www.pwc.de/familienunternehmen

Cybersicherheit in Familien-unternehmen

pwc

WIFU WITTENER INSTITUT FÜR FAMILIENUNTERNEHMEN UNIVERSITÄT WITTEN/HERDECKE

NTES Family Business Academy | *by PwC*

Und es passiert doch!

„Uns kann das nicht passieren“, ist der Head of IT des Familienunternehmens überzeugt. Und dann passiert es doch. Als am 27. Dezember in der Produktion des mittelständischen Fahrradherstellers nichts mehr funktioniert, wird er entdeckt: der Cyberangriff. Die Hacker:innen hatten ihn über die Feiertage sorgfältig vorbereitet, die Systeme verschlüsselt und damit das Unternehmen in der so wichtigen Bestellphase nach Weihnachten und vor dem Saisonbeginn im Frühjahr empfindlich getroffen. Wie so oft. Die Forderung: Entschlüsselung gegen Lösegeld – in Bitcoin. Der Fachbegriff dafür: Ransomware-Angriff – aktuell die beliebteste Form des Cyberangriffs.

Der eigentliche Angriff findet schon ein halbes Jahr vorher statt – über Phishing („Password Fishing“), also den Versuch, über manipulierte Webseiten, E-Mails oder Nachrichten an Passwörter oder persönliche Daten zu kommen. Zwei Monate lang durchleuchten die Angreifenden systematisch und unentdeckt die Systeme des Unternehmens.
Erst dann schlagen sie zu und verschlüsseln die Daten. Bis heute ist nicht klar, wie sie genau vorgegangen sind. Das Gefühl bei den Verantwortlichen: Machtlosigkeit.

Vier Wochen dauert es, bis die Systeme zumindest notdürftig wiederhergestellt werden und die Produktion wieder laufen kann. Und das Familienunternehmen hat Glück. Die Lager sind für das Nachweihnachtsgeschäft gut gefüllt, der Webshop wird über einen Technologieprovider in der Cloud abgewickelt. Die Kunden bemerken den Angriff nur vereinzelt. Negative Auswirkungen auf das Geschäft gibt es nicht. Aber auch nur, weil die Mitarbeitenden kompromisslos mit anpacken und bereit sind, die fehlenden IT-Prozesse durch ungewohnte manuelle Prozesse, sogenannte Workarounds, auszugleichen.

So glimpflich wie der Fahrradproduzent kommen nicht alle Unternehmen davon. Bei einem mittelständischen Gashersteller und -vertreiber sind noch ein Jahr nach dem Cyberangriff die Auswirkungen durch Workarounds zu spüren, die Systeme nicht komplett wiederhergestellt.

Auch hier kommt es kurz nach den Weihnachtsferien zu einer bösen Überraschung. Dass die IT-Systeme kompromittiert wurden, bemerkt das Unternehmen erst, als die Werkstore sich nicht mehr öffnen und schließen lassen. Und auch hier haben sich die Cyberkriminellen, eine hoch spezialisierte Gruppierung, bereits Wochen vorher Zugriff auf die Infrastruktur verschafft, vermutlich mittels über gezielte Phishing-Angriffe erhaltene Nutzungszugangsdaten. Nach der unentdeckten Erkundung werden Daten zunächst kopiert und anschließend verschlüsselt, Backup-Speicher gelöscht oder manipuliert. Spuren werden dabei bewusst verwischt, um die Forensik zu erschweren. Die Forderung: Entschlüsselung gegen Kryptowährung.

Und das konnte passieren, obwohl das Unternehmen vor einiger Zeit einen echten Cyberangriff geprobt und die damaligen Systeme für sicher befunden hatte. Daher hatte es der Inhaber nicht für möglich gehalten, dass sein Unternehmen tatsächlich Opfer einer Cyberattacke werden könnte. Aber „einen hundertprozentigen Schutz gibt es nicht“, weiß Peter Vahrenhorst, seit 2001 Leiter des Kompetenzzentrums Cybercrime beim Landeskriminalamt Nordrhein-Westfalen. „Hacker suchen systematisch nach Schwachstellen in IT-Systemen und probieren so lange, bis sie fündig werden.“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Ransomware als „eine Art von Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird ein Lösegeld (englisch: Ransom) verlangt. Entweder sperrt ein solches Schadprogramm den kompletten Zugriff auf das System oder es verschlüsselt bestimmte Nutzerdaten.“[1]

Als Standard-Modus-Operandi gilt die sogenannte Double Extortion. Dabei erfolgt die Erpressung durch Verschlüsselung der Systeme bei gleichzeitiger Drohung mit Veröffentlichung von zuvor durch die Erpresser abgezogenen sensiblen Daten. Teilweise werden auch Geschäftspartner des betroffenen Unternehmens erpresst, wenn keine Zahlung erfolgen sollte und ein Bezug zwischen den gestohlenen Daten und einem Geschäftspartner hergestellt werden kann (sog. Second-State-Extortion).[2]

[1] www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html.
[2] Vgl. BKA, Cybercrime – Bundeslagebild 2021, S. 2.

Gefangenendilemma Lösegeld: Verlockung groß, Schaden größer

Der Mittelständler zahlt nicht. Aus gutem Grund: „Sie wissen nicht, ob sie für die Zahlungen tatsächlich alle erforderlichen Schlüssel erhalten und vor allem, ob die Erpresser anschließend mit weiteren Forderungen, zum Beispiel in Bezug auf die Veröffentlichung der zuvor kopierten Daten, weitere Zahlungen einfordert“, sagt Derk Fischer, Experte für Cyberkriminalität bei PwC. „Bei Systemen, die einmal infiziert wurden, besteht außerdem die Gefahr, dass sie weiterhin schadhaft sind. Außerdem sprechen sich Lösegeldzahlungen schnell in der Cyber-Community herum – und das zahlende Unternehmen macht sich selbst zu einem noch attraktiveren Angriffsziel.“

Das sieht auch Prof. Dr. Eric Bodden, Informatiker mit dem Schwerpunkt Secure Software Engineering an der Universität Paderborn und Direktor Softwaretechnik und IT-Sicherheit am Fraunhofer IEM, so: „Statt […] Milliarden an Euro jährlich dem organisierten Verbrechen und den Staaten, die diese Verbrecherbanden beheimaten, zukommen zu lassen, sollten deutsche Unternehmen die Gelder vielmehr in ihre eigene IT-Sicherheit investieren, um somit einerseits die Hürden für weitere Angriffe zu erhöhen und andererseits die Finanzströme der Verbrecherbanden versiegen zu lassen.“ Bodden und zahlreiche weitere IT-Sicherheitsfachleute bezeichnen Lösegeldzahlungen bei Ransomware-Angriffen daher auch als geostrategisches Risiko und fordern die Politik in einem offenen Brief zum Handeln auf.[3] Schließlich seien Ransomware-Angriffe seit Jahren ein Werkzeug des organisierten Verbrechens, das allein in Deutschland Schäden in Milliardenhöhe verursacht. Gewinne kämen dabei primär Staaten zugute, die Deutschland eigentlich sanktioniert, an vorderster Stelle Russland.[4]

Die einhellige Empfehlung der Expert:innen lautet daher, Lösegelder nicht zu zahlen und die betroffenen Systeme neu aufzusetzen, auch wenn das länger dauert.

Das macht auch der Gashersteller, nachdem er sämtliche IT-Systeme vom Internet getrennt, verbleibende Systeme heruntergefahren und das BSI, IT-Sicherheits-spezialist:innen, die Kriminalpolizei und das Landes-kriminalamt eingeschaltet hat. „Es sieht aus wie der Hühnerhaufen, nachdem sich der Fuchs ein Huhn geschnappt hat“, schildert der Inhaber die Situation. Die Federn müssen seine Mitarbeitenden einzeln aufsammeln.

In den ersten Wochen nach dem Angriff beginnen Ursachensuche und Workarounds – mit Telefon, Stift und Papier. „Es fühlt sich an wie nach einem schweren Verkehrsunfall. Es geht weiter, aber viel langsamer“, bestätigt auch der Leiter IT des Fahrradherstellers und rät zu kontinuierlichen Investitionen in Cybersicherheit. „Wenn man nur einmal abends keine Chips isst, heißt das nicht, dass man danach fit und schlank ist.“

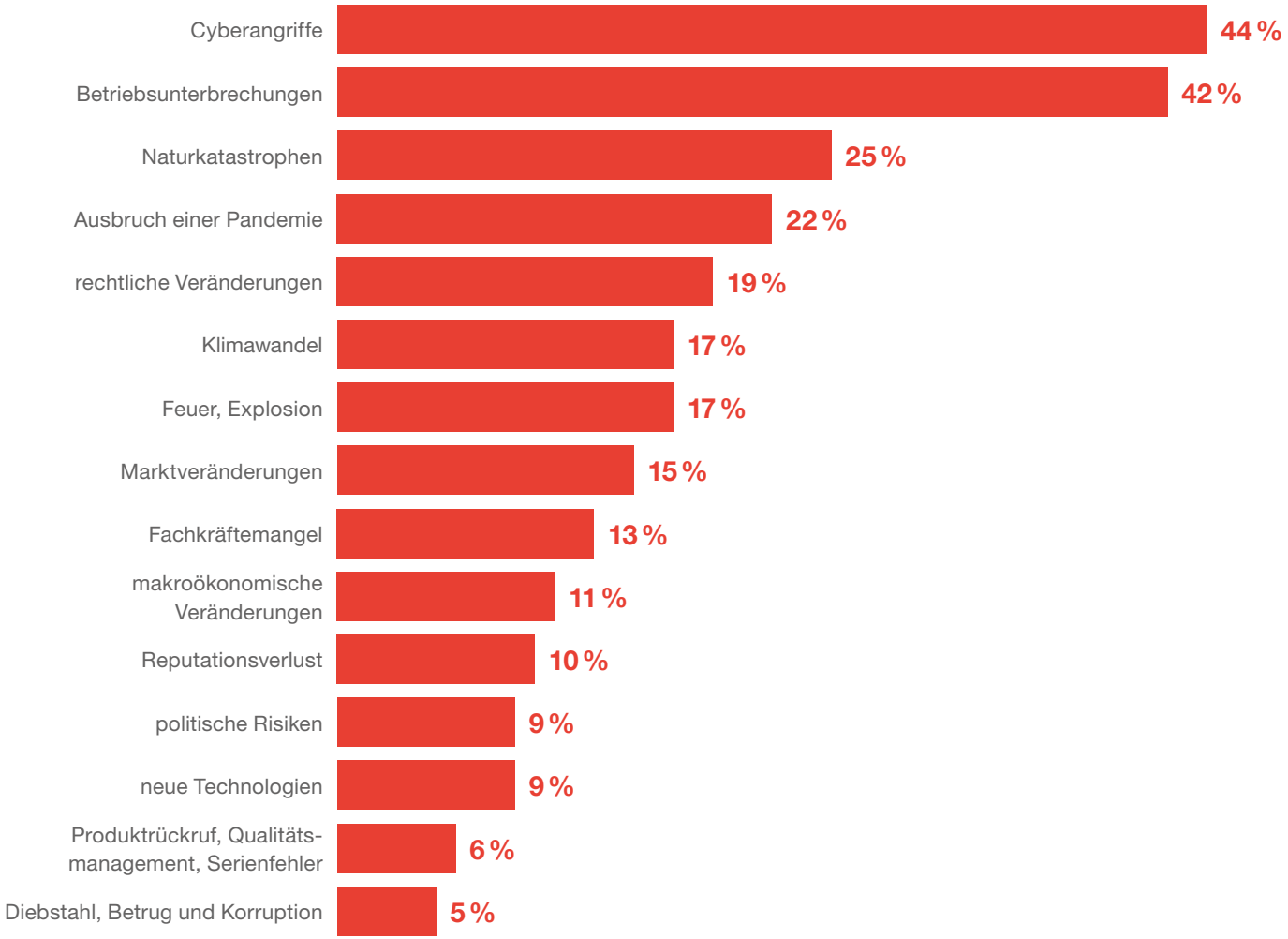
Für beide ist klar: Cybersicherheit ist kein reines IT-Thema. Sie betrifft alle Bereiche des Unternehmens – von der IT über die Personalabteilung, die operativen Geschäftsbereiche und die Unternehmenskommunikation bis zur Geschäftsführung. Letztere muss die Gefahren ernst nehmen, auch wenn das Unternehmen noch so klein ist, und Cybersecurity als regelmäßigen Agendapunkt akzeptieren. „Gerade bei mittelständischen Unternehmen hält sich hartnäckig der Irrglaube: ‚Ich bin zu klein. Wer sollte mich schon angreifen?‘ Das ist eine fatale Fehleinschätzung, die den Kriminellen in die Hände spielt“, sagt Kriminalhauptkommissar Vahrenhorst.

[3] Vgl. https://ransomletter.github.io/.
[4] Laut einer Studie der BBC wurden 2021 drei Viertel (74 %) aller Ransomware-Lösegelder an Cyberkriminelle in Russland gezahlt, www.bbc.com/news/technology-60378009.

Cyberangriffe: das größte Geschäftsrisiko

Zumal das Risiko gerade für mittelständische Unternehmen existenzbedrohend sein kann. Cyberangriffe sind nach dem Allianz Risk Barometer 2022 weltweit daher auch das größte Geschäftsrisiko, noch vor Betriebsunterbrechungen und Naturkatastrophen.[5]

Die zehn größten Geschäftsrisiken weltweit



Quelle: Allianz Risk Barometer 2022.

[5] In Deutschland werden Betriebsunterbrechungen als noch größeres Risiko als Cyber eingeschätzt (55 % vs. 50 %).

Hauptgrund: der Boom an Ransomware-Angriffen – wie beim Fahrradhersteller und beim Gashersteller. Jens Krickhahn, Practice Leader Cyber bei der Allianz Global Corporate & Specialty (AGCS) in Zentral- und Osteuropa, hat dafür eine einfache Erklärung: „Der Einsatz der Verschlüsselungssoftware kostet nur wenige Euro und erfordert geringe technische Kenntnisse. Die Kommerzialisierung der Internetkriminalität macht es einfacher, Schwachstellen in großem Stil auszunutzen." Krickhahn erwartet daher auch mehr Angriffe auf Lieferketten[6] und kritische Infrastrukturen.

Die verstärkte Gefahr von Cyberangriffen bestätigt auch das Bundeskriminalamt (BKA) in seinem *Bundeslagebild Cybercrime 2021*: Demnach ist die Anzahl der Cyberstraftaten 2021 um 12 % gegenüber dem Vorjahr auf knapp 150.000 gestiegen. Und das sind nur die offiziellen Zahlen. Denn nur 6 % der Angriffe werden von den Opfern entdeckt. „Wer als Unternehmen glaubt, noch nie von Hackern angegriffen worden zu sein, hat es noch nicht gemerkt", lautet daher ein Sprichwort unter IT-Fachleuten.

[6] Bei Angriffen auf die Lieferkette (Supply-Chain-Angriffe) erfolgt der Zugriff auf das Netzwerk eines Unternehmens über Drittanbieter oder Lieferanten, was sie schwer nachvollziehbar und damit besonders gefährlich macht. Dabei wird der von einem Zulieferer entwickelte Softwarecode oder eine Anwendung kompromittiert. Durch den Einsatz der Software gelangt der manipulierte Code in die IT des Unternehmens, denn der Kunde vertraut in der Regel seinem Zulieferer und prüft die Updates oder Zugriffe auf die eigene IT entsprechend weniger. Ist der Schadcode einmal in der eigenen Unternehmens-IT, kann er entsprechend Systeme lahmlegen oder Daten ausspionieren.

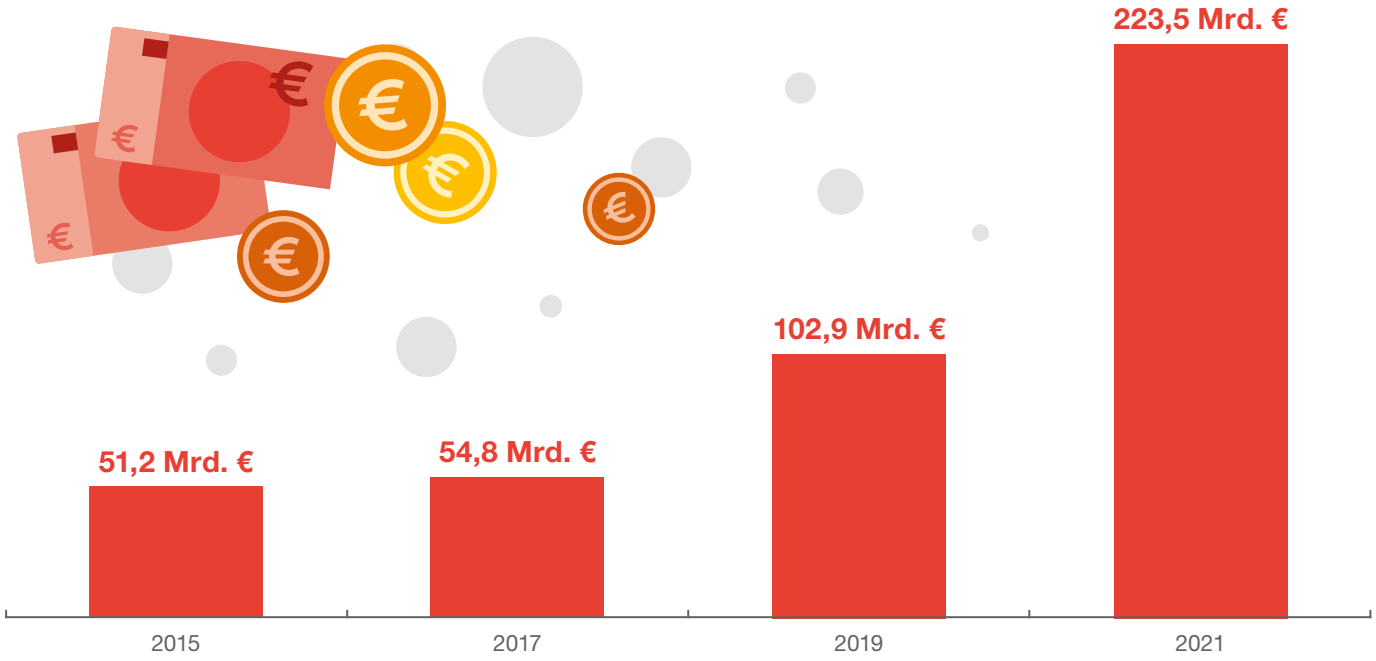
Cyberkriminalität: ein lukratives Geschäftsmodell

Der Schaden, der Jahr für Jahr durch Cyberangriffe entsteht, ist erheblich. Der Branchenverband der deutschen Informations- und Telekommunikationsbranche Bitkom e. V. beziffert ihn in einer repräsentativen Studie aus dem Jahr 2021 für die deutsche Wirtschaft auf 223 Milliarden Euro pro Jahr – das ist mehr als doppelt so viel wie noch vor zwei Jahren (103 Mrd. Euro)[7]. Verursacht vor allem durch Erpressung, den Ausfall von Informations- und Produktionssystemen sowie die Störung von Betriebsabläufen. Zur Einordnung: Das entspricht etwa dem Bruttoinlandsprodukt von Portugal.

Ein Grund dieser enormen Steigerung ist dabei auch, dass viele Unternehmen in der Pandemie (teils gezwungenermaßen) ihre Mitarbeitenden ins Homeoffice geschickt haben. „Die höhere Zahl verteilter Angriffspunkte macht die unternehmenseigene IT vulnerabler. Für die Angreifenden ergeben sich daraus deutlich mehr Einfallstore als vor der Coronapandemie“[8] heißt es beim Institut der Deutschen Wirtschaft in Köln (IW). Es beziffert den Schaden durch Homeoffice im Jahr 2021 auf 52,5 Milliarden Euro – 300-mal höher als den Schaden durch Wohnungseinbrüche. Vor der Pandemie (2019) waren es 21,5 Milliarden Euro.

Schäden durch Cyberangriffe

Schäden von Unternehmen, die in den letzten zwölf Monaten einen Cyberangriff hatten



Quelle: Bitkom e. V., 2021.

[7] Bitkom, Angriffsziel deutsche Wirtschaft: Mehr als 220 Milliarden Euro Schaden pro Jahr, www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr.
[8] Institut der Deutschen Wirtschaft, IW-Kurzbericht 54/2021, Cybersicherheit: 52,5 Mrd. Schaden durch Angriffe im Homeoffice, www.iwkoeln.de/studien/barbara-engels-525-mrd-euro-schaden-durch-angriffe-im-homeoffice-518890.html.

Die größten Cybergefahren

- **Ransomware**
  Bei Ransomware-Angriffen dringen Cyberkriminelle in die Systeme von Unternehmen ein und verschlüsseln sie mit einer speziellen Schadsoftware. Alle betroffenen Systeme werden dadurch unbrauchbar. Die IT ist in einer Art Geiselhaft. Für den Schlüssel zur Wiederherstellung verlangen die Angreifenden immense Summen.

- **Datendiebstahl**
  Wenn Angreifende in IT-Systeme eingedrungen sind, stehlen sie systematisch sensible Informationen wie Kundendaten, Geschäftsgeheimnisse und Forschungsergebnisse. Sie erpressen die Bestohlenen damit, die Daten im Internet zu veröffentlichen, wenn sie kein Lösegeld zahlen.

- **DDoS-Attacken**
  Mit sogenannten Distributed-Denial-of-Service (DDoS)-Attacken überfluten die Angreifenden ein Zielsystem mit Anfragen und blockieren dadurch dessen Funktionen. Erreicht wird dies durch die Übernahme einer großen Anzahl unbeteiligter Dritt-IT-Systeme, deren Rechenkapazität zur Datenüberflutung am Zielsystem genutzt wird (bekannt als sogenannte Botnetz-Angriffe).

- **Kombinierte Erpressung**
  Immer häufiger werden die oben genannten Angriffstypen kombiniert. Verweigert das Unternehmen die Lösegeldzahlung zur Entschlüsselung der Daten, folgt die Erpressung für die Nichtveröffentlichung gestohlener Daten. DDoS-Attacken erhöhen den Druck, da das Unternehmen im Zweifel aufgrund des IT-Notfallbetriebs angreifbar ist.

Cyberversicherung ist keine Lösung

Cyberangriffen sind Unternehmen nicht machtlos ausgeliefert. Im Gegenteil. 80 bis 90 % der Angriffe lassen sich durch das Einspielen erforderlicher Updates und Sicherheitspatches sowie ein entsprechendes Bewusstsein der Mitarbeitenden verhindern[9], ist Michael Waidner, Leiter des Fraunhofer Instituts für Sichere Informationstechnologie, überzeugt.

Sich auf die Versicherung zu berufen, die im Angriffsfall den durch Betriebsunterbrechung und Systemwiederherstellung entstandenen Schaden reguliert, ist dagegen keine Lösung, auch wenn sich Cyberversicherungen im Jahresbudget einplanen lassen. Die Preise für Policen sind aber in den letzten Jahren angesichts der potenzierten Gefahren von Cyberangriffen signifikant gestiegen.

Dazu kommt, dass Versicherungen auch nur dann Verträge abschließen, wenn Unternehmen alle Möglichkeiten ausschöpfen, sich vor Cyberangriffen zu schützen.[10] Dazu zählen das Managementsystem zur Informationssicherheit des Unternehmens genauso wie konkrete Sicherheitsmaßnahmen, zum Beispiel automatische bzw. regelmäßige Sicherheitsupdates, Offline-Datensicherung oder Cloud-Back-up-Lösungen, die Sensibilisierung der Mitarbeitenden, der Schutz sensibler Daten, Firewallstrukturen sowie die Absicherung der Fernzugriffsmöglichkeiten auf IT-Systeme und Clouddienste.

Damit kommt der Vorsorge besondere Bedeutung zu, um für den Ernstfall vorbereitet zu sein und auf einen Business-Continuity- bzw. Notfallplan zugreifen zu können. Denn nach dem Angriff ist Geschwindigkeit gefordert. „Je länger ein Unternehmen wartet, desto größer wird der Schaden“, weiß Peter Vahrenhorst. Der Notfallplan müsse daher in Fleisch und Blut übergehen.

> Oft möchten Unternehmerfamilien der firmeneigenen IT keinen Zugriff auf intimste Informationen aus dem Familienkreis gewähren und wählen für den Betrieb ihrer digitalen Kommunikations- und Kollaborationsplattformen andere, weniger geschützte Anbieter. Das ist riskant.“
>
> **Prof. Dr. Tom Rüsen**
> Vorstand der WIFU-Stiftung und
> Geschäftsführender Direktor des WIFU

[9] Vgl. Convent, Wir haben Alarmstufe Rot, 4. Jahrestagung Cybersecurity, Forum für Datensicherheit, Datenschutz und Datenethik, 28.10.2021, www.convent.de/cybersecurity.
[10] Vgl. Klaus-Dieter Sohn, Familienunternehmen vor schwarzen Bildschirmen, FAZ, 8.11.2011.

Notfallplan für den Ernstfall

Im Notfallplan ist festzuhalten, wie die Geschäftstätigkeit auch bei Systemausfällen aufrechterhalten werden kann. Zudem müssen die Befugnisse klar sein. Wer darf den Notfallplan aktivieren, wenn der Chef im Urlaub ist? Wer ist Mitglied des Krisenstabs? Welche Behörden sind einzuschalten? Welche Dienstleister unterstützen? Wie werden Kunden, Lieferanten, Mitarbeitenden oder gegebenenfalls die Öffentlichkeit informiert? Gibt es Sicherheitskopien der Unternehmensdaten, die eine schnelle Wiederherstellung des Geschäftsbetriebs ermöglichen? Sind Zugangsdaten auch offline verfügbar? Gibt es eine Cyberversicherung, die die Schäden abdeckt?

Der westfälische Gashersteller wusste, wie er vorgehen muss, und konnte einen noch größeren Schaden für das Unternehmen vermeiden. Der Inhaber zieht daher eine positive Bilanz. „A lot of pain – damals und heute – a lot of gain – bis heute und in der Zukunft“, bilanziert er. Ein Jahr später hat das Unternehmen die wesentlichen Teile der IT-Infrastruktur nach höchsten Sicherheitsstandards neu gebaut. Damit er sich beim nächsten Mal nicht wieder fühle wie ein „Maikäfer auf dem Rücken“.

Die Unternehmerfamilie – ein weiteres Risiko

Um existenzbedrohende Schäden durch Cyberangriffe abzuwenden, sind Unternehmen gefordert, in die Verbesserung ihrer IT zu investieren und – vor allem – ihre Mitarbeitenden zu schulen und zu sensibilisieren. Denn laut Bitkom-Studie sind in 61 % der von Cyberangriffen geschädigten Unternehmen die Mitarbeitenden dafür verantwortlich, teils auch nachdem sie bereits aus dem betroffenen Unternehmen ausgeschieden sind. John Boles, ehemaliger stellvertretender Leiter beim FBI und seit 2018 Partner und Experte im Bereich Cyber, Privacy and Forensics bei PwC US, geht sogar von einer noch höheren Quote aus. Er sagt: „95 % der Cyberangriffe sind auf menschliches Versagen zurückzuführen."

Familienunternehmen mit ihrem erhöhten Reputationsrisiko ist es besonders wichtig, in Cybersicherheit zu investieren, zumal der Familienverbund zusätzliche Einfallstore ins Unternehmen öffnet oder aber die Familienmitglieder selbst gefährdet. Etwa wenn Familienmitglieder im privaten Umfeld die gleichen Passwörter verwenden wie im Unternehmen oder wenn innerhalb der Familie sensible Daten über Chatgruppen (z. B. WhatsApp) ausgetauscht werden.[11,12] Ein besonderes Risiko besteht zudem, wenn Aufenthaltsorte und Reisepläne von Familienmitgliedern bekannt werden.

Auch für sogenannte Social-Engineering-Angriffe sind Familienunternehmen besonders anfällig. Hier werden Mitarbeitende bzw. Mitglieder der Unternehmerfamilie als vermeintlich schwächste Glieder in der Sicherheitskette ausgenutzt und manipuliert. Verbreitet ist beispielsweise der sogenannte CEO-Fraud bzw. Cheftrick. Hier gibt sich ein Hacker für den Geschäftsführer, ein Vorstands- oder ein Familienmitglied aus und veranlasst eine dringende Überweisung durch den Mitarbeitenden bzw. das Familienmitglied. Fortschritte im Bereich KI/Deepfake erleichtern solche Social-Engineering-Angriffe, da sich zum Beispiel die Stimme einer bestimmten Person leicht synthetisieren lässt.

Daher müssen auch Mitglieder der Unternehmerfamilie besonders sensibilisiert und hinsichtlich Cyberrisiken geschult werden. Professionelle Hilfe bei der Einrichtung und Verwaltung der Kommunikationsstrukturen sind mehr als angeraten.

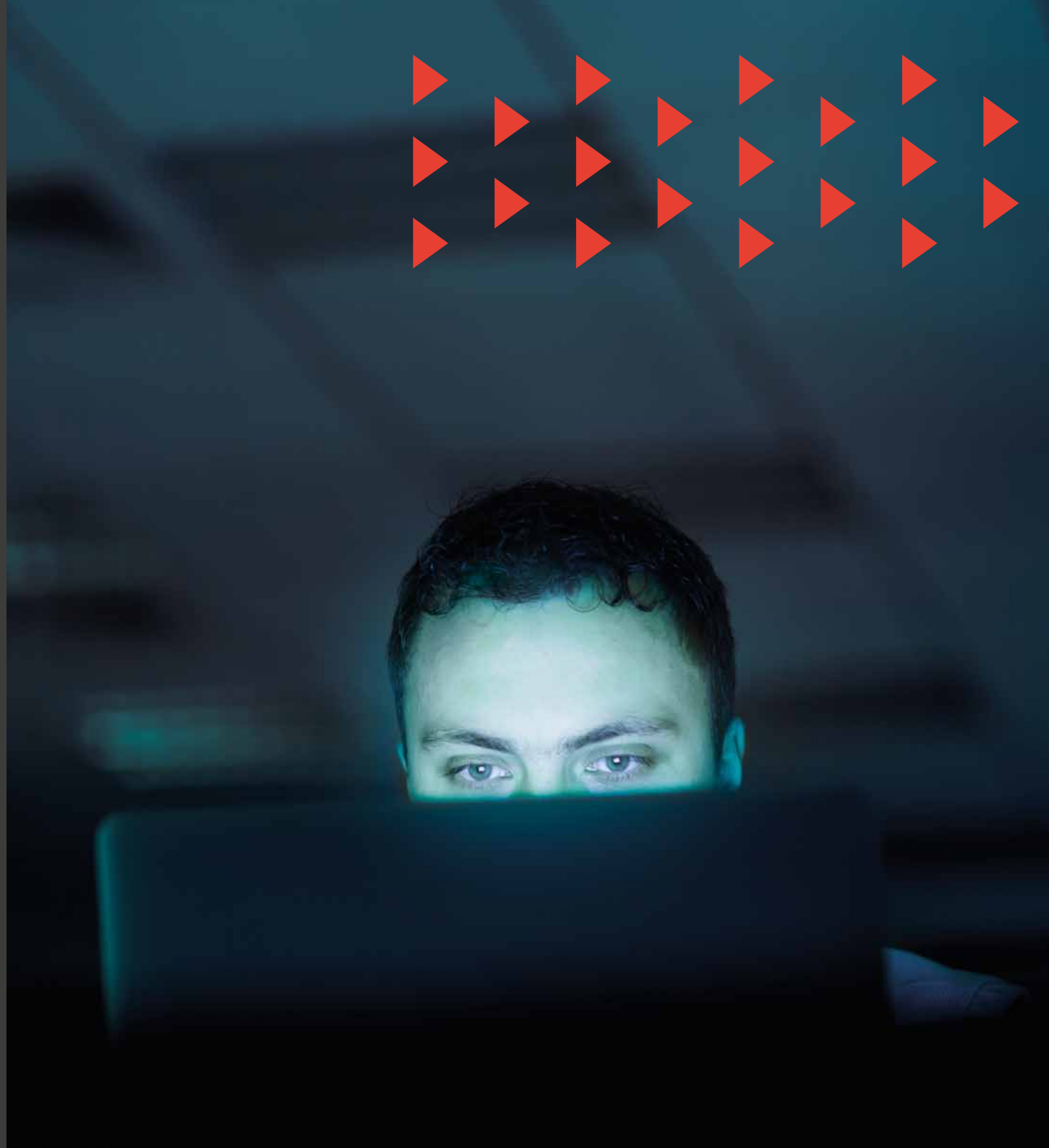
[11] Siehe hierzu auch Rüsen, T. A. (2021). Management der Unternehmerfamilie 4.0 – Formen eines digitalisierten Familienmanagements und Ansätze den Austausch und Zusammenhalt in einer Lockdown-Situation zu organisieren. FuS – Familienunternehmen und Strategie. 02/2021, 42–48.

[12] Zum digitalen Reifegrad einer Unternehmerfamilie siehe Rüsen, T. A., Heider, A. K., Hülsbeck, M., & Orenstrat, R. (2021). Der Einfluss der Unternehmerfamilie auf den Digitalisierungsprozess des Familienunternehmens. Determinanten und Wirkung des „Digitalen Reifegrades" einer Unternehmerfamilie. Studie des Wittener Instituts für Familienunternehmen (WIFU).

Fazit: Hidden war gestern!

Die fortschreitende Digitalisierung in allen Bereichen bietet neue Möglichkeiten für Unternehmen, verschiebt allerdings die Risikolage und öffnet Möglichkeiten für Straftäter:innen. Das gilt für Unternehmen wie Privatpersonen, für Behörden wie Institutionen. Familienunternehmen sind ein besonders attraktives Angriffsziel, zumal Hacker:innen Familien mit der Veröffentlichung privater Daten drohen und sie damit erpressen und Reputationsschäden für das Unternehmen und die Familie verursachen können.

Die Bekämpfung von Cyberkriminalität ist eine gesamtgesellschaftliche Aufgabe und es bedarf gemeinsamer Anstrengungen aller Akteure, um mit den exponentiell steigenden Bedrohungen mithalten zu können. Insbesondere ist auch ein anderer Umgang mit Cybersicherheit notwendig. Ein Grund, warum Deutschland bei der Netzsicherheit vergleichsweise schlecht dasteht, sieht Dr. Haya Shulmann, Director Cybersecurity Analytics und Defence am Fraunhofer Institut SIT daher darin, dass „in Sachen IT-Sicherheit […] hier jeder sein eigenes Süppchen“ koche. Notwendig ist mehr Austausch – und vor allem in Familienunternehmen mehr Offenheit und Transparenz, da diese vielfach besonders verschlossen sind. Schließlich kann es jeden erwischen. Es ist nur eine Frage der Zeit.



Wie Sie für mehr Cybersicherheit sorgen

Technische Prävention

- Verteilen Sie kritische Applikationen, etwa durch die Speicherung in der Cloud. Cloudanbieter haben ein besonders großes Interesse am Schutz ihrer Systeme und profitieren von Größenvorteilen.
- Segmentieren Sie Ihre Netze und nutzen Sie in den Netzen auch physisch getrennte Systeme.
- Nutzen Sie Privileged Access Management (PAM), also den privilegierten Zugriff auf Infrastrukturen und Anwendungen.
- Filtern Sie den externen Datenverkehr Ihrer Clients durch Proxies (Mail Proxy, Web Proxy).
- Sichern Sie Netzwerke etwa durch VPN-Zugänge und nutzen Sie Mail Proxies als Verstärkung der E-Mail-Sicherheit.
- Erzwingen Sie eine hohe Passwortkomplexität bzw. Zwei-Faktor-Authentifizierung.
- Setzen Sie mehrere Sicherheitsebenen ein.
- Trennen Sie unterschiedliche Admin-Netze (VLANs) und Zugänge, auch physisch.
- Sichern Sie Back-ups physisch separat und üben Sie die Wiederherstellung.
- Behalten Sie, sofern wirtschaftlich möglich und sinnvoll, für den Ernstfall Altsysteme für die Sicherung von Datenbeständen.
- Etablieren Sie technisch die Möglichkeit, remote zu arbeiten. So bleiben Sie auch bei fehlender Infrastruktur am Arbeitsplatz arbeitsfähig, wenn Ihr Backend funktioniert.

Organisatorische Prävention

- Definieren Sie die kritischen Kernprozesse für Ihr Unternehmen und machen Sie diese bekannt.
- Das Geschäft muss im Ernstfall auch ohne die IT funktionieren können – definieren und üben Sie Papier/Bleistift-Prozesse.
- Bereiten Sie eine Fallback-Lösung zur „Office-Ebene“ vor, gegebenenfalls auch mit einer separaten Plattform (z. B. Google Suite).
- Schließen Sie, wenn möglich, eine Cyberversicherung ab und nutzen Sie den enthaltenen forensischen Support.

Im Krisenfall

- Reduzieren Sie umgehend die Angriffsfläche auf Null.
- Stellen Sie die kreditorische Buchhaltung und die Kundenversorgung sicher, durch Papier/Bleistift-Prozesse – komplett unabhängig von der IT.
- Holen Sie sich sofort Hilfe von einem spezialisierten Dienstleister für die Etablierung eines Incident-Response-Teams.
- Schalten Sie unmittelbar die lokalen Polizeibehörden ein und melden Sie den Vorfall an das BSI.
- Halten Sie sich arbeitsfähig mit E-Mail, Videokonferenzen, Chatsystemen.
- Etablieren Sie ein Krisenteam, in dem auch die Geschäftsführung vertreten ist; ein Cyber-Angriff ist keine reine IT-Sache.
- Etablieren Sie eine IT-Taskforce und lassen Sie die IT-Verantwortlichen fokussiert an der Wiederherstellung arbeiten.
- Kommunizieren Sie aktiv an Ihre Mitarbeitenden, Lieferanten und Kunden.

Ihre Ansprechpersonen

Uwe Rittmann
Leiter Familienunternehmen
und Mittelstand
PwC Deutschland
uwe.rittmann@pwc.com

Prof. Dr. Tom Rüsen
Vorstand der WIFU-Stiftung/
Geschäftsführender Direktor
des WIFU
tom.ruesen@wifu-stiftung.de

Prof. Dr. Thomas Clauß
Inhaber des WIFU-Stiftungslehrstuhls
für Corporate Entrepreneurship und
Digitalisierung in Familienunternehmen
thomas.clauss@uni-wh.de

Britta Wormuth
Geschäftsführerin INTES Akademie
für Familienunternehmen
b.wormuth@intes-akademie.de

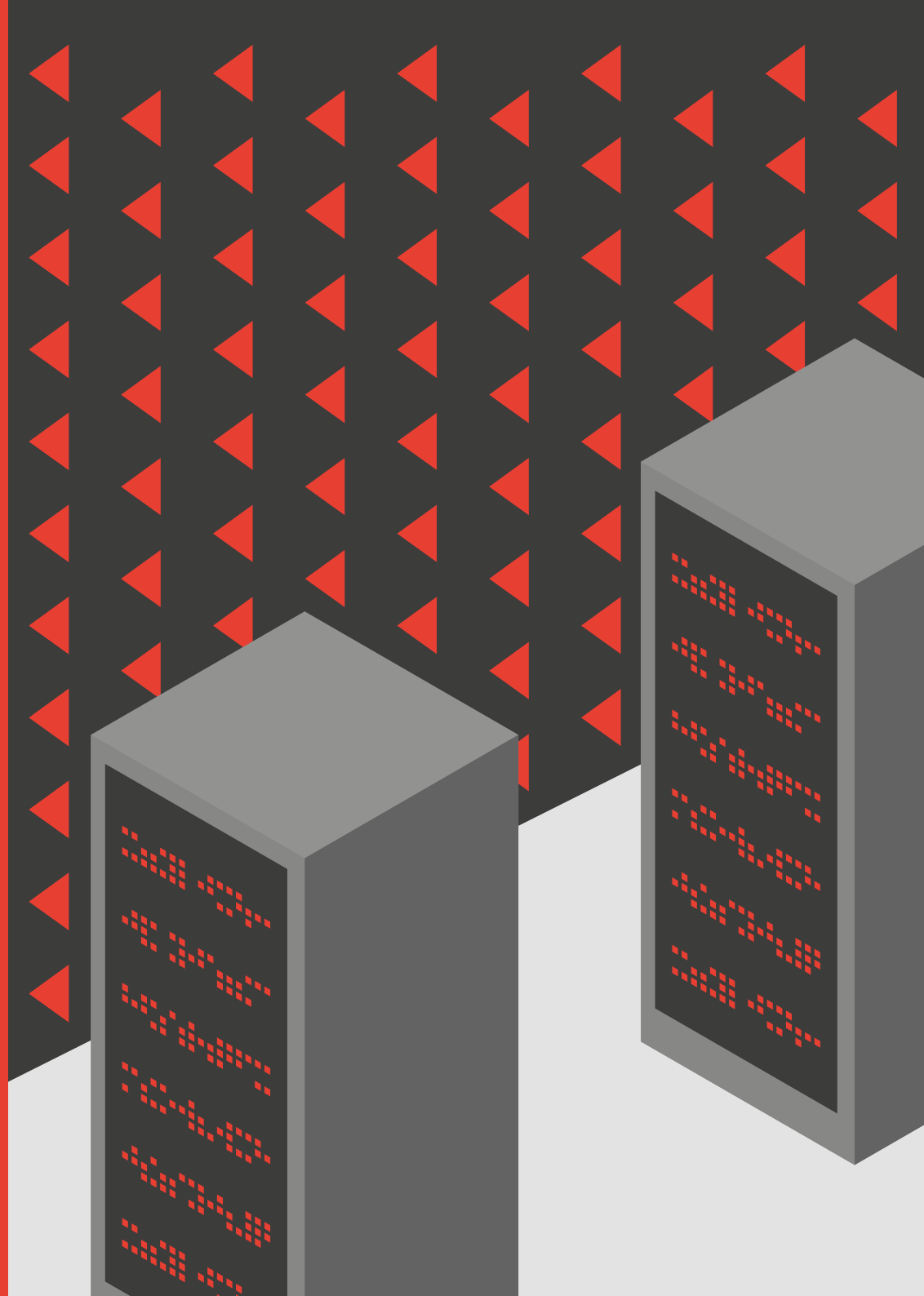
Derk Fischer
Partner und Experte Cyber
Security & Privacy
PwC Deutschland
dernk.fischer@pwc.com

Familienunternehmen und Mittelstand
Wir sind dafür da, Sie noch besser zu machen!

PwC gilt als führender Partner für Familienunternehmen und den Mittelstand. Seit über 25 Jahren verfügen wir über einen eigenen Geschäftsbereich für Familienunternehmen und Unternehmerfamilien mit einem einzigartigen Netzwerk an dezidierten Expert:innen, die speziell für die Arbeit mit Familienunternehmen ausgebildet sind – und das weltweit in 157 Ländern. Allein in Deutschland arbeiten rund 4.000 unserer Mitarbeiter:innen für Familienunternehmen und mittelständische Gesellschaften. Kompetenz, Erfahrung und Leidenschaft prägen unsere Arbeit als Berater:innen.

Unser ganzheitlicher Beratungsansatz von der Strategie zur Umsetzung synchronisiert die Interessen des Unternehmens und der Inhaberfamilien und ist damit exakt auf ihre Bedürfnisse zugeschnitten. Die Arbeit für Familienunternehmen und Mittelstand bedeutet für uns Verpflichtung und Verantwortung – und ist bei uns „Chefsache“: Uwe Rittmann leitet den Bereich bundesweit.

www.pwc.de/familienunternehmen
www.intes-akademie.de



www.pwc.de/familienunternehmen
www.intes-akademie.de