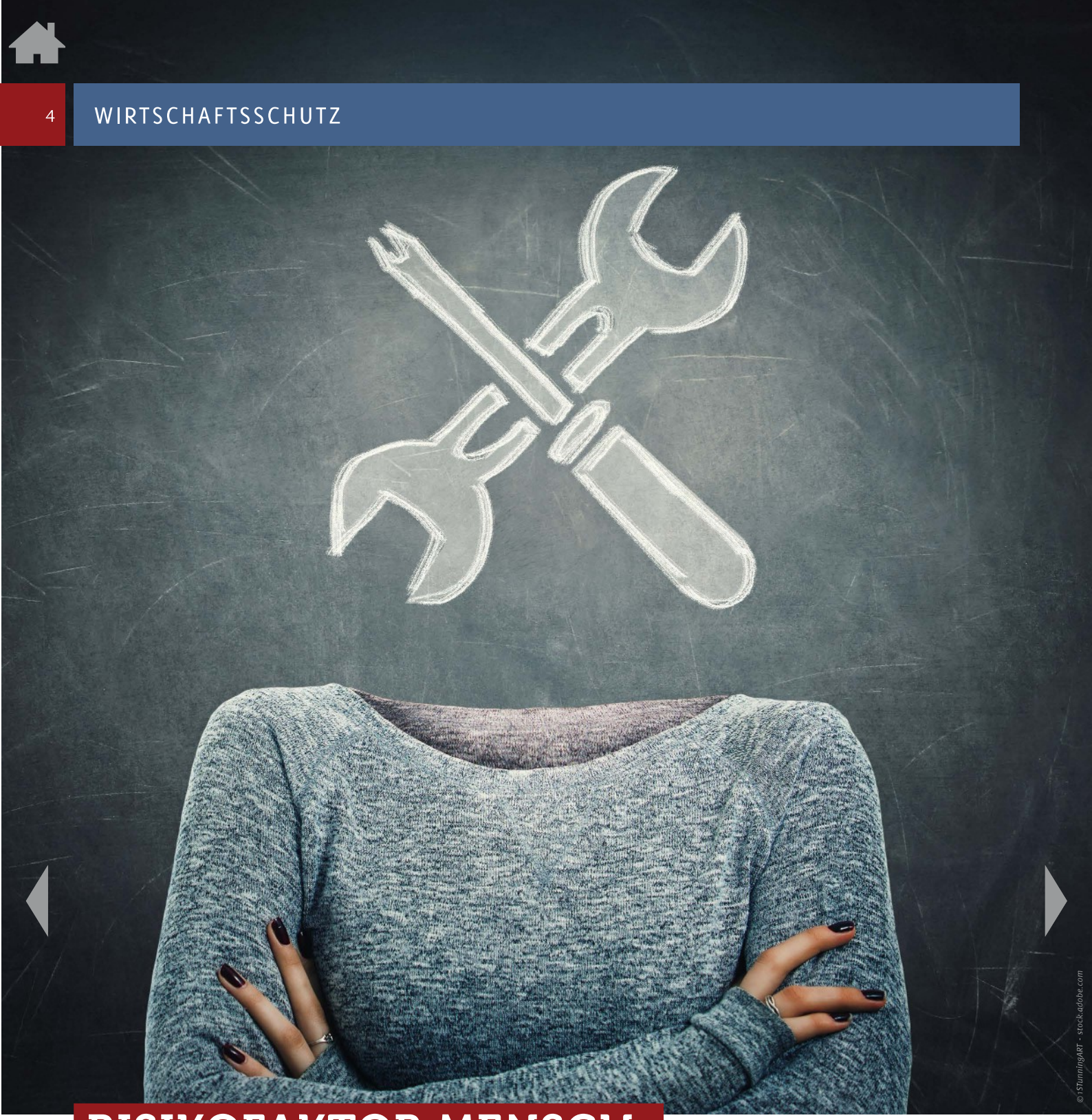

RISIKOFAKTOR MENSCH: VON DER GEFAHR ZUR RESSOURCE!

„Wie kann ich meine Mitarbeiter davon abhalten, das Falsche zu tun?“. So oder so ähnlich lauten die Fragen, die sich Unternehmen stellen, die ihren Betrieb vor Cyberattacken schützen wollen. Der Mensch, also der oder die Mitarbeiter/-in, steht dabei oft als die Gefahrenquelle im Fokus. Schließlich sind es Menschen, die einen Link in einer Phishing-Mail öffnen. Es ist der Kollege, der unbedarft einen fremden USB-Stick ansteckt und es ist die Kollegin, die bereitwillig Passwörter über das Telefon weitergibt, nur weil das Gegenüber angibt, der Systemadministrator zu sein.

Es werden Anhänge geöffnet, Überweisungen getätigt, Sicherheitssysteme umgangen und das nicht aus dem Willen heraus, dem Unternehmen zu schaden. Dies passiert, weil wir Menschen gelernt haben, gesellschaftlichen Normen und Regeln zu folgen. So haben wir gelernt, Autoritäten zu folgen oder verspüren das Bedürfnis, uns für Gefallen zu revanchieren oder jemandem mit schwerer Last die Tür aufzuhalten. Derartige Handlungen vollbringen wir täglich viele Male und diese sind für uns so selbstverständlich, dass sie völlig automatisch und unbewusst ablaufen.

DER MENSCH ALS GEFAHR?!

Diese „hilfsbereiten" Automatismen sind tief in uns verankert. Wer die Trigger für solche gelernten und automatisierten Handlungsabläufe kennt, kann Menschen und ihre Handlungen beeinflussen und bewusst „auslösen". Da genügt es, ein großes und schwer wirkendes Paket in den Händen zu halten und die Wahrscheinlichkeit, die Tür aufgehalten zu bekommen, steigt (auch in einem eigentlichen gesicherten Bereich) signifikant. Bekannte Betrugsmaschen wie der sogenannte „CEO-Fraud", wo Mitarbeiter vom vermeintlichen Top-Manager des Unternehmens durch Autorität und Zeitdruck bewusst so unter Druck gesetzt werden, dass sie große Geldsummen ohne große Rückfragen freigeben, zeigen, wie gefährlich solche Manipulationstaktiken sind. Wie enorm das Schadenspotenzial solcher Taktiken ist, zeigen die Verluste, die Unternehmen aufgrund solcher Angriffe in den vergangenen Jahren verzeichneten. So kann davon ausgegangen werden, dass bereits 90 % der deutschen Unternehmen mindestens einmal von Datendiebstahl, Sabotage oder Spionage betroffen waren.

SCHÄDEN DURCH DATENDIEBSTAHL, SABOTAGE ODER SPIONAGE = MEHRERE MILLIARDEN EURO JÄHRLICH.

Es ist also durchaus berechtigt darüber nachzudenken, wie Unternehmen vor solchen Angriffen geschützt werden können. Genau an diesem Punkt kommt dann oft die zu Beginn gestellte Frage – wie Mitarbeitende davon abgehalten werden können, etwa aus unreflektierter Autoritätshörigkeit oder purer Höflichkeit Opfer eines solchen Angriffs zu werden.

Dabei ist nicht der Mensch an sich das Problem. Es ist vielmehr die Tatsache, dass diese Verhaltensweisen eben in den meisten Fällen unbewusst und unreflektiert ablaufen und ein „Ausbrechen" aus den gewohnten Mustern genauso wie das Melden solcher Vorfälle aufgrund einer negativen Fehlerkultur mit Scham und Angst vor Konsequenzen behaftet ist.

MIT WENIGEN ADAPTIONEN IM ARBEITSALLTAG KÖNNEN BEDEUTSAME (SICHERE) UNTERSCHIEDE ERZIELT WERDEN.

WIE HANDELN MITARBEITER IM SINNE DER INFORMATIONSSICHERHEIT?

AUTOMATISIERTE VERHALTENSWEISEN BEWUSSTMACHEN

Genau an dieser Stelle ist der Ansatzpunkt, solche Angriffe effektiv zu verhindern oder es den Angreifern zumindest so schwierig als möglich zu machen. Mitarbeiter müssen darin bestärkt werden, diese gewohnten und unreflektierten Verhaltensmuster abzulegen. Das geht nur, wenn Scham und Angst vor Konsequenzen abgebaut werden.

Die meisten Menschen kostet es zum Beispiel Überwindung, bei einer (scheinbaren) Autoritätsperson bei (vorgespieltem) Zeitdruck und trotz angedrohter Konsequenzen auf die Einhaltung der Sicherheitsbestimmungen zu bestehen. Es stellt sich also die Frage, wie den Mitarbeitenden dabei geholfen werden kann, aus diesen Automatismen auszubrechen, bewusst eine Handlung zu tätigen und Vorfälle im Anlassfall sofort zu melden.

Gemeint ist nicht, alle sozialen Normen, Umgangsformen und höfliches Handeln abzulegen. Es geht darum, dass sich Mitarbeiter ihre bisherigen automatisierten Handlungen bewusst und somit einer Reflexion zugänglich machen. Damit Mitarbeiter gewohnte Verhaltensweisen ablegen und durch bewusstes Handeln ersetzen, braucht es Rahmenbedingungen, die durch die Organisationsstruktur hergestellt werden können. ›››

1. NOTWENDIGE RESSOURCEN ZUR VERFÜGUNG STELLEN

Eine wichtige Voraussetzung ist, dass Mitarbeitern notwendige Ressourcen bereitgestellt werden, damit sie die von ihnen verlangten Maßnahmen auch umsetzen können. Gemeint sind zum einen Handlungsanleitungen und Policies, auf die sich Mitarbeiter berufen können und die ihnen Handlungssicherheit geben – auch entgegen gelernter sozialer Normen zu agieren. Mitarbeiter müssen darin bestärkt werden, auf Sicherheitsmaßnahmen zu bestehen und nicht etwa durch Führungskräfte dafür getadelt oder sogar bestraft werden. Zum anderen sind damit Ressourcen gemeint, die die Einhaltung von Sicherheitsmaßnahmen direkt unterstützen. So kann etwa das leidige Passwortthema schnell und sicher durch die Bereitstellung einer „Schlüsselbund-Applikation" gelöst werden.

2. FEHLERKULTUR UND VORFALLMANAGEMENT

Es braucht eine Atmosphäre, in der beinah oder tatsächlich erfolgte Angriffe niederschwellig gemeldet werden können. So können Schwachstellen zeitnah behoben und bei Angriffen schnell reagiert werden. Das bedeutet zum einen das Melden von (Sicherheits-) Vorfällen zu bestärken und zum anderen eine Meldestelle einzurichten, wo die Meldungen von einer sachkundigen Stelle, die den Vorfall bewerten kann, entgegengenommen werden. Ein anonymes Meldesystem oder ein Ombudsmann könnten erste Maßnahmen sein. Eine weitere Entwicklungsmöglichkeit wäre der interne oder sogar interorganisationale Austausch über (beinah) Angriffe im Sinne eines „Lessons Learned Prozesses".

3. BEDEUTSAMKEIT UND RELEVANZ DES HANDELNS WÜRDIGEN

Mitarbeiter müssen den Kontext und die Relevanz ihrer Handlungen für das Unternehmen verstehen und durch ihre Führungskraft als relevantes Element zum Schutz des Unternehmens verstanden, so behandelt und entsprechend wertgeschätzt werden.

> **„ES IST WEDER KOMPLIZIERT NOCH TEUER, AUS DEM „RISIKOFAKTOR MENSCH" EINE RESSOURCE FÜR DIE INFORMATIONSSICHERHEIT EINES UNTERNEHMENS ZU MACHEN.**

Wenn Mitarbeiter einen Sinn darin sehen, verdächtige Situationen bewusst wahrzunehmen, sie die Relevanz ihrer Rolle im Kampf gegen solche Angriffe vermittelt bekommen und dafür die notwendigen Rahmenbedingungen zur Verfügung haben, ist die Wahrscheinlichkeit signifikant höher, dass solch ein Angriff erfolglos bleibt oder zumindest gemeldet wird und somit schnell reagiert werden kann. Diese drei Elemente lassen sich im Arbeitsalltag schnell und kostengünstig umsetzen und haben dabei ein enormes Potenzial, die Informationen und damit den Erfolg des Unternehmens nachhaltig zu schützen.

Dieser Artikel ist mit freundlicher Unterstützung von Teresa Allum entstanden.