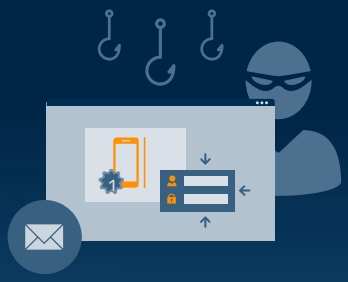
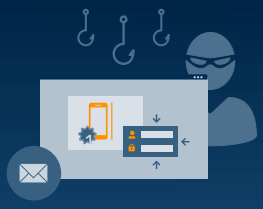


hvs consulting

Report Phishing-Simulation Beispiel GmbH

MS Teams
09.02.2026

IS-FOX



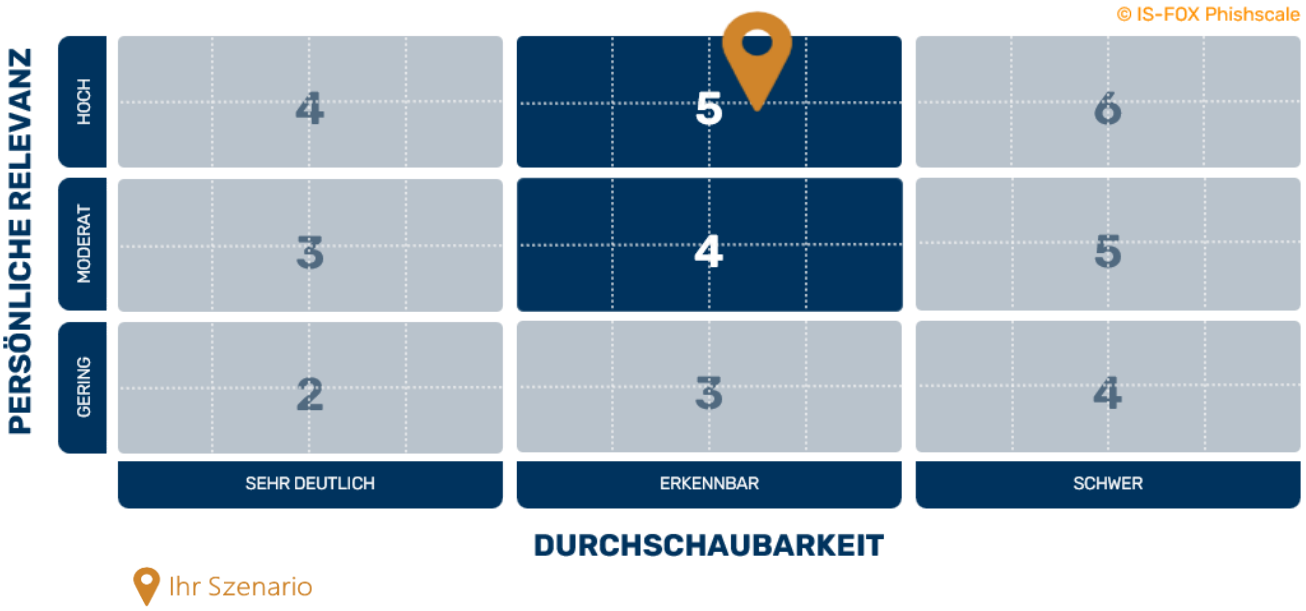
1 Ihr Szenario „MS Teams“

1.1 Rahmenbedingungen

Szenario	MS Teams
Beginn	05.02.2026 - 10:00 Uhr
Ende	06.02.2026 - 15:00 Uhr
IS-FOX Phishscale	5
Domain	microsaftteams.de
Absender	Microsoft Teams <noreply@microsaftteams.de>
Erkennungsmerkmale	• Domain microsaftteams.de • Absender noreply@microsaftteams.de • maskierter Link https://www.microsaftteams.de/?rid=example • Extern-Markierung

1.2 IS-FOX Phishscale

Der IS-FOX Phishscale ist eine Adaption des NIST Phish Scale und dient zur Einordnung der Schwierigkeitsstufe des durchgeführten Szenarios anhand der Bewertungskriterien „persönliche Relevanz für den Empfänger" und der „Durchschaubarkeit der versendeten E-Mail".
Die Kriterien werden jeweils in drei Stufen unterteilt. Die persönliche Relevanz (in den Stufen: gering, moderat und hoch) des Szenarios beschreibt, inwiefern der Inhalt der E-Mail für den einzelnen Empfänger substanziell ist, und somit persönliche Betroffenheit weckt.
Das Kriterium der Durchschaubarkeit (in den Stufen: sehr deutlich, erkennbar und schwer) gibt den Schwierigkeitsgrad der Erkennungsmerkmale der E-Mail bzw. der Landingpage an.
Jede Stufe wird entsprechend der Schwierigkeit (1-3) bewertet und folglich setzt sich der IS-FOX Phishscale aus fünf verschiedenen Schwierigkeitsstufen (2-6) zusammen.

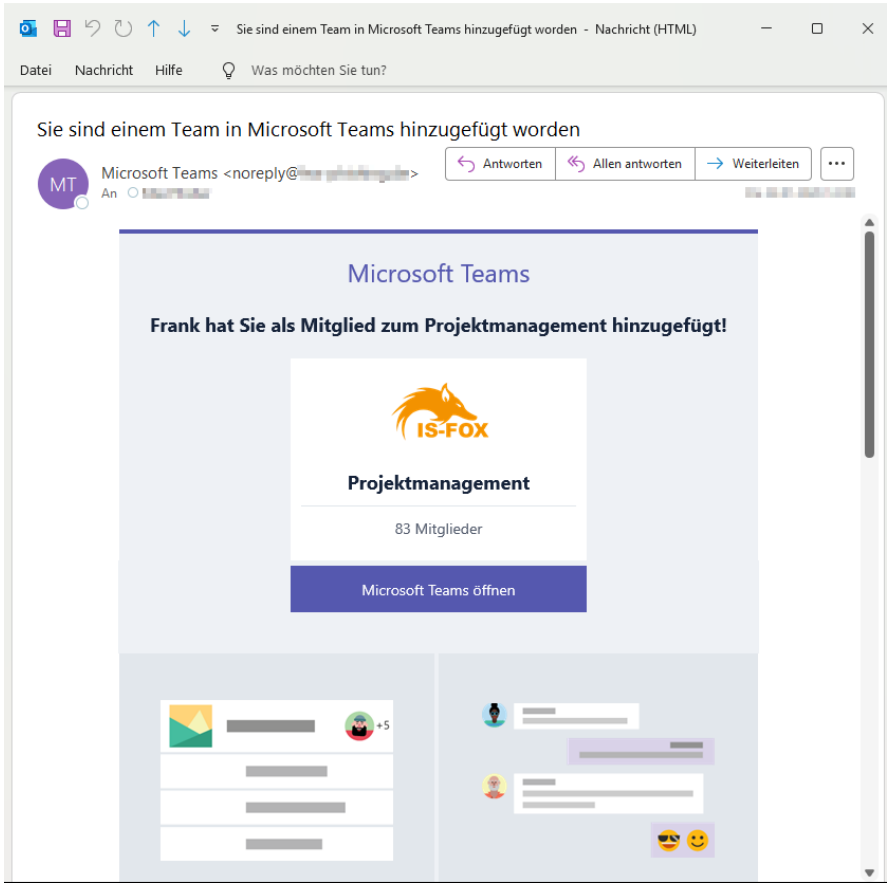


Das durchgeführte Szenario „MS Teams" wird in der Schwierigkeitsstufe 5 eingeordnet.

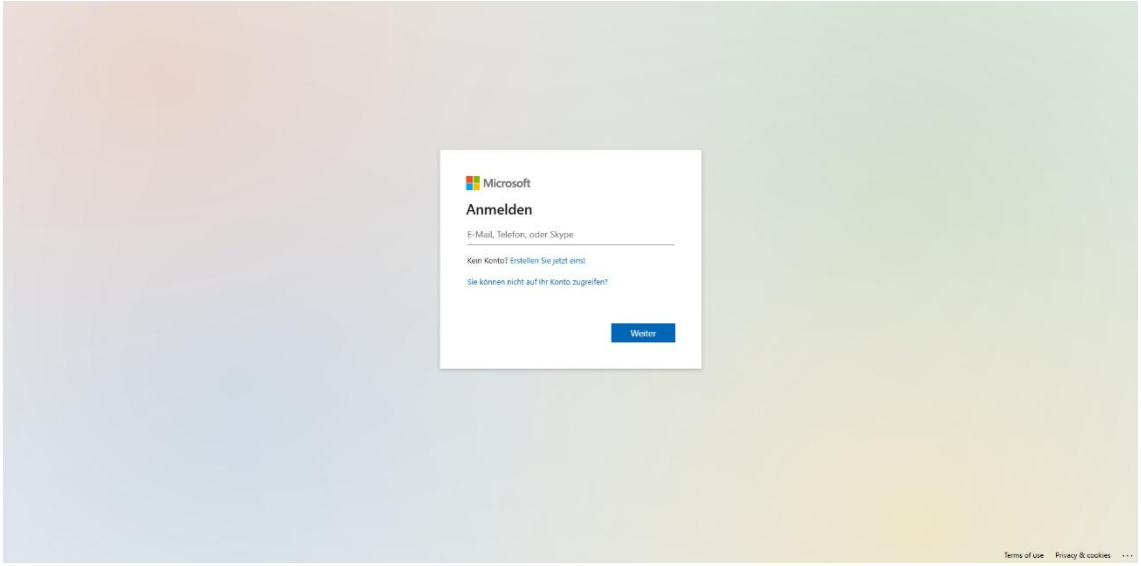
Ziel der Kampagne ist eine kontinuierliche Sensibilisierung der Mitarbeiter anhand realitätsnaher Szenarien, die einen beruflichen Kontext besitzen (dunkelblau markierter Bereich). Daher sind persönlich nicht relevante Themen und zu einfache oder zu schwer durchschaubare E-Mails für die gewünschte Entwicklung nicht zielführend.

Die Erkennungsmerkmale (siehe Kapitel 1.1) und somit die Durchschaubarkeit der Simulation können ebenfalls auf andere Angriffsvektoren angewendet werden und sollen den Mitarbeiter zeigen, wie sie sich vor möglichen reellen Phishing-Angriffen schützen können.

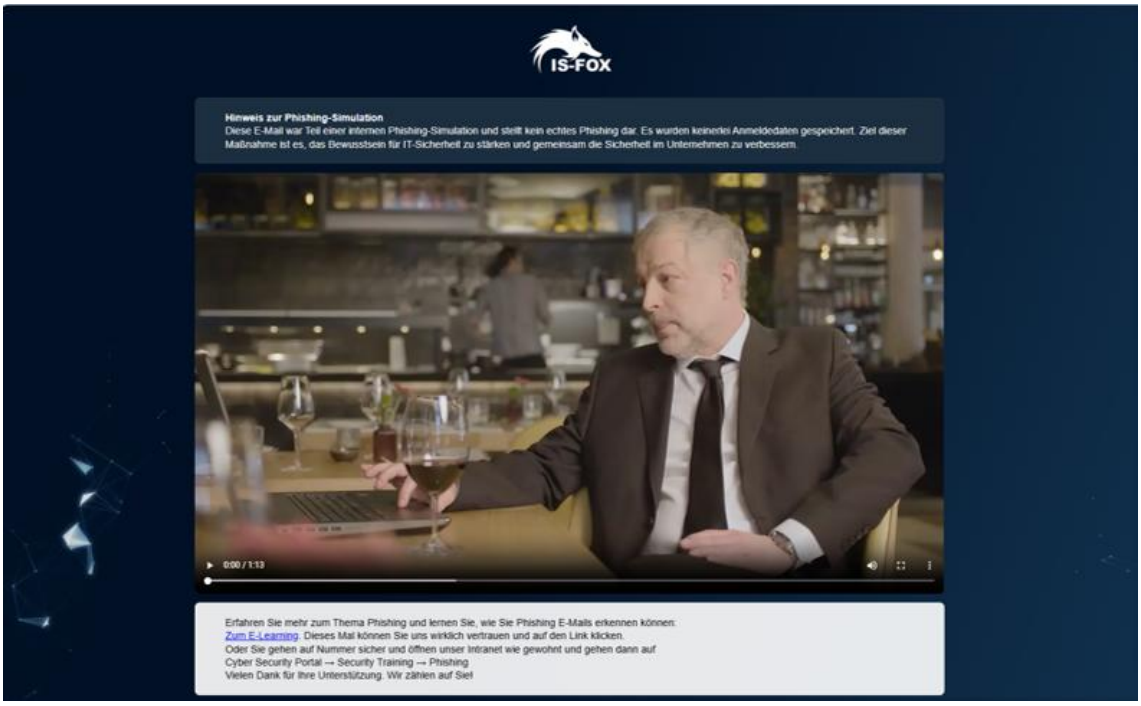
1.3 Phishing-E-Mail

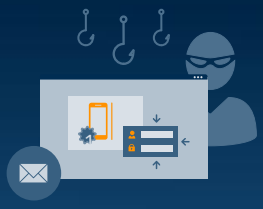


1.4 Landingpage



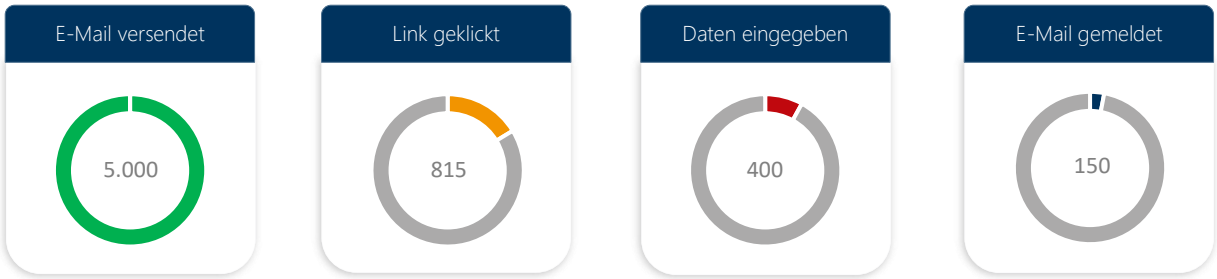
1.5 Auflöseseite





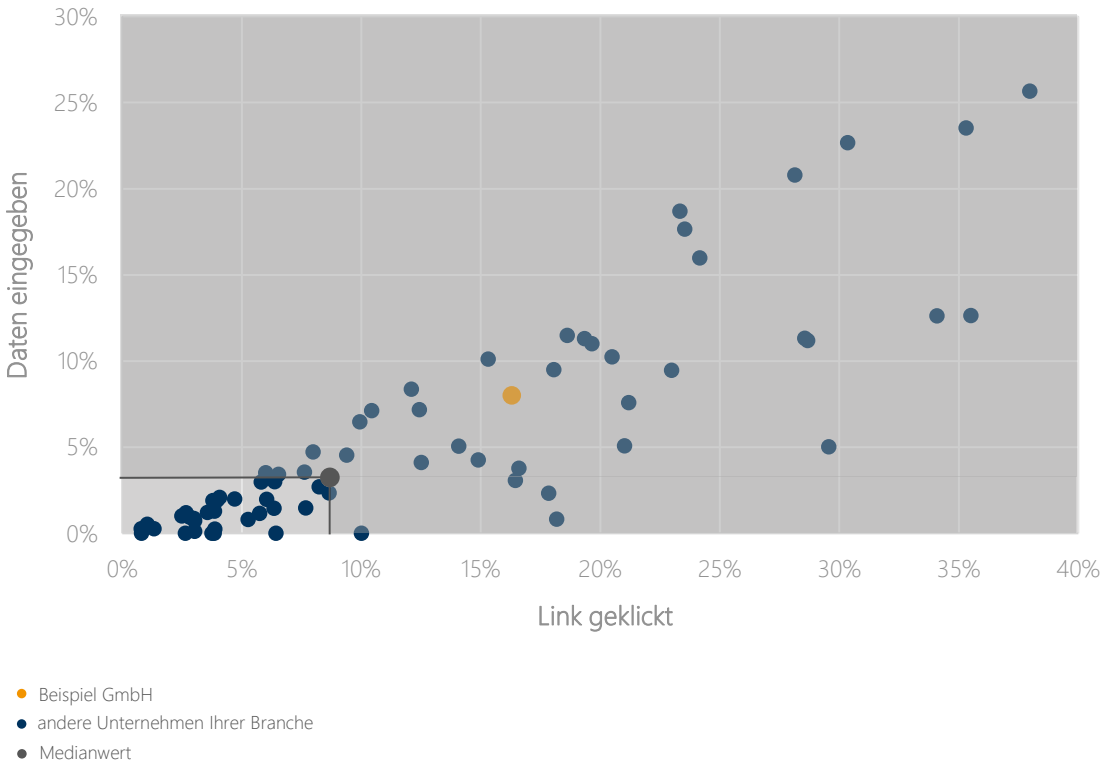
2 Ergebnis der Phishing-Simulation

2.1 Ergebnis

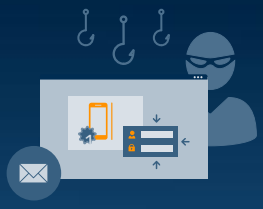


100 % | 16,3 % | 8,0 % | 5,9 %

2.2 Benchmark

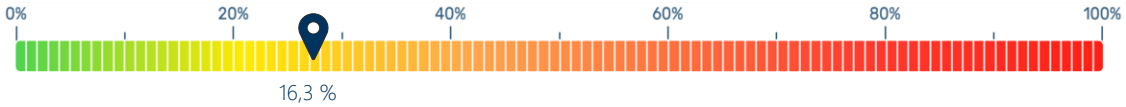


In dieser Analyse wird die Performance mehrerer Unternehmen Ihrer Branche anhand zweier zentraler Kennzahlen bewertet. Auf der x-Achse wird die Anzahl der Nutzer in Prozent dargestellt, die auf den Link in der E-Mail geklickt haben. Nachdem die Nutzer auf den Link geklickt haben, geben sie anschließend Anmeldedaten ein, um auf die Auflöseseite zu gelangen. Diese Eingabedaten sind auf der y-Achse prozentual abgebildet.

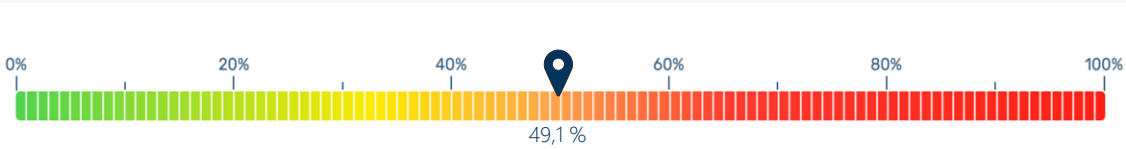


Jedes Unternehmen Ihrer Branche wird durch einen Punkt in einem Koordinatensystem dargestellt, wobei der Medianwert als zentrale Referenzgröße dient. Der Median zeigt den Punkt, an dem die Hälfte der Unternehmen besser und die andere Hälfte schlechter abschneiden. Um die Performance visuell darzustellen, werden Unternehmen, die über dem Median liegen, auf einer helleren Fläche positioniert. Diese Unternehmen haben also eine bessere Performance in Bezug auf die Anzahl der Klicks oder die Menge an eingegebenen Daten im Vergleich zum Median. Unternehmen, deren Werte unter dem Median liegen, erscheinen auf einer dunkleren Fläche, was auf eine schwächere Performance hinweist.

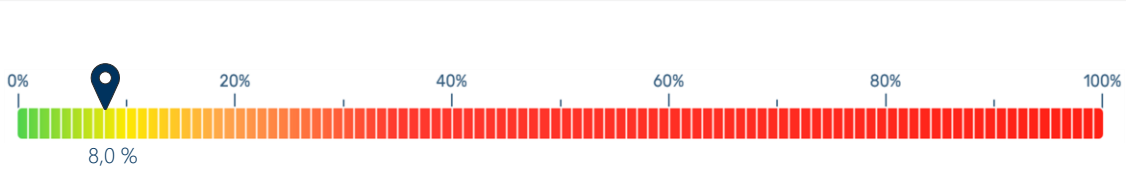
2.3 Interpretation



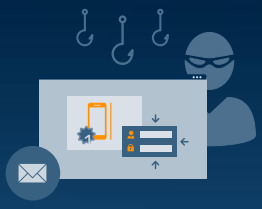
Die Klickrate von 16,3 % spricht für eine grundlegend vorhandene, dennoch ausbaufähige Grundsensibilisierung zum Thema Phishing.



Das Verhältnis von “Link geklickt” und “Daten eingegeben” liegt mit 49,1 % im erwarteten Bereich unseres bisherigen Benchmarks.



In Summe hätten also 8,0 % der Benutzer wahrscheinlich Daten preisgegeben.

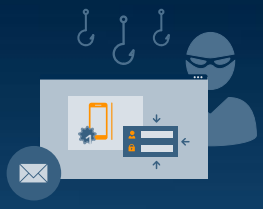


Die Melderate von 5,9 % zeigt eine ausbaufähige Sensibilisierung der Mitarbeiter hinsichtlich der Wege, auf denen eine Phishing-E-Mail bei Ihnen im Unternehmen gemeldet werden kann.

Das Ergebnis im unternehmensweiten Test kann sehr stark schwanken.

Abteilungen oder kleinere Standorte innerhalb eines Unternehmens warnen sich oft schnell über den sogenannten „Flurfunk", was dazu führen kann, dass die Klickraten der Phishing-Simulation in diesen Bereichen geringer sind. In Unternehmen mit großen Open-Space-Büros sind die Ergebnisse eines Phishing-Tests daher häufig besser als in stark dezentralisierten oder verteilten Organisationen, in denen die Kommunikation über potenzielle Bedrohungen langsamer erfolgt.
Mobiles Arbeiten (z.B. im Homeoffice) kann einen ähnlichen Effekt auf die Klickraten haben, da dieser Personenkreis i.d.R. auch nicht vom Flurfunk profitiert.
Ein weiterer, technischer Aspekt ist, dass der Versand von externen E-Mails an eine große Empfängergruppe kontrolliert über mehrere Stunden erfolgt, um eine Überbelastung der Serversysteme zu vermeiden. In einigen Fällen erhalten Mitarbeiter die Phishing-E-Mail erst, nachdem andere sie bereits geöffnet und darüber gesprochen haben. Dies kann die Wahrscheinlichkeit verringern, dass eine Person auf den Phishing-Link klickt, da die Warnungen aus dem Team bereits durch den „Flurfunk" verbreitet wurden.

Zudem kann die Landingpage nach mehrfachem öffnen durch die Browser-Hersteller (z.B. Google Chrome oder Mozilla Firefox), automatisch als „Suspicious Site" markiert werden. Wenn dann weitere Personen auf den Link klicken, erhalten diese eine deutliche Warnung. Dies kann die Klickrate eines Phishing-Angriffs massiv verringern.



3 Über HvS-Consulting

Wir sind davon überzeugt, dass die Werte unserer Gesellschaft auch im Cyber-Raum geschützt werden müssen. Deshalb helfen wir Organisationen seit 2002, sich mit dem richtigen Zusammenspiel aus Technologien, Prozessen und Menschen selbst zu schützen. Unser Portfolio im Überblick:

Technologien

Offensive Security
Security Assessments, Advanced Cyber Attacks, Red Teaming

Defensive Security
Incident Response (24/7), CDC Maturity Assessments, Security Architekturen

Prozesse

ISMS Consulting
ISO27k, KRITIS, TISAX, etc.

BCMS Consulting
Kontinuitätsstrategien & Notfallübungen

Menschen

Security Awareness
Live Hacking, Awareness Kampagnen, Phishing-Simulationen, E-Learning

Unsere Produkte für Security, Datenschutz und Compliance sind in der Marke „IS-FOX" gebündelt. Unser Erfolgsrezept: wir sind

Fach-Spezialist

Durch unsere Security-Consultants, Incident-Response-Spezialisten und Datenschutz-experten wissen wir, wo der Schuh wirklich drückt. Deshalb sind unsere Inhalte auch "Auditoren-proofed".

Marketing-Spezialist

Wir nehmen den Themen die Komplexität, die Fremdwörter und kommen zum Punkt: knackig, verständlich, nachvollziehbar, immer mit konkreten Tipps - genau deshalb bleibt auch es auch hängen.

E-Learning-Spezialist

Unser Multimedia-Team erstellt die IS-FOX-Produkte selbst: vom Storyboard, über Animations- und Grafikdesign bis hin zur Produktion. Deshalb können wir auch sehr schnell individualisieren.

> 20	> 60	> 500	> 1 Mio.
Jahre Erfahrung	**engagierte Spezialisten**	**zufriedene Kunden**	**geschulte Mitarbeiter**

Folgende Kunden vertrauen uns im Bereich Security Awareness (Auszug): Abus, Amadeus, Allianz, Audi, Bosch, DZ Bankengruppe, Dr. Oetker, Evonik, Finanz Informatik, die Flughäfen DUS, CGN, FRA, HAM, MUC, ZRH, Geberit, Giesecke & Devrient, Groz-Beckert, Helmholtz Zentren, Henkel, Hornbach, IATA, Kuka, LBBW, Lidl, Müller Group, Lanxess, Loacker, Lufthansa Group, Munich RE, Osram, Otto Fuchs, Pro7Sat1, Rational, Rewe Group, Rohde & Schwarz, RWE, Saar LB, SAP, thyssenkrupp, ZF.