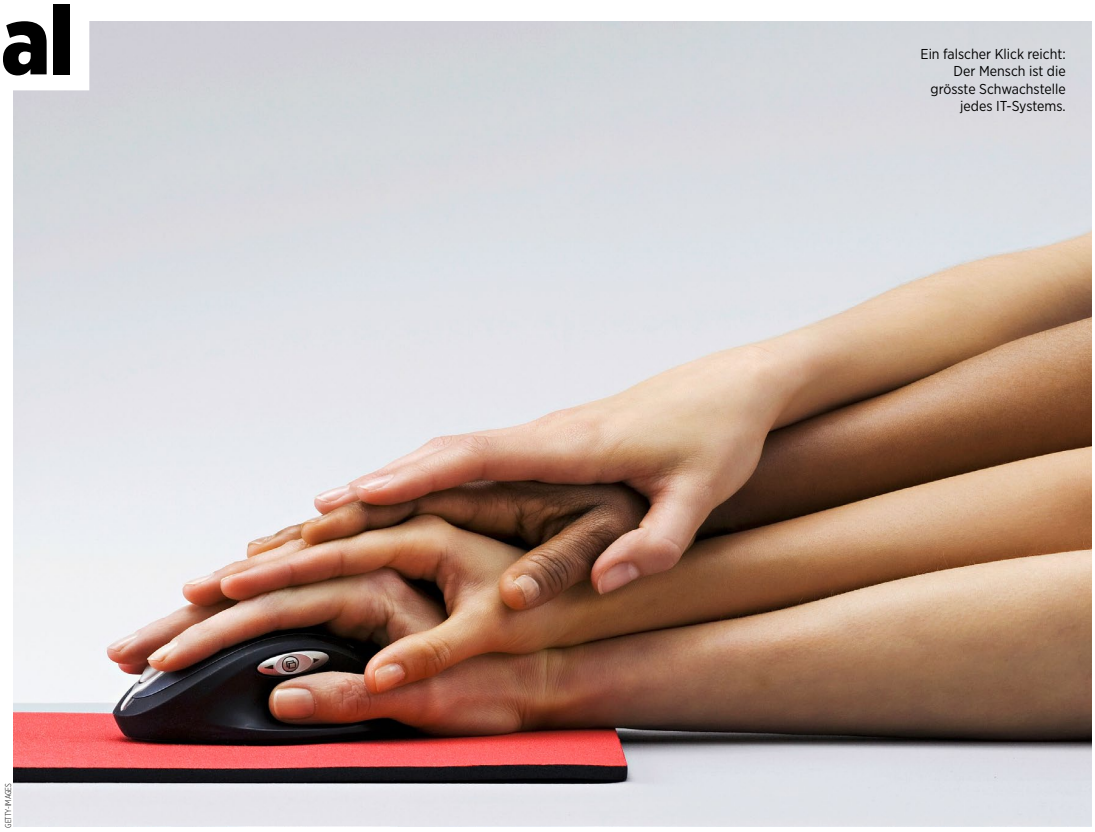
Faktor *Mensch* mit grossem Potenzial

Mitarbeitende haben einen entscheidenden Einfluss auf die Cybersicherheit eines Unternehmens. Personalisierte Botschaften helfen, ihr Online-Verhalten zu verbessern.

CARLOS CASIÁN UND HÉLÈNE DONNA STAUBLI



Ein falscher Klick reicht: Der Mensch ist die grösste Schwachstelle jedes IT-Systems.

GETTY IMAGES

Verschlüsselung von IT-Systemen, Diebstahl von vertraulichen Daten oder Drohungen, um Geld zu erpressen: Cyberkriminelle entwickeln ihre Praktiken und Angriffsmethoden laufend weiter, um Unternehmen effizienter anzugreifen. Cybervorfälle gehören zu den Top drei der Geschäftsrisiken, und die Prognosen sowie Schätzungen zeigen ein einheitliches Bild: Cyberangriffe und die daraus entstehenden Kosten werden weiter zunehmen. Diese Entwicklung hat sich in den letzten Jahren auch im Cyberversicherungsmarkt gezeigt. Starke Korrekturmassnahmen wie Prämienerhöhungen und Deckungseinschränkungen wurden umgesetzt – insbesondere für mittlere und grössere Unternehmen.

Der Risikodialog ist durch die Erfahrungen der letzten Jahre gereift und hat dazu beigetragen, dass Cyberrisiken besser erkannt und adressiert werden. Die Cyberrisikoberatung von Unternehmenskunden umfasst verschiedene Bereiche: das Aufzeigen der aktuellen Gefahrenlage, das Besprechen der individuellen Risiken, das Modellieren der verschiedenen Cybervorfälle hinsichtlich Eintrittswahrscheinlichkeit und Schadenausmass, die Evaluation von Cybersicherheitsmassnahmen (Key Controls), Peer-Vergleiche anhand von Benchmarkdaten sowie die Diskussion zum geeigneten Risikotransfer.

Eine Studie des Risikoberaters Marsh zeigt, dass die strikte Einhaltung der zwölf Key Controls einen grossen Einfluss auf die Schadenprävention hat und die Versicherer damit die Risiken einheitlicher selektionieren können. Heute ist der Cyberversicherungsmarkt deutlich ausbalancierter mit einem gestärkten Commitment zu dieser noch immer stark wachsenden Versicherungssparte.

Online-Verhalten schulen, Awareness schaffen

Sind damit die Cyberrisiken ganzheitlich erfasst und ist die Risikoberatung als ausgereift und fit für die Zukunft zu bezeichnen? Der Dialog aus technischer Sicht und die dazugehörigen Key Controls sind bereits in vielen Unternehmen auf einem guten Stand. Beim Faktor Mensch hingegen schlummert noch ein grosses Potenzial. In den letzten Jahren wurde bereits viel in das Thema Awareness investiert und erreicht, doch es steckt nach wie vor in den Kinderschuhen. Schätzungen zufolge werden deutlich mehr als 50 Prozent der erfolgreichen Cyberangriffe mit Phishing-Attacken initiiert. Währenddessen beschränkt sich die Diskussion heute oft auf die Frage, ob jährliche Awareness-Trainings durchgeführt werden oder nicht. Das Verhalten der Mitarbeitenden hat einen entscheidenden Einfluss auf die Cybersicherheit eines Unternehmens. Cyberkriminelle nehmen sie ins Visier, um in das Unternehmensnetzwerk einzudringen. Bei simulierten Phishing-Kampagnen beträgt die Klickrate nicht selten mehr als 20 Prozent – auch bei Unternehmen, die jährliche Trainings durchführen.

50
Prozent
der erfolgreichen Cyberangriffe werden mit Phishing-Attacken initiiert.

Ein Blick in die Forschung aus den letzten Dekaden zeigt die Bestrebungen, «gutes» Online-Verhalten zu ermitteln und zu beschreiben, um daraus Massnahmen abzuleiten. Der wissenschaftliche Fokus wurde dabei insbesondere auf normatives Training – «Du sollst keine verdächtigen E-Mails oder Anhänge öffnen» – oder auf Charaktereigenschaften der Mitarbeitenden wie «neugierig» oder «impulsiv» gelegt. Ersteres scheint nur bedingt wirksam zu sein, Letzteres nur bedingt beeinflussbar. Diese Faktoren spielen beim Risikoverhalten eine Rolle, jedoch müssen die individuellen Verhaltensweisen, Motivationen und Umfelder sowie die Kultur eines Unternehmens adressiert werden.

Aus der Risikoforschung wissen wir, dass personalisierte Botschaften anstelle von Standard-Awareness-Schulungen mit beschränktem Bezug zum eigenen Unternehmen ein grosses Potenzial haben, um Verhaltensveränderungen herbeizuführen und die Cybersicherheit zu erhöhen. Die Frage stellt sich nun, wie sich die wichtigen, individuellen Risikofaktoren der Mitarbeitenden erheben und zusammen mit der Kultur eines Unternehmens zu gezielten Botschaften ableiten lassen – und wie diese in wirksame Gegenmassnahmen umgewandelt werden können.

Gezielte Botschaften statt Pauschalaussagen

Ein Schweizer Forschungsteam der HSLU und der ZHAW untersucht gemeinsam mit Partnern aus der Wirtschaft zurzeit mittels Methoden aus der Marktforschung die verhaltensbasierten und kulturellen Faktoren. Das Ziel: ein skalierbares Diagnostik-Tool zu entwickeln, das anhand von wenigen Fragen diese Faktoren erfassen kann. In einem ersten Schritt werden Botschaften für die Mitarbeitenden entwickelt, die ihre Verhaltensweisen nachhaltig positiv beeinflussen, sodass die Klickrate auf Phishing-Mails und die Reaktionen auf sonstige Manipulationsversuche gesenkt werden. Danach werden gezielte Cyber-Awareness-Schulungen entwickelt. Im Fokus stehen die zu internalisierenden Botschaften und ein handlungsbasiertes Lernen. Denn man lernt in der Regel am besten, wenn man etwas anwendet.

Wenn der Faktor Mensch annähernd so gut verstanden wird wie die technischen Aspekte der Cybersicherheit, lässt sich der Risikodialog ganzheitlich erfassen. Dazu benötigt es weitere interdisziplinäre Zusammenarbeit zwischen Forschung und Wirtschaft, um die richtigen Schlüsse zu ziehen und die Diskussion zu lancieren. Die Vorteile sind vielfältig: Einerseits wirkt sich die Erweiterung der zur Verfügung stehenden Informationen um den Faktor Mensch positiv auf die Risikoeinschätzung der Unternehmen aus, und sie können gezieltere Trainings anbieten, um die Cyberexponierung weiter zu reduzieren. Anderseits können Versicherer mit mehr Informationen das Risiko besser erfassen. Dies kann zu einem Pricing führen, das die Investitionen eines Unternehmens besser in der Prämie widerspiegelt.

Carlos Casián, Fachspezialist Special Risks, und Hélène Donna Staubli, Teamleiterin Special Risks, Kessler & Co AG

Digitale Transformation: *Vertrauen* als Erfolgsrezept

Ein wirksamer Umgang mit **Cyber- und Datenschutzrisiken** stärkt das Vertrauen der Anspruchsgruppen.

MATTHIAS BOSSARDT

Unter dem Begriff «Digitale Transformation» arbeiten viele Unternehmen daran, digitale Technologien in ihre Geschäftsabläufe zu integrieren. Sie versprechen sich dadurch eine gesteigerte Kundenzufriedenheit, effizientere Geschäftsabläufe sowie insgesamt mehr Agilität und eine bessere Wettbewerbsfähigkeit. Allerdings gibt es auch eine Kehrseite: Durch den verstärkten Einsatz digitaler, teilweise neuer Technologien und die intensivierte Nutzung von Daten vergrössert sich die Angriffsfläche für Cyberattacken. Gleichzeitig steigt das Risiko von Datenschutzverletzungen.

Ohne Vertrauen keine digitale Transformation

Die teilweise (noch) grossen Vorbehalte von internen Anspruchsgruppen wie beispielsweise Risiko- oder Compliance-Funktionen, aber auch von Kunden, Regulatoren und Geschäftspartnern gegenüber neuen Technologien und der intensiveren Datennutzung führen dazu, dass digitale Transformationsprogramme verzögert werden, den erwarteten Nutzen nicht erzielen oder gar vollständig scheitern. Das Schaffen von Vertrauen gegenüber den verschiedenen Anspruchsgruppen wird so zu einem wesentlichen Wettbewerbsfaktor eines Unternehmens.

Dies bestätigt die Studie «KPMG Global Tech Report 2023». Darin zeigen sich die digitalen Führungskräfte einerseits zuversichtlich, dass der Einsatz von Technologie in allen Bereichen ihres Unternehmens zu Produktivitätssteigerungen führen wird. Anderseits wurde mangelndes Vertrauen, insbesondere hinsichtlich der Cybersicherheit und des Datenschutzes, als Hauptfaktor genannt, der den Fortschritt der Transformation verlangsamen kann. Angesichts der fortschreitenden Migration zu Cloud-Infrastrukturen gaben zudem 40 Prozent der Befragten an, dass die Verbesserung der Sicherheit zu einem der wichtigsten Ziele ihrer Cloud-Projekte geworden ist.

Sicherheit stärkt Kundenbindung

Viele Unternehmen sehen Cybersicherheit mittlerweile nicht mehr nur als eine Notwendigkeit zur Vermeidung von Ausfällen, sondern auch als Chance im Markt. Unternehmen, die in puncto Sicherheit gute Leistungen erbringen, erzielen einen Wettbewerbsvorteil. So geben 63 Prozent der Unternehmen, die an der KPMG-Studie teilgenommen haben, an, dass die Verbesserung der Cybersicherheit und des Datenschutzes ihnen dabei hilft, ein Kundenerlebnis zu schaffen, das die Kundenbindung stärkt.

Um maximal von der digitalen Transformation profitieren zu können, behalten die Technologieführer Cybersicherheits- und Datenschutzaspekte bewusst im Auge. Viele Unternehmen haben festgestellt, dass ein proaktives Management dieser Themen in der Frühphase von Transformationsprojekten die Erfolgsquote deutlich erhöht. Bewährt hat sich dabei der Security-/Privacy-by-Design-Ansatz. Dieser bettet die Sicherheit in den Kern des Unternehmens ein und ist ein breit akzeptiertes Prinzip: 62 Prozent der Unternehmen managen Risiken in den frühen Projektphasen mit diesem Ansatz, um die Erfolgsquote von Transformationsprogrammen zu erhöhen.

Mittlerweile ist in vielen Unternehmen das Bewusstsein vorhanden, dass Investitionen in die richtigen Werkzeuge und Prozesse innerhalb der Entwicklungsumgebung zu einem frühen Zeitpunkt eine sichere und vertrauenswürdige Grundlage schaffen. Damit ist das Unternehmen in der Lage, die Verwirklichung seiner digitalen Ambitionen zu beschleunigen. Sicherheit und Vertrauen zu schaffen, ist jedoch nicht nur eine technische Herausforderung. Vielen Technologiefunktionen mangelt es noch immer an der notwendigen Governance und Koordination im Unternehmen, um Transformationsinitiativen effektiv zu unterstützen und die verantwortungsvolle Nutzung von Technologien und Daten nachhaltig sicherzustellen und zielgruppengerecht zu kommunizieren. All dies ist eine notwendige Voraussetzung, um das Vertrauen der internen und externen Anspruchsgruppen zu erlangen und den versprochenen Nutzen der digitalen Transformation zu realisieren.

Matthias Bossardt, Leiter Cyber & Digital Risk Consulting, KPMG Schweiz