VaaS – Verschlüsselung als Mehrwert-Dienst für Hoster, Provider und Systemintegratoren

Ronald Kuhls – Snr. Pre-Sales Consulting
ronald.kuhls@rohde-schwarz.com
Eric Behrendt - Channel Sales Manager
eric.behrendt@rohde-schwarz.com

Rohde & Schwarz SIT GmbH

ROHDE&SCHWARZ

Umweltfaktoren IT Sicherheit

Datenschutz, TKG, GDPdU

IT Sicherheitsgesetz

Sarbanes-Oxley Act (SOX)

BSI Grundschutz

ISO9001, AQAP

Basel II & III

Geheimschutz (VSA)

IT-Sicherheitsgesetz – Entwurf 08/2014

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Allgemein

Ziele:
IT-Systeme und digitale Infrastrukturen Deutschlands sollen die sichersten der Welt werden

Themen:
•Verbesserung der IT-Sicherheit bei Unternehmen, insbes. bei kritischen Infrastrukturen
•Schutz der Bürgerinnen und Bürger in einem sicheren Net
•Schutz der IT des Bundes
•Stärkung des Bundesamtes für Sicherheit in der Informationstechnik
•Erweiterung der Ermittlungs-zuständigkeiten des Bundeskriminal-amtes im Bereich Cybercrime

Speziell für Kritische Infrastruktur

•Meldepflicht von Cyberangriffen (auch anonym)

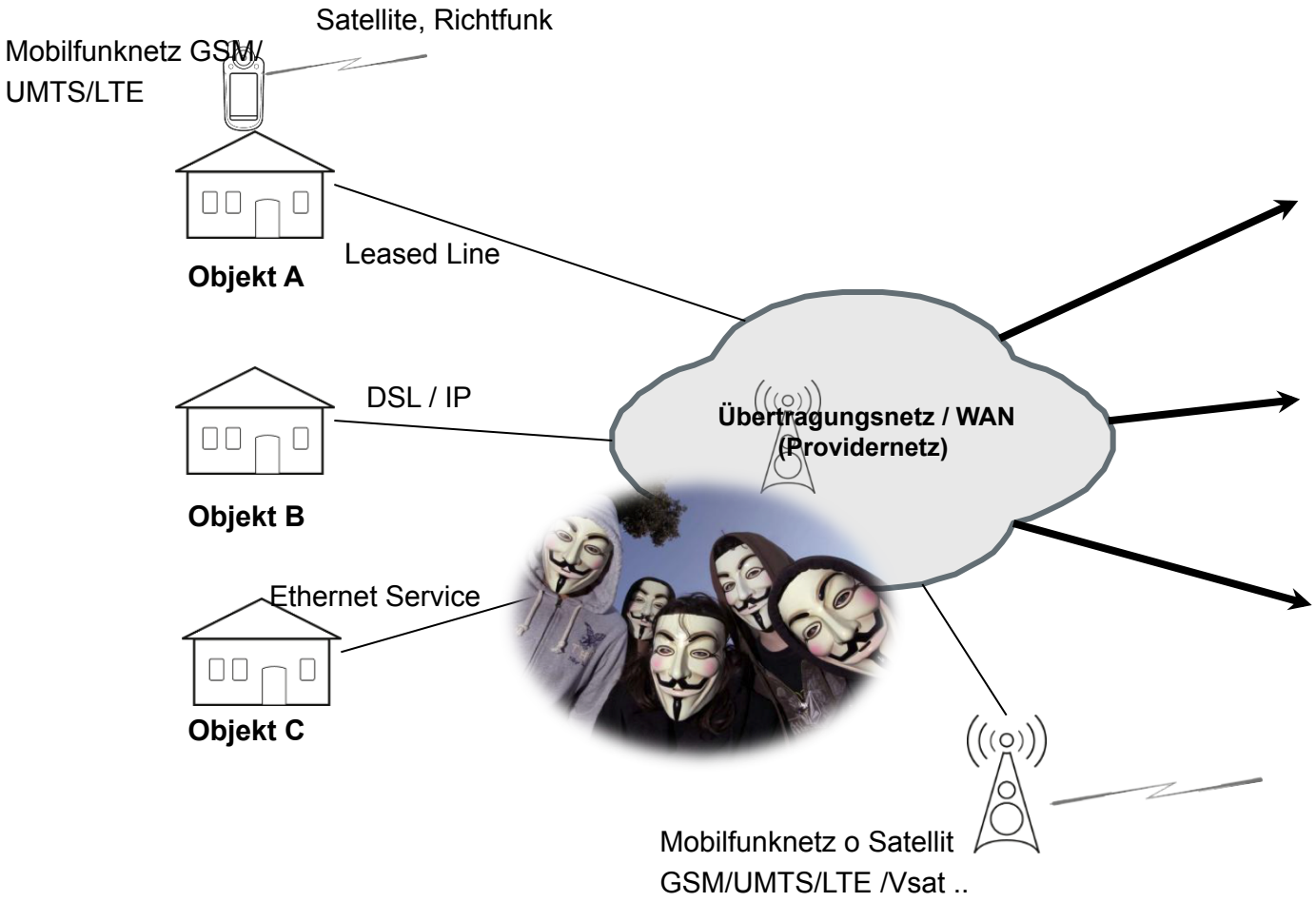
Ab 2015 bindend für Unternehmen der kritischen Infrastruktur:
Bis 2017 haben Unternehmen Zeit für Umsetzung, anschließen sollen Überprüfungen aller 2 Jahre

Datenzustände und Sicherungsmaßnahmen

- **Data @ Rest bzw. Daten in Ruhe**
  - Festplattenverschlüsselung — bleiben nicht ewig nur dort
  - Datenbank Kontentverschlüsselung — **Schlüssel-** und Zugangsverwaltung
  - Datei Verschlüsselung — **Schlüssel**- und Zugriffsverwaltung

- **Data in Motion bzw. Daten auf Reise**
  - Meisten Angriffe erfolgen auf oder über die Kommunikationswege
    - Pishing
    - DoS
    - Abhören
    - Unterschieben
    - Verändern

Schwachstelle Kommunikation



Was tun?

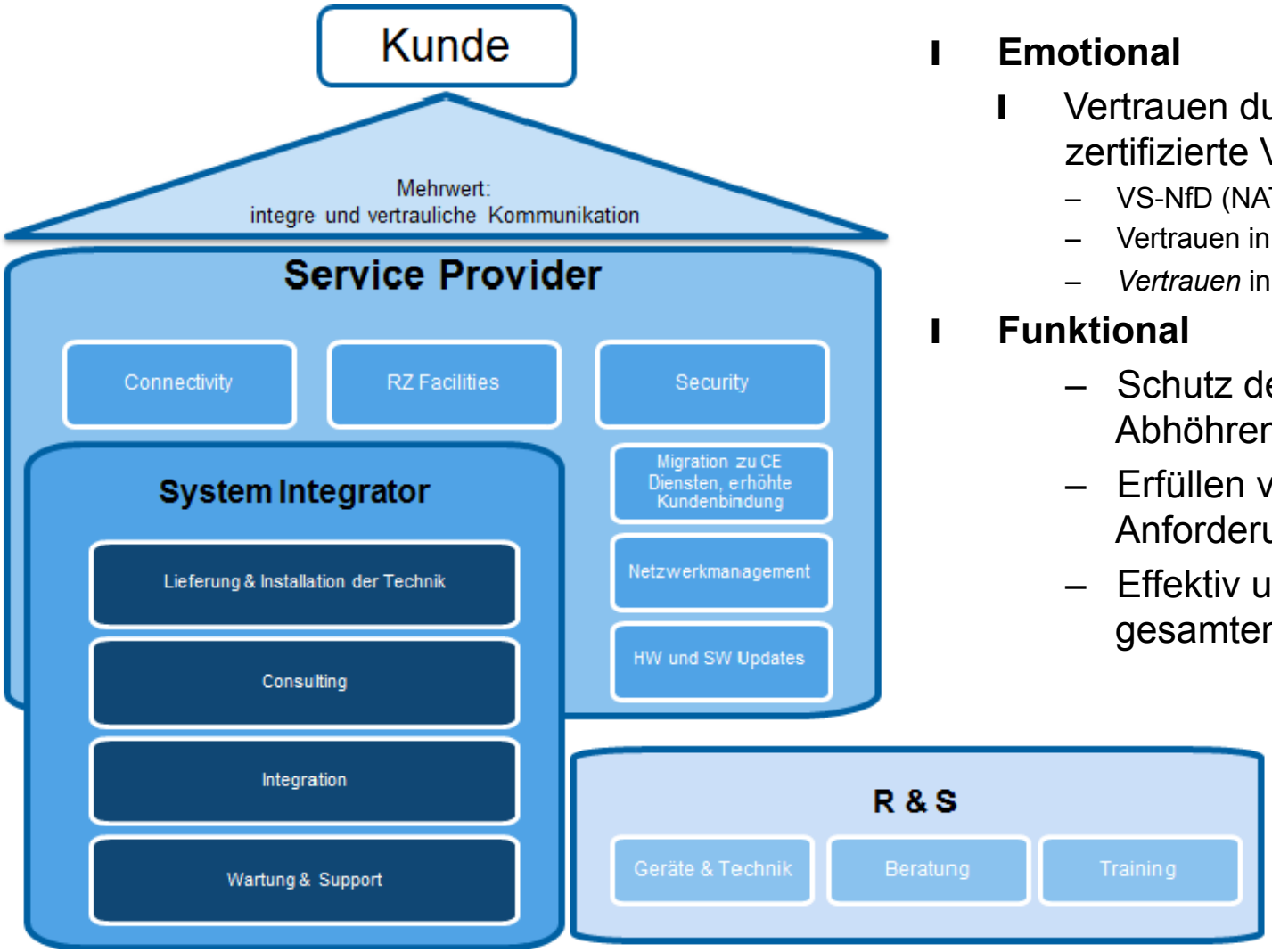
- **Verschlüsseln! Was? und Wo?**
  - Wo schließen sie Türen ab?
  - Wie verschicken sie Werte?
- **Authentisieren! Wie? Wo?**
  - Wie viele Prüfungen auf dem Weg vom Parkplatz zum Abflug?
- **Womit und Wie Verschlüsseln und Authentisieren?**
  - Fahren Sie mit ihrem Wohnmobil stets zur Arbeit?
  - Wieviel Schlüssel haben Sie am Schlüsselbund?

- **Was darf es kosten?**
- **Was habe ich davon ?**
  - Ruhig schlafen? Kaum Betriebsaufwand? Vertrauen der Kunden? Wenig Rückwirkung auf den „Normal Betrieb“?

Schutzmaßnahmen

- **Einsatz vertrauenswürdiger IT, Zertifizierung und Zulassung**
  - Vor allem in sicherheitskritischen Bereichen sollten ausschließlich Komponenten eingesetzt werden, die sich einer Zertifizierung nach einem international anerkannten Zertifizierungsstandard unterzogen haben.(BSI Zulassung : VS NfD, CC EALx)
  - TeleTrust e.V. […] empfiehlt deshalb mit Nachdruck mindestens bei Cloud-Speicherung und **vertraulicher Kommunikation** den Einsatz von Technologie deutscher oder europäischer Anbieter […]

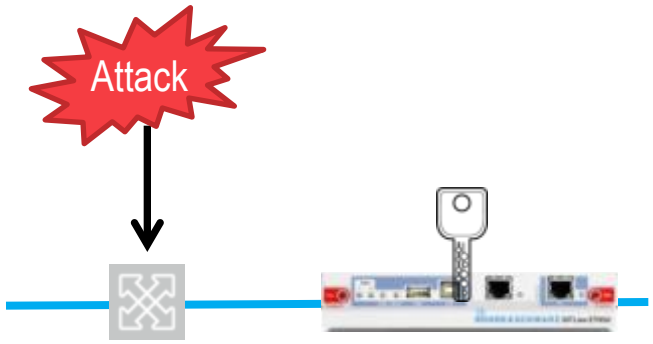
Verschlüsselung als Mehrwert für Endkunden



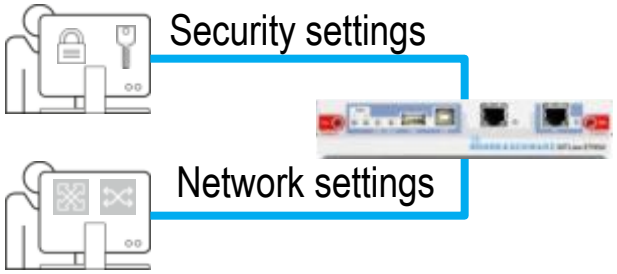
- **Emotional**
  - Vertrauen durch zugelassene, zertifizierte Verschlüsselung
    - VS-NfD (NATO restricted)
    - Vertrauen in den Anbieter
    - *Vertrauen* in die Übertragungswege
- **Funktional**
  - Schutz der Übertagung gegen Abhöhren und Manipulation
  - Erfüllen vom Compliance Anforderungen
  - Effektiv und effizient über den gesamten Lebenszyklus

Warum extern verschlüsseln anstatt im Netzknoten

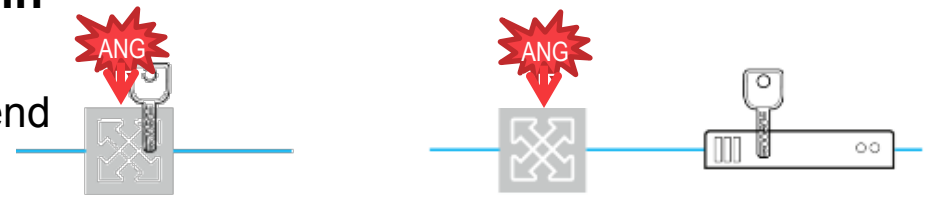
- **trennt Sicherheit vom Netzwerk**
  - Angreifer attackieren oft Netzwerkknoten; hijacked Router gefährden eingebaute Sicherheitsmechanismen



- **physische Separierung trennt Netzwerk- und Sicherheitsmanagement bbereits physisch,**

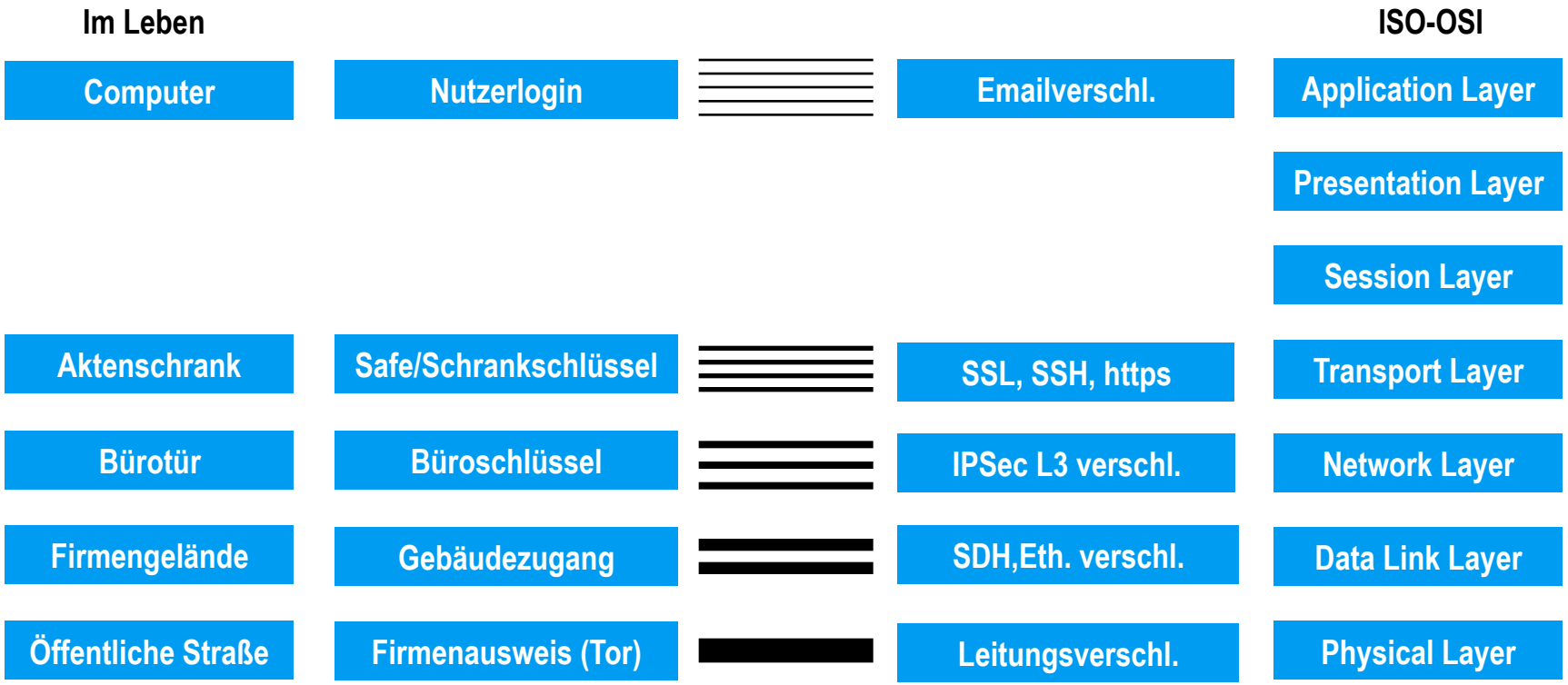


- **Separate Verschlüsselung erlaubt Multi-Vendor Netze und**
- **Risiken und Fehlerpotential wächst in komplexen Systemen exponentiell**
  - Komplexe Systeme sind kaum umfassend prüfbar



Netze und Sicherheit

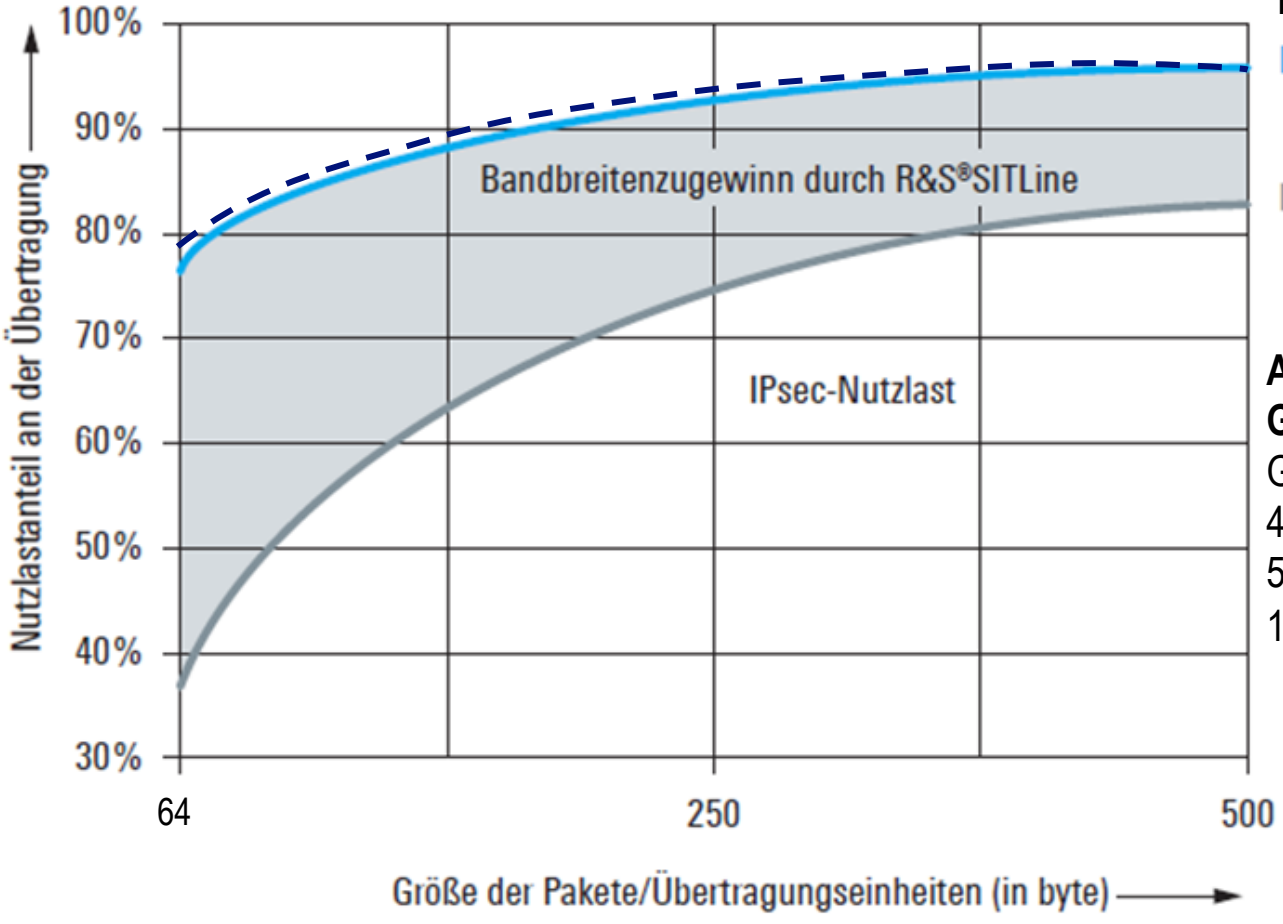
- **Die 7 ISO-OSI Layer und Sicherheitslinien**
- **= Strukturierte Sicherheit oder „gestaffelte Verteidigung“**



Verschlüsselungsansätze im Vergleich

ISO-OSI Ebene	Layer 1 (WDM, Link)	Layer 2 (Ethernet)	Layer 3 (IP)
Pro's	+ Kein Overhead + Wenig Angriffsfläche (verschlüsselter Bitstrom) + Geringste Latenz	+ Geringer Overhead + Point-Multipoint und Multipoint- Multipoint + Geringe Latenz + Wenig Angriffsfläche (verschlüsselte Datenpakete) + Protokoll unabhängig (IPv4, v6; FCoE; …)	+ Flexibler Einsatz Vermittlung und Übertragung gekoppelt + Point-Multipoint and *Full-mesh* + Mobile use cases + Cross vendor operation (IPsec standard) + Many access services are IP based
Con's	– Punkt zu Punkt – Kein Integritätsschutz – Schlüsselmanagement ist problematisch (key negotiation key exchange) – Selten End to End	– L2 Dienst notwendig – IP Ádressierung nicht sichtbar	– Vermittlung und Übertragung gekoppelt – Rel. großer Overhead – IPSec ist ohne Multicast – Hohe Latenz – komplexe Verwaltung
Verschlüsselung für …	Standleitungen	Leitungsvermittlung (auch LAN)	Geroutete Netze
Beispiel	▪ DWDM Verschlüsselung	▪ Verschlüsseltes Ethernet VPN [EPL, EVPL (VPWS), ELAN, EVPLAN(VPLS)]	▪ IPSec, GetVPN

Datenstau durch Verschlüsselung? Kommt darauf an …



Ethernet pur

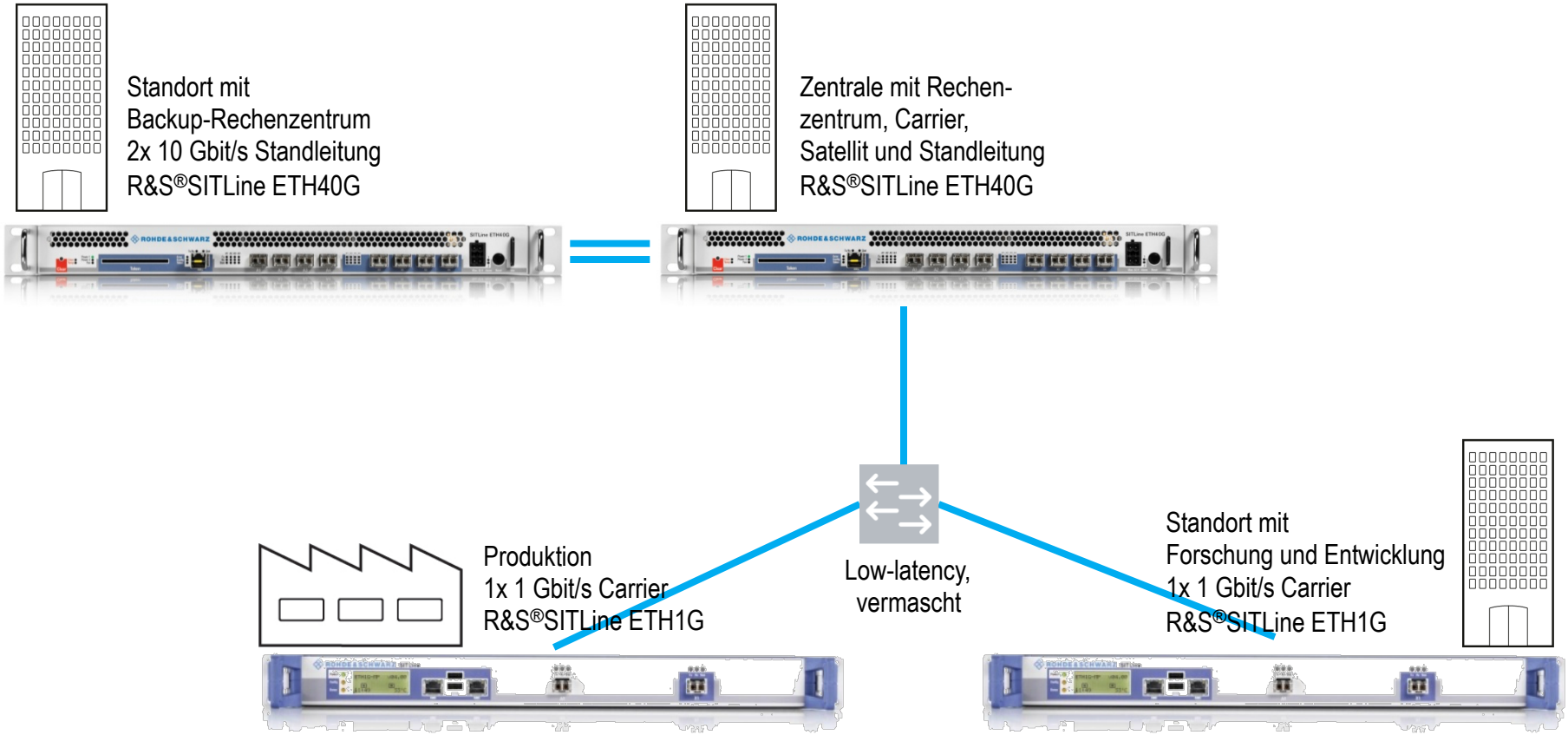
L2-Verschlüsselung

IPsec-Verschlüsselung

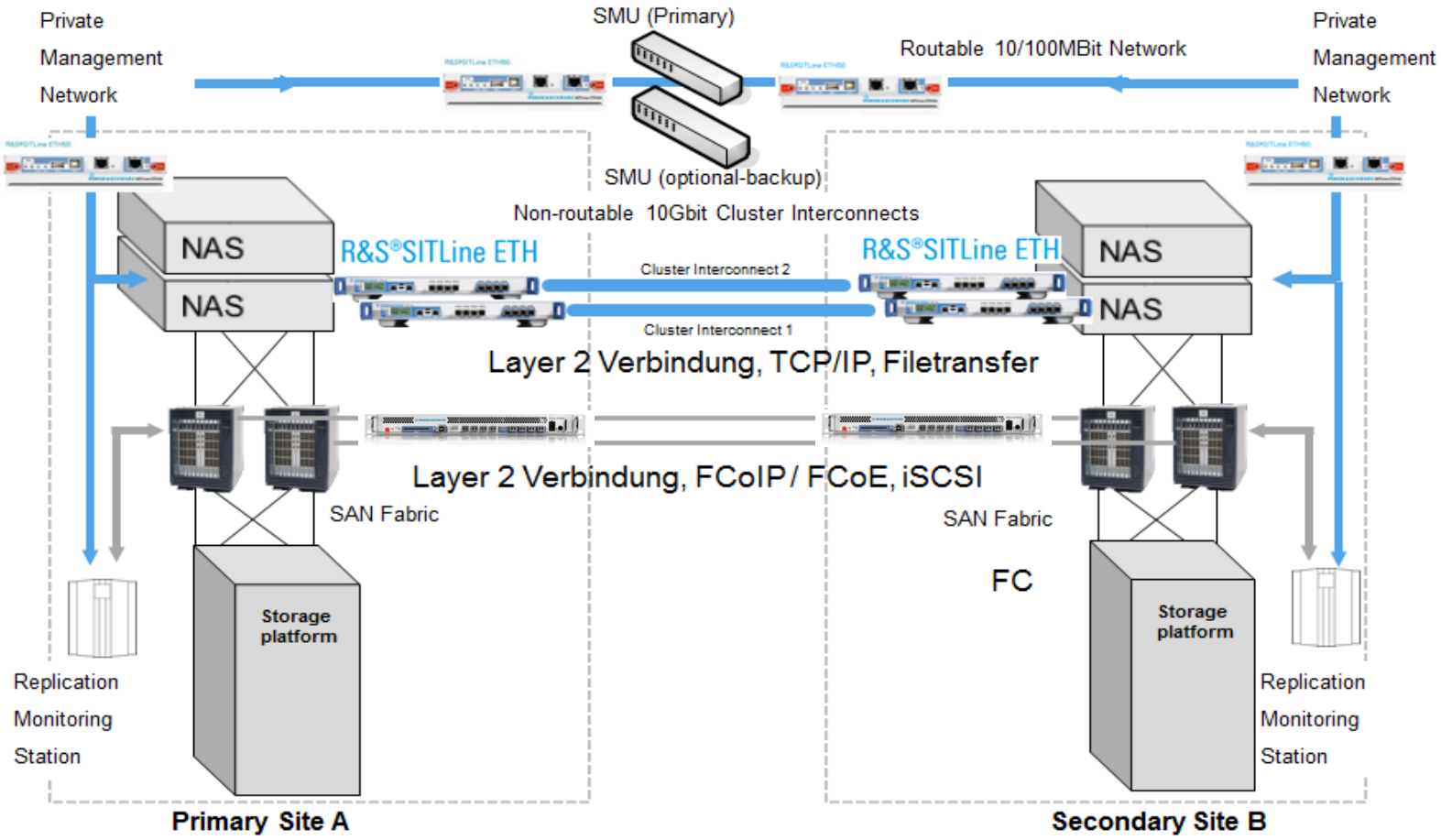
Aufteilung IP-Pakete nach Größe („IMIX Traffic“)

Größe	Anzahl
40 Byte	7
576 Byte	4
1500 Byte	1

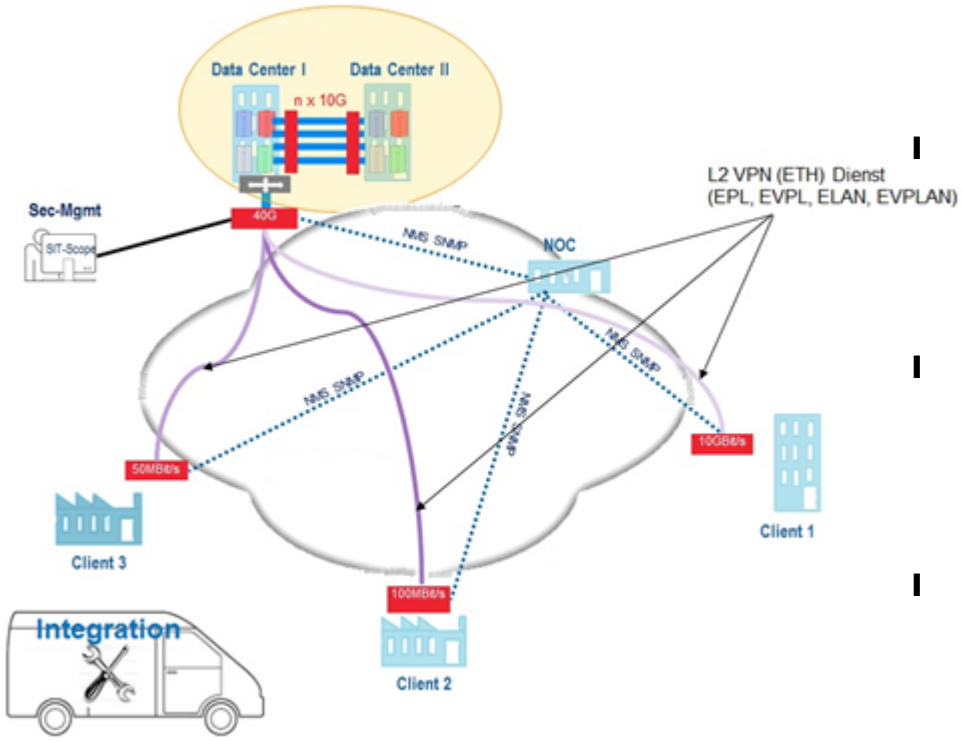
Anwendung:
Low-Latency und sichere RZ-Kopplung



Anwendung: gesicherte SAN Kopplung



VaaS mit gesicherten Layer 2 Cloud Dienst



- **Punkt zu Punkt / zu Mehrpunkt Verbindungen**
  - Physikalisch pro Port abgebildet
    - Kundenindividuelles Equipment
  - Logisch dargestellt
    - auf VLAN Basis
- **Ethernet WAN-Dienste**
  - Ethernet Private Line (EPL)
  - Ethernet Private Line (EPLAN)
  - Ethernet Virtual Private Line (EVPL)
  - Ethernet Virtual Private LAN (EVPLAN)
- **Bandbreiten je Standort**
  - 40Gbit/s; n*10Gbit/s; 1Gbit/s; n*1Gbit/s,
  - 100Mbit/s; n*100Mbit/s
  - 50,25,10 Mbit/s (auch als EFM via DSL)
  - 1-10 Mbit/s als EFM via DSL
- **Management**
  - Netzwerkmanagement (inband)
  - Sicherheitsmanagement
    - über Partner (wg TKÜV, vglbar mit managed IP)
    - alternativ als Secure ++ Dienst –> Kunde

You act.
We protect.