Das Problem mit den unfairen Bewertungen

Wie Unternehmen dagegen vorgehen können

Wo finde ich einen guten Arzt, den besten Kühlschrank, das schönste Hotel? Portale wie Tripadvisor, Jameda oder Ebay liefern Verbrauchern mit Kundenbewertungen entsprechende Informationen. Fallen sie positiv aus, tragen sie erheblich zum Umsatz der Unternehmen bei. Sind sie negativ, können sie äußerst geschäftsschädigend sein, wenn sich Kunden als Folge für Produkt oder Dienstleistung der Konkurrenz entscheiden.

VON RENATE REITH

Was das Shoppen im Internet anbelangt, orientieren sich laut einer Umfrage von Bitkom Research 63 Prozent der Käufer an Onlinebewertungen. Doch ein Problem, mit dem Online-Händler zu kämpfen haben, sind unfaire Bewertungen. Das geht aus einer Studie des Händlerbundes im Jahr 2017 unter 1000 Händlern hervor. Demnach waren 95 Prozent der Befragten betroffen. In fünf Prozent der Fälle gingen sie von Fake-Beurteilungen der Konkurrenz aus. „Dadurch sinkt ihr Ranking, und sie verlieren deutlich an Image und Sichtbarkeit im Netz", sagt Sandra May, Volljuristin beim Händlerbund. Wenn Kunden so getäuscht werden, koste die Firmen das bares Geld.

Mitunter sind diese Bewertungen äußerst kurios. „Es werden Produkte bewertet, die der Händler gar nicht führt oder Dinge moniert, wie der Benzinrasenmäher, der ohne Netzstecker geliefert wurde", nennt May Beispiele.

Das Problem mit den Bewertungen zieht sich durch alle Branchen. „Es trifft auch die freien Berufe wie Architekten, Anwälte und Ärzte", sagt Arno Lampmann, Fachanwalt für gewerblichen Rechtsschutz in Köln. Allen voran Ärzte. „Sie sind bei Jameda zwangsgelistet", sagt Lampmann. Jameda weigere sich, Ärzte aus der Plattform zu nehmen mit dem Hinweis, dass alle Daten über sie ohnehin öffentlich seien, so der Anwalt.

„Diese Position ist aber nicht mehr neutral, wenn Jameda über kostenpflichtige Premiumpakete Geld verdient", betont Lampmann. Je nach gebuchtem Umfang beinhalten sie etwa Fotos der Praxis, Online-Terminbuchungen – und eine bessere Platzierung. Im Grunde kein schlechter Service für Patienten. Jedoch werden Ärzte, die davon keinen Gebrauch machen, schlechter präsentiert.

„Wir haben fast täglich Anfragen von verzweifelten Ärzten, die sich gegen eine schlechter gestellte Präsentation oder Bewertungen auf Jameda zu wehren versuchen", sagt Lampmann. Es sei zudem perfide, wenn die Plattform die Ärzte dazu auffordere, schlechte Bewertungen doch einfach zu kommentieren. Hier müssen sie wegen der ärztlichen Schweigepflicht nämlich vorsichtig sein. „Ärzte dürfen streng genommen noch nicht einmal bestätigen, dass der Bewertende ihr Patient ist", sagt Lampmann. Er sieht aber einen Lichtblick: „Drei Gerichte haben inzwischen Ärzten einen Anspruch auf Löschung von der Plattform zugestanden, es besteht daher Hoffnung, dass Jameda sein Geschäftsmodell in Zukunft anpassen wird."

Die Betroffenen sind also nicht machtlos. „Es gibt mehrere Angriffspunkte", erläutert Matthias Hechler, dessen Anwaltskanzlei seinen Sitz in Schwäbisch Gmünd hat und ebenfalls auf Bewertungen im Netz spezialisiert ist. „Betroffene haben gegen das Internetportal einen Anspruch auf Löschung, wenn die Bewertung unwahre Tatsachen oder Schmähkritik enthält", erklärt er. Kenne man den Bewerter, so habe man gegen diesen dieselben Ansprüche auf Löschung und Unterlassung. Außerdem dürften nur Personen mit einer eigenen Erfahrung eine Bewertung abgeben. „Diese Erfahrung muss der Bewerter nachweisen, was er oft nicht kann", sagt Hechler.

Auch gerechtfertigte negative Bewertungen könne man oft löschen lassen, weil der Portalbetreiber die Authentizität nicht nachweisen könne, sagt Hechler. „Bleibt die Löschung erfolglos und kennt man den Bewerter, kann man sich mit diesem oft auf eine freiwillige Löschung einigen, wenn man dessen Problem löst."

Vom Kauf von 5-Sterne-Bewertungen, um sein Ranking im Netz zu verbessern, rät Rebekka Weiß, Leiterin Vertrauen & Sicherheit vom Digitalverband Bitkom, ab. „Nicht nur, weil man damit seinen potenziellen Kunden einen Bärendienst erweist, sondern auch weil die Portale hart durchgreifen, wenn sie solche Fake-Bewertungen entdecken", sagt sie. Auch wettbewerbsrechtlich seien sie problematisch, sodass Abmahnungen drohten.

Diebstahl, Betrug, Erpressung oder Spionage gegen Firmen gab es schon immer. Doch anders als früher finden solche Delikte heute verstärkt in der digitalen Welt statt. Wenn es um die IT-Sicherheit in der Informationsgesellschaft geht, ist das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, die wichtigste Anlaufadresse. Die Behörde mit Sitz in Bonn beschäftigt mehr als 900 Informatiker, Physiker, Mathematiker und andere Mitarbeiter. Das BSI wendet sich an öffentliche Verwaltungen in Bund, Ländern und Kommunen, an Unternehmen und Privatanwender.

WELT: Die digitale Transformation erreicht inzwischen auch die kleinen und mittelständische Unternehmen, steigt damit für sie die Wahrscheinlichkeit, Ziel von Cyberangriffen zu werden?
BSI: Wir gehen davon aus, dass die Bedrohungslage, um Opfer eines Cyberangriffs zu werden, nach wie vor hoch ist. Je digitalisierter unser Alltag, also auch unser Berufsumfeld ist, desto angreifbarer werden wir. Das ist leider die Kehrseite der sonst notwendigen und wichtigen Digitalisierung. Bei vielen kleineren Betrieben und Mittelständlern herrscht häufig zudem noch die Meinung vor, dass nur große Unternehmen zur Zielscheibe für Cyber-Kriminelle werden. Tatsächlich ist das Know-how im deutschen Mittelstand ein attraktives Ziel für Täter und es besteht jederzeit die Gefahr, Opfer von Angriffen zu werden.

Worin liegen die größten Gefahren für die Unternehmen – Spionage, Sabotage oder Datendiebstahl...?
Wir sehen bei allen Angriffsformen ein deutliches Wachstum. Die einen sind vom CEO-Fraud – Kriminelle geben sich als Chefs aus – betroffen, andere von Ransomware, bei der alle Daten verschlüsselt, also unlesbar gemacht werden. Wer seine Cybersicherheitsstrategie nach dem Prinzip wählt „Was kann mich am ehesten treffen", unterschätzt die Dynamik neuer Angriffsformen. Es hilft wirklich nur eines: Investieren Sie in die Cyber-Sicherheit Ihres Unternehmens oder Betriebs. Der Return of invest ist Sicherheit, Kundenzufriedenheit und -vertrauen. Unschätzbare Werte. Damit das Ganze gelingt, sollte die Führungsetage mit gutem Beispiel vorangehen. Aufgrund der Vorbildfunktion für die Mitarbeiter, der Bereitstellung von Budget und nicht zuletzt wegen der existenzbedrohenden Ausmaße eines Cyber-Angriffs, muss Cyber-Sicherheit Chefsache sein.

Wie hoch sind die Schäden durch solche Angriffe?
Hierzu liegen uns keine abschließenden Zahlen vor. Der Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien) hat 2017 von 55 Milliarden Euro jährlich gesprochen. 2018 von 43 Milliarden Euro im Jahr bei Attacken auf deutsche Industrie. Nur Betreiber kritischer Infrastrukturen sind dazu verpflichtet, IT-Sicherheitsvorfälle zu melden. Der mittelständische Betrieb im Ort oder der Handwerksbetrieb um die Ecke gehören in der Regel nicht dazu. Diese können aber gerne freiwillige Meldungen abgeben, etwa über die Allianz für Cyber-Sicherheit. Viele trauen sich nicht, den Angriff auf zu Beispiel ihr Datensystem preiszugeben – aus Angst vor einem Reputationsschaden.

Wer sind typischerweise die Täter und welches Interesse verfolgen sie mit ihren Angriffen?
Die überwältigende Mehrheit der Täter handelt aus finanziellem Interesse und mit kriminellen Motiven. Alles was es für diese Form der Kriminalität braucht, ist ein gewisses Maß an Fachkenntnis und einen Computer. Daneben gibt es Cyber-Angriffe mit dem Ziel, Wissen zu stehlen und auch Sabotage-Angriffe hat es bereits gegeben, etwa bei den Cyber-Angriffen auf die Stromversorgung der Ukraine. Sie bilden nach den Zahlen allerdings die Ausnahme.

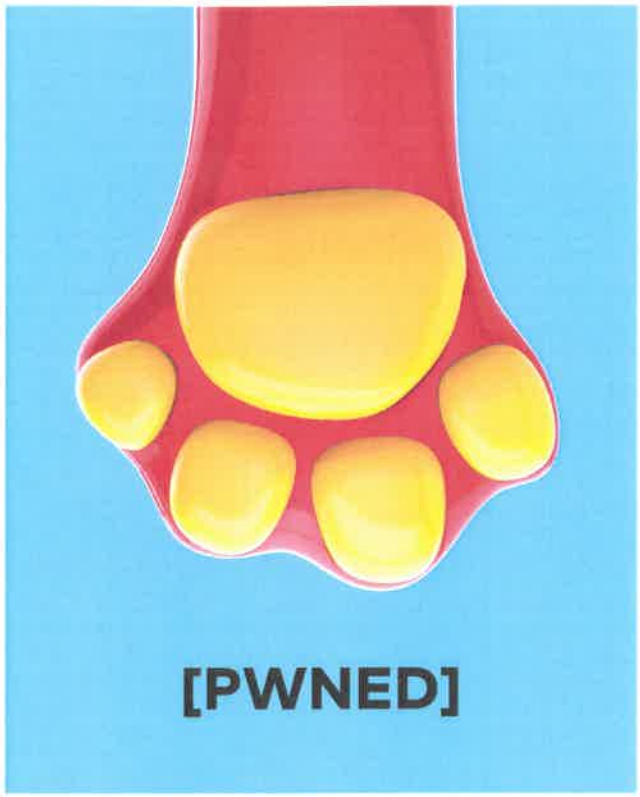
Sind sich die Unternehmen bewusst, wie angreifbar sie sind?
Viele ja, aber nicht alle handeln auch danach. Das Thema ist ja nicht nur in den Medien präsent, sondern auch in den Innungen, Verbänden und Kammern. Mit der Allianz für Cyber-Sicherheit, in der fast 4000 Teilnehmer organisiert sind, konnte das BSI ein breites Netzwerk gründen, in dem wir die Unternehmen und Betriebe informieren, wie und wo sie sich gegenseitig unterstützen können. Auch hier zeigt sich, wer seine Erfahrungen teilt, schützt nicht nur sich, sondern in Zukunft auch andere vor den verheerenden Folgen eines Angriffs.

Wie können die Unternehmen sich vor Cyber-Attacken schützen?
Der erste und wichtigste Schritt ist getan, wenn sie sich entschließen, in Cyber-Sicherheit zu investieren und zu verstehen, dass Cyber-Sicherheit kein reiner Kostenfaktor, sondern ein Erlöstreiber und Wettbewerbsvorteil ist. Bei dem nachfolgenden Prozess stehen wir als BSI mit unseren IT-Grundschutzprofilen mit Rat und Tat zur Seite. Hier werden Schritt für Schritt Maßnahmen und Möglichkeiten aufgezeigt, die am Ende dazu führen sollen, dass alle Einheiten eines Unternehmens bestmöglich geschützt sind.

Wie sinnvoll sind beispielsweise sogenannte Penetrationstests, bei denen Hacker im Auftrag der Unternehmen nach Sicherheits-Schwachstellen suchen?
Pen-Tests können eine sinnvolle Maßnahme sein, um das IT-Sicherheitsniveau des eigenen Netzwerks zu überprüfen. Dazu sollten im Vorfeld einige Rahmenbedingungen geklärt werden und man benötigt einen vertrauenswürdigen Dienstleister. Auf unseren Webseiten haben wir ein Liste qualifizierter und zertifizierter IT-Sicherheitsdienstleister zur Verfügung gestellt.

Technische Sicherheitsvorkehrungen sind natürlich wichtig – wie steht es um den Faktor Mensch?
Menschen können Anwendungsfehler machen oder falsche Konfigurationen vornehmen, die dann zu Schwachstellen in der Technik führen. Deshalb ist es so wichtig, nicht nur in Soft- und Hardware zu investieren, sondern auch in die Köpfe eines Unternehmens. Die letzte Cyber-Sicherheitsumfrage des BSI ergab aber auch, dass der Faktor Mensch bei der Abwehr eine ebenso wichtige Rolle spielt wie die Technik. Deshalb sind regelmäßige Schulungen, z.B. zum sicheren Umgang mit E-Mails, wichtig. Diese sind immer noch das verbreitetste Einfallstor für Cyber-Angriffe.

Die Fragen stellte Christina Petrick-Löhr



Die Tatze – englisch „paw" – ist ein Symbol aus der Hacker-Szene. „You just got pwned" bedeutet so viel wie „Du wurdest besiegt". Ursprünglich wurde das Wort „owned" verwendet – doch ein Tippfehler auf der Tastatur machte daraus „pwned"

DANIEL KALKER/DPA/PICTURE ALLIANCE

ANGRIFF aus dem Cyber-Raum

Mittelständler sind ein Top-Ziel für Kriminelle. Das Bundesamt für Sicherheit in der Informationstechnik rät zu mehr Investitionen

CEO-Fraud: Die Masche mit dem Chef-Namen

Die Mail kam angeblich vom Geschäftsführer, adressiert an den Finanzchef des Unternehmens. Gefragt wurde der Finanzchef, ob er den ganzen Tag Zeit hätte, um die finanzielle Seite einer streng geheimen **Firmenübernahme** abzuwickeln. Es ging immerhin um fast ein halbe Million Euro. Eine kleine Unregelmäßigkeit in der Absenderadresse machte den Finanzchef misstrauisch, zudem hatte er schon früher von ähnlichen Fällen gehört.
Der Finanzleiter zog zunächst die eigenen IT-Fachleute, dann auch das **Landeskriminalamt** hinzu. In Abstimmung mit der Polizei machten die unvisierten Opfer das Spiel der Betrüger vorgeblich mit, um deren Masche detailliert analysieren zu können. Technisch und psychologisch gingen die Cyber-Kriminellen höchst raffiniert und manipulativ zu Werke – dass sie am Ende leer ausgingen, lag vor allem an der gesunden Wachsamkeit des Finanzchefs.
Dokumentiert hat den Fall der Autor Thomas Stasch. Dessen Arbeitgeber, ein kommunaler IT-Dienstleister, war das Ziel der Attacke. Fälle von sogenanntem CEO-Fraud wie diesen gibt es immer wieder – und oft genug funktioniert der Trick.

Wertschätzend digital weiterbilden

Um Arbeitsabläufe zu verbessern, sollten alle Mitarbeiter eingebunden werden – Bundesweit helfen 26 Kompetenzzentren

Der Mittelstand in Deutschland investiert zu wenig in die Digitalisierung. Dennoch verweisen Experten auf Fortschritte in Bezug auf die digitale Weiterbildung in den Unternehmen. „Die Unternehmen sind für das Thema Digitalisierung sensibilisiert. Sie wissen, um auf dem Markt bestehen zu können, um konkurrenzfähig zu bleiben, muss digitalisiert werden", sagt Marie Landsberg, Referentin von „Mittelstand 4.0-Kompetenzzentrum Berlin".

VON HEIKE KOWITZ

Aktuell finden 90 Prozent der Unternehmen das Thema Weiterbildung wichtig. Knapp zwei Drittel der Unternehmen in Deutschland bieten ihren Mitarbeitern Möglichkeiten an, sich in Sachen Digitalisierung schlau zu machen. Vor zwei Jahren waren es erst 56 Prozent, wie der Digitalverband Bitkom berichtet. Bitkom und TÜV-Verband (VdTÜV) hatten gemeinsam eine repräsentative Studie in Auftrag gegeben, bei der 504 Unternehmen ab zehn Mitarbeitern befragt wurden. Demnach stehen den Beschäftigten im Schnitt jährlich 2,3 Arbeitstage und 709 Euro für Weiterbildung aller Art zur Verfügung. 42 Prozent der Befragten sagen, Weiterbildungen seien zu teuer. Jedes vierte Unternehmen findet kein passendes Angebot und jedem fünften fehlt der Überblick über das Angebot auf dem Weiterbildungsmarkt, so Ergebnisse der Studie.

29 Prozent verzichten auf Weiterbildung der bestehenden Belegschaft, weil es günstiger ist, Mitarbeiter neu einzustellen. Jedes fünfte Unternehmen bildet gar nicht weiter. Oftmals hätten auch Mitarbeiter kein Interesse an einer Weiterbildung (24 Prozent).

Die dafür zur Verfügung gestellten finanziellen Mittel sowie die eingeräumte Zeit seien in der Regel viel zu knapp bemessen, sagt Michael Fübi, Präsident des TÜV-Verbands. Bei einem externen Anbieter koste ein Seminartag jedoch zwischen 450 und 500 Euro.

Marie Landsberg ist hingegen der Auffassung: Weiterbildung müsse nicht teuer sein. Die Verbände, die Handelskammern sowie die 26 auf Digitalisierung spezialisierten Kompetenzzentren, die bundesweit vom Bundeswirtschaftsministerium unterstützt werden, böten sogar kostenlose Angebote an. „Es hakt nicht am fehlenden Geld. Es hakt aber vor allem an zeitlichen Ressourcen", sagt Landsberg. Dabei müsse digitale Weiterbildung nicht bedeuten, eine sehr teure Software einzuführen, die die Mitarbeiter erst langwierig lernen müssten. „Passt eine digitale Anwendung zu den bisherigen Abläufen oder verbessert diese sogar, steigt die Motivation, sich Wissen dazu anzueignen und das Neue zu nutzen", so die Bildungsexpertin.

In mehr als der Hälfte der Unternehmen fehlt eine Strategie für die Vermittlung digitaler Kompetenzen. „Wir haben kein Erkenntnisproblem, es geht um die Umsetzung", sagt Bitkom-Präsident Achim Berg.

Kleine und mittelständische Unternehmen, die die Hilfe eines Kompetenzzentrums annehmen, kommen mit einem konkreten Problem. „Wir bieten Orientierung", versichert Marie Landsberg. Die Unternehmenskultur müsse vorab beleuchtet werden. Und: „Wir haben einen Digitalcheck-Mittelstand entwickelt, mit dem Firmen sehen, wo sie in Sachen Digitalisierung aktuell stehen und wie sie sich weiterentwickeln können."

Gut die Hälfte der für die Digitalisierungs-Studie befragten Unternehmen gibt an, dass es keine Zeit für entsprechende Freistellungen gibt. Die Ressourcen im Mittelstand seien gegrenzt, räumt Marie Landsberg ein. Bei den Digitalisierungsmaßnahmen müssten daher von Beginn an die Mitarbeiter mit einbezogen werden. „Digitale Lösungen funktionieren nur, wenn sie von den Mitarbeitern akzeptiert werden."

Von der Führungsebene müssten die Angestellten als Experten auf ihrem Gebiet wahrgenommen werden. Es müsse eine Kommunikation auf Augenhöhe stattfinden. „Eine Führungskultur, die auf Wertschätzung basiert, erleichtert die digitale Weiterbildung", sagt die Bildungsexpertin. Für die Weiterbildung bieten sich auch digitale Lernformate an. Aktuell nutzen jedoch nur 32 Prozent der Unternehmen digitale Lernangebote, so die Studie. Knapp 50 Prozent setzen dagegen auf Seminare im eigenen Haus mit externen Referenten oder Fachleuten aus dem eigenen Unternehmen. 24 Prozent greifen auf externe Offline-Seminarangebote zurück.

Dabei könnten mit digitalen Lernformaten wie Online-Seminaren oder Lern-Apps die Inhalte individuell und flexibel gestaltet werden, findet Achim Berg. „Nie war es für Mitarbeiter einfacher, unabhängig von Zeit und Ort zu lernen." Im Berliner Kompetenzzentrum hält man viel von einem „Mix der Formate". Seminare und Workshops könnten beim Einstieg nützlich sein, sagt Marie Landsberg. „Beim Austausch mit anderen lernt man viel. Aber es gibt auch digitale Formate, die man orts- und zeitunabhängig, nutzen kann. Die Dienstreise entfällt, Mitarbeiter können sich flexibel und selbstbestimmt weiterbilden."