DDoS Angriffe – kein Grund zur Entwarnung

Lernen Sie, wie Sie mit TÜV Rheinland und der DDoS Lösung von Link11 Ihr Unternehmen vor hochvolumetrischen Angriffen schützen!

TÜVRheinland®
Genau. Richtig.

Ihre Referenten

Robert Specht

Channel and Alliance Manager

TÜV Rheinland i-sec GmbH

Marko Richter

Channel Manager

Link11 GmbH

TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema
1	TÜV Rheinland i-sec GmbH
2	Link11- DDoS Angriffe – kein Grund zur Entwarnung!

TÜV Rheinland i-sec GmbH

Standorte Deutschland

- Köln (HQ)
- München
- Gelnhausen
- Saarbrücken
- Hannover
- Hamburg

Fachliches Kompetenzteam

- 20 × Sales
- 20 × Security Engineering
- 60 × Management Beratung
- 45 × Professional Service und Betrieb

Kernbranchen und Sitz unserer Kunden

- Finanzen
- Automobil
- Energiewirtschaft
- Chemie/Pharma
- Telekommunikation
- Int. Mischkonzerne
- Transport/Logistik
- Öffentlicher Dienst
- Handel

! Projekteinsatz an 25.000 Tagen in 2017.

TÜV Rheinland – Globaler Partner für Ihre Sicherheit

Prüfen und Schützen seit 1872

139 Mio. € Umsatz

600 Spezialisten

Industrie 1.0
Mechanische Produktion

Industrie 2.0
Massen-produktion & Elektrizität

Industrie 3.0
Elektronik & IT Systeme

Industrie 4.0
Cyber-Systeme, Social, Mobile, Analytics, Cloud

! Die 4. industrielle Revolution wird durch die Nutzung von Cyber-Systemen definiert.

TÜVRheinland®
Genau. Richtig.

DDoS-Angriffe – kein Grund zur Entwarnung!

Agenda

- Bedrohungslage Q3 2018 durch DDoS Angriffe
- Wann ist die Gefahr eines Angriffes am höchsten
- Angriffsvolumen und Multivektoren-Angriffe
- Schutzlösungen im Überblick
- Link11

Rückblick Q3 2018

15.934 Attacken

Die vom LSOC registrierten Attacken erreichten zwischen Juli und September mit 15.934 Attacken erneut einen sehr hohen Wert.

+71 % Zuwachs

Im Vergleich zum vorherigen Quartal hat die Zahl der DDoS-Attacken im 3. Quartal um 71 % zugenommen.

885 Attacken/Tag

Am 17. August starteten DDoS-Angreifer innerhalb von 24 Stunden 885 Attacken.

Rückblick Q3 2018

370,5 Gbps

Das LSOC registrierte eine Spitzenbandbreite von 371 Gbps sowie zahlreiche weitere Attacken mit mehr als 300 Gbps.

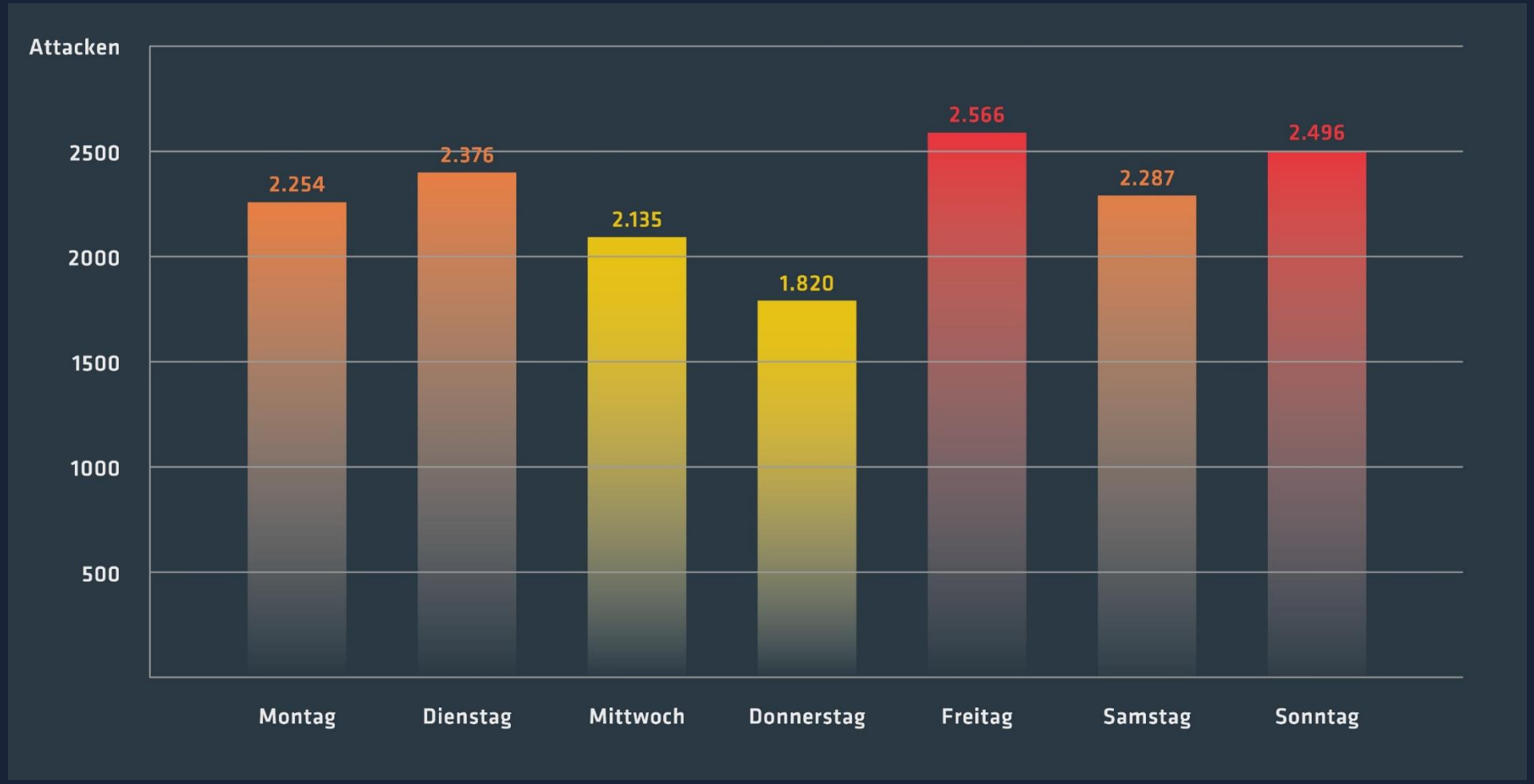
16-24 Uhr

DDoS-Angreifer kennen weder Feierabend noch Wochenende, zwischen 16 und 24 Uhr starten sie die meisten Attacken.

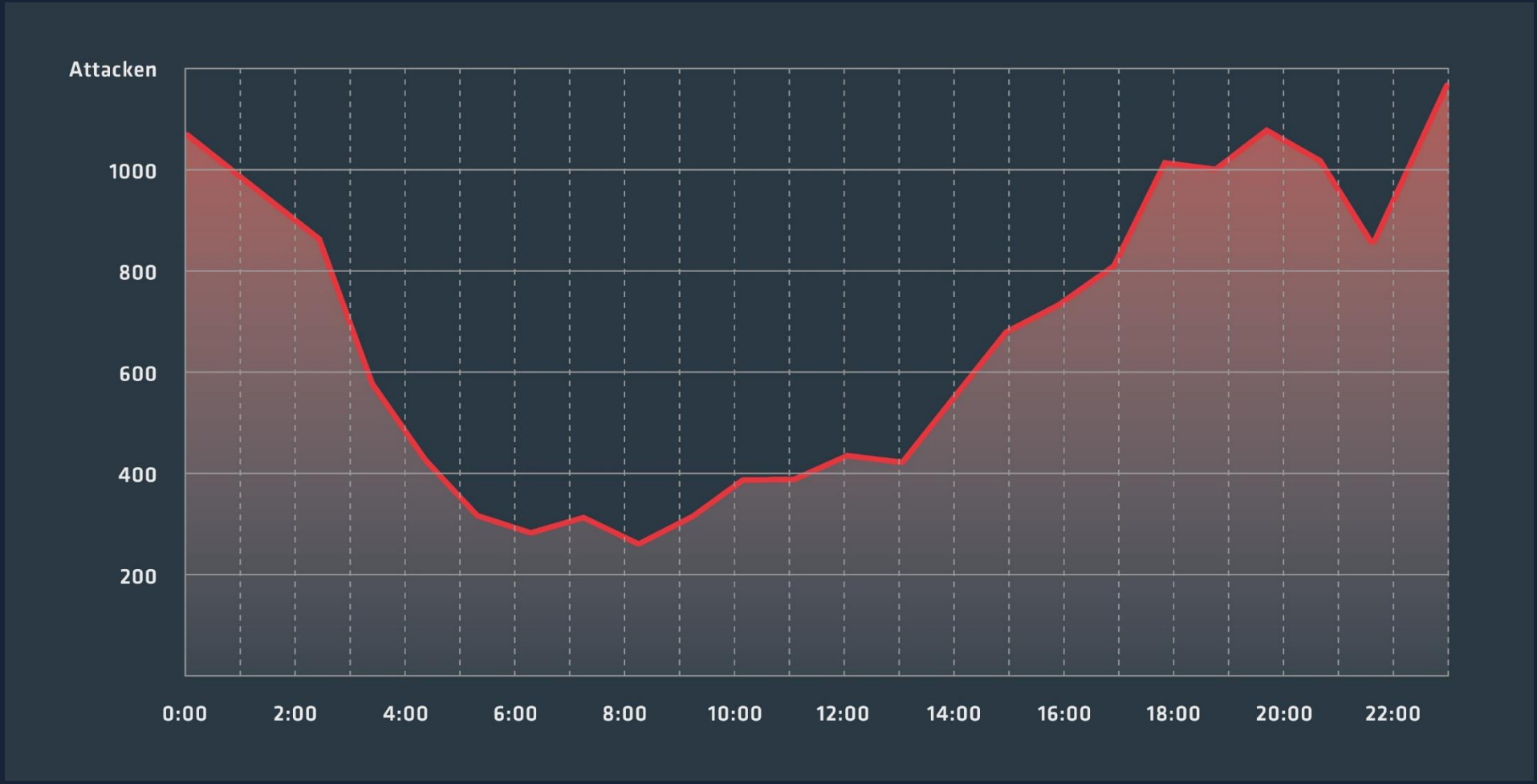
59 % Multivektor

In über der Hälfte aller DDoS-Attacken, nämlich 59 %, kombinierten die Angreifer mehrere Vektoren, um ihr Ziel zu erreichen.

DDoS-Attacken nach Wochentagen



DDoS-Attacken nach Uhrzeit



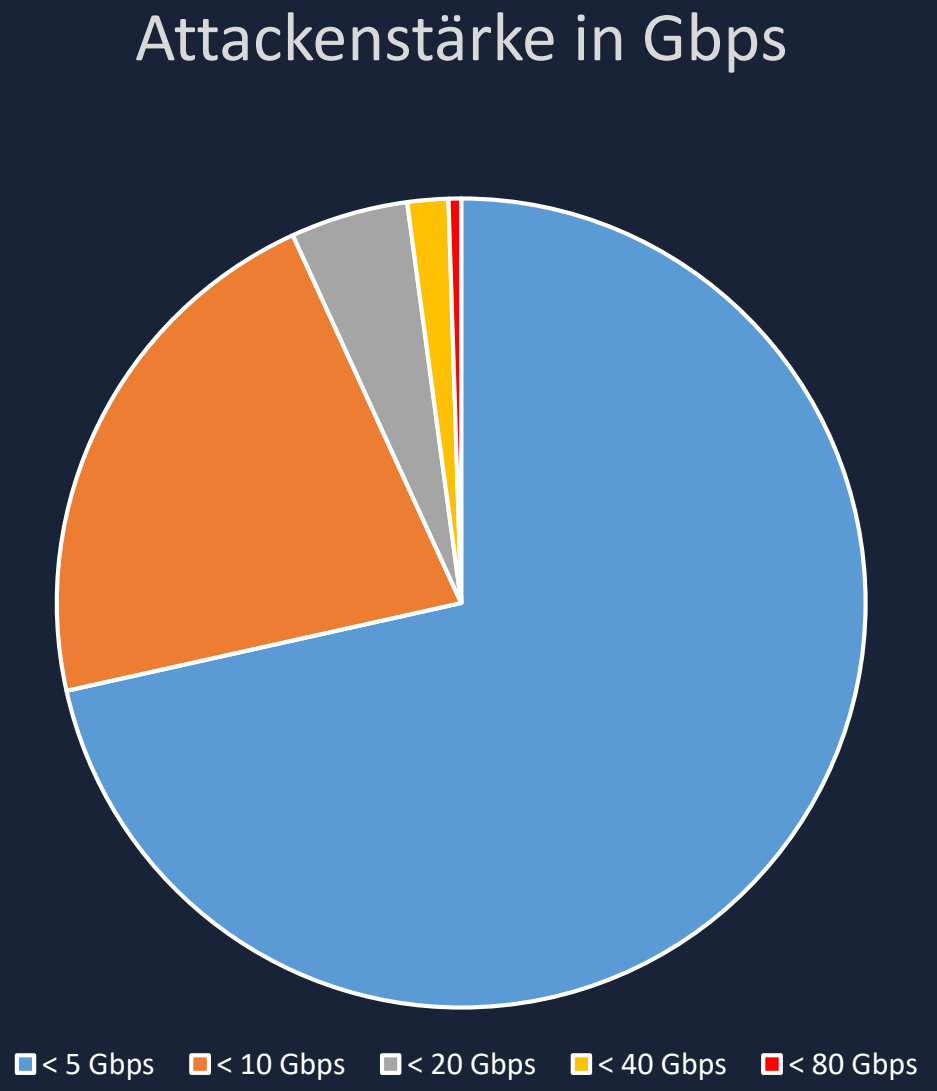
- Angriffe finden i.d.R. zu Zeiten statt, in denen IT Abteilungen schlecht besetzt sind
- Vermehrt werden Portale und Apps attackiert, wenn diese am meisten genutzt werden

Angriffsvolumen von DDoS-Attacken

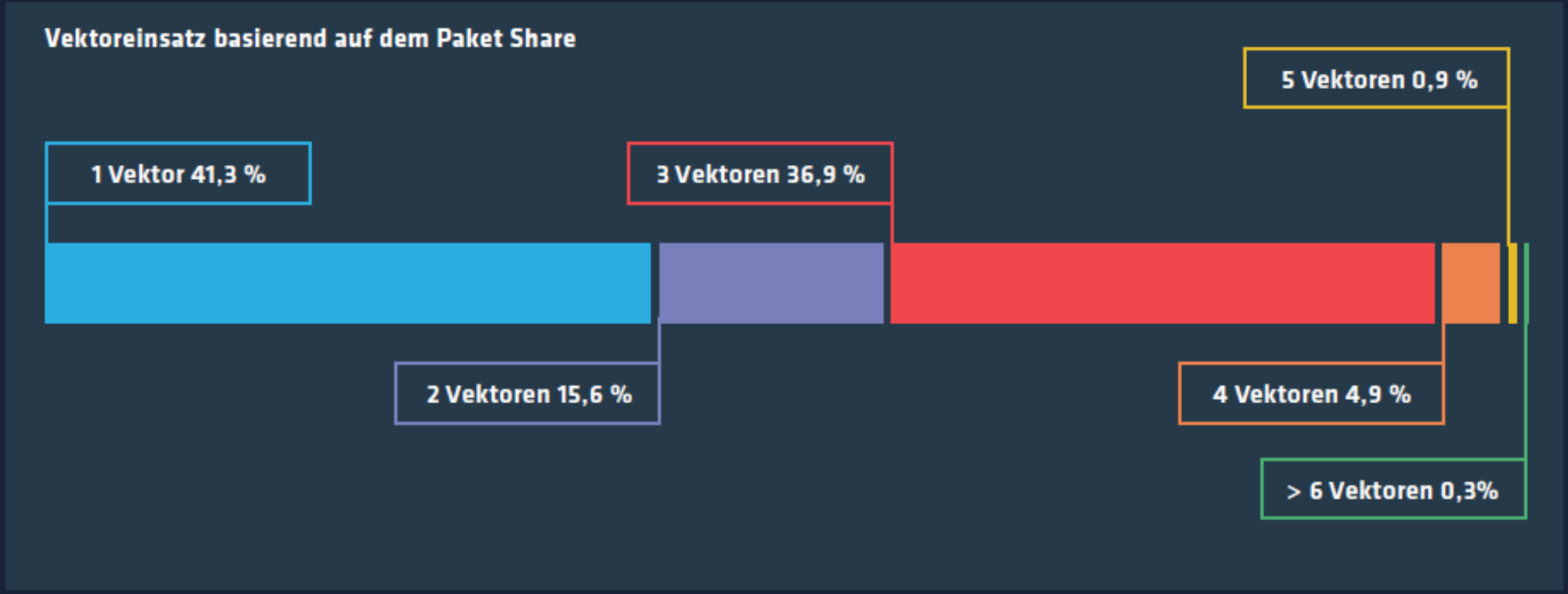
Kleinvolumige Angriffe bis 5 Gbps sind nach wie vor der STANDARD mit **71,3%**

Angriffe mit bis zu 40 Gbps legten auf 28% zu, was einer **Steigerung von 250%** zum Vormonat entspricht

48 Attacken mit **mehr 80 Gbps**

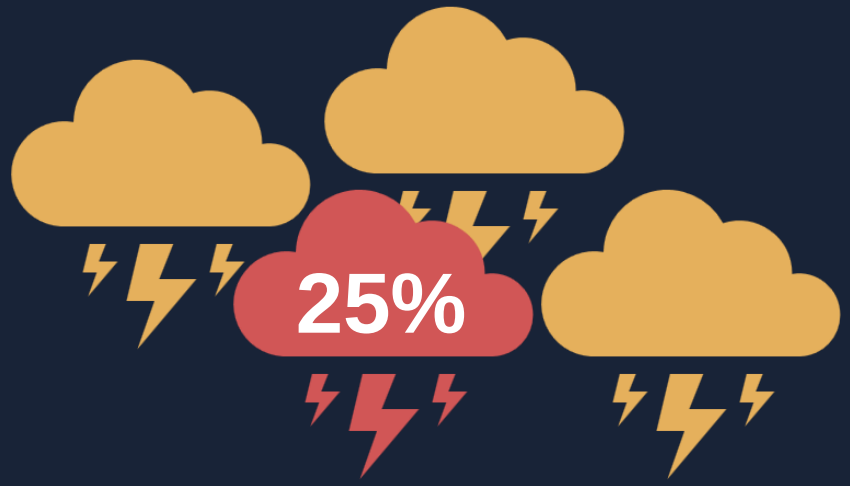


Multivektoren-Angriffe



MODERN CYBERCRIME

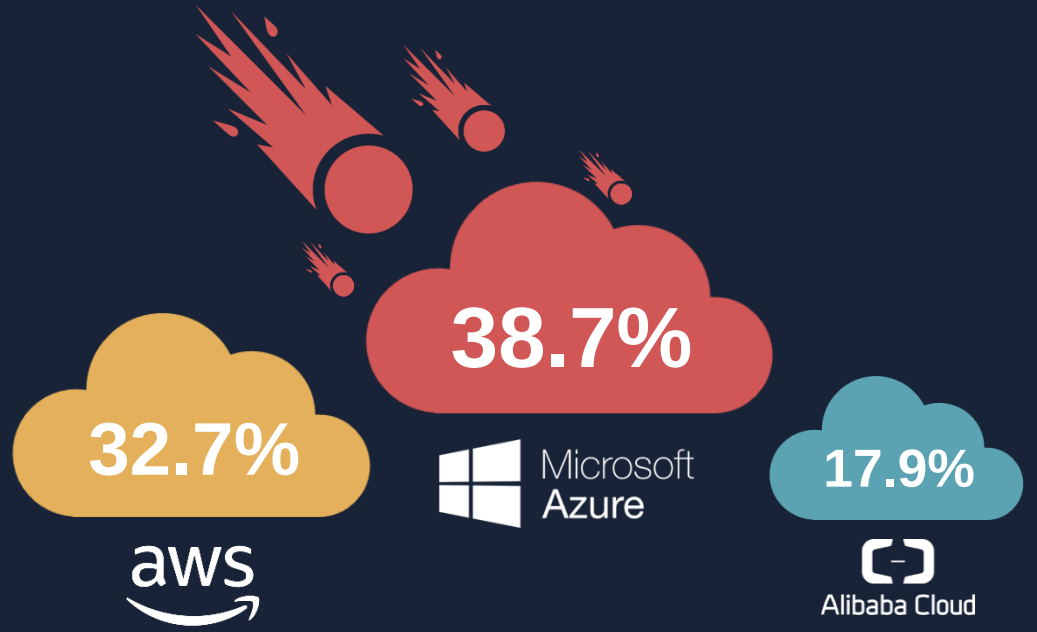
June 2017 ➡ June 2018



A quarter of attacks in Europe was run off public cloud servers.

Equating to a 35% rise compared with the previous year.

Source: Data accrued by DDoS mitigation software supplier, Link11



The Microsoft Azure platform emerged as the most readily exploited by DDoS attackers.

Source: Data accrued by DDoS mitigation software supplier, Link11

Schutzlösungen

Bordmittel (Firewall, Router, Load Balancer, …)
+ kein zusätzlicher Invest, Einhaltung der eigenen TOMs und Datenschutzstandards
- Begrenztes Schutzniveau, Limitierte Netzwerkanbindung, Schutzniveau = Außenanbindung, hoher Wartungsaufwand

DDoS-Appliances
+ Granulare Filterung, gute Angriffserkennung, Einhaltung der eigenen TOMs und Datenschutzstandards möglich, Schutz lokaler Infrastruktur
- Skalierung begrenzt, hohe Anschaffungskosten, Schutzniveau=Außenanbindung, hoher Wartungsaufwand, aufwändige Integration

ISP Backbone DDoS Schutzlösungen
+ Schutz vor sehr großen Volumenangriffen
- Lange Mitigationszeiten, Nicht Provider-Neutral, Keine Angriffserkennung von Applikationsattacken / komplexen Attacken

Cloud Web-Schutz
+ Granulare Filterung, gute Angriffserkennung, unbegrenzte Skalierbarkeit, schnelle Integration, Redundanz, Schutz vor riesigen Attacken
- Datenschutzstandards des Landes, in dem der Filter steht, sind zu beachten, ggf. Zertifikat-Weitergabe, zusätzlicher Infrastruktur-Schutz notwendig

Cloud Infrastruktur-Schutz
+ Granulare Filterung, gute Angriffserkennung, unbegrenzte Skalierbarkeit, schnelle Integration, Redundanz, riesige Attacken, lokale Infrastruktur
- Datenschutzstandards des Filterstandortes beachten, zusätzlicher Applikationsschutz notwendig

Schutzlösungen/Kombinationen

Appliance + Infrastruktur DDoS Schutz Standby

Einsatzszenario:
Kunde mit großen Aussenbandbreiten (min. 20Gbit Uplinks)

Zu beachten:
Häufiges Umschalten ist zu vermeiden
Aufwendige Administration
I.d.R. ist kein Schutz für Applikationen (Layer7) beinhaltet

Vorteile:
Entspricht hohen Datenschutzanforderungen

ISP Backbone + Web DDoS Protection

Einsatzszenario:
Kunde mit einem oder wenigen Providern und Standorten

Zu beachten:
Zu klären sind die Abläufe für die Mitigation

Vorteile:
Entspricht hohen Datenschutzanforderungen
Schutz von Layer 3-7

Cloud Infrastruktur & Web DDoS Protection

Einsatzszenario:
Kunden ohne 24x7 SOC/NOC

Zu beachten:
Datenschutzbestimmungen
Konfiguration von BGP Routen
Bei GRE Verbindungen beachten Sie die MTU Sizes

Vorteile:
Schutz von Layer 3-7
Kombinierbar mit vielen weiteren Addons

Link11 Facts

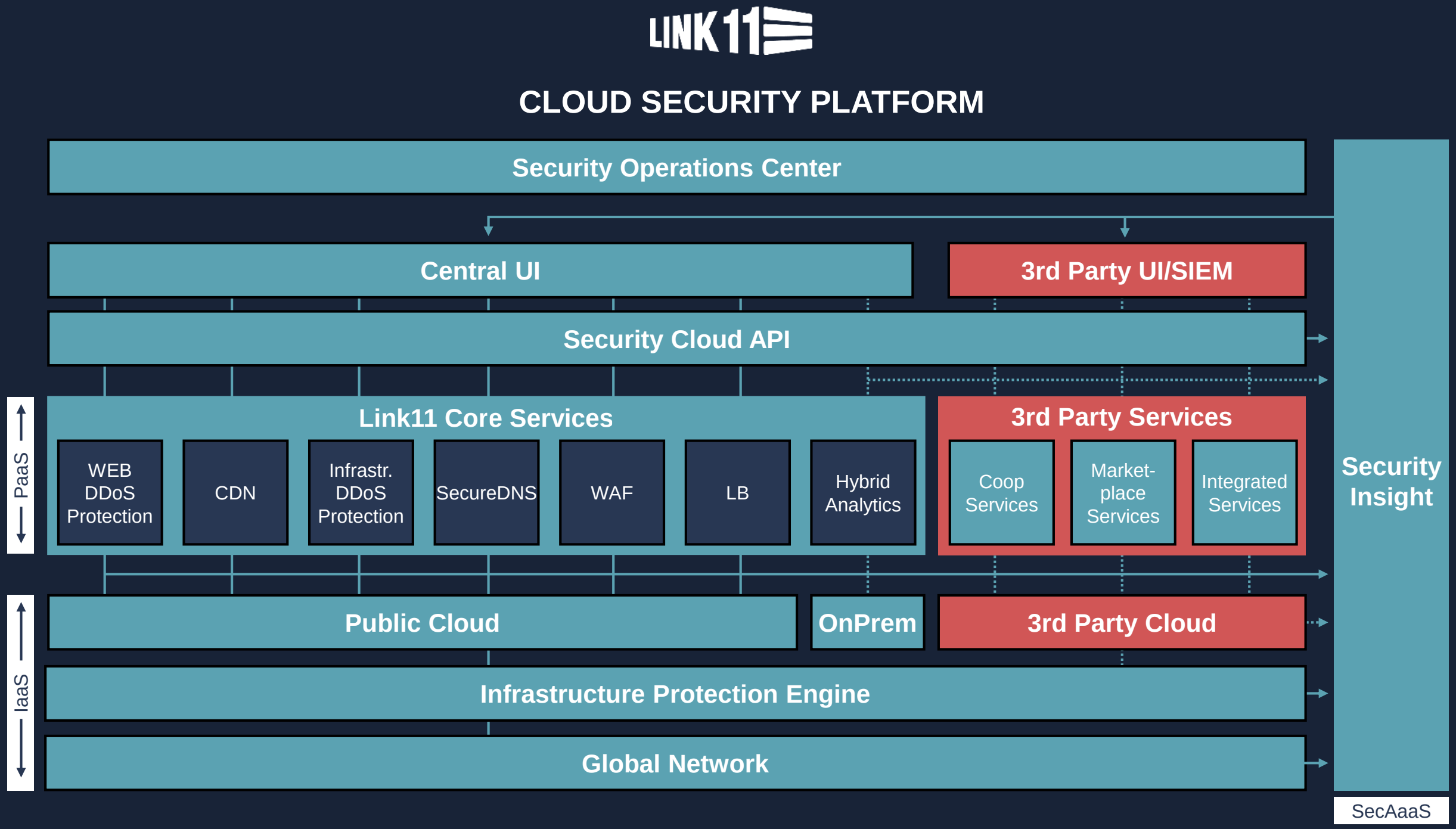
Zum Patent angemeldete Filtertechnik

Portfolio:
DDoS Schutz, WAF, Secure DNS

BSI zertifiziert für kritische Infrastrukturen

Erfahrung seit 2005 mit DDoS Schutz

Partner der LKA`s, BKA und Mitglied des G4C


LINK11
CLOUD SECURITY PLATFORM
Security Operations Center
Central UI
3rd Party UI/SIEM
Security Cloud API
Link11 Core Services
WEB DDoS Protection
CDN
Infrastr. DDoS Protection
SecureDNS
WAF
LB
Hybrid Analytics
3rd Party Services
Coop Services
Market-place Services
Integrated Services
PaaS
Public Cloud
OnPrem
3rd Party Cloud
IaaS
Infrastructure Protection Engine
Global Network
Security Insight
SecAaaS


LINK11
QUESTIONS?

Kontakt

Robert Specht

Channel and Alliance Manager

robert.specht@i-sec.tuv.com

+49 221 56783 464

TÜV Rheinland i-sec GmbH

Am Grauen Stein

51105 Köln

www.tuv.com/informationssicherheit

Marko Richter

Channel Manager

m.richter@link11.com

+49 69-2649297704

Link11 GmbH

Lindleystrasse 12

60314 Frankfurt am Main

www.link11.com

TÜVRheinland®
Genau. Richtig.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Regelmäßig aktuelle Informationen im
Newsletter und unter www.tuv.com/informationssicherheit