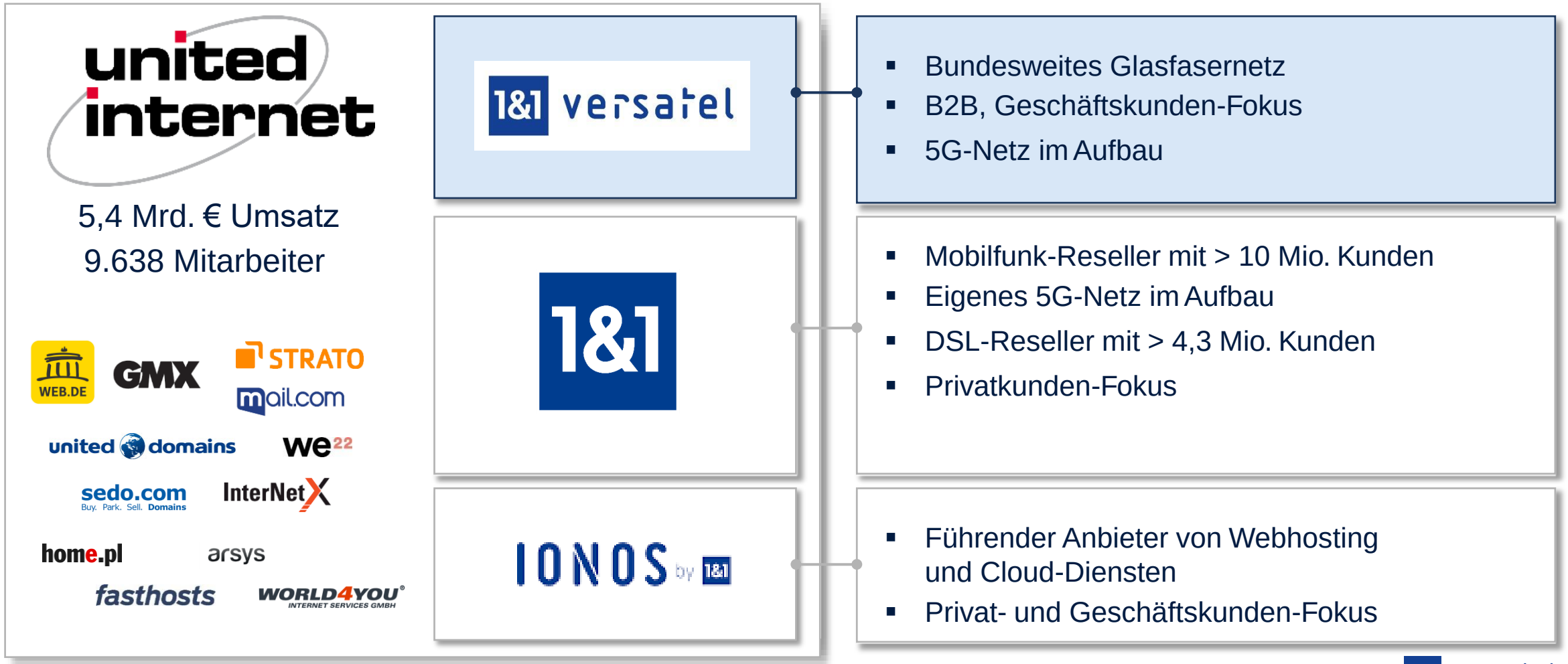
Erstklassiger DDoS-Schutz – Made in Germany

1&1 Versatel – 28.9.2023

1&1 Versatel

1&1 Versatel - eines der zentralen Unternehmen innerhalb der United Internet Gruppe



Was Sie heute erwartet

1 Warum bieten wir mehr an, als den Netzzugang?

2 Unser Lösungsportfolio

3 Aufrechterhaltung der Arbeitsfähigkeit - 1&1 DDoS Protect

4 Minimierung betrieblicher Aufwendungen für unsere Kunden

5 Mehr als nur DDoS Schutz - Erkennung und Abwehr von Angriffen

1

Warum bieten wir mehr an, als den Netzwerkzugang?

Die Treiber hinter unserem Lösungsportfolio

New Work

2022 haben **24,2 %** aller Erwerbstätigen in Deutschland von zu Hause aus gearbeitet. Davon nutzen 14,7 % täglich oder mindestens die Hälfte der Arbeitszeit das Homeoffice.

STATISTISCHES BUNDESAMT
https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Qualitaet-Arbeit/Dimension-3/home-office.html

New Work ist mehr als Home Office. Es ändert sich nicht nur, **wo** gearbeitet wird, sondern auch **wann** und mit welchen **Arbeitsmitteln**.

1&1 versatel

Künstliche Intelligenz

KI-Anwendungen sind auf dem Vormarsch.
Vor allem in Branchen, die besonders gut mit Daten umzugehen wissen, kann künstliche Intelligenz einzelnen Betrieben unter die Arme greifen.
Gesamtwirtschaftlich wird KI das Fachkräfteproblem allerdings nicht lösen.

Institut der deutschen Wirtschaft / https://www.iwd.de/artikel/kann-kuenstliche-intelligenz-den-fachkraeftemangel-lindern-580263/

1&1 versatel

Regulierung

1&1 versatel

Cyber-Sicherheitslage

84 Prozent der Unternehmen beobachten im Vergleich zu 2022 einen **Anstieg der Bedrohungslage**. Als Gründe werden die zunehmende Prozessdigitalisierung, professionellere Hackerorganisationen sowie die geopolitische Lage angegeben. 2023 ist zudem die **Sorge vor** Hackerangriffen in Form von **DDoS-Attacken** (Distributed Denial of Service) im Vergleich zu 2022 deutlich gestiegen. Die derzeitigen **Top-Risiken**: **Phishing-Kampagnen** und **Ransomware**. Für jedes zweite Unternehmen ist es eine große Herausforderung, mit den Methoden der Kriminellen und dem technologischen Fortschritt Schritt zu halten.

Von Cyber Security zu Cyber Resilience – Studie von Lünendonk im Auftrag von KPMG
https://kpmg.com/de/de/home/themen/2023/05/studie-belegt-truegerisches-sicherheitsgefuehl-bei-unternehmen.html

4,3 Millionen Euro

Kosten eines Datenlecks für deutsche Unternehmen

51%

51% der Organisationen planen eine Erhöhung der Investitionen in IT-Sicherheit in Folge eines Datenlecks, inklusive der Planung und dem Test von Incident Response- (IR-)Maßnahmen, Mitarbeitenden-Trainings und Werkzeuge zur Erkennung und Abwehr von Angriffen

1,76 Millionen Euro

Deutsche Unternehmen, die stark auf KI und Automatisierung setzen, verkürzen Lebenszyklen von Datenlecks um 81 Tage und senken die Folgekosten pro Vorfall um 1,76 Millionen Euro

IBM Cost of a Data Breach Report 2023 / https://www.ibm.com/reports/data-breach

1&1 versatel

Weltweite Krisen und Konflikte

- Klimawandel
- Lieferketten
- Inflation
- Ukraine-Krieg
- Pandemie

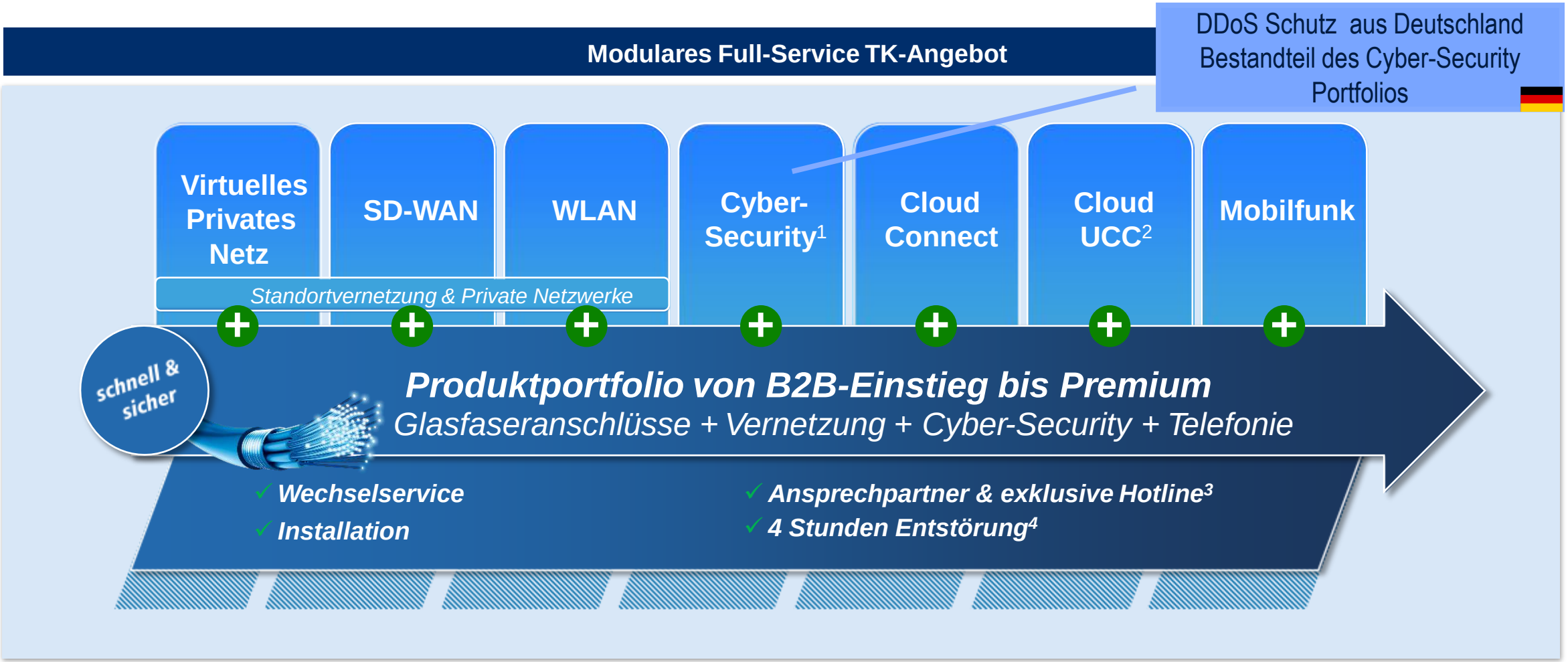
1&1 versatel

2

Unser Lösungsportfolio

Wie wir die Herausforderungen angehen

Unser B2B Produktportfolio für alle Unternehmensanforderungen



1) Cyber-Security: Professioneller Schutz gegen Cyberattacken, Phishing Emails, Betrugs- und Erpressersoftware. 2) UCC: Unified Communication & Connectivity = Cloud Telefonanlagen und Video-Konferenz-Systeme. 3) Service Operation Center (SOC) in Deutschland sowie 24/7-Geschäftskunden-Hotline. 4) Service Level Agreement mit Industriestandard für Geschäftskunden und Carrier; Sichere Prozesse nach ITIL V3 und Zertifizierungen nach ISO 27001, ISO 27001 auf der Basis von IT-Grundschutz, ISO 20000 und ISO 9001

3

Aufrechterhaltung der Arbeitsfähigkeit

1&1 DDoS Protect

DDoS-Angriffe nehmen zu

Im Jahr 2022 stieg die Zahl der DDoS-Angriffe im Vergleich zum Vorjahr weltweit um 150%.

Die Zahl der Angriffe in Nord-, Mittel- und Südamerika stieg sogar noch schneller, um 212% im Vergleich zu 2021.

Mehr als die Hälfte der Angriffe richtete sich gegen Unternehmen in der EMEA-Region.

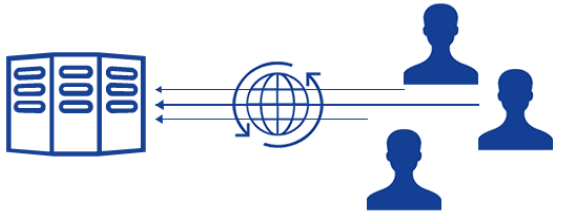
Auf Nord-, Mittel- und Südamerika entfielen 35% der Angriffe, während 7% der Angriffe auf APAC-Organisationen abzielten.

All About SECURITY über den radware 2022 Global Threat Analysis Report
https://www.all-about-security.de/radware-bericht-fuer-2022-boesartige-ddos-angriffe-steigen-um-150/

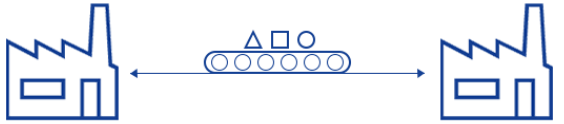
Es betrifft unsere Kunden

Wie abhängig ist Ihr Unternehmen von einem funktionierenden Internet-Access?

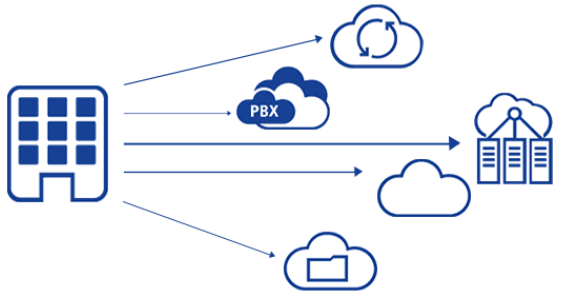
Services aus dem Rechenzentrum



Remote User



Digitale Lieferketten



Cloud-Nutzung für kritische Prozesse

DDoS Angriffe können jedes Unternehmen, jede Behörde treffen

FINANZAUFSICHT

Hackerangriff auf die Bafin

AKTUALISIERT AM 04.09.2023 - 09:40

Die deutsche Finanzaufsicht ist Opfer eines Hackerangriffs. Betroffen ist nur die öffentlich zugängliche Internetseite.

Die Finanzaufsicht Bafin hat mit den Folgen eines Hackerangriffs auf ihre öffentlichen Internetseiten zu kämpfen. „Aufgrund eines Distributed-Denial-of-Service-Angriffs (DDoS) ist die Website der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) seit Freitag, dem 1. September 2023, nur eingeschränkt erreichbar“, teilte die Behörde am Montag auf Anfrage mit.

Bafin: Hackerangriff auf öffentliche Website der Finanzaufsicht (faz.net)

https://www.faz.net/aktuell/finanzen/bafin-hackerangriff-auf-oeffentliche-website-der-finanzaufsicht-19149361.html

Arten von DDoS-Attacken

Darstellung anhand des OSI-Modells

7	Anwendungen (Application)	Application Layer Attack
6	Darstellung (Presentation)	
5	Sitzung (Session)	
4	Transport (Transport)	Volumetric Attack
3	Vermittlung/Paket (Network)	
2	Sicherung (Data Link)	
1	Bitübertragung (Physical)	

Welche Optionen gibt es prinzipiell?

Lokal
im Rechenzentrum des Kunden

„Der Türsteher hinter der Tür“

- DDoS-Appliances beim Kunden vor Ort
- Unabhängig vom Service Provider
- Unabhängig von der Netzgröße
- Erfordert Know-How im Betrieb
- Schützt nur vor Angriffen bis zur Kapazität der eigenen Bandbreite (also fast gar nicht…)

Zentral
im Netz des Service Providers

Vollständige Integration

- DDoS-Schutz im Netz des Service Providers implementiert
- Schützt den Datenverkehr des Kunden über den jeweiligen Service Provider
- Schützt auch kleine Netze und einzelne IPs
- Schützt vor Angriffen jenseits der Kunden-Bandbreite

Übergreifend
aus der Cloud

Nur für die Großen

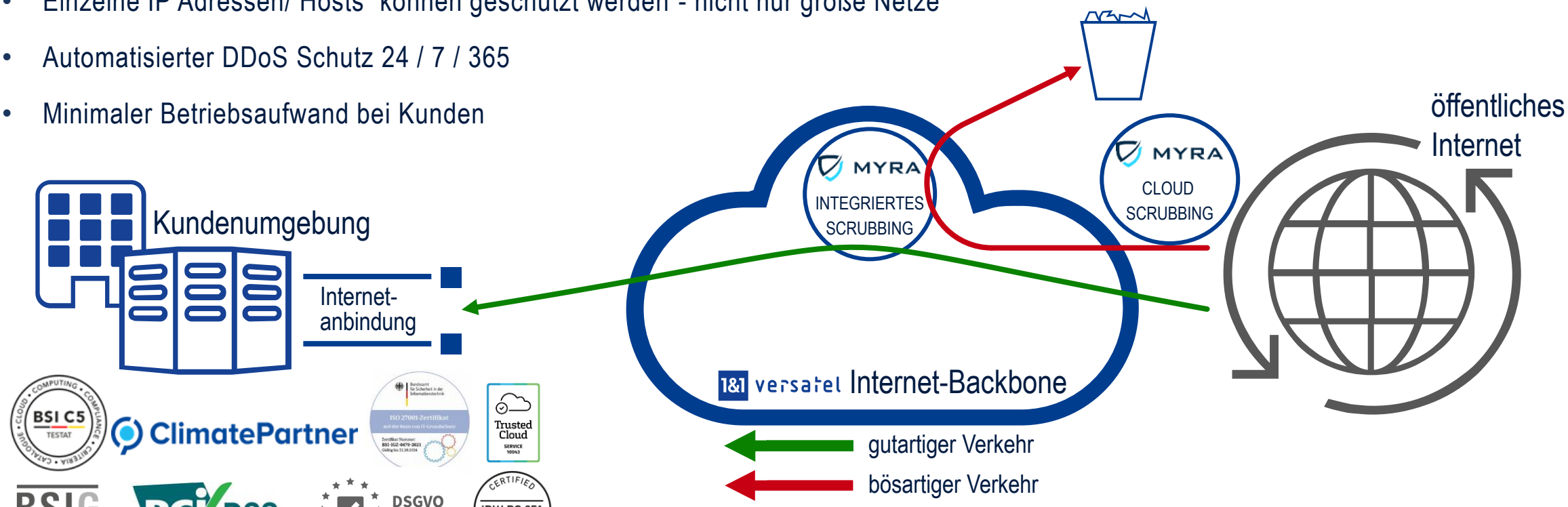
- Einsetzbar bei Netzen ≥ /24
- Provider-unabhängig
- Erfordert teilweise zusätzliche Leitung

auch Hybrid

Unsere Lösung: 1&1 DDoS Protect auf Basis von Myra Security

Technologie und Netz aus Deutschland

- Myra Security erfüllt ALLE vom BSI festgelegten Leistungsmerkmale für qualifizierte DDoS-Mitigationsdienstleister
- 1&1 DDos Protect schützt unabhängig von der DDoS Angriffsstrategie auch bei Multi-Vektor-Angriffen
- Einzelne IP Adressen/ Hosts können geschützt werden - nicht nur große Netze
- Automatisierter DDoS Schutz 24 / 7 / 365
- Minimaler Betriebsaufwand bei Kunden

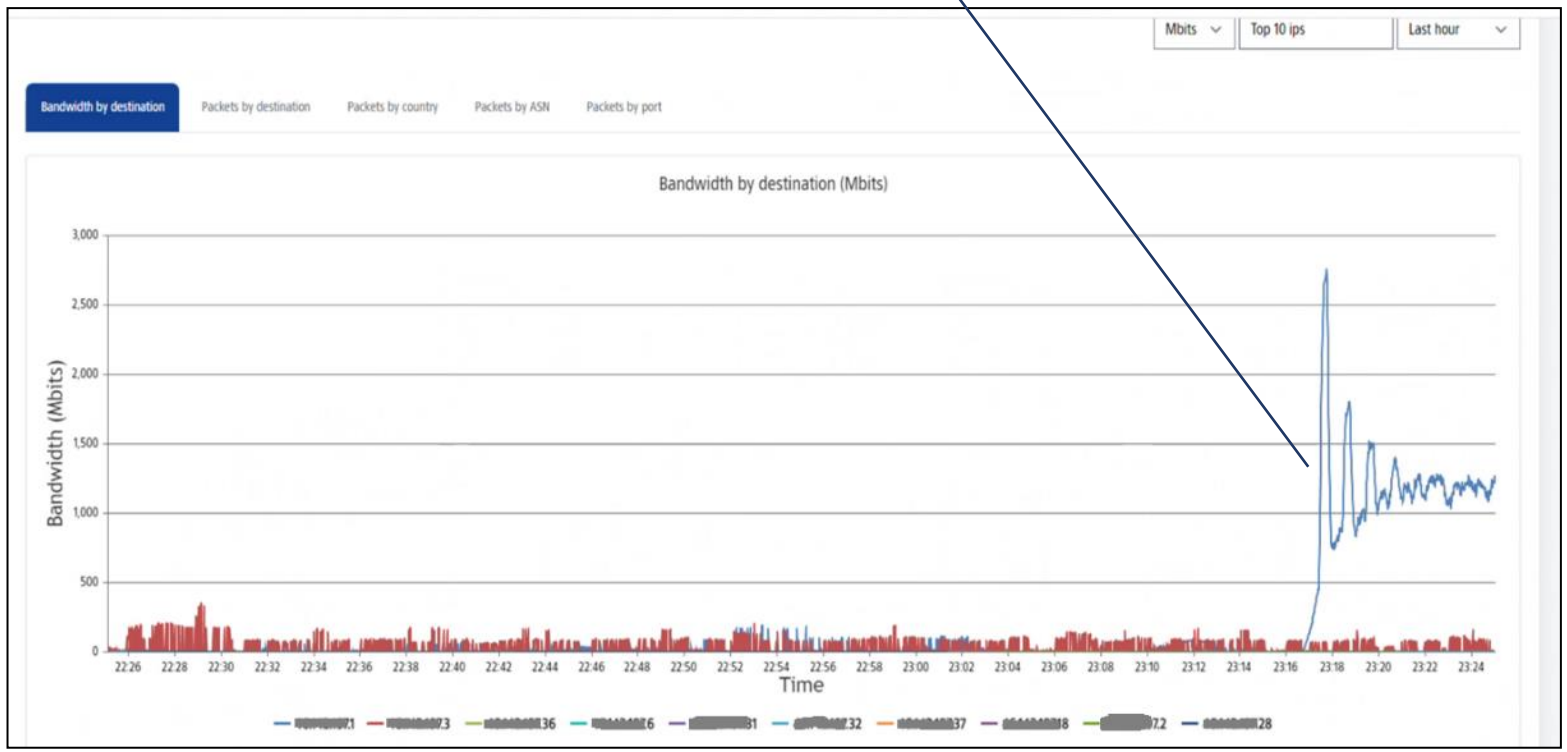


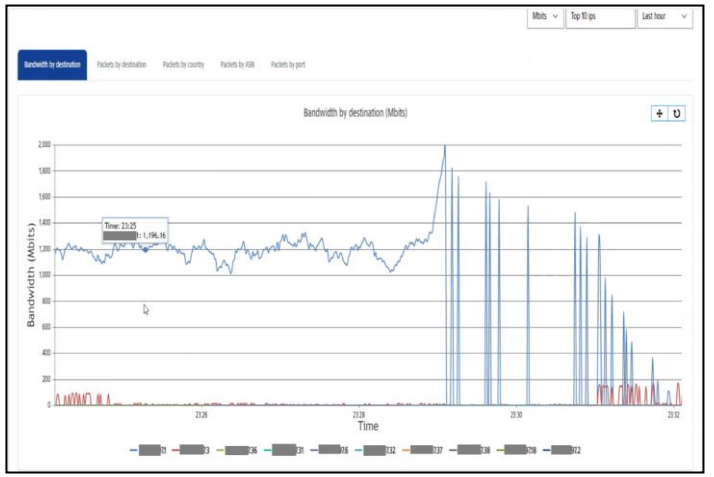
Wissen was passiert – Portaleinblicke beim DDoS Angriff (1. Welle)

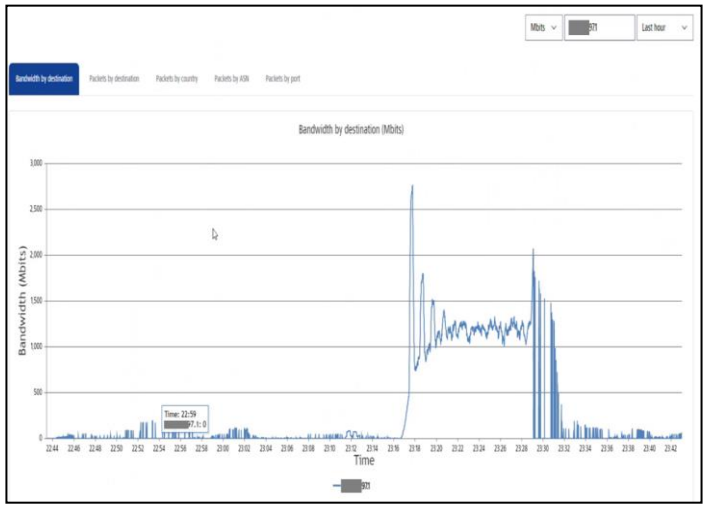
Der Blick auf den Datenverkehr der Peering Router der 1&1 Versatel

1. Ein Kundennetz wird angegriffen.
2. Der Angriff wird bereits an den Netzgrenzen des 1&1 Versatel Netzes abgefangen.
3. Die Kundenrouter erhalten den gereinigten Datenverkehr.
4. Alle Systeme des Kunden arbeiten normal.

Ein DDoS Angriff löst den Schutzmechanismus aus (hier bei 1,3 Gbit/s)







4

Minimierung betrieblicher Aufwendungen der Kunden

1&1 DDoS Protect

1&1 DDoS Protect – Aufwandsarm für den Betrieb des Kunden

Der schnelle Weg zum DDoS Schutz

- Automatisiert
- Unterbrechungsfrei
- Ohne Kundenbetrieb
- Portal Monitoring sofort

Was macht 1&1 DDoS Protect besonders?

Wir ergänzen Technik mit menschlicher Intelligenz

Wir sind der Service Provider mit einem Myra Scrubbing Center im eigenen Netzwerk

Mit unserer Architektur bedienen wir Kunden jeder Größenordnung und Branche

Alle reden über Digitale Souveränität. Wir leben sie.

5

Mehr als nur DDoS Schutz Erkennung und Abwehr von Angriffen

Managed Detection and Response

Egal ob Schutz oder Compliance…

Unternehmen müssen mehr tun

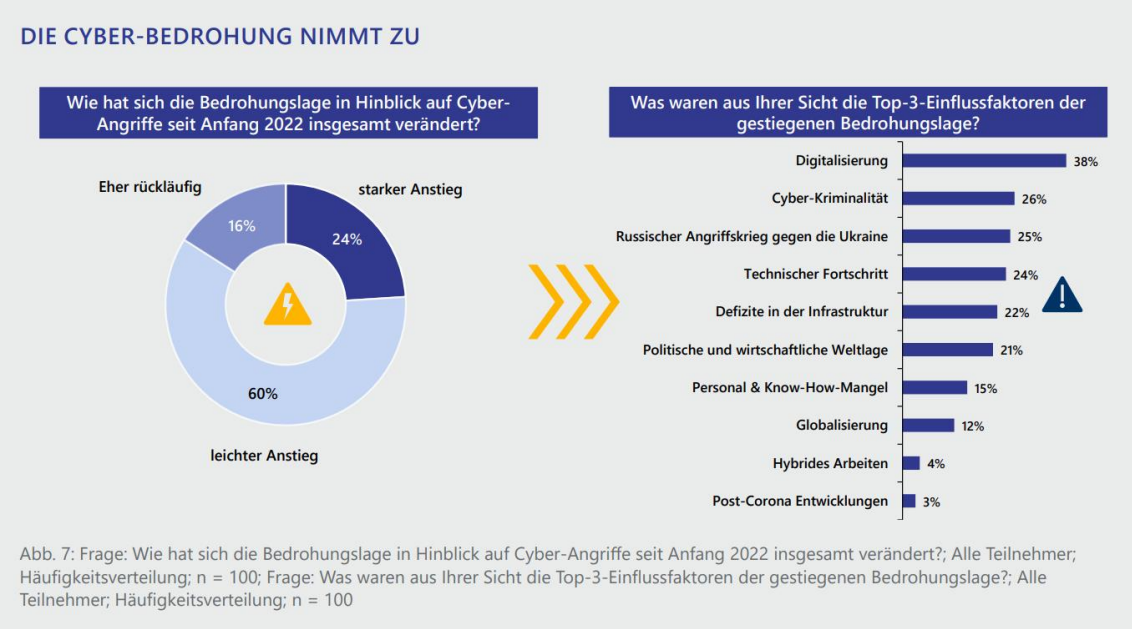


Abb. 7: Frage: Wie hat sich die Bedrohungslage in Hinblick auf Cyber-Angriffe seit Anfang 2022 insgesamt verändert?; Alle Teilnehmer; Häufigkeitsverteilung; n = 100; Frage: Was waren aus Ihrer Sicht die Top-3-Einflussfaktoren der gestiegenen Bedrohungslage?; Alle Teilnehmer; Häufigkeitsverteilung; n = 100

Von Cyber Security zu Cyber Resilience – Studie von Lünendonk im Auftrag von KPMG
https://kpmg.com/de/de/home/themen/2023/05/studie-belegt-truegerisches-sicherheitsgefuehl-bei-unternehmen.html

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

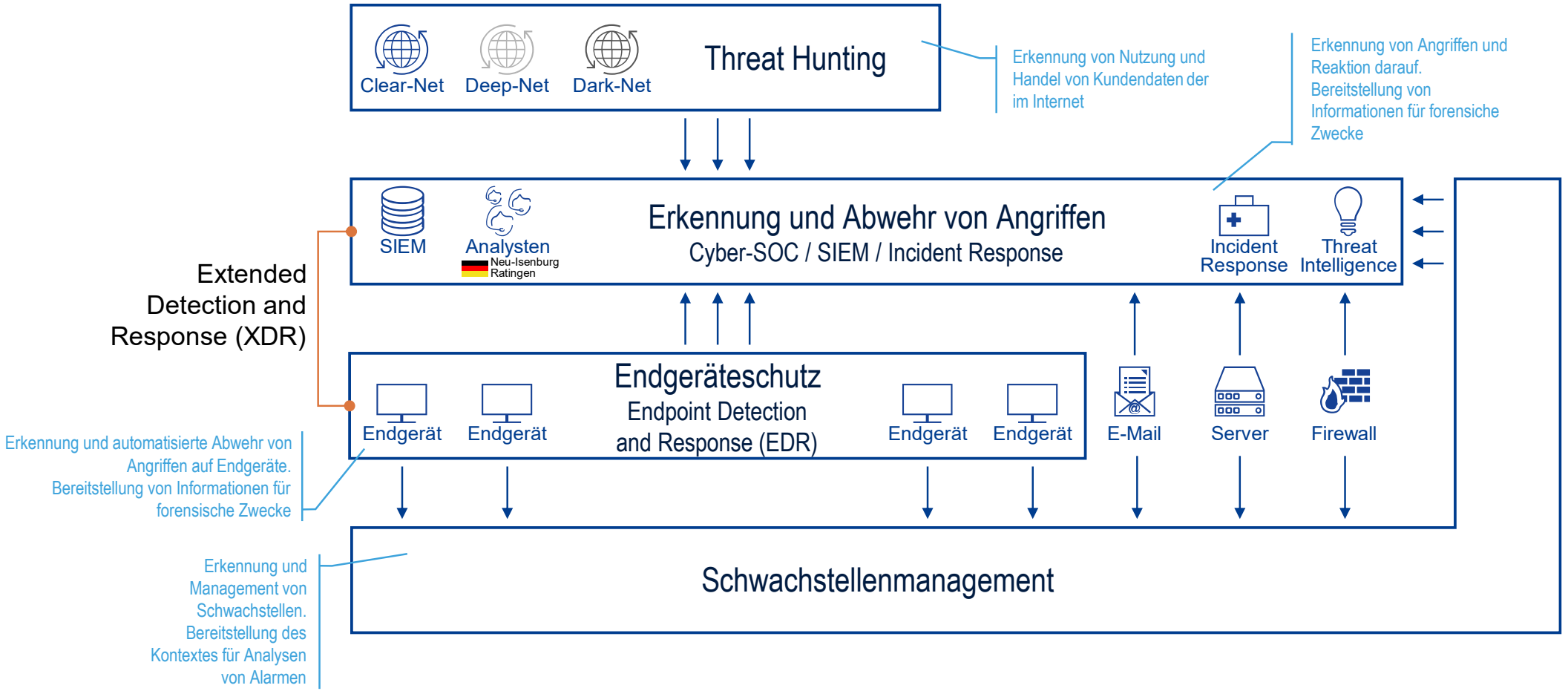
§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, **angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen**, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst **ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung**. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.

Cyber-Security Portfolio – Baustein: Managed Detection and Response

Angriffe können nur abgewehrt werden, wenn sie erkannt wurden




HAMBURG
HANNOVER
BERLIN
DORTMUND
DÜSSELDORF
KÖLN
KASSEL
LEIPZIG
FRANKFURT A.M.
NÜRNBERG

1&1 versatel