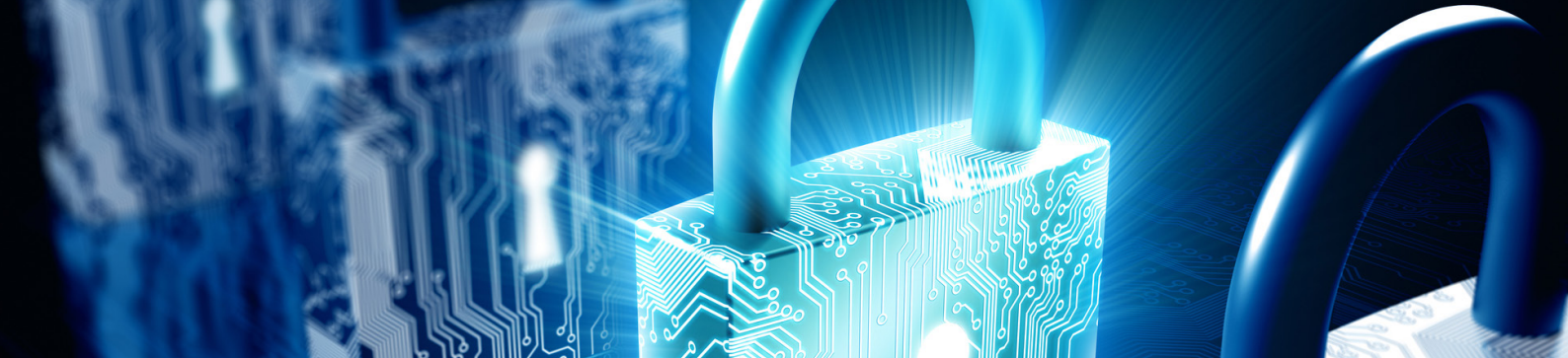


The background of the top half of the page features a conceptual image of several padlocks. The padlocks are rendered with a glowing blue, circuit-like texture, symbolizing digital security. They are arranged in a row, with the central one being the most prominent and brightly lit. The overall color scheme is a deep blue with white highlights from the glowing circuits.

colt

Ethernet-Sicherheit ist
wichtiger denn je

www.colt.net



Der weltweite IP-Traffic soll sich laut Prognosen in den nächsten 5 Jahren verdreifachen. Gleichzeitig steigen die Anforderungen an die Sicherheit bei der Speicherung und Übertragung vertraulicher Daten. Mit zunehmender Virtualisierung von Datenspeichern geben die Dateneigentümer jedoch die Sicherheit in fremde Hände. Weitere potentielle Sicherheitsrisiken entstehen aufgrund der Datenübertragung durch mehrere Provider, Cloud-Hosts und LCR-Algorithmen (Least Cost Routing). Das hat zu einer erheblichen Zunahme von Datenschutzverletzungen geführt, auch im Hinblick auf die Intensität und die Auswirkungen.

Im vergangenen Jahr ist in der EU die Datenschutzgrundverordnung (DSGVO) in Kraft getreten, von der alle Unternehmen und Organisationen betroffen sind, die Waren oder Dienstleistungen innerhalb der EU anbieten. Doch die DSGVO betrifft auch Dritte, die mit persönlichen Daten in Berührung kommen (z. B. Cloud-Provider oder Rechenzentren), ganz gleich, ob sich das Unternehmen oder die Daten innerhalb der EU befinden oder nicht. Fast jedes Unternehmen oder Rechenzentrum, das Daten verarbeitet oder auch nur eine Webpräsenz anbietet, ist für den Schutz der Daten seiner Benutzer aus der EU verantwortlich und haftbar. Die Strafen bei Verstößen sind drakonisch: 2 - 4% des weltweiten Jahresumsatzes oder 20 Millionen Euro (je nachdem, welcher Betrag höher ist).

“Im April 2018 gelang es Hackern, die Verschlüsselung eines Kryptowährungs-Unternehmens zu knacken und mehrere Millionen Euro zu erbeuten. Sie lenkten in einem Interexchange-Knoten in Chicago den Traffic eines Cloud-Dienstes zu einem Server in Russland um. Dieser Vorfall ist symptomatisch für die Problematik des Datentransports im Netz, denn der Server in dem Interexchange-Knoten, über den der Angriff erfolgte, stammte von einem Drittanbieter und verfügte nicht über die notwendigen Sicherheitsfunktionen. Gegen derartige Man-in-the-Middle-Angriffe helfen nur die höchsten Sicherheitsstandards.”

Da sich die globalen Regulierungsbehörden mit dem dringenden Thema Informationssicherheit befassen, müssen Unternehmen eine kohärente und ganzheitliche Strategie für ihre gesamte Technologieinfrastruktur verfolgen. Dadurch rückt das Netzwerk in den Fokus der Sicherheit im Unternehmen.

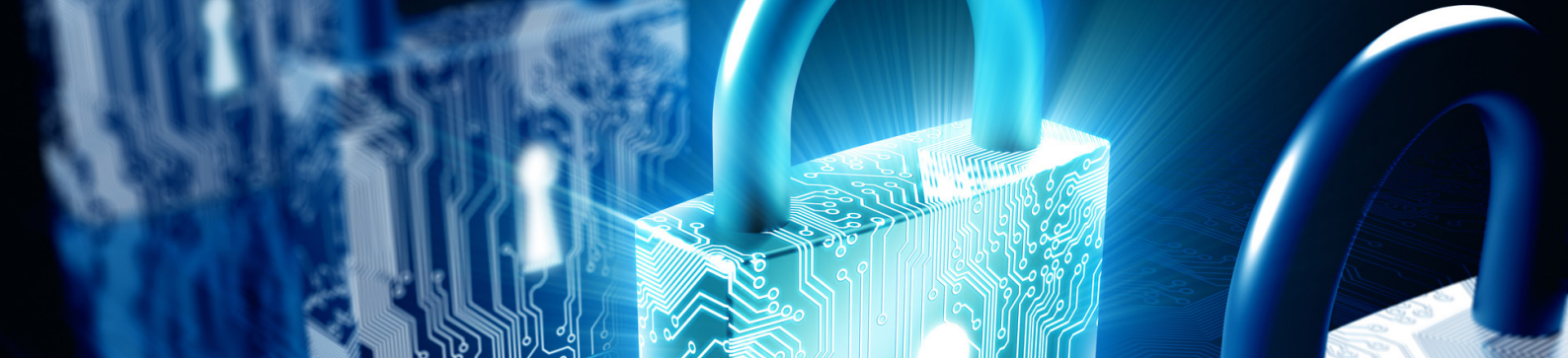
Colt bietet mit Ethernet Encryption eine besonders wichtige Erweiterung seiner Ethernet Services. Diese neueste Ergänzung des Cybersecurity-Programms zielt angesichts verschärfter Bedrohungen und Regularisierungsaufgaben insbesondere auf eine höhere Netzwerksicherheit.

Ethernet Line Encryption: einfach und jederzeit verfügbar

Ethernet Line Encryption ist in Europa, Nordamerika und Asien für Metro-, nationale oder internationale Ethernet-Leitungen verfügbar und bietet Ende-zu-Ende-Verschlüsselung für Hochgeschwindigkeitsverbindungen bis zu 10 Gbit/s, Schlüsselverwaltung durch Colt sowie 24x7-Support durch das Colt Service Assurance-Team.

Ethernet Line Encryption ist besonders relevant für alle Unternehmen, die mit sensiblen Daten arbeiten, z. B.:

- Banken, die eine hohe Sicherheit für Geldautomaten und Filialen benötigen
- Börsen, die auf eine hohe Qualität und eine geringe Verschlüsselungslatenz für Transaktionen und Kursdaten angewiesen sind
- Behörden, denen der Schutz von gespeicherten Daten vor Angriffen aus dem Ausland durch modernste Verschlüsselungstechniken wichtig ist
- Versorgungsbetriebe, die sensible Daten von entfernten Einrichtungen empfangen
- Alle Unternehmen, die innerhalb der EU tätig sind oder über Online-Shops Bestellungen aus der EU annehmen, z. B. Finanzinstitute, Autovermieter, Einzelhändler, Fluggesellschaften usw.



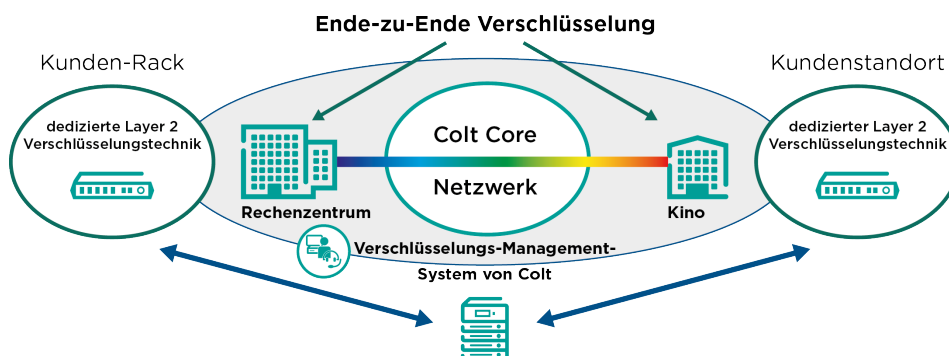
Internationale Filmfestspiele Berlin (Berlinale)

Seit 2009 stellt Colt als Digital Cinema Partner der Berlinale breitbandige Netzwerkservices und Internetzugänge mit bis zu 10 Gbit/s zur Verfügung. Im Jahr 2019 begrüßte das Festival 22.000 Fachbesucher, darunter über 3.500 Journalisten aus 82 Ländern, und verkaufte rund 335.000 Tickets an Festivalbesucher, ein neuer Besucherrekord. In diesem Jahr hat Colt im laufenden Betrieb ein Proof-of-Concept von Ethernet Line Encryption durchgeführt.



Ziel war die lückenlose Absicherung einer Ethernet-Verbindung mit 1 Gbit/s zwischen dem Colt Rechenzentrum in Berlin und einem Kino, in dem einer der Festivalfilme gezeigt werden sollte. Die Inhalte wurden im DCP-Format (Digital Cinema Package) von den Berlinale-Servern an das Kino übertragen und direkt verschlüsselt, um Datenlecks zu vermeiden, denn viele Filme werden auf der Berlinale uraufgeführt. Die Verschlüsselung erfolgte dabei nicht nur auf der physischen Ebene im Rechenzentrum, sondern auch während der Übertragung über das Netzwerk, um lückenlose Sicherheit zu gewährleisten.

Colt stellte modernste Verschlüsselungstechnologie bereit und konnte gleichzeitig die Auswirkungen auf die Ethernet-Service-Performance minimieren - nur 11 µs zusätzliche Latenzzeiten wurden an jedem Ende hinzugefügt.

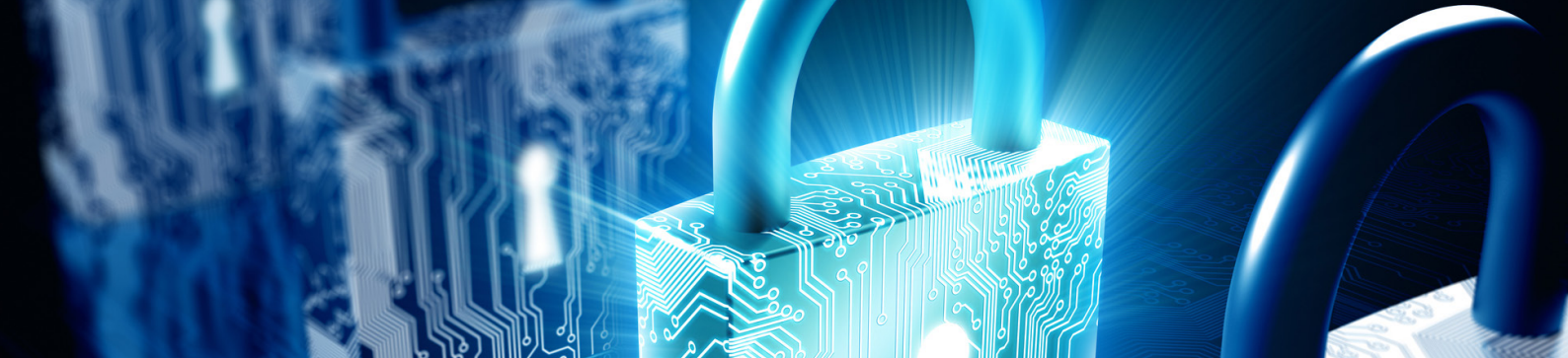


Andere Fallbeispiele von Ethernet Line Encryption:

Krankenkasse mit sicherem IP VPN

Anforderung: Eine Krankenkasse mit 152 Filialen muss bei der Übertragung von Daten an das Rechenzentrum verschiedenste EU-Vorschriften einhalten, darunter die DSGVO, den PCI DSS (Payment Card Industry Data Security Standard) und SOX (Sarbanes-Oxley). Zudem muss das Netzwerk eine redundante Architektur unterstützen.

Lösung: Die unterschiedlichen Standortbandbreiten von 10/50/100 Mbit/s konnten mit standardmäßigen MPLS Services via IP VPN realisiert werden. Das Netzwerk umfasst 152 Standorte, aufgeteilt auf 3 WANs. An allen Standorten befinden sich 1-GbE-Ports und der Verschlüsselungsdienst läuft über MACSec+ Tunnel. So wird der gesamte Ethernet-Frame verschlüsselt und ist damit auch während der Übertragung im Netzwerk vorschriftsgemäß geschützt.



Finanzdienstleister mit globalem Netzwerk

Anforderung: Finanzdienstleistungen decken einen großen Bereich ab, darunter Privat- und Geschäftskunden-Banking, Vermögensverwaltung, Investment-Banking, Immobilien usw. Zu all diesen Dienstleistungen gehört die Speicherung und Übertragung vertraulicher Daten.

Lösung: Die sensiblen Daten bedürfen nicht nur dem angemessenen Schutz, es müssen auch alle Vorgaben der DSGVO erfüllt werden. Das sichere Layer-2 Unternehmensnetzwerk unterstützt jetzt verschiedene Bandbreiten von 10 Mbit/s, 1 Gbit/s und 10 Gbit/s. Alle Verbindungen sind mit Layer-2-MACSec+ verschlüsselt, das für bestmögliche Bandbreite und geringe Latenz sorgt.

Können Sie sich auf Anwendungen zur Verschlüsselung verlassen?

Neue Risiken für Verschlüsselungsverfahren gehen von Quantencomputern aus, denn viele der heutigen Verfahren können ihrer Rechenleistung nicht standhalten. Diese Quantencomputer sind beileibe keine Zukunftsmusik mehr, sondern werden voraussichtlich in den nächsten 5 Jahren zur Realität. IBM bietet seit 2019 bereits den ersten cloud-basierten Quantencomputer.

Die meisten aktuellen Verschlüsselungsverfahren basieren auf Standards aus dem letzten Jahrhundert und letztlich haben Verfahren wie IPSec nur überlebt, weil sie allgegenwärtig sind und Alternativen fehlen. Bei IPSec erfolgt der Schlüsselaustausch nach der DH-Methode (Diffie Hellman). Diese DH-Schlüssel basieren auf mathematischen Mustern, die der Rechenleistung von Quantencomputern nicht standhalten werden.

Um diesen Risiken zu begegnen, werden neue Standards entwickelt, die ab 2022 eingeführt werden sollen. Heute implementierte Sicherheitsgeräte müssen also upgrade-fähig sein. Die Verschlüsselungsprodukte von ADVA können vor Ort auf den neuesten Stand gebracht werden und verfügen schon heute über die nötige Rechenleistung für zukünftige Sicherheitsverfahren.



Für weitere Informationen
www.colt.net/de

Tel: 0800 26584 636
E-mail: sales@colt.net

