www.pwc.de/cybersecurity

Point of View

Kann Cyber Security glücklich machen?

Ein Gespräch über das Spannungsfeld zwischen Regulation und Autonomie mit der Glücksforscherin Maike van den Boom und dem Cyber-Security-Experten Jürgen Schulze, PwC Deutschland

pwc

”

I like to think that the ‘h’ in Cybersecurity stands for ‘happiness’.

Gene Spafford, Professor und führender Experte für Computersicherheit

“

Inhaltsverzeichnis

Einleitung 4

1 Glück und Cybersicherheit – ein Widerspruch? 5

2 Befähigen statt einschränken – menschenzentrierte Cyber Security 9

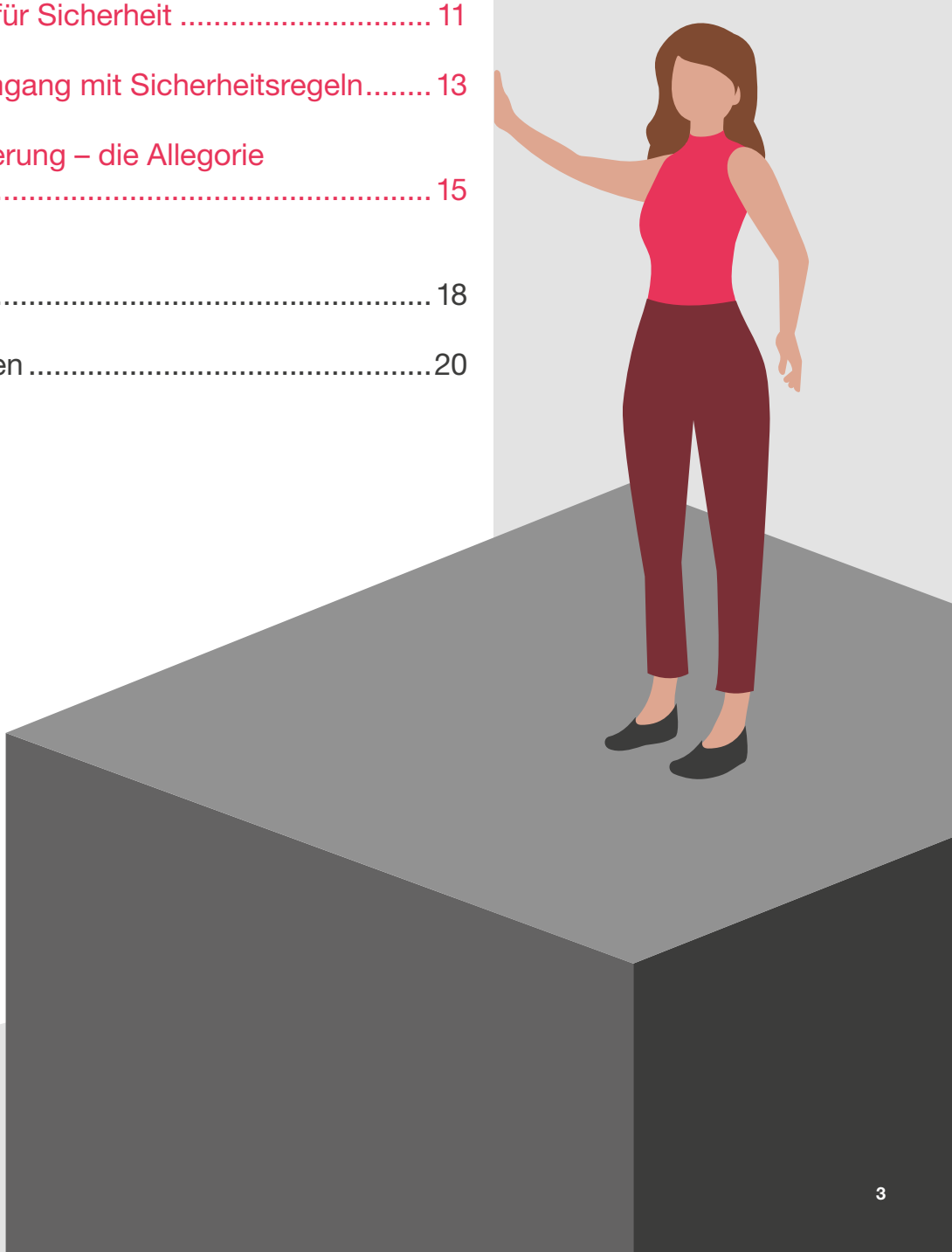
3 Sinn als Erfolgsfaktor für Sicherheit 11

4 Über den richtigen Umgang mit Sicherheitsregeln 13

5 Vertrauen und Absicherung – die Allegorie der Glaswand 15

Literaturverzeichnis 18

Ihre Ansprechpartner:innen 20

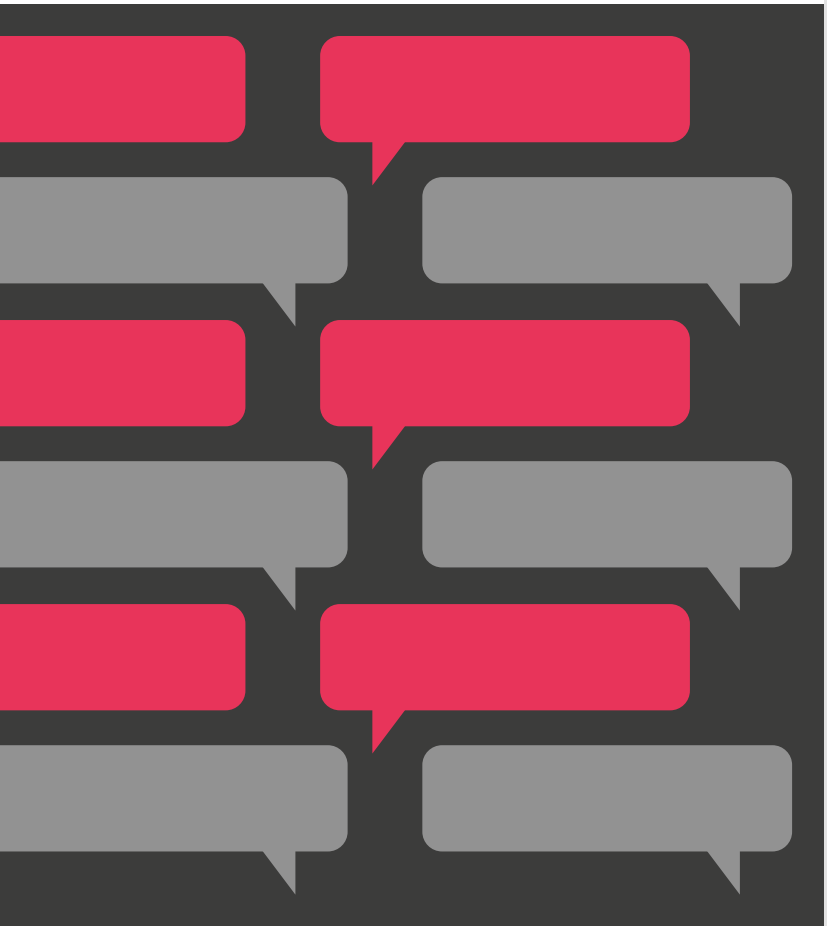


Einleitung

Erfolgreiche Unternehmen brauchen heutzutage beides: Sicherheit und Glück. Dabei geht es im Folgenden nicht um das Glück im Sinne eines glücklichen Händchens, sondern um das Glücklichsein jeder einzelnen Person. Glückliche Mitarbeiter:innen sind eine wichtige Basis für Innovation und damit ein langfristiger Wettbewerbsvorteil. Cyber Security sorgt hingegen für das digitale Überleben des Unternehmens in Anbetracht von Bedrohungen – zum Beispiel durch den fahrlässigen Umgang mit unternehmenswichtigen Daten, Internetkriminalität, Erpressung oder Sabotage.

Glück und Cybersicherheit sichern das Fortbestehen des Unternehmens, unterliegen aber unterschiedlichen Ansprüchen. Cyber Security verlangt nach Regulierung und Beschränkung. Gleichzeitig gehört Überregulierung laut des diesjährigen CEO Survey von PwC zu den größten Sorgen der CEOs in Deutschland.

Glückliche Mitarbeiter:innen wollen Freiheit und Autonomie. Glücksexpertin Maike van den Boom und Cybersicherheitsexperte Jürgen Schulze wagen den Schulterschluss und gehen diesem scheinbaren Widerspruch in einem Gespräch auf den Grund. Sie erklären mit einem Seitenblick auf Skandinavien, wie sich Cybersicherheit und der Umgang damit auf Jobzufriedenheit und letztendlich auf den Erfolg des gesamten Unternehmens auswirken können.



Glücksforscherin trifft Cyber-Security-Experten

Maike van den Boom

Maike van den Boom ist Bestsellerautorin und eine der bekanntesten Glücksforscher:innen Deutschlands. Sie hilft deutschen Unternehmen bei ihren Transformationsprozessen nach dem Vorbild der hoch digitalisierten und innovativen Skandinavier:innen. Maike van den Boom gibt dabei Impulse durch Keynotes und Workshops und begleitet Unternehmen langfristig als Sparringspartnerin. Nachdem sie in Deutschland, den Niederlanden und Mexiko gelebt hat, wohnt sie seit 2018 in Stockholm. Ihr Ziel ist es, dem Glück der Deutschen auf die Sprünge zu helfen – individuell, im Job und als Gesellschaft. Ihr jüngstes Buch heißt „Acht Stunden mehr Glück – Warum die Menschen in Skandinavien glücklicher arbeiten und was wir von ihnen lernen können“ (Fischer 2018, https://maikevandenboom.de/buchautorin/).

Jürgen Schulze

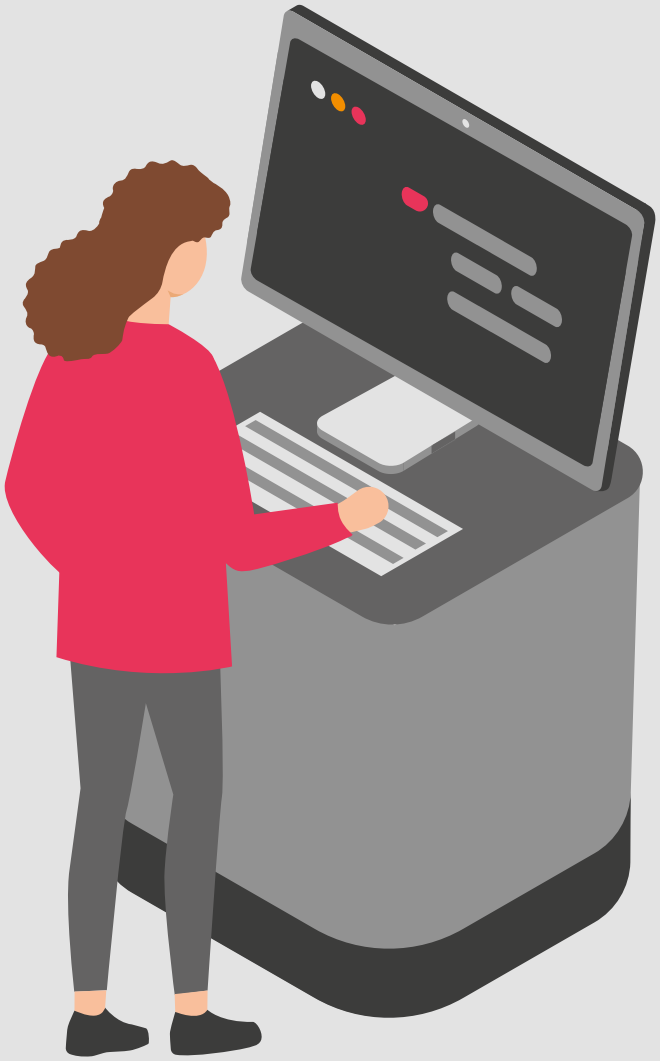
Jürgen Schulze ist Experte für Cybersicherheit bei PwC Deutschland im Bereich Cyber Security & Privacy. Er startete Anfang der 80er-Jahre als Fachbuchautor und arbeitet seit 38 Jahren in verschiedenen nationalen und internationalen Managementpositionen in der IT-Industrie; seit 20 Jahren vornehmlich im Bereich Informationssicherheit, unter anderem auch mithilfe künstlicher Intelligenz. Vor seiner Zeit bei PwC Deutschland nutzte er eine zweijährige Auszeit, um für sein derzeit im Endspurt befindliches Buchprojekt zu recherchieren (https://coterminus.com).

1 Glück und Cybersicherheit – ein Widerspruch?

Warum sind sowohl Cybersicherheit als auch Glück – verstanden als das Glücklichsein des:der Einzelnen – für Unternehmen so wichtig? Wie hängen beide zusammen? Warum ist der Mensch für Cyber Security so ein wichtiger Faktor?

Jürgen: Cybersicherheit und Glück in einem Atemzug zu nennen, mag auf den ersten Blick abwegig erscheinen und entspricht nicht den gängigen Sichtweisen. Und doch kommt dem Menschen in der Cybersicherheit eine besondere Rolle zu. Je nach Quelle stützen sich zwischen 60 und 98 Prozent aller Cyberattacken auf Social Engineering – auf zwischenmenschliche Manipulation. So geht es bei der Cybersicherheit darum, die digitale Infrastruktur sowie alle Mitarbeiter:innen bestmöglich abzusichern, das Unternehmen vor externen und internen digitalen Bedrohungen zu schützen und damit sicherzustellen, dass die Wertschöpfung unterbrechungsfrei läuft und die Marke ein vertrauensvolles Ansehen genießt. Wie es den Mitarbeiter:innen dabei geht, spielt jedoch bisher kaum eine Rolle. Warum sollten sich Unternehmen bei der Cybersicherheit auch mit dem Thema Glück befassen, Maike?

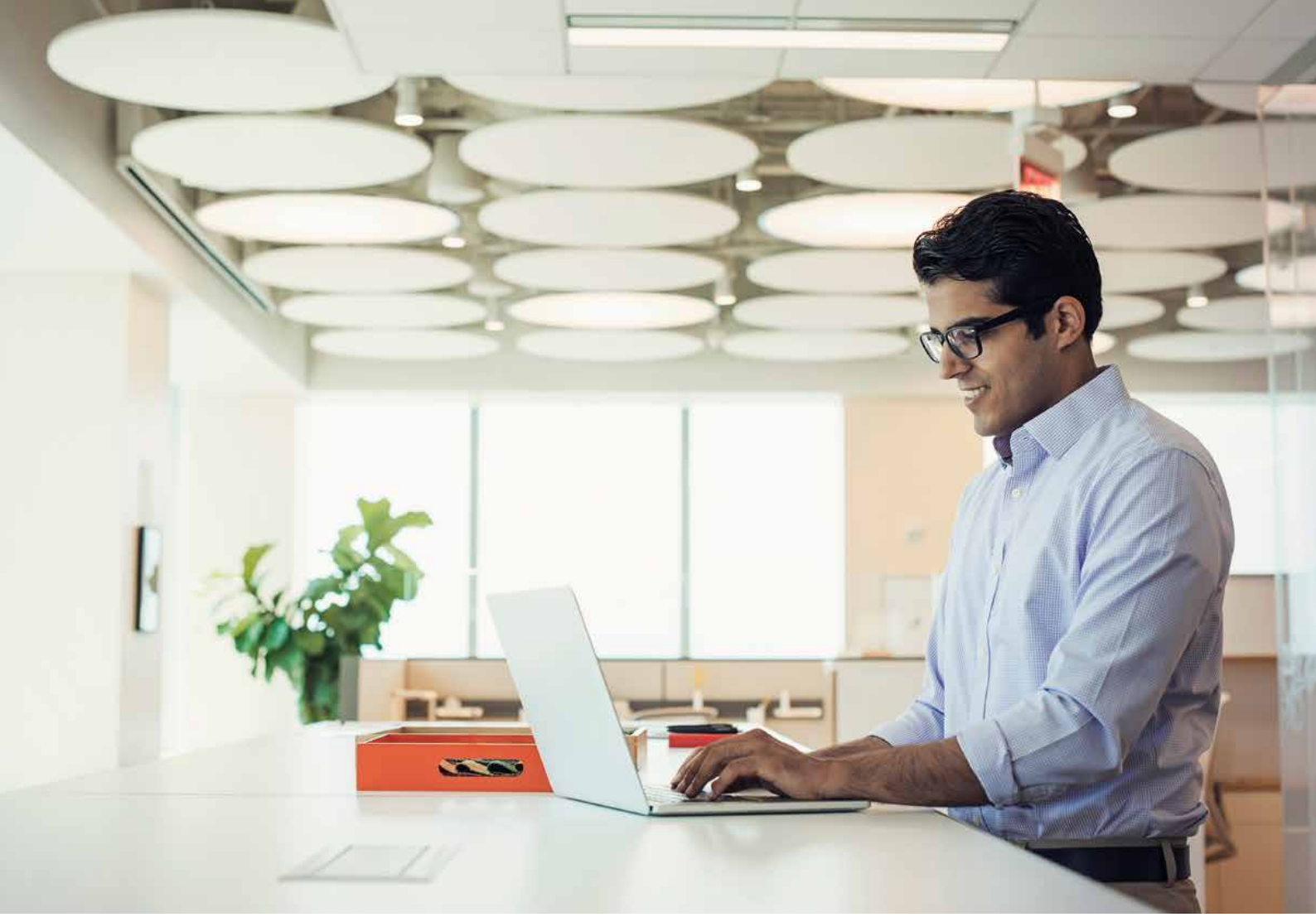
Maike: Mitarbeiter:innen, die sich wohlfühlen und in ihrem Job glücklich sind, sind engagierter, kreativer und produktiver und steigern so auch die Innovationskraft des Unternehmens – bzw. die Effektivität der Cybersicherheit. Denn glückliche Menschen sind Neuem gegenüber aufgeschlossen und trauen sich mehr. Sie denken mit und sind dadurch zum Beispiel weniger anfällig für Betrugsmaschen. Sie arbeiten darüber hinaus besser zusammen und fühlen sich ihrem Arbeitgeber loyal verbunden. All diese Vorteile des Glücklichseins sind hinreichend empirisch belegt, auch wenn sie auf den ersten Blick vage scheinen und in der Praxis schwer mess- und vergleichbar sind.



Erfolgreiches Unternehmertum braucht ein geschütztes Umfeld

„Sicherheit ist ein Grundbedürfnis des Menschen, das im limbischen System verankert ist. Die Sicherheit kann bedroht sein oder geschützt. Auf Bedrohung reagiert der Mensch mit Flucht, blindem Angriff oder Starre; nur in einem geschützten Umfeld, das Sicherheit gewährleistet, ist daher erfolgreiches autonomes und wertschöpfendes Unternehmertum denkbar. In einer Welt, die sich mit zunehmendem Tempo digitalisiert, ist Cyber Security eine Grundbedingung für Fortschritt, Wohlstand, Sinnstiftung und Freude.“

Felix von der Planitz, PwC (RA, StB, People Caretaker und Glückssucher)



Jürgen: Die Auswirkungen der Versäumnisse im Bereich Cybersicherheit zeigen sich üblicherweise sehr schnell und sehr deutlich. Sie sind in den wirtschaftlichen Folgen auch leichter messbar. Man denke hier zum Beispiel an einen Produktionsausfall durch verschlüsselte Daten infolge eines Ransomware-Angriffs. In ihrer unmittelbaren Wirkung erweisen sie sich allerdings als sehr viel schmerzvoller. Ganz besonders in der letzten Eskalationsstufe durch eine Meldung bei der Bundesanstalt für Finanzdienstleistung (BaFin) oder der Bundesnetzagentur, bei anderen Regulierungsbehörden oder in den Medien. Auch Produktivität lässt sich zumindest metrisch gut messen und je nach Verlaufskurve kann man auch taktisch gut eingreifen, wenn die unmittelbaren Ursachen bekannt sind.

Maike: Bei Kreativität und Innovationskraft sieht das etwas anders aus. Hier kündigt sich das Unheil langsamer und leiser an – oder gar nicht. Klassischen Messgrößen fehlt hier die Aussagekraft und die Spätfolgen der Unterschätzung dieser Erfolgsfaktoren lassen sich im Ereignisfall schlecht bis gar nicht auf ihren Ursprung zurückführen.

Jürgen: Und doch scheint Glück für eine erfolgreiche Digitalisierung und in der Folge für Cyber Security eine sehr wichtige Rolle zu spielen. So sehen die Autor:innen der OECD-Studie *How's Life in the Digital Age?* neben dem Risiko von Cyber-Security-Verletzungen in digitalen Technologien auch ein großes Ungleichheitsrisiko für die Gesellschaft aufgrund einer digitalen Kluft. Hier geht es sowohl um digitale Fertigkeiten als auch um emotionale und soziale Fähigkeiten, die mit der sicheren Navigation in der Onlinewelt verbunden sind. Der souveräne Umgang mit digitalen Hilfsmitteln hat offenbar messbar einen Einfluss auf das Wohlbefinden und damit auch auf das individuelle Glück der Arbeitnehmer:innen, vor allem im Bereich der digitalen Sicherheit. Kurz gesagt: Damit die Digitalisierung zum Wohle der Menschen funktioniert, müssten laut der Studie gleiche digitale Chancen, eine weit verbreitete digitale Kompetenz und eine starke digitale Sicherheit aufgebaut werden.

Maike: Genau so denkt und lebt man dies zum Beispiel bei unseren nordischen Nachbar:innen. In einem Interview sagte mir Peter Karlberg aus der staatlichen Agentur Skolverket, die das schwedische Schulministerium berät: „Nur wenn die Kinder digitale Kompetenz erwerben, können sie für ihr Leben Verantwortung übernehmen und einen sinnvollen Beitrag für die Gesellschaft leisten. Wenn sie nicht lernen, dass man Codes schreiben und Filme manipulieren kann und dass nicht alles stimmt, was im Netz steht, werden sie Opfer der Welt." Bereits seit 2006 setzt Schweden darauf, schon die digitale Kompetenz der Kleinsten in der Schule zu stärken. So werden sie seitdem mit Endgeräten wie Laptops und Tablets ausgerüstet.

Jürgen: Digitale Kompetenz halte ich auch im Kontext der Cyber Security für enorm wichtig. Es ist ja so: Jede neue Errungenschaft – auch und gerade jede digitale Neuerung – macht unser Leben erst mal komplizierter. Und zwar so lange, bis der Verstand die Hürden genommen hat, um zu erkennen, dass bestimmte Maßnahmen sinnvoll sind. Einige wenige sehen darin eine sportliche Herausforderung. Die meisten anderen sehen eher den schmerzvollen Prozess des Lernens, der Umgewöhnung, der Schulung, der Umstrukturierung, Korrektur und Nachbesserung, bis alles so läuft, wie erhofft und erwartet.

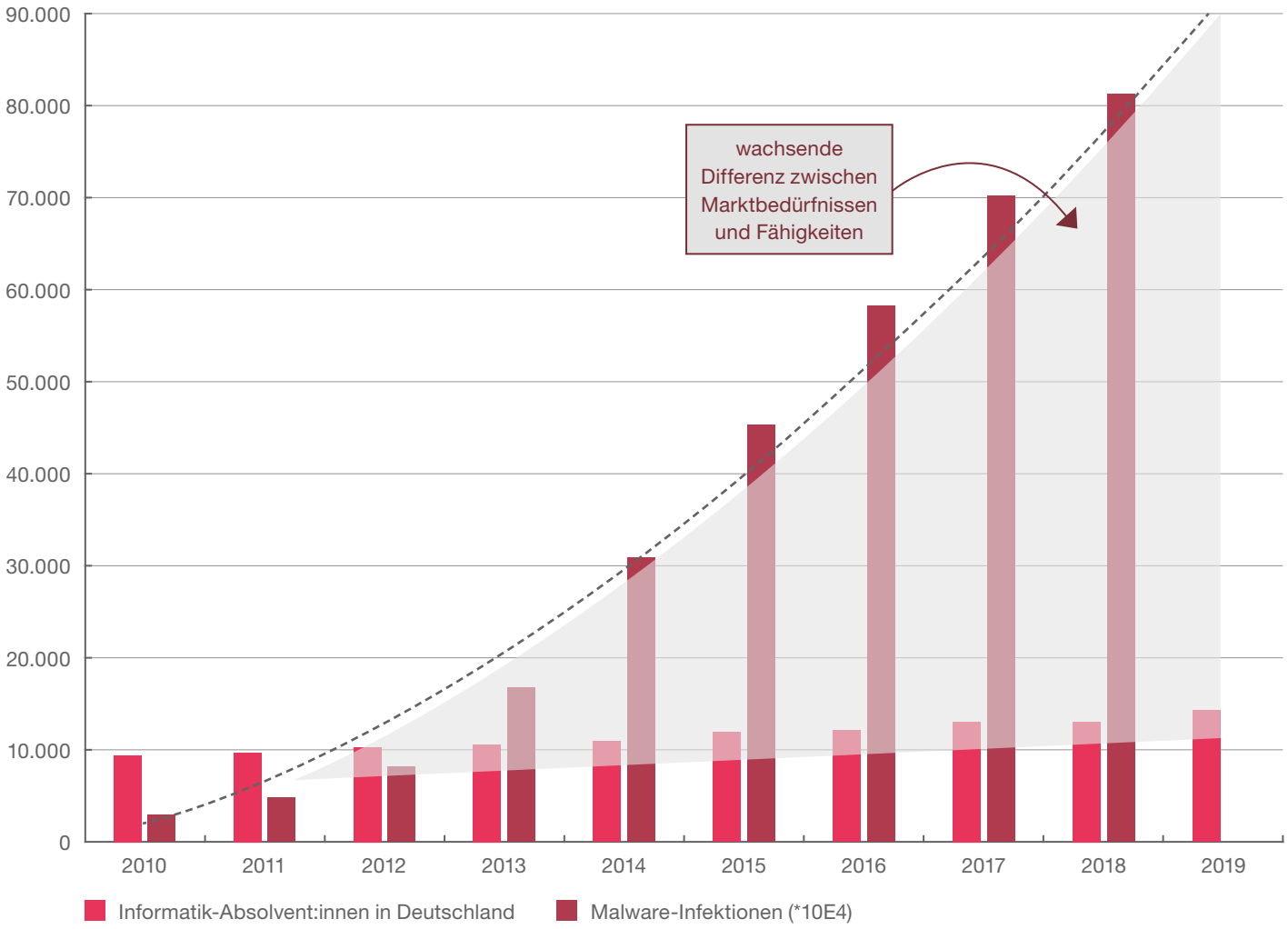
Aktuell sieht es manchmal so aus, als ob menschliche Fertigkeiten der digitalen Revolution hinterherhinken. Das gilt nicht nur für den Umgang mit neuen Technologien, sondern fängt schon beim Grundverständnis an. Etwas nicht zu können, was andere können, ist schon schlimm genug. Wenn Menschen jedoch das Gefühl haben, etwas Grundlegendes nicht mehr zu begreifen, dann fühlen sie sich unbehaglich und bedroht. Ihre Unkenntnis versuchen sie zu verstecken, ihre persönliche Integrität zu gewährleisten. Die Erkenntnis, nicht geschützt zu sein, oder die Unwissenheit darüber, ob man geschützt ist, kann sich negativ auf die Gemütslage der Betroffenen auswirken.

Maike: Was bedeutet das aus Sicht der Cyber Security für die Bedrohungslage?

Jürgen: Man könnte den Eindruck gewinnen, dass das Böse dem Guten im Moment mit nahezu quadratisch wachsender Geschwindigkeit davonläuft – zumindest, wenn man die Anzahl der IT-Fachkräfte im Verhältnis zu der rasant steigenden Bedrohungslage betrachtet. Wenn man noch berücksichtigt, dass sich digitale Bedrohungen nicht nur im Internet, sondern sehr gern auch zum Beispiel in Produktionsstraßen, in der Messtechnik und in ähnlichen unspektakulär analogen Bereichen tummeln, wird schnell das ganze Ausmaß des Dilemmas deutlich.

Maike: Da gilt es, einen kühlen Kopf zu behalten! Und das zeigt, wie wichtig es ist, nicht nur auf die Expert:innen zu blicken – sondern eben auch auf die digitale Kompetenz und das Wohlbefinden der gesamten Belegschaft.

Abb. 1 Eine beängstigende Korrelation? Es läuft auseinander, was zusammengehört.



Quellen: Statistisches Bundesamt, Statista

Takeaways

- Glückliche Mitarbeiter:innen sind engagierter, kreativer, produktiver und innovativer.
- Versäumnisse im Bereich der Cyber Security sind in den wirtschaftlichen Folgen leicht messbar. Bei Kreativität und Innovationskraft versagen klassische Messgrößen. Negative Effekte zeigen sich schleichender.
- Digitale Kompetenz ist eine der wichtigsten Voraussetzungen für das individuelle Glück in einer zunehmend digitalisierten Welt.
- Nicht geschützt zu sein oder nicht zu wissen, ob man vor Cyberattacken geschützt ist, wirkt sich negativ auf die Gemütslage und damit schlussendlich auch auf die Produktivität aus.

2 Befähigen statt einschränken – menschenzentrierte Cyber Security

Wie kann der Mensch in die Cyber Security miteinbezogen werden? Welche unterschiedlichen Ansätze sind dafür verbreitet? Wie kann das Denken in den nordischen Ländern dabei helfen?

Maike: In welchem Verhältnis steht Cyber Security denn üblicherweise zu den Mitarbeiter:innen?

Jürgen: Die Aufgabe von Cyber Security im herkömmlichen überholten, aber immer noch gern gepflegten Sinne liegt darin, alles zu verhindern, was der Organisation ein Problem bereiten könnte. In der modernen Auffassung von Cyber Security sollte sie Mitarbeiter:innen in die Lage versetzen, ihr geistiges und kreatives Potenzial möglichst ohne Einschränkung unter bestmöglicher Nutzung der zur Verfügung stehenden Hilfsmittel zu entfalten. Der perfekte Ansatz aus Sicht der Mitarbeiter:innen wäre demnach, dass Cybersicherheit befähigt und nicht einschränkt.

Maike: Gibt es in der Praxis schon Ansätze für so eine Befähigung?

Jürgen: Mitarbeiter:innen sollten den Sicherheitsmechanismen und den Technologien dahinter vertrauen können. Sie sollten jedoch auch die psychologische Sicherheit empfinden können, dass ihr Unternehmen ihnen vertraut und ihnen der Umgang mit sensiblen Daten sowie sensibler digitaler Infrastruktur zugetraut wird. Das wirkt nicht immer so. Nehmen wir zum Beispiel Verschwiegenheitserklärungen, die üblicherweise ein integraler Bestandteil eines Arbeitsvertrags sind. Dies gilt auch für den Verweis auf die IT-Sicherheitsrichtlinien des Arbeitgebers. Diese sind in der Regel eine Kombination aus Anweisungen für den Umgang mit der unternehmenseigenen IT und in Aussicht gestellten Sanktionen für persönliche Fehler im Umgang damit.

Maike: Gegenseitiges Vertrauen sollte also an die Stelle von Sanktionen treten!

Jürgen: Richtig. Ansonsten können Mitarbeiter:innen schnell das Gefühl entwickeln, in erster Linie ein enormes Risiko für die digitalen Kronjuwelen zu sein, was ihnen dann in regelmäßigen Belehrungen immer wieder bestätigt wird. Mitarbeiter:innen, die ständig in der gefühlten Gefahr leben, nicht gut genug fürs Digitale ausgebildet zu sein und möglicherweise teure und sogar die Karriere beendende Fehler bei der Bedienung ihrer digitalen Werkzeuge zu machen, werden ihr Potenzial nicht ausschöpfen und sich selbst in ihrer Kreativität limitieren.

Maike: Wie nimmt man den Menschen die Angst und gewährleistet trotzdem die Sicherheit im Unternehmen?

Jürgen: Im Normalfall wird die Sicherheit über Regeln und die daraus resultierenden technischen Lösungen, Prozesse und Vorschriften für regelkonformes Verhalten forciert. Üblicherweise sind wir Cyber-Security-Expert:innen das, was man im angloamerikanischen Raum gemeinhin als „party poopers“ bezeichnet: Spaßbremsen, Neinsager:innen, Bedenkenträger:innen und Angstmacher:innen, die man besser nicht fragt, wenn man seine Arbeit schnell und unkompliziert erledigen möchte. Wie es auch anders geht, zeigt das Beispiel von Thomas Tschersich, Chief Security Officer (CSO) der Deutschen Telekom: Bei ihm und seinem Team wird jedem geholfen, der zur Umsetzung eines Projekts Fragen hat, die die Konzernsicherheit betreffen könnten. Mitarbeiter:innen werden in die Lage versetzt, etwas zu tun, was sie ohne Hilfe möglicherweise nicht oder nur außerhalb gewisser Richtlinien hätten tun können. Dazu gibt es entsprechende Anleitungen und Hintergrundinformationen.

Maike: Das ist eine andere Philosophie, eher ein Servicegedanke.

Jürgen: Ganz genau. Es steht nicht der Versuch im Vordergrund, Gründe gegen ein Projekt zu finden und damit wertvolle Energien und gute Laune zu verbrennen. Mitarbeiter:innen sind dann zufriedener oder – um es mit deinen Worten zu formulieren – glücklicher, denn sie dürfen auch mal einen Fehler machen, da dieser über Technologie aufgefangen wird. Zum anderen spüren sie, dass ihren Fähigkeiten im Umgang mit ihren digitalen Werkzeugen und den entsprechenden Prozessen vertraut wird. Sie trauen sich dann auch mehr, was der Innovationskraft des Unternehmens zugutekommt. Die Security-Abteilung mutiert also vom Bedenkenträger zum Enabler. Da spielt Vertrauen eine wichtige Rolle.

Maike: Allerdings. Vertrauen ist generell die Basis für den Erfolg eines Unternehmens. Denn erst mit dieser psychologischen Sicherheit im Rücken ist das sogenannte Empowerment, das eigenständige und autonome Handeln der Mitarbeiter:innen, möglich. Und allen Bedenkenträger:innen darf ich bereits auf den Weg geben, dass Studien ergeben haben, dass sich Menschen, denen Vertrauen geschenkt wird, auch vertrauenswürdiger verhalten. Und die mit Zutrauen einhergehende Handlungs- und Gedankenfreiheit ist ein integraler Teil des Glücksempfindens, das zum Beispiel das hohe Glücksniveau der Einwohner:innen der nordischen Länder erklärt.

Jürgen: Was macht die nordischen Länder denn so besonders?

Maike: Sie sind laut dem World Values Survey die emanzipiertesten Länder der Welt. Freiheit und eigenständiges Denken werden hier schon „in die Kinderseelen eingeschrieben“. Jedoch auch das Bewusstsein, dass wir niemals frei sind, wenn wir nicht bereit sind, auch die Verantwortung für unser Tun zu übernehmen. Das Konzept heißt „frihet under ansvar“, Freiheit unter Verantwortung. Und wenn mir wirklich etwas an dir liegt, dann ermutige ich dich nicht nur, deine Freiheit zu nutzen und einen beherzten Sprung zu tun, sondern lege netterweise eine Matratze hin, damit du dir nicht alle Knochen brichst, wenn du wider Erwarten nicht auf beiden Füßen landest.

Jürgen: Wie ließe sich dieses Verständnis auf die Cyber Security übertragen?

Maike: Man könnte Cyber Security so gesehen als einen Ausdruck der Fürsorge für die Belegschaft verstehen. Der scheinbare Widerspruch – ich regle und reguliere das für dich – durchzieht das gesamte Denken in den nordischen Ländern: So sind eine Menge Dinge zentral vom Staat geregelt, die Erinnerung an den TÜV, gratis Mittagessen in der Schule und Laptops für alle Schüler:innen ab der 10. Klasse. „Der Staat ist stark, um das Individuum stark und unabhängig zu halten – davon sind die meisten Schwed:innen überzeugt. Den Einzelnen wird etwas an Last genommen.“ So hatte es zumindest der damalige ARD-Skandinavienkorrespondent Tilmann Bünz im Interview mit mir erklärt. Und ich habe lange gebraucht, um es richtig zu verstehen.

Takeaways

- Der weitverbreitete Ansatz der Cyber Security wird mit Verhinderung und Einschränkung sowie Kontrollen und Sanktionen verbunden.
- Eine moderne Auffassung von Cyber Security basiert auf einem vertrauensvollen Verhältnis zu den Mitarbeiter:innen. Sie setzt auf Befähigung und Offenheit.
- Das Denken in den nordischen Ländern folgt dem Prinzip „Freiheit unter Verantwortung“ und steht der modernen Auffassung von Cyber Security sehr nahe.
- Gegenseitiges Vertrauen ist der Schlüssel: Mitarbeiter:innen sollten den Sicherheitsmechanismen und Technologien vertrauen. Unternehmen sollten das eigenständige Handeln der Mitarbeiter:innen durch Vertrauen stärken.

3 Sinn als Erfolgsfaktor für Sicherheit

Was gilt es bei der Kommunikation von Sicherheitsthemen zu beachten? Wie entstehen Widerstände der Belegschaft und wie lassen sie sich auflösen? Wie sieht eine vertrauensvolle Unternehmenskultur im Kontext der Cyber Security aus?

Jürgen: Ende der 90er-Jahre wurde klar, dass es durch den Datumswechsel von 99 auf 00 technische Herausforderungen geben würde. Regierungen von Ländern wie Schweden, Norwegen, Dänemark, Finnland und Belgien nutzten die Gunst der Stunde, um ihre Bürger:innen mit neuen Computern auszustatten. Bezahlt vom Arbeitgeber und verbunden mit verlockenden Steuervergünstigungen im Rahmen eines landesweiten Ausbildungsprogramms. Man kann ein Problem also auch als Herausforderung betrachten oder gar als Chance nutzen. Ist diese Denkweise der Grund dafür, dass Digitalisierung dort beispielsweise überwiegend positiv wahrgenommen wird?

Maike: Der Ton und die Absicht motivieren oder bremsen. Es ist wichtig, sich darüber im Klaren zu sein, dass die Art, wie Sicherheitsthemen kommuniziert werden – in unserem Beispiel Cybersicherheit –, die Kultur eines Unternehmens beeinflusst. Man sollte also nicht immer nur über Gefahren reden, sondern Erfolgsgeschichten der Cyber Security feiern. Wenn Regulierungen nicht im positiven Kontext dargeboten werden, wird Digitalisierung als Gefahr wahrgenommen und nicht als Chance, unser aller Leben zu verbessern. Die mit ihr verbundene Cyber Security wird als Kontrollmittel erfahren und nicht als Mittel, Freiheit zu ermöglichen. Sie ist Druckmittel, nicht Ausdruck des Schützenwollens. Das verunsichert die Mitarbeiter:innen, verletzt sie in ihrem Stolz, als potenziell nicht selbst denkende, vertrauenswürdige Menschen wahrgenommen zu werden. Das Resultat ist ganz logisch: Widerstand und schlechte Laune. Genau das Gegenteil von dem, was wir uns eigentlich wünschen.

Jürgen: Wie äußert sich so ein Widerstand? Und wie kann vermieden werden, dass es zu Widerständen kommt?

Maike: Es hat nachhaltigen Einfluss auf den Zusammenhalt im Team, die Arbeitsfreude und die Produktivität. Studien dazu weisen immer wieder darauf hin, dass positive Emotionen einen Einfluss auf die Variablen haben, die für den Erfolg im Job und Unternehmen maßgeblich sind: Kreativität, Engagement im Job, positive Bewältigungsstrategien, Gesundheit, Teamwork und Zusammenarbeit, Zufriedenheit der Kund:innen, Führung und Leistung.

Menschen wollen verstehen, warum etwas getan wurde, vielleicht nicht im kleinsten Detail, aber die Intention muss klar sein. Der Erfolg einer Cyber-Security-Strategie hängt in hohem Maße vom Commitment der Menschen ab. Es macht Menschen unzufrieden, wenn sie sich an Dinge halten müssen, die für sie keinen Sinn ergeben. Was dann erblüht, ist die Renaissance der Widerwilligkeit. In der Psychologie nennt man das „Reaktanz“. Sanktionen, die als zu übergriffig und als nicht nachvollziehbar erfahren werden, können früher oder später auf Widerstand stoßen. Sie werden dann mehr oder weniger offensichtlich boykottiert. Unerwünschtes Verhalten kann sogar verstärkt werden. Menschen sind sehr kreativ, wenn sie sauer sind.

Jürgen: Regeln zu umgehen oder zu boykottieren ist für die Cybersicherheit sehr problematisch. Eine Führungskraft, die ich mal auf das Thema Glück ansprach, sagte mir: „Bei der Arbeit sollen die Leute abliefern. Glücklich sein können sie gern zu Hause!“ … Bei dieser Einstellung ist der Widerstand ja regelrecht vorprogrammiert. Das ist Gift für die Cyber Security.

Maike: So ist es. Im Umkehrschluss ist eines der wichtigsten Sicherheitselemente in Sachen Cyber Security nicht die Regulierung selbst, sondern das Verständnis, das durch intensiven Dialog mit den Menschen entsteht. Die Belegschaft muss fühlen, dass sie mit all ihren laienhaften Zweifeln und ihrer für Security-Expert:innen vielleicht unbegründeten Skepsis gesehen und ernst genommen werden. Jede:r im Unternehmen muss Regeln infrage stellen können, sich an ihnen reiben können und zwar öffentlich, am besten im Intranet oder auf anderen digitalen Kollaborationsplattformen im offenen Dialog. Denn die beste Rückversicherung sind immer noch die Menschen selbst, wenn man sie involviert und einlädt, Verantwortung zu übernehmen und selbst zu denken. Dazu gehört gern auch, Regeln lösungsorientiert infrage zu stellen. Und dann macht Cyber Security auch nicht unglücklich – im Gegenteil, sie kann ein Werkzeug sein, den Mitarbeiter:innen Respekt und Wertschätzung zu zeigen, indem man sie bei einem so wichtigen Thema involviert. Gerade, wenn die Wichtigkeit des Themas dort noch nicht angemessen angekommen ist.

Jürgen: Unternehmen sollten also die Zweifel ihrer Belegschaft ernst nehmen, wenn sie wirkliches Commitment und Engagement der Menschen erreichen möchten?

Maike: Alles andere wäre betriebswirtschaftlich fahrlässig. Und auch aus Sicht der Glücksforschung plädiere ich für diesen Ansatz, weil Menschen genau dann glücklich sind, wenn sich ihnen der Sinn ihres Tuns erschließt. Und diesen Sinn mit Informationen und – nicht zu vergessen – mit Spaß zu liefern, ist die Aufgabe der Menschen, die im Unternehmen mit Cyber Security betraut sind. Wegen der sich ständig ändernden Sicherheitserfordernisse ist Cybersicherheit im Prinzip nichts anderes als eine Transformation, die wir in Unternehmen täglich sehen. Zumindest sollte das so sein. Jede Veränderung ist zum Scheitern verurteilt, wenn man die Menschen nicht mit ins Boot holt. Und schaut man sich jetzt die nordischen Länder an, sind diese wahre Involvierungskünstler. Transparenz, Wissen zu teilen und außerhalb der Silos zu denken, ist dort Teil der Unternehmens-DNA. Cyber Security ist ein strategischer, unternehmensübergreifender Prozess und nicht ein Tool, das angewendet wird. Ohne das Einbeziehen der Mitarbeiter:innen werden tiefgreifende Veränderungen einer bestehenden Cyber-Security-Philosophie nicht funktionieren. Deshalb ist es ratsam, alle Phasen eines Veränderungsprozesses zu durchlaufen, angefangen beim Ernstnehmen der Ängste durch Aufmerksamkeit. Über aktives und gemeinsames Gestalten, um den Sinn der Maßnahmen zu verstehen und gegenseitiges Vertrauen aufzubauen. Um dann eine gute Basis zu haben, wenn die Mitarbeiter:innen in der Implementationsphase auch die negativen Folgen zu spüren bekommen. Danke sagen und Wertschätzen nicht vergessen.

Jürgen: Das klingt nach einer Menge Miteinanderreden!

Maike: Genau! Das wäre mein Rat: Man muss Cyber Security zum lebendigen Gesprächsthema im Unternehmen machen und der Belegschaft helfen, den Sinn dahinter zu verstehen, und Rückfragen zu und Kritik an den Regulierungen dankbar annehmen. Sie sind ein Zeichen der Teilhabe. So entsteht die Möglichkeit, mit den Mitarbeiter:innen in einen lebhaften Dialog zu treten. Wenn sich Unternehmensleiter:innen jetzt genervt überlegen „Wie lange das wohl wieder dauert? Dazu haben wir keine Zeit!“, haben sie vermutlich recht. Sie investieren Zeit. Investieren! Um später ein Mehrfaches an Zeit zu gegebener Zeit und an anderer Stelle zurückzugewinnen. Durch Mitarbeiter:innen, die motiviert sind, weil sie sich gesehen und einbezogen fühlen, als Folge davon selbstständig denken und Verantwortung übernehmen. Das spart Zeit und sorgt für positive Energie. Auf diese Art können Unternehmen Vertrauen aufbauen und trotzdem Regulierungen einführen, die Risiken minimieren.

Takeaways

- Kontroll- und Druckmittel verunsichern Mitarbeiter:innen und erzeugen Widerstände.
- Der Erfolg einer Cyberstrategie hängt vom Commitment der Menschen ab.
- Menschen sind dann glücklich, wenn sich ihnen der Sinn ihres Tuns erschließt. Ein offener Dialog trägt dazu bei, den Sinn von Sicherheitsmaßnahmen zu vermitteln.
- Die Art der Kommunikation ist entscheidend. Cyber Security sollte nicht nur als Kontrollmittel positioniert werden – sondern auch als Mittel, um Freiheit zu schaffen.

4 Über den richtigen Umgang mit Sicherheitsregeln

Wie lassen sich Sicherheitsregeln auf ein angemessenes Maß reduzieren? Welche Rolle spielen regulatorische Vorgaben? Wie ist der Zusammenhang zwischen Regelwerk und Technik?

Jürgen: Wir sind jetzt schon mehrfach auf die Themen Vertrauen und Verantwortung gestoßen. Sind skandinavische Unternehmen in dieser Hinsicht weiter?

Maike: Nach skandinavischer Denke sind Vertrauen und Verantwortung die beste Rückversicherung. Auch wenn die skandinavischen Musterschüler:innen nerven, kann man richtig gut bei ihnen abgucken: Sie sind über alle Hierarchien hinweg persönlich ansprechbar, was den Wissenstransfer im gesamten Unternehmen fördert. Das beeinflusst die Haltung der Menschen gegenüber der Digitalisierung. Bei der Arbeit an meinem zweiten Buch sah ich das immer wieder in skandinavischen Unternehmen, wo die Menschen jeder Form von Digitalisierung oder Automatisierung extrem offen, ja schon beinahe mit freudiger Erwartung entgegensehen. Das Gefühl, ernst genommen zu werden und wichtig zu sein, ist der Grund, weshalb Menschen gern arbeiten: Sie kennen nicht nur den Sinn der Maßnahmen, sondern erkennen auch ihre eigene Bedeutung für das Ganze. Gerade deshalb binden sich begehrte Mitarbeiter:innen dauerhaft an ein Unternehmen und vertreten die Marke positiv nach außen.

> Cyber Security muss ein integraler Teil der Digitalisierungsstrategie eines Unternehmens sein. Da Digitalisierung nur dann funktioniert, wenn sie auf der Kultur des Unternehmens und dessen Wertesystems fußt, wird Cyber Security damit automatisch zum Teil der idealerweise als positiv empfundenen Firmenkultur.
>
> Felix von der Planitz, PwC (RA, StB, People Caretaker und Glückssucher)

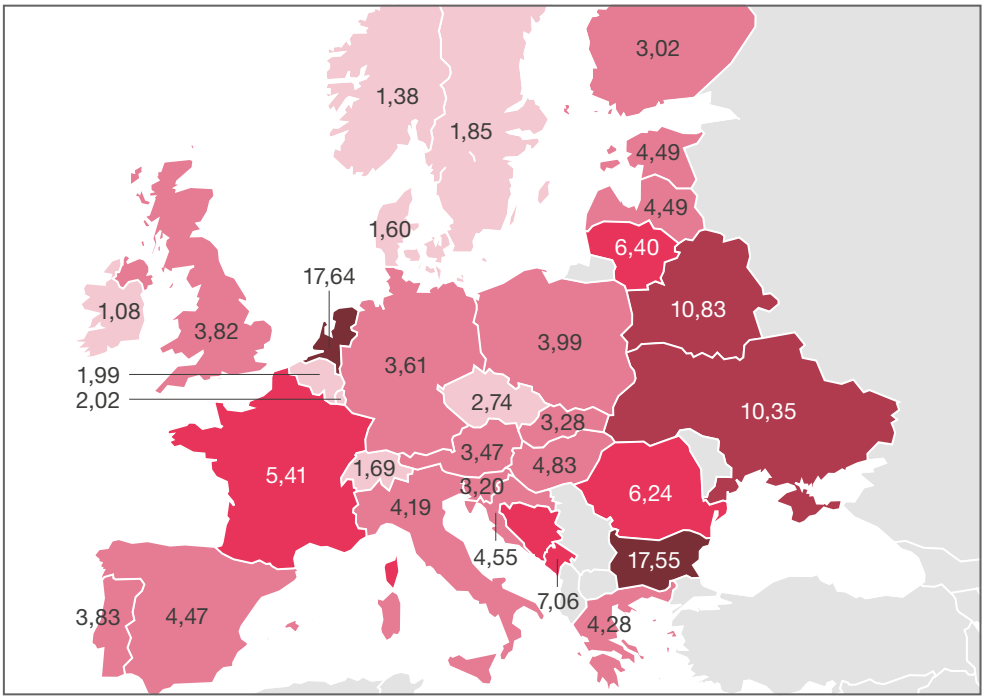
Jürgen: Effektiver wäre es also, die Mitarbeiter:innen ihre Arbeit tun zu lassen, ohne ihr geistiges und kreatives Potenzial einzuschränken. Sie zu befähigen, nicht zu verunsichern. Dazu müssen die Verantwortlichen als Hilfe empfunden werden, keinesfalls als Bedrohung. Zeitgemäßes Management von Cyber Security bedeutet deshalb, ein Spielfeld abzustecken, auf dem sich die Mitarbeiter:innen bestmöglich abgesichert bewegen können. Dies bestätigt auch die OECD-Studie. Dort heißt es, dass Digitalisierung nur dann zum Wohlbefinden der Menschen beiträgt, wenn unter anderem eine starke digitale Sicherheit geschaffen wurde. Viele mögliche Fehler können durchaus schon über Technologie eingefangen werden, die dem Menschen wie Assistenzsysteme im Auto sinnvolle und sichere Optionen vorschlagen, oder ihn gegebenenfalls sogar präventiv warnen und zur aktiven Mitarbeit motivieren.

Maike: Dazu bedarf es allerdings einer Menge Vertrauen. Unternehmen, die Cyber Security ernst nehmen, sollten auch nicht vergessen, die Unternehmenskultur, die Digital Trust erst möglich macht, mit zu verändern. Und da fühlen wir gleich den schmerzlichen Widerspruch zwischen Vertrauen und Kontrolle – und zwischen Freiheit und Regeln. In Deutschland setzt man mehr auf Kontrolle, in den skandinavischen Unternehmen auf Vertrauen, wenige Regeln und viel Transparenz. Peder Holk Nielsen, CEO der Biotech-Firma Novozymes und nach Forbes 2016 einer der 30 Global Gamechanger, hat das gut auf den Punkt gebracht. Er sagt: „Wir sollten eine gute Balance zwischen Organisation und Freiheit anstreben, damit alle Pfeile grob in eine Richtung weisen, wir aber nicht die Leidenschaft und die Kraft der Individuen verlieren."

Jürgen: Ganz ohne Regeln geht es aber in der Regel nicht. Wie sieht ein gesunder Umgang damit aus?

Maike: Neben der positiven Kommunikation sollten Regeln, welcher Art auch immer, weise eingesetzt und kommuniziert werden, denn sie können Mitarbeiter:innen zwar Orientierung geben, aber – in der falschen Dosierung – auch schnell viel Energie entziehen. Unternehmen sollten also zunächst ihr Regelwerk unter die Lupe nehmen und nicht ihre Belegschaft. Bei der Einordnung hilft immer auch die Frage: Was ist wirklich notwendig und was fällt unter die Kategorie gesunder Menschenverstand?

Abb. 2 Die skandinavischen Länder gehören zu den glücklichsten Ländern der Welt – und zu den am wenigsten anfälligen Ländern für Cybercrime. Ein Zufall?



Cyberverbrechen: Europas sicherste und am wenigsten sichere Länder

Prozentsatz der Rechner, die Cyberattacken ausgesetzt waren (Januar–Oktober 2019)

- +11 %
- 8–11 %
- 5–8 %
- 3–5 %
- 1–3 %

Quelle: Statista

Takeaways

- Die Verantwortlichen für Cyber Security müssen als Hilfe wahrgenommen werden, nicht als Bedrohung.
- Regeln sollten bewusst und sparsam eingesetzt sowie klar kommuniziert werden.
- Unternehmen müssen die technischen und prozessualen Grundlagen schaffen, um ihre Mitarbeiter:innen bestmöglich zu schützen.
- Je besser die technische Absicherung ist, desto weniger Regeln sind notwendig.

Jürgen: Wenige Regeln sind in der Praxis natürlich nur möglich, wenn der Arbeitgeber seine Hausaufgaben gemacht und die technischen und prozessbezogenen Grundlagen geschaffen hat. Regulatorische Voraussetzungen sind der Grundstock für die Entwicklung einer rechtskonformen Strategie. Der aktuelle Stand der Technik ist hier das Maß der Dinge. Und der ist in konstanter Bewegung. Die Folgen mangelhafter Absicherung seitens des Arbeitgebers dürfen nicht auf die Mitarbeiter:innen abgewälzt werden. Ist hier gut vorgesorgt, beschränken sich die Regulierungen auf das allgemeine Verständnis für den Umgang mit Systemen und Informationen und setzen kein tiefes Wissen für technische Abläufe mehr voraus.

Maike: Es gibt dementsprechend auch einen klaren Zusammenhang zwischen den kulturellen Faktoren und einer zeitgemäßen, technisch sicheren Umsetzung.

Jürgen: Ja, genau. Die Eintrittswahrscheinlichkeit für Fehler im Umgang mit Regularien sinkt dann, wenn Nichtwissen und Fehlinterpretation eben dieser Regularien an Relevanz verlieren. Viele Regeln resultieren in vielen Fehlern. Die Hoffnung, technische Unzulänglichkeiten mit regelmäßigen Trainings für Security Awareness auszugleichen, ist bestenfalls trügerisch, wird generell sehr kontrovers diskutiert. Nicht von den Anbietern dieser Trainings, aber zum Beispiel vom Security-Guru Bruce Schneier, der SecAware-Maßnahmen in der Regel als wirkungslos einschätzt. In seinem Artikel im Magazin DARKReading empfiehlt er stattdessen, die Budgets in sichere Software-Entwicklung und bessere Security-Schnittstellen zu investieren.

5 Vertrauen und Absicherung – die Allegorie der Glaswand

Wie können Unternehmen für ihre Mitarbeiter:innen eine sichere Umgebung schaffen? Wie sieht eine vertrauensvolle Zusammenarbeit aus?

Maike: Der Glaube an den gesunden Menschenverstand scheint in Skandinavien besonders stark ausgeprägt zu sein. Der Mensch ist gut und will nur sein Bestes geben, so lautet dort die Grundannahme. Cyber Security ist in der Folge „nur“ dazu da, die Mitarbeiter:innen darin zu unterstützen, ihre Arbeit gut und sicher zu bewältigen. Die Absicht ist das, was den dahinter liegenden Unterscheid ausmacht. Es ist ein Service für Menschen, die einen guten Job machen wollen – kein Sanktionsmittel für Menschen, die dem Unternehmen schaden wollen: behüten statt kontrollieren.

Jürgen: Diese Einstellung setzt aber eben einen großen Vertrauensvorschuss voraus. Können sich Unternehmen das leisten?

Maike: Vertrauen neigt dazu, sich selbst zu bewahrheiten. Wenn wir davon ausgehen, dass wir Menschen nicht vertrauen können, haben wir recht. Wenn wir davon ausgehen, dass wir Menschen vertrauen können, haben wir ebenfalls recht. Denn wann immer wir Menschen Vertrauen schenken, neigen sie dazu, sich vertrauenswürdig zu erweisen, wie der Wirtschaftsprofessor Christian Björnskov herausgefunden hat. Andersherum entzieht man den Mitarbeiter:innen Energie, eigenen Antrieb und Selbstverantwortung durch verstärkte Kontrollen. Sprich: Man muss dann auch verstärkt kontrollieren, prüfen, dokumentieren, rückversichern. Vertrauen und Zutrauen hingegen lässt Menschen und Unternehmen wachsen.

> Vertrauen und Zutrauen lässt Menschen und Unternehmen wachsen.
>
> Maike van den Boom, Bestsellerautorin und Glücksforscherin

Jürgen: Das Sprichwort „Vertrauen ist gut, Kontrolle ist besser“ entspricht also genau nicht der Grundidee einer vertrauensvollen Zusammenarbeit. Das Spannungsfeld zwischen Vertrauen und Fremdbestimmung lässt sich aber nie ganz auflösen. Es gibt schließlich gesetzliche Vorschriften, die sich nicht so einfach durch die eigene Unternehmenskultur ersetzen lassen. Wie würdest du dieses Spannungsfeld beschreiben?

Maike: Das erinnert mich an den schlimmsten Moment in meinem Leben während meines zweijährigen Aufenthalts in Mexiko: Kaufhaus in Mexiko City mit offenem Atrium und drei Stockwerken, in denen sich die Rolltreppen befanden. Meine Tochter Elisa, damals zwei Jahre alt, rannte im obersten Stockwerk los. Ich habe sie laufen lassen, weil das Atrium mit Glas abgesichert war. Nur dann auf einmal einen Meter weit nicht mehr und dann ist Elisa an der Innenseite der Glaswand weiter zum Atrium hingelaufen, auf einem 30 Zentimeter Vorsprung zum Abgrund. Ich habe dann nur süß geflötet: „Komm Elisa, komm zu Mama!“ In einem sehr ruhigen Ton, damit sie sich umdreht und lächelnd die zwei Meter zu mir zurückgeht. Ich habe danach im Auto erst einmal zehn Minuten durchgeatmet. Allegorie: Du kannst die Mitarbeiter:innen laufen lassen, solange die Glaswände da sind, um sie zu schützen und solange sie sich auch darauf verlassen können. Sicher, unaufdringlich, transparent. Genau in solch einer Kultur möchten Menschen heutzutage arbeiten. Das ist es, was Mitarbeiter:innen an ein Unternehmen bindet und neue Menschen anzieht – und eben auch die Cyber Security nachhaltig stärkt.

Jürgen: Das ist ein sehr passendes Bild! Abschließend möchte ich festhalten, dass sich vieles, was wir angesprochen haben, mit den Erkenntnissen unserer globalen Cyber-Security-Studie *Digital Trust Insights* deckt: Cybersicherheit trägt genau dann entscheidend zum Unternehmenserfolg bei, wenn gegenseitiges Vertrauen, der Schutz der Privatsphäre der Angestellten und ein fundiertes Werteverständnis für den Umgang mit Daten gelebt werden. Cyber Security ist daher zwar notwendig, aber gewiss kein Übel, sondern eine Chance, eine vertrauenswürdige und freie Unternehmenskultur zum Ausdruck zu bringen, in der glückliche und entspannte Menschen ihr Bestes geben können.

Cyber Security nachhaltig verankern

Wie wichtig sind transparente Absicherungsmaßnahmen – eben die erwähnten Glaswände – für die Cybersicherheit und die Belegschaft?

Das Bild mit den Glaswänden als Schutz vor Fehlverhalten ist eindeutig nachvollziehbar. Es tauchen jedoch weitere Fragen auf: An welche Stellen montiere ich die Glaswände und wie kommen sie dort hin? Entstehen nicht immer neue Risiken, die neue Glaswände benötigen? Mit diesen Fragen fordert Cyber Security alle Changemaker in Unternehmen zum Schulterschluss auf, um die notwendige Veränderung und Bewusstwerdung zur nachhaltigen und effektiven Verankerung von Cyber Security zu realisieren!

Wie lässt sich dieser Schulterschluss am besten realisieren?

Aus meiner Sicht können die wenigsten Herausforderungen der aktuellen Zeit in Silos oder Einzeldisziplinen in Unternehmen gelöst werden. Ich empfehle meinen Kund:innen, den Plattformgedanken auch innerhalb von Unternehmen zu etablieren und zu nutzen. Dem Schulterschluss mit der Personalabteilung, die den Verhaltens- und Wertekompass der Mitarbeiter:innen vom Recruiting bis zum Ausscheiden aus dem Unternehmen maßgeblich prägt, sollte daher eine hohe Priorität gegeben werden. Ein wacher Wertekompass ermöglicht Mitarbeiter:innen in Situationen mit neuen Risiken, die noch nicht durch eine Glaswand gesichert sind, sich sicher zu fühlen und aus Sicherheit und Vertrauen zu handeln.

Eine Einschätzung von Daniela Hanauer, Partnerin bei PwC Deutschland und Expertin für Compliance, Integrität und Digitale-Ethik-Verantwortung

Takeaways

- Die Absicht macht den Unterschied: Cyber Security sollte behüten statt kontrollieren.
- Vertrauen fördert vertrauenswürdiges Verhalten – und macht verstärkte Kontrollen der Mitarbeiter:innen im Idealfall überflüssig.
- Vertrauen und Fremdbestimmung sind in einem Spannungsfeld, das sich nie ganz auflösen lässt. Ein Grund dafür sind zum Beispiel gesetzliche Vorschriften.
- Unternehmen sollten ihre Mitarbeiter:innen mit Schutzmaßnahmen vor Fehltritten absichern – transparent und unaufdringlich.

Ever sit and watch a pendulum swing back and forth? It's fascinating just how many swings it takes before that pendulum slowly swings back into balance. The same can be said for the balancing act that companies need to perform between security and enablement. If you pull too tightly on the security controls, tension among your workforce is quick and apparent. 'Let me do my job' freely and without constraint is the rallying cry in that situation. That said, if you let that pendulum swing too far in the other direction – providing your workforce with an abundance of access without proper security controls – the threat to the business rises considerably. Instead, think of that pendulum swinging and striving to find that very fine but important balance to deliver a securely enabled, yet agile workforce. Couple that with the notion of trusting your people to ultimately 'do the right thing' with their access, and you'll be well on your way to a trust-based workplace that runs securely and efficiently.

Mark McClain, CEO and founder of SailPoint

Literaturverzeichnis

Maike van den Boom
Wo geht's denn hier zum Glück?, Fischer 2015, https://www.amazon.de/dp/3596032644.

Maike van den Boom
Acht Stunden mehr Glück: Warum Menschen in Skandinavien glücklicher arbeiten und was wir von ihnen lernen können, Fischer 2018, https://www.amazon.de/dp/3810530506.

Maike van den Boom
Blog, https:/maikevandenboom.de/ueber-cybersecurity-glueck-und-vertrauen/.

Jürgen Schulze
Coterminus – Nach mir die digitale Sintflut?, Manuskript 2021.

Jürgen Schulze
Blog Coterminus, https://coterminus.com/de_de/?post_id=143.

Daniela Hanauer
Digitale Ethik (Chancen, Orientierung und Haltung für verantwortungsbewusste Unternehmen in der digitalen Welt), https://www.pwc.de/de/managementberatung/risk/digitale-ethik.html.

Dr. Robert Paffen, Daniela Hanauer et al.
Paper & Studie: Digitale Ethik: Orientierung, Werte und Haltung für eine digitale Welt, pwc Feb 2020, https://www.pwc.de/de/managementberatung/pwc-digitale-ethik-white-paper.pdf.

Mark McClain
Joy and Success At Work – Building Organizations That Don't Suck (The Life Out Of People), Forbes Books 2020, https://www.amazon.de/dp/1950863042.

Scott Adams
How to Fail at Almost Everything and Still Win Big, Penguin 2013, https://www.amazon.de/dp/0241003709.

Guy Kawasaki
Enchantment, Penguin 2011, https://www.amazon.de/dp/0241953650.

Richard J. Gerrig (Zimbardo)
Psychologie mit E-Learning, Pearson Studium 2018, https://www.amazon.de/dp/3868943234.

Daniel Goleman
Emotional Intelligence: 25th Anniversary Edition, Bloomsbury Publishing 2020, https://www.amazon.de//dp/1526633620.

Bimal Parmar
Employee negligence: the most overlooked vulnerability, Computer Fraud & Security, Bd. 3 2013, S. 18–20, https://www.sciencedirect.com/science/article/abs/pii/S1361372313700307.

Ricardo Semler
Maverick, Warner Business Books 1993, https://www.amazon.de/dp/0446670553.

Vineet Nayar
Employees First, Customers Second, Harvard Business Press 2010, https://www.amazon.de/dp/1422139069.

Scott Adams
The Joy Of Work – Dilbert's Guide to Finding Happiness at the Expense of Your Co-workers, Harper Business 1998, https://www.amazon.de/dp/0887308716.

PwC
Digital Trust Insights 2021, www.pwc.de/de/cyber-security/digital-trust-insights-2021.pdf, 2021.

OECD (Hg.)
How's Life in the Digital Age?, www.oecd-ilibrary.org/science-and-technology/how-s-life-in-the-digital-age_9789264311800-en, 2019.

David Crouch
Almost Perfect – How Sweden Works and What We Can Learn From It, Blink Publishing 2019, https://www.amazon.de/dp/1788701569, Bonnier Books Ltd.

Anna Kraft, Jennifer Sparr, Claudia Peus
Giving and Making Sense About Change: The Back and Forth Between Leaders and Employees, Journal of Business and Psychology, Bd. 33(1) 2018, S. 71–87, https://link.springer.com/article/10.1007/s10869-016-9474-5.

Lene Rachel Andersen und Tomas Björkman
Das skandinavische Geheimnis – Eine europäische Geschichte von Schönheit und Freiheit, Phänomen-Verlag 2020, https://www.amazon.de/dp/8412201256.

Andrew J. Oswald, Eugenio Proto und Daniel Sgroi
Happiness and Productivity, Journal of Labor Economics, Bd. 33(4) 2015, S. 789–822, https://www.journals.uchicago.edu/doi/10.1086/681096.

Charles Henri DiMaria, Chiara Peroni und Francesco Sarracino
Happiness matters: Productivity gains from subjective well-being, Journal of Happiness Studies, Bd. 21 2020, S. 139–160, https://mpra.ub.uni-muenchen.de/77864/1/MPRA_paper_56983.pdf.

Business News Daily Editor
Happy, Loyal Employees Need to Feel Trusted at Work, www.businessnewsdaily.com/9507-employee-trust-benefits.html, Business News Daily, 11. Mai 2020.

Adéle Da Veigha und Jan H. P. Eloff
An Information Security Governance Framework, Information Systems Management, Bd. 24(4) 2007, S. 361–372, https://www.tandfonline.com/doi/abs/10.1080/10580530701586136.

Chon Abraham, Ronald R. Sims, Sally Daultrey, Anne Buff und Anne Fealey
MIT Sloan Management Review, Cambridge Bd. 60(3) 2019, S. 1–8, https://sloanreview.mit.edu/issue/2019-spring/.

Ralph Dombach
Security Awareness ist Zeitverschwendung, www.security-insider.de/security-awareness-ist-zeitverschwendung-a-567723/, Security Insider, 2016.

Geert Hofstede
Lokales Denken, globales Handeln – Interkulturelle Zusammenarbeit und globales Management, beck im dtv 2017, https://www.amazon.de/dp/342350952X.

Prof. Dr. habil. Josef Wieland, Dr. Roland Steinmeyer und Prof. Dr. Stephan Grüninger (Hg.)
Handbuch Compliance-Management – Konzeptionelle Grundlagen, praktische Erfolgsfaktoren, globale Herausforderungen, Erich Schmidt Verlag 2020, S. 901–930, https://www.amazon.de/dp/3503187847.

Julian Nida-Rümelin und Nathalie Weidenfeld
Digitaler Humanismus – Eine Ethik für das Zeitalter der Künstlichen Intelligenz, Piper 2018, https://www.amazon.de/dp/349205837X.

Deutscher Bundestag
Enquete-Kommission Internet hat sich konstituiert, www.bundestag.de/webarchiv/textarchiv/2010/29545289_kw18_de_enquete-201626, 2010.

Michael Swanagan
Social Engineering, https://purplesec.us/social-engineering/, PurpleSec, 2021.

World Values Survey
www.worldvaluessurvey.org/WVSContents.jsp.

TechRepublic
More than 3.5 million people needed worldwide to work in cybersecurity, https://www.techrepublic.com/videos/more-than-3-5-million-people-needed-worldwide-to-work-in-cybersecurity/.

Ihre Ansprechpartner:innen

Jürgen Schulze
Manager
Mobiltel.: +49 151 40773588
juergen.schulze@pwc.com

Daniela Hanauer
Partnerin
Mobiltel.: +49 1511 1720054
daniela.hanauer@pwc.com

Sie haben Fragen oder Anmerkungen? Wir freuen uns auf den Austausch!

Mit freundlicher Unterstützung und Input von: Franziska Sefranek, Felix v. d. Planitz, Benedict Gross, Arnd Chrostowski, Thomas Tschersich, Annika Schnappinger, Christian Pfeiffer, Phil Horn, Felix Baumann, Daniela Hanauer, Mark McClain, Jörg Asma, Martin Valkyers, Sophia Guggenberger, David Etter, Alina Gerhards und Heiko Beier.

#DigitalTrust #DigitaleEthik #GlückUndVertrauen #HappyNordicLeadership #IAM #Innovation #Kreativität #peoplefirst #Privatsphäre #SecCostAnalytics #TrustInTransformation #TechnischeSicherheit #ZeroTrust

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 155 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Rund 12.000 engagierte Menschen an 21 Standorten. 2,3 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

www.pwc.de