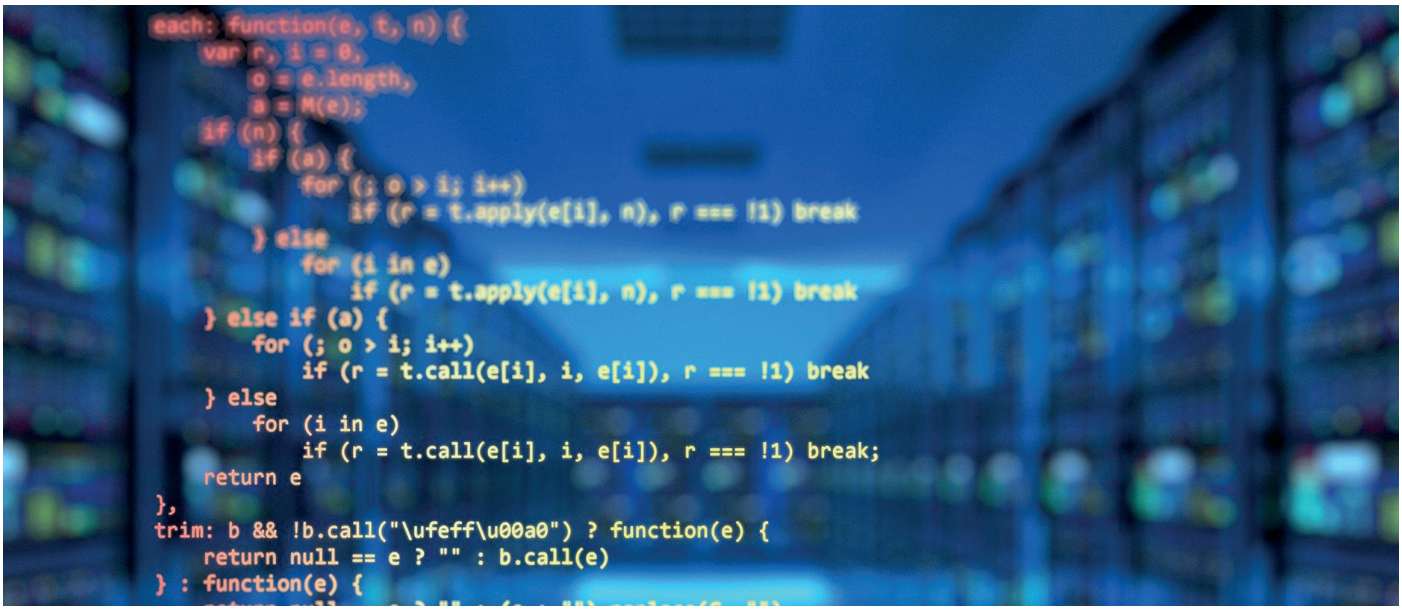
Georedundante Datacenter sicher verbinden

Layer-1-Datenverschlüsselung für Datacenter Interconnect



Bernfried Pawlowski, Klaus Pollak

Aktuelle WDM-Systeme (WDM – Wavelength Division Multiplexing) verbinden georedundante Standorte über mehrere 100 km Distanz mit bis zu 600 Gbit/s. Sie müssen sehr sicher, hochverfügbar und leistungsfähig sein. Dabei wird oft unterschätzt, wie einfach Glasfaserverbindungen abgehört werden können. Für deren Absicherung sind deshalb Verschlüsselungslösungen auf Layer-1-Ebene sinnvoll, weil sie die Laufzeiten nicht verzögern und die Datenraten nicht reduzieren.

Bernfried Pawlowski und Klaus Pollak sind Pre-Sales Consultants bei der Corning Services GmbH

Eine der grundlegenden Sicherheitsanforderungen bei der Speicherung und Verarbeitung von Daten in der Informations- und Operationstechnik (IT & OT) ist die uneingeschränkte Nutzbarkeit der eingesetzten Datacenter-Interconnect-Systeme. Kein Hardware- oder Softwareausfall darf die zu bearbeitenden Daten nachhaltig stören oder unbrauchbar machen. Eine redundante Auslegung der Router, Switche und Speichermodule sowie deren Spannungsversorgung und Be-/Entlüftung gehören daher zu den fundamentalen Konstruktionsmerkmalen sicherer Anlagen. Darüber hinaus bietet nur eine räumliche Trennung der redundanten Komponenten eine umfassende Verfügbarkeit. Sogenannte georedundante Datacenter spiegeln bzw. verteilen die Daten dabei auf Systeme, die hunderte von Kilometer auseinanderliegen. Damit werden die Anlagen vor lokalen Angriffen von Dritten, aber auch vor lokal wirkenden Naturereignissen (Hochwasser, Sturm usw.) geschützt.

Eine der grundlegenden Sicherheitsanforderungen bei der Speicherung und Verarbeitung von Daten ist die uneingeschränkte Nutzbarkeit der eingesetzten Datacenter-Interconnect-Systeme (Foto: Corning Services)

Mit der Datacenter-Interconnect-Technik wird die übertragungstechnische Kopplung der georedundanten Datacenter ermöglicht. WDM-Systeme erhöhen die Datenkapazität der koppelnden Glasfaserleitungen um ein Vielfaches und ermöglichen mit zusätzlichen optischen Überwachungs- und Protektions-Mechanismen ein vollständig knoten- und kantendisjunktes Datacenter bis zur Tier-4-Klassifizierung (99,995% garantierte Verfügbarkeit).

Sichere Datenverschlüsselung

Ein handelsüblicher Biegekoppler für ca. 1.000 € ermöglicht das unbemerkte Auslesen der Daten, da die Kommunikation durch den Zugriff nicht gestört wird. Der Hacker hat so Zugriff auf Kommunikationsdaten und die bestehende Netzstruk-

tur, z.B. auf die MAC- und IP-Adressen der Server. WDM-Technik bietet neben der hohen Daten-Performance und den optischen Überwachungs-/Protektionsmechanismen die Möglichkeit, alle zu übertragenden Daten zwischen den georedundanten Datacentern geheim mit Layer-1-Verschlüsselung zu transportieren.

Die Verschlüsselung auf der Layer-1-Ebene erfolgt direkt auf der Ebene des Wellenlängen-Multiplexings und umfasst einzelne Datenströme, komplette Wellenlängen oder die gesamte WDM-Übertragung. Die eingesetzten WDM-Trans-/Muxponder haben dabei auf der Hardware implementierte Krypto-Chipsätze, die sämtliche Verschlüsselungsalgorithmen enthalten. Durch diese Bauweise und durch die Platzierung der Schlüsselinformation im WDM-Layer (genauer im OTN-Layer) entsteht keine zusätzliche Laufzeitverzögerung und keine Reduzierung der Datenraten, wie das bei Verschlüsselungsmechanismen der höheren Ebenen (z.B. Layer 2 und Layer 3) der Fall ist. Die Layer-1-Verschlüsselung ist deshalb auch für hohe Datenraten über große Entfernungen beispielsweise auf angemieteten Glasfasern die am besten geeignete Absicherung.

Die symmetrische Komponente der Layer-1-Verschlüsselung ist die „Rohdatenverschlüsselung“ nach dem internationalen Advanced Encryption Standard (AES) mit einem 256-bit-Schlüssel und zusätzlicher Integritätsprüfung, z.B. gemäß Galois-Counter-Mode-Algorithmus (GCM).

Der Schlüsselaustausch zwischen den beiden WDM-Endstellen erfolgt mittels der asymmetrischen Komponente der Layer-1-Verschlüsselung. Durch dieses Privat-/Public-Key-Verfahren nach Diffie-Hellman mit Schlüssellängen von mindestens 2.048 bit und turnusmäßiger Schlüsselerneuerung wird die Identifizierung des Kryptoschlüssels durch Dritte verhindert.

Verschlüsselung für Kritis

Verschlüsselungslösungen für kritische Infrastrukturen (Kritis) erfüllen zum Teil die Vorgaben der BSI-Krypto-Richtlinie BSI TR-02102. Die Richtlinie beschreibt, welche Verschlüsselungsverfahren und welche Schlüssellängen eingesetzt werden dürfen.

Diese Zulassung umfasst nicht nur die Verschlüsselungsverfahren und Methoden, sondern zertifiziert auch den Entwicklungs- und Produktionsprozess des Herstellers inklusive der Lieferkette zum Endkunden und dem sicheren Betrieb der Systeme. Wird z.B. bei einer Verschlüsselungsbaugruppe das Gehäuse geöffnet, werden sofort alle Schlüssel unwiederbringlich gelöscht und geben einem Angreifer keine Möglichkeit, die Schlüssel zu kopieren (Tamper-Protection).

WDM-Systeme mit den BSI-Zulassungen VS-NfD (Verschlusssache – nur für den Dienstgebrauch) und VS-V (Verschlusssache – vertraulich) sind am Markt verfügbar.
Neben der Verschlüsselung nach BSI-Zulassung verfügt Corning Services als herstellerunabhängiger Systemintegrator über WDM-Lösungen mit Verschlüsselung, die speziell auf die Bedürfnisse (Redundanz, Zuverlässigkeit, Managementsystem) der Kritis-Unternehmen angepasst sind.

Post-Quanten-Verschlüsselung

Von der Entwicklung von Quantencomputern verspricht man sich einen weiteren großen Schritt in Richtung wesentlich leistungsfähigerer Computer. Allerdings gibt es die Befürchtung, dass mit Quantencomputern heute verwendete Verschlüsselungstechniken nicht mehr sicher sind. Aus heutiger Sicht ist die symmetrische Verschlüsselungstechnik z.B. mit dem Standard AES-256 nicht betroffen, jedoch die zum Schlüsselaustausch verwendeten asymmetrischen Verschlüsselungsverfahren wie Diffie-Hellman könnten gegebenenfalls leichter „geknackt“ werden. Der Grund dafür ist die dem Diffie-Hellman Verfahren zugrunde liegende mathematische Operation für die Generierung des Transportschlüssels aus einem öffentlichen und einem privaten Schlüssel. Es besteht die Befürchtung, dass ein Rückschluss auf den privaten Schlüssel mithilfe eines Quantencomputers einfacher möglich ist.

Sogenannte Post-Quantum-Encryption-Verschlüsselungsmethoden werden derzeit erforscht (z.B. McEliece oder Frodo), sind aber noch nicht abschließend qualifiziert. Eine weitere Möglichkeit des sicheren Schlüsselaustausches ist das QKD-Verfahren (Quantum Key Distribution), das auf Basis von Photonenverschränkung funktioniert und bereits sehr vielversprechend in der Praxis angewendet wird.

Auch wenn bis dato noch kein Datum für die Einführung von Quantencomputern genannt werden kann, sollte die Auswahl von Equipment mit Verschlüsselungstechnik bereits heute die Möglichkeit zum Implementieren von Post-Quantum-Encryption ermöglichen. Dazu muss die Softwarearchitektur flexibel genug sein, um nachträgliche Verschlüsselungstechniken nachrüsten zu können.

www.corning-services.de

Optimierte Konzepte

Corning Services liefert Systeme für Datacenter-Interconnect-Projekte von führenden Herstellern der Branche, erstellt Systemplanungen, Ausführungskonzepte und setzt für die Montage und Inbetriebnahme der Technik eigene spezialisierte Service-Teams ein. Bei der Umsetzung kundenspezifischer Systemlösungen spielen neben den Funktionen und Leistungsmerkmalen auch Aspekte wie die Nachhaltigkeit sowie die strategische Ausrichtung eine Rolle bei der Systemauswahl.