Handelsblatt
DIENSTAG, 9. FEBRUAR 2021, NR. 27

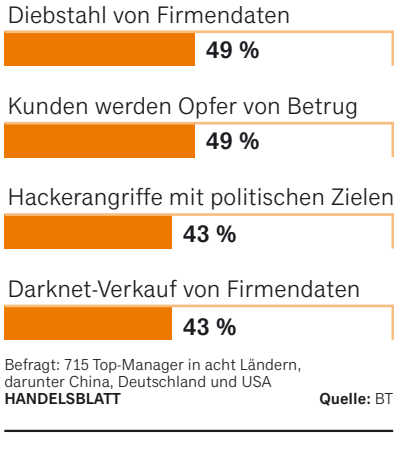
Einblick

## Cybergangster finden mehr Einfallstore

Es ist ein Tag für die Onlinesicherheit. Mehr als 170 Staaten weltweit beteiligen sich am heutigen „Safer Internet Day“. Die von der Europäischen Union (EU) 2004 mitgegründete Aktion zielt vor allem darauf, Kinder und Jugendliche für einen sicheren Umgang mit digitalen Medien zu sensibilisieren. Auch in Deutschland beteiligen sich landesweit zahlreiche Institutionen und Unternehmen – mit Ratgebern, Seminaren oder Konferenzen. Sie klären auf über Fallen beim Onlineshoppen, Passwort- und Identitätsschutz oder Gefahren der Social-Media-Nutzung. Die Corona-Pandemie habe gezeigt, wie wichtig das Internet dafür sei, die eigenen Fähigkeiten zu verbessern oder das Wissen zu vergrößern, teilte die EU im Vorfeld des Safer Internet Day mit. „Jedoch entstehen mit Chancen auch Risiken“, heißt es dort.

### Wachsende Bedrohung

**Anteil der Entscheider,** die 2020 im jeweiligen Bereich ein höheres Risiko festgestellt haben, in Prozent

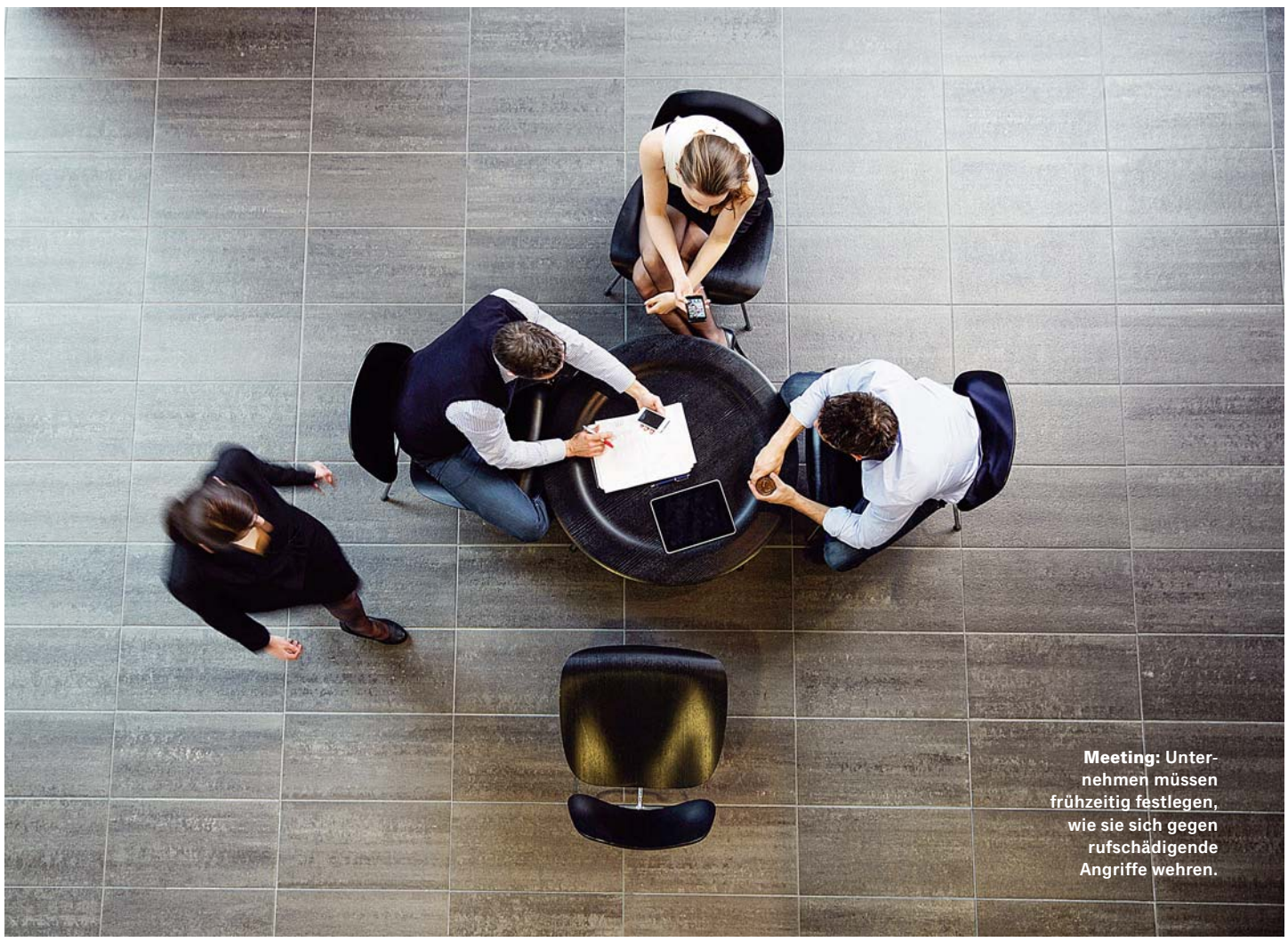



Befragt: 715 Top-Manager in acht Ländern, darunter China, Deutschland und USA
**HANDELSBLATT** **Quelle:** BT

Das erleben derzeit auch die Verantwortlichen in Unternehmen. Parallel zur rasch steigenden Digitalisierung des Betriebs und der Vernetzung auch mit Lieferanten oder Kunden hat die Pandemie den Online-Anteil der Arbeit noch einmal stark gesteigert. Homeoffice oder Webkonferenzen mit Geschäftspartnern allerdings bieten Cyberkriminellen neue Angriffspunkte – und sie versuchen sie offenbar zu nutzen. Einen sprunghaften Anstieg der Bedrohungen im vergangenen Jahr zeigt eine Ende Januar veröffentlichte Studie des britischen Telekommunikationskonzerns BT. So berichtete rund die Hälfte der Unternehmen, dass Angriffe auf Daten von Hackern zugenommen und dass Onlinebetrüger zudem verstärkt ihre Kunden ins Visier genommen hätten.

Für die Autoren der Studie rückt der Chief Information Security Officer (Ciso) damit in den Fokus – dessen Expertise und Führungskraft sei zentral für „den Erfolg des digitalen Geschäfts“. „Wenn wir Dienstleistungen und Daten nicht schützen können, wird sich die digitale Zukunft mit all ihren versprochenen sozialen und ökonomischen Vorteilen nicht einstellen“, warnt Kevin Brown, Managing Director bei BT Security. Thomas Mersch

IMPRESSUM
**Redaktion:** Thomas Mersch, Stefan Merx



**Meeting:** Unternehmen müssen frühzeitig festlegen, wie sie sich gegen rufschädigende Angriffe wehren.

Look

Reputationsmanagement

# Den guten Ruf verteidigen

Das Internet erleichtert Attacken auf das Ansehen von Unternehmen. Im Kampf gegen Beschimpfungen oder Verleumdungen hilft eine klare Abwehrstrategie. Besonders wichtig im Ernstfall: schnelles Handeln.

**Manuel Heckel** Köln

Aus Partnern wurden Feinde – und die Fehde ging online: Gleich zwei Webseiten hatte ein Unternehmer ins Internet gestellt, um seinen ehemaligen Kompagnon in den Schmutz zu ziehen. Getarnt waren die Texte als kritische journalistische Berichte, deren Autoren aber waren erfunden. Das perfide Ziel: Das Ansehen des ehemaligen Geschäftspartners sollte leiden – gestritten wurde um Anteile an einer Firma. „Die Texte wirkten wie ein Fahndungsaufruf“, erinnert sich Rechtsanwalt Ruben Hofmann von der Kanzlei Heuking Kühn Lüer Wojtek in Köln. „Unser Mandant ist dadurch fast in die Insolvenz geschlittert.“ Trotz digitaler Verschleierungsversuche konnte der Angreifer überführt werden. Die Webseiten verschwanden aus dem Netz, ein Gericht sprach dem Angegriffenen zudem 50.000 Euro Schadensersatz zu.

Die Dimension ist besonders, das Risiko jedoch alltäglich: Das Internet ermöglicht es Unternehmen, ihre Marke und ihre Produkte viel einfacher in die Welt zu tragen. Doch umgekehrt können Webseiten, Foren und Bewertungsplattformen auch Einfallstore sein, um den Ruf einer Firma zu schädigen. Jenseits von sachlicher Kritik kommen aus dem digitalen Raum Angriffe, die Mitarbeiter und Manager verunglimpfen – oder das Vertrauen als Hersteller oder Arbeitgeber untergraben. „Die Möglichkeiten, die Reputation zu beschädigen, sind vielseitiger geworden – die Bandbreite der Angriffe ist groß“, sagt Lars Niggemann, Inhaber der Agentur Prevency in Wuppertal, die Unternehmen beim digitalen Reputationsmanagement berät.

**51**

**Prozent**
der Deutschen fühlen sich von Cyberrisiken bedroht – der zweithöchste Wert nach den Sorgen über den Klimawandel.

Quelle: Axa Future Risks Report 2021

Der Experte warnt, dass es für potenzielle Angreifer immer einfacher werde, auch ausgefeilte Attacken zu starten. Programme, mit denen sich etwa Bilder oder Videos eines Vorstands manipulieren lassen, sind problemlos verfügbar. Und im sogenannten Darknet, einem besonders auf Anonymität ausgerichteten Teil des Internets, lasse sich bereits „Desinformation-as-a-Service“ per Kryptowährung bestellen. „Es ist günstig, und es erfordert kein besonderes technisches Know-how“, sagt Niggemann. Anonyme Spezialisten machen sich auf Bestellung daran, den Ruf eines Unternehmens zu ruinieren.

### Die Täter sind oft Ex-Mitarbeiter

Verantwortlich für solche digitalen Taten seien meist ehemalige Mitarbeiter oder verbitterte Kunden, sagt Rechtsanwalt Hofmann. „Wenn sich jemand richtig viel Mühe macht, dann hat er meistens ein persönliches Motiv.“ Dabei halten sich die wirtschaftlichen Folgen noch in Grenzen. Der Versicherer Axa, der seit einigen Jahren eine Police für den Fall von Cyberattacken anbietet, musste nach eigener Aussage noch keinen Schaden abwickeln, der aus einem rein auf die Reputation gerichteten Angriff resultierte.

Deutlich gefährlicher sind heute klassische IT-Angriffe, die das Unternehmen lahmlegen sollen. Sie können etwa durch einen Produktionsausfall hohe Kosten verursachen – und zugleich das An-

sehen eines Unternehmens massiv verschlechtern. Insgesamt ein stark unterschätztes Risiko, sagt Berater Niggemann: „Ist der Schaden angerichtet, sind Unternehmen bereit, sehr viel Geld für das Reputationsmanagement auszugeben. Im Vorfeld tun sie sich dagegen häufig schwer."

Experten raten, dass Unternehmen in ihre IT-Sicherheitsstrategien auch ein Kapitel aufnehmen, in dem es um Folgen von Angriffen auf die Reputation geht – inklusive eines Handlungsleitfadens für die Verantwortlichen. Wer keinen klaren Plan hat, läuft Gefahr, bis zu einer Gegenreaktion viel Zeit zu verlieren. Und je länger ein Angriff dauert, je länger eine Verunglimpfung im Netz steht oder je länger ein Shitstorm tobt, desto unkontrollierbarer wird die Situation: „Beim Thema Cyber ist Schnelligkeit Trumpf. Sowohl bei der Abwehr als auch bei der Kommunikation", sagt Sabine Träumer, die die Cyberversicherung im Industriekundengeschäft der Axa leitet.

### Gefälschte Tests gegen die Konkurrenz

Auch aus einem weiteren Grund ist zügiges Handeln angebracht. Im Alltagsgeschäft von Anwalt Hofmann geht es häufig um beleidigende Kommentare oder gefälschte Bewertungen, die das Produkt eines Unternehmens herabwürdigen sollen. Aktuell beschäftige ihn ein Unternehmen, das mit falschen Testergebnissen die FFP2-Masken eines Mandanten diskreditieren will. „Das beste Mittel, so etwas zu löschen, ist eine einstweilige Verfügung", sagt er. Das Problem: Firmen müssen dieses rechtliche Mittel innerhalb von etwa vier Wochen einsetzen, nachdem sie den problematischen Beitrag entdeckt haben. Gehen sie erst später dagegen vor, kann sich das Verfahren schnell über mehrere Monate ziehen, berichtet Hofmann.

## Die Gefahren im Blick

Anteil der Befragten in Prozent

**Das Vertrauen ins Management** ist durch die Maßnahmen zur Wahrnehmungen von IT-Risiken gestiegen.

**Dieser Aussage stimme ich ...**

| | |
|---|---|
| ... voll zu. | 11 % |
| **... überwiegend zu.** | **41%** |
| ... eher zu. | 36 % |
| ... eher nicht zu. | 2 % |
| ... überwiegend nicht zu. | 5 % |
| ... gar nicht zu. | 5 % |

**Maßnahmen zur Wahrnehmung von Cybergefahren** haben die Sicherheit im Unternehmen erhöht.

**Dieser Aussage stimme ich ...**

| | |
|---|---|
| ... voll zu. | 31 % |
| **... überwiegend zu.** | **41%** |
| ... eher zu. | 24 % |
| ... eher nicht zu. | 2 % |
| ... überwiegend nicht zu. | - |
| ... gar nicht zu. | 2 % |

Befragt: 900 IT-Sicherheitsexperten weltweit, 32 Prozent davon aus Deutschland, Österreich und der Schweiz, 2020
**HANDELSBLATT** **Quelle:** Lucy Security

Wer nicht unangenehm überrascht werden will, muss das Reputationsmanagement zur stetigen Aufgabe machen – und Plattformen im Blick behalten, auf denen ein Angriff starten könnte. Monitoring-Tools helfen dabei, die Vielzahl an Kanälen zu beobachten. „Es hilft, seine Risikolandschaft zu kennen", sagt Berater Niggemann. Ist etwa die Furcht vor gefälschten Bewertungen, die das Produkt eines Unternehmens herabwürdigen sollen, besonders groß, sollte darauf ein Fokus liegen. Ist einem Unternehmen die eigene Arbeitgebermarke wichtig, sollten die entsprechenden Bewertungsseiten begleitet werden. Und steigen die Followerzahlen bei Facebook, Twitter oder Instagram, hilft hier eine klare Vorgabe, wie mit beleidigenden oder verleumdenden Botschaften umgegangen wird. Fehle eine entsprechende Struktur, sei es kein gesteuerter Ablauf, sagt Niggemann, „sondern nur eine persönliche Entscheidung des jeweiligen Social-Media-Managers".

> Wenn sich ein Angreifer richtig viel Mühe macht, dann hat er meistens ein persönliches Motiv.
>
> **Ruben Hofmann**
> Rechtsanwalt in Köln

Ein verbindliches Vorgehen verschafft im Ernstfall Klarheit und kürzt Diskussionen ab. Werden einzelne Personen verunglimpft, wie es der Gesellschafter mit seinem Kompagnon versuchte, kann es zu finanziellen Ansprüchen kommen. Für Firmen dagegen bleibt die Hoffnung auf Geldentschädigung gering, selbst wenn ein Angreifer ermittelt wird. Unternehmen müssten exakt nachweisen, dass eine digitale Attacke zu einem Umsatzverlust geführt habe, berichtet Hofmann. Verliert ein Projektentwickler einen wichtigen Großkunden, weil der im Netz von gefälschten Untreuevorwürfen gelesen hat, kann das gelingen. Doch wenn sich Kunden oder Fachkräfte aufgrund eines negativen Bildes im digitalen Raum abwenden, lässt sich das nicht in Geld umrechnen: „Diese Kausalität nachzuweisen, das ist in der Praxis kaum zu schaffen", sagt Hofmann.

Im IT-Ernstfall sollten zum Krisenstab im Unternehmen keinesfalls nur Programmierer gehören, fordern Reputationsfachleute. Neben den Juristen kommen häufig auch Datenschutzbeauftragte ins Spiel – geht es doch in vielen Fällen um persönliche Informationen über Kunden oder Mitarbeiter. Zusätzlich sind Kommunikatoren gefragt. Die Anbieter von Cyberversicherungen stellen angegriffenen Unternehmen gern Spezialisten zur Seite. Das ist ein kalkuliertes Investment: Ein fixes und entschlossenes Vorgehen hilft, den Versicherungsschaden einzugrenzen. „Unternehmen brauchen den richtigen Krisenmanager, der durch die Stolperfallen führt", sagt Axa-Expertin Träumer.