Ausgabe 7 | 12. April 2024 | 76. Jahrgang | www.DHZ.net

# Jeden kann es treffen

Mit organisierten Cyberattacken versuchen Kriminelle auch im Handwerk schnelles Geld zu verdienen. Hundertprozentigen Schutz gibt es kaum. Es gilt, das Schlimmste zu verhindern **VON STEFFEN GUTHARDT**

Neun von zehn Unternehmen in Deutschland werden Opfer von Datendiebstahl, Spionage oder Sabotage. Zu diesem Ergebnis kommt eine Studie des Digitalverbandes Bitkom. „Die Frage ist nicht, ob ein Handwerksbetrieb angegriffen wird, sondern wann es passiert“, sagt Stephan Blank, Referatsleiter für Digitalisierung beim Zentralverband des Deutschen Handwerks. Denn mit Cyberattacken ließe sich eine Menge Geld verdienen. „Deshalb gehen die Hacker immer organisierter vor und Angriffe finden automatisiert und in großem Umfang statt. Die Kriminellen nutzen neueste KI-Software, um Sicherheitslücken in den Systemen der Betriebe aufzuspüren.“ Die Größe des Unternehmens spielt nach Erfahrung des Experten keine Rolle. Einen Fünf-Mann-Betrieb könne es genauso erwischen wie einen Mittelständler mit 100 Beschäftigten. „Entscheidet für die Angreifer ist lediglich, ob eine Sicherheitslücke besteht und das Ziel, wie etwa Lösegeld zu erpressen, schnell erreicht werden kann.“

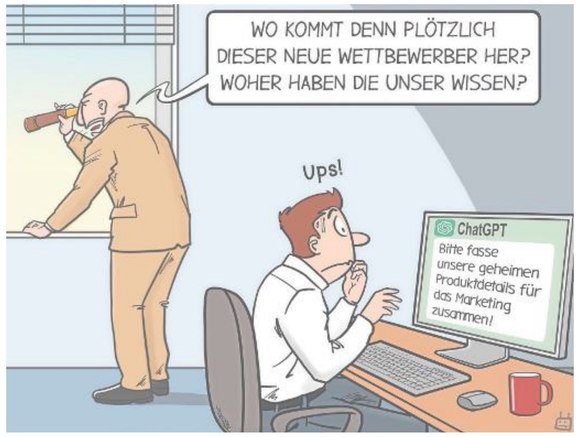


Illustration: dieKleinert.de/Christian Möller

**Betriebe können zu Multiplikatoren werden**

Laurin Baier, Technologie- und Innovationsberater bei der Handwerkskammer für München und Oberbayern, beobachtet zudem, dass Handwerksbetriebe gerne als Multiplikatoren für Cyberattacken genutzt werden. „Die Kriminellen verschaffen sich Zugang zum Mailserver des Betriebs und schicken schadhafte E-Mails an deren Kunden.“ Auf diesem Weg ließe sich in kurzer Zeit eine sehr hohe Anzahl von Unternehmen angreifen. Leider seien Betriebe oftmals ziemlich unvorbereitet auf die Angreifer. „Aktive Anfragen zu Präventionsmaßnahmen sind relativ selten. Häufig melden sich die Betriebe erst, wenn sie sich schon in Panik befinden, weil ein Angriff stattgefunden hat“, weiß Baier. In solchen Fällen müsste die Kammer an die Zentrale Ansprechstelle Cybercrime der Polizeien (ZAC) verweisen. Denn in diesem Fall liege eine Straftat vor, und die Behörde sei verpflichtet zu ermitteln. Dies gestaltete sich in der Praxis jedoch oftmals schwierig, da die Angreifer sich meist außer Reichweite befinden würden.

Baier rät Unternehmen, sich frühzeitig mit einem IT-Sicherheitskonzept zu beschäftigen. Eine kostenfreie Erstberatung bieten die Handwerkskammern für ihre Mitglieder an. Für die Umsetzung konkreter Maßnahmen sei es sinnvoll, mit einem IT-Dienstleister zusammenzuarbeiten, der das Unternehmen dauerhaft begleitet. Zumindest sollten sich die Betriebe um einen Basisschutz kümmern, meint Holger Bär, Beauftragter für Innovation und Technologie bei der Handwerkskammer für Oberfranken. Dazu zähle etwa die Sicherheit von Passwörtern, regelmäßige Softwareupdates, Virenscanner und eine Firewall.

**Sicherheitsbewusstsein kann beliebte Einfallstore schließen**

Einen großen Stellenwert misst Bär einer Schlung von Mitarbeitern bei. „Ohne sie hilft mir die beste Technik nichts“, weiß der Berater. Mit einem gewissen IT-Sicherheitsbewusstsein könnten dubiose E-Mails mit einem schadhaften Link oder einem verseuchten Anhang besser erkannt werden. „Die Mitarbeiterschulung ist Chefsache und sollte den gleichen Stellenwert haben wie Arbeitsschutz oder Brandschutz“, meint Bär. Auch eine Art Notfallkoffer sei unverzichtbar. „Dazu zählt eine Datensicherung, das Rechtemanagement, Passwörter und ein Plan für das Krisenmanagement“, ergänzt Laurin Baier.

Einig sind sich die Experten, dass Handwerksbetriebe nicht auf Lösegeldforderungen von Erpressern eingehen sollten, sondern im Ernstfall immer die Behörden informieren, um das weitere Vorgehen abzustimmen. Stephan Blank verweist hier auf die Gesetzeslage in den USA, die Vorbildcharakter für Deutschland haben könnte. So kann sich in den Vereinigten Staaten ein Unternehmen strafbar machen, wenn es sich auf die Erpresser einlässt und Lösegeld bezahlt. Häufig gehe dieses Geld an Personen oder Länder, die auf Sanktionslisten stehen. „Seitdem sind die Ransomware-Angriffe in den USA zurückgegangen“, weiß Blank. Das Geld sollten Betriebe lieber vorbeugend in ihre IT-Sicherheit investieren.

GASTKOMMENTAR

## Wenn plötzlich nichts mehr geht …

Ein Cyberangriff kann jedes Handwerksunternehmen treffen **VON KARL-SEBASTIAN SCHULTE**

Stellen Sie sich vor, es ist Montagmorgen. Sie leiten einen Baubetrieb und in wenigen Tagen steht der Spatenstich für Ihr bisher größtes Bauvorhaben bevor. Sie haben eben Ihren PC hochgefahren, um noch einmal die Bebauungspläne zu sichten. Als Sie eine unscheinbare E-Mail öffnen, erscheint plötzlich die Meldung: „Ihre Datenstruktur ist verschlüsselt worden.“ Um wieder Zugriff auf Ihre IT-Systeme zu erhalten, sollen Sie eine gewaltige Summe an die Hacker überweisen. Egal was Sie versuchen: Die Schadsoftware blockiert Ihr System. Nichts funktioniert.

*Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Neben Kommunalverwaltungen sind KMU zu den beliebtesten Opfern der bandenmäßig organisierten cyberkriminellen Schattenwirtschaft geworden.“*

**Karl-Sebastian Schulte**
Geschäftsführer des Zentralverbandes des Deutschen Handwerks und Beiratsvorsitzender der Allianz für Cyber-Sicherheit
Foto: ZDH/Henning Schacht

Der Ernstfall ist eingetreten, der Betriebsablauf lahmgelegt: Sie können keine Rechnungen stellen, keine Löhne überweisen. Die digitale Baustelleneinteilung ist nicht aufrufbar. Sie haben keinen Zugriff auf die Buchhaltung, das Onlinebanking oder die elektronische Arbeitszeiterfassung der Mitarbeiter. Baustoffe können nicht bestellt werden. Und an das fertige Angebot für die Mittwoch einzureichende Ausschreibung kommen sie ebenso wenig, wie an ihre Emails, den Firmenkalender oder die Kundendaten.

Wer auf eine Cyber-Attacke vorbereitet ist, kennt die jetzt nötigen technischen und organisatorischen Schritte: Schaden minimieren, den IT-Dienstleister und die Sicherheitsbehörden einschalten. Da ihr Betrieb leider nicht auf eine solche Situation eingestellt ist, bleibt ungewiss, wie lange Sie blockiert sind. Sie können nicht auf Backups oder Notfallsysteme zurückgreifen und auf einen professionellen IT-Dienstleister haben sie bislang aus Kostengründen verzichtet. Darum kümmert sich nebenher ein Bekannter, der gerade im Urlaub ist. Wenn Sie über Wochen hinweg arbeitsunfähig bleiben, können Kunden absprungen und Folgeaufträge verloren gehen. Schließlich sehen Sie sich gezwungen, das Lösegeld zu zahlen, um die Schäden auf ein Minimum zu begrenzen.

Sie mögen jetzt einwenden: Dass so etwas einem eher kleineren Handwerksbetrieb passiert, das ist doch eher unwahrscheinlich. Ist es aber leider nicht! Das genau ist der Trugschluss, dem immer noch zu viele kleine und mittlere Unternehmen (KMU) unterliegen. Längst betreffen Cyberangriffe wie das zuvor ausgeführte Beispiel einer Ransomware-Attacke nicht nur große Konzerne, sondern sie machen auch vor Handwerksbetrieben keinen Halt. Und was gravierender ist: Solche Attacken können schnell existenzgefährdende Dimensionen annehmen. Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Neben Kommunalverwaltungen sind KMU zu den beliebtesten Opfern der bandenmäßig organisierten cyberkriminellen Schattenwirtschaft geworden. Der Digitalverband Bitkom beziffert den Schaden der deutschen Wirtschaft im letzten Jahr auf 206 Milliarden Euro.

Das Gegenmittel lautet Cyberresillienz. Dazu gehören technische und organisatorische Maßnahmen wie regelmäßige Sicherheitsupdates, Backups, Mitarbeiterschulungen, ein vorbereitetes Notfallmanagement oder auch eine passende Cyber-Police. Das alles ist auch für kleine Betriebe kein Hexenwerk. Um den schwerwiegenden Folgen und besonders der Hilflosigkeit, wie auf eine solche Cyberattacke reagiert werden soll, vorzubeugen, hat der ZDH mit dem Mittelstand-Digital Zentrum Handwerk die Initiative Cybersicherheit im Handwerk (www.cybersicherheit-handwerk.de) ins Leben gerufen. Die passgenauen Empfehlungen richten sich an KMU aus verschiedenen Gewerken und reichen von den Grundlagen der Informationssicherheit bis zu professionellem Vorfallmanagement. Auch die Allianz für Cyber-Sicherheit als starkes Netzwerk verschiedener Wirtschaftsteilnehmer informiert kostenlos zu Bedrohungslagen und praxisnahen Sicherheitsmaßnahmen mit zahlreichen Angeboten, wie Check-Listen, Cyber-Sicherheits-Tage, Web-Talks und Podcasts.

Das Handwerk setzt verstärkt auf innovative digitale Lösungen und ist damit wirtschaftlich erfolgreich. Bei jeder Digitalisierungsmaßnahme sollte auch die Cyber-Sicherheit mitgedacht werden - getreu dem Motto „Digitalisierung meines Unternehmens - aber sicher!“ Cyber-Sicherheit ist damit so etwas wie Brandschutz des 21. Jahrhunderts.

## Ein Angriff, der das Lebenswerk zerstören will

Bei einer Cyberattacke können sämtliche Daten im Unternehmen verloren gehen. Zwei Handwerksbetriebe berichten, wie sie sich vor Kriminellen schützen

Albert Pöllath hätte 2019 beinahe alle Daten seines Unternehmens verloren. Der Spezialist für Tore, Türen und Antriebe aus dem oberpfälzischen Erbendorf wurde Opfer einer Cyberattacke. Der Angriff kam überraschend, denn Pöllaths damaliger IT-Dienstleister beteuerte stets, dass der Betrieb gut geschützt sei und kein Grund zur Beunruhigung bestehe. Zunächst waren nur drei Computer im Netzwerk betroffen. Pöllaths IT-Berater sah weiter keinen Grund zum Handeln. Doch der Betriebsinhaber zeigte sich zunehmend beunruhigt und recherchierte schließlich selbst, ob sein Betrieb wirklich ausreichend geschützt sei. Das Ergebnis war niederschmetternd. Pöllath alarmierte den Dienstleister sofort eine neue externe Datensicherung anzulegen. Gerade noch rechtzeitig, wie sich wenig später herausstellte. Nur Stunden nachdem die langwierige Sicherung abgeschlossen war, verschlüsselten die Hacker das komplett Netzwerk. Nichts ging mehr.

**Betriebe sollten sich nicht erpressen lassen**

„In einem solchen Moment kann dein ganzes Lebenswerk, die viele Arbeit und das Geld, das du in deine Firma investiert hast, zerstört werden“, sagt Pöllath rückblickend. Glücklicherweise konnte der Betrieb mit der neuen Sicherung schnell wieder auf alle Daten zugreifen und seine regulären Arbeitsabläufe relativ schnell wieder aufnehmen. Auf die Lösegeldforderungen der Erpresser ging Pöllath nicht ein und rät auch anderen Betroffenen, dies nicht zu tun. „Sie haben keine Garantie, dass die Hacker das System wirklich wieder freigeben oder vielleicht nicht noch höhere Forderungen stellen.“

Pöllath nahm den Vorfall zum Anlass, die IT-Sicherheit in seinem Unternehmen zu hinterfragen und neu aufzustellen. Als Erstes wechselte er den IT-Dienstleister, über den er sich bis heute noch ärgert: „Es gibt leider einige schwarze Schafe auf dem Markt und Betriebe sollten genau hinschauen, mit wem sie zusammenarbeiten. Leider ist es für den Laien jedoch kaum möglich, gute von schlechten Anbietern zu unterscheiden.“ Pöllath empfiehlt, im persönlichen Gespräch einmal nachzufragen, ob der Dienstleister die 3-2-1-Regel kennt und beachtet. Nach dieser goldenen Regel sollten Daten immer dreifach auf zwei unterschiedlichen Medien gesichert werden, wobei sich eine davon außerhalb des Betriebs befindet.

Mit seinem neuen Dienstleister ist Pöllath hochzufrieden. Die Systeme wären deutlich weniger fehleranfällig als früher. Das sei eine andere Liga. Auch kleinere Betriebe sollten nicht versuchen, sich selbst um die hochkomplexe IT-Infrastruktur zu kümmern, sondern professionelle Unterstützung suchen. Denn es gebe einige Sicherheitsfaktoren, die der Unternehmer gar nicht allein überblicken könne.

**Anhänge und Links sind das größte Einfallstor**

Die Hardware ist ein zweiter Aspekt, auf den der Betriebsinhaber seit dem Angriff verstärkt achtet. Bei allen neuen Investitionen, die Pöllath in seine IT tätigt, denkt er den Sicherheitsaspekt von vornherein mit und wählt danach seine Technik aus. Einen großen Stellenwert haben für ihn zudem Schulungen, um bei den Mitarbeitern ein Sicherheitsbewusstsein aufzubauen. „Das Haupteinfallstor sind E-Mails mit infizierten Anhängen und Links, die unbedacht geöffnet werden.“ Nicht zuletzt rät Pöllath den Unternehmern, sich persönlich mit IT-Sicherheit auseinanderzusetzen. „Es geht schließlich um meine Existenz, die sollte ich nicht allein in die Hände anderer legen“. Der Betriebsinhaber informiert sich fortwährend, wie sich das Unternehmen am besten schützen lässt. Dazu zählt er momentan die Zwei-Faktor-Authentisierung. Dafür muss ein Nutzer seine Identität über zwei voneinander unabhängige Komponenten nachweisen, um einen Zugriff zum System zu erhalten. „Für die IT-Sicherheit gilt das gleiche, wie für alle Lebensbereiche: Hirn einschalten und mit offenen Augen durch die Welt gehen“, resümiert Albert Pöllath.

*Es geht um meine Existenz, die sollte ich nicht allein in die Hände anderer legen.“*

**Albert Pöllath**
Geschäftsführer
Josef Pöllath GmbH
Foto: privat

**Ein geplanter Angriff kann Schwachstellen aufdecken**

Christina Böhm führt das SR-Malereiunternehmen im oberfränkischen Strullendorf. Früher dachte die Betriebsinhaberin, dass ihre Firma mit rund 30 Mitarbeitern zu klein sei, um für Hacker ein attraktives Ziel zu sein. Doch inzwischen ist sie sensibilisiert, nachdem sie von immer mehr Angriffen auf andere Handwerksbetriebe hört, darunter ein Cyberangriff mit einem wirtschaftlichen Schaden von 150.000 Euro. „Glücklicherweise ist ein solcher Angriff bislang an uns vorübergegangen, aber wir dürfen uns nicht entspannt zurücklehnen.“ Sie hat sich deshalb Unterstützung bei der Handwerkskammer für Oberfranken geholt und mit dem Digitalberater Holger Bär einen sogenannten White-Box-Test durchgeführt. Das ist ein erlaubter Angriff auf das Firmennetzwerk, um Schwachstellen aufzudecken. Die Firewall erkannte den Angriff und koppelte alle Rechner automatisch vom Netzwerk ab, um eine Infizierung zu vermeiden. „Uns wurde gesagt, dass das die beste Reaktion ist und wir sehr gut vor einer Cyberattacke geschützt sind.

*Man muss am Ball bleiben, denn die Hacker tun es auch.“*

**Christina Böhm**
Geschäftsführerin
SR-Malereiunternehmen GmbH
Foto: Dominik Ochs Fotografie

Christina Böhm möchte aber noch mehr tun. So führt sie regelmäßig Mitarbeiterschulungen durch und will eine Cyberversicherung abschließen, um für den Ernstfall gewappnet zu sein. „Man muss am Ball bleiben, denn die Hacker tun es auch, sagt sie. **sg**



www.DHZ.net | 76. Jahrgang | 12. April 2024 | Ausgabe 7

# „Der Schaden kann existenzbedrohend sein“

Der Nutzen einer Cyberversicherung wird nach Einschätzung von Anja Käfer-Rohrbach, stellvertretende Hauptgeschäftsführerin des Gesamtverbandes der Deutschen Versicherungswirtschaft, viel zu häufig unterschätzt. Die meisten Betriebe würden sich immer noch zu sicher fühlen **INTERVIEW: STEFFEN GUTHARDT**

**Frau Käfer-Rohrbach, sind kleine Handwerksbetriebe für Hacker überhaupt interessant genug, um eine Cyberversicherung in Betracht zu ziehen?**

Auch ein kleiner Betrieb sollte sich nicht in Sicherheit wiegen. Gezielte Hackerangriffe auf einzelne Unternehmen sind eher die Seltenheit. Phishing-Angriffe werden hingegen immer häufiger automatisiert, möglichst breit und wahllos gestreut. Deshalb ist es relativ egal, welche Größe ein Unternehmen hat. Jeder kann das Pech haben, von einem Angriff betroffen zu sein.

**Die Zahl der Cyberangriffe nimmt zu. Spiegelt sich das in den Versicherungsabschlüssen wider?**

Wir führen regelmäßig Umfragen unter potenziellen Kunden von Cyberversicherungen durch. Dabei zeigt sich zwar, dass das Risikobewusstsein steigt, aber es noch sehr viel Luft nach oben gibt. Die Marktdurchdringung der Cyberversicherungen ist noch lange nicht dort, wo sie in Anbetracht der Gefahrenlage sein sollte.

**Werden die wirtschaftlichen Risiken eines Angriffs unterschätzt?**

Diesen Eindruck haben wir. Eine Betriebsunterbrechung infolge eines Cyberangriffs kann ein Unternehmen teilweise über Wochen erheblich einschränken. Auch ein Datenabfluss kann teuer werden. Der wirtschaftliche Schaden eines Angriffs kann erheblich und im schlimmsten Fall existenzbedrohend sein.

**Das Verständnis dafür scheint aber noch zu fehlen. Warum?**

Einerseits ist vielen Unternehmern die Digitalisierung nicht in die Wiege gelegt. Nur die wenigsten von ihnen sind bereits IT-Experten. Es bedarf deshalb viel Aufwand, um sich das notwendige Know-how anzueignen, um die Bedeutung der IT-Sicherheit und den Nutzen einer Cyberversicherung zu verstehen. Anderseits ist es auch Aufgabe von Maklern und Versicherern das komplexe Thema verständlich zu vermitteln.

**Ist für jeden Betrieb eine Versicherung sinnvoll?**

Grundsätzlich steigt mit zunehmender Digitalisierung im Unternehmen der Bedarf eines Schutzes. Ein Handwerker, der noch sehr analog arbeitet und den Computer lediglich nutzt, um neue Ware zu bestellen oder eine Kundendatei zu verwalten, kann sich diese berechtigte Frage stellen.

**Was kostet mich die Versicherung?**

Dies variiert und ist etwa von der Unternehmensgröße abhängig. Auch die aktuelle Schadensbelastung bei den Versicherern wirkt sich auf die Prämien in diesem noch jungen Segment aus. Ich kann dazu keine konkreten Zahlen nennen.

**Wie sollte ein Handwerker vorgehen, der sich absichern möchte?**

Der erste Schritt ist die Prävention. Solange der Betrieb nicht ausreichend vor IT-Sicherheitsrisiken geschützt ist, kann man die Obliegenheiten der Versicherer nicht erfüllen. Deshalb werden professionelle IT-Dienstleister benötigt, um sein Unternehmen entsprechend aufzustellen. Erst im nächsten Schritt sollte man mit den Versicherungen ins Gespräch kommen.

Anja Käfer-Rohrbach, stellvertretende Hauptgeschäftsführerin im Gesamtverband der Deutschen Versicherungswirtschaft. Foto: GDV

**Was ist mit Obliegenheiten gemeint?**

Versicherungsinteressenten füllen in der Regel zunächst einen Risikofragebogen aus. Hier werden die vorhandenen Sicherheitsstandards abgeklärt. Dazu zählen etwa vorhandene Datensicherungen und die Trennung zwischen Back-up und laufendem System. Auch bedarf es eines Rechtemanagements, sodass nicht jeder im Unternehmen auf sensible Geschäftsbereiche zugreifen kann. Weiterhin werden Mitarbeiterschulungen vorausgesetzt. Die Obliegenheiten können sich je nach Versicherer unterscheiden, die genannten Basics sollte ein Betrieb aber in jedem Fall erfüllen, um sich versichern lassen zu können bzw. einen bestehenden Versicherungsschutz nicht zu gefährden. Wir raten zudem, die Daten über eine Cloud zu verwalten und professionell abzusichern.

**Und welche Leistungen sollte die Versicherung in jedem Fall abdecken?**

Der Eigenschadenbereich ist die erste wichtige Säule. Eine Betriebsunterbrechung sollte genauso versichert sein, wie die Wiederherstellung verschlüsselter oder gelöschter Daten. Die zweite Säule ist der Drittschadenbereich. Ist mein System kompromittiert und ich leite unwissentlich einen Virus weiter, sollte die Versicherung auch die Schäden bei den Betroffenen abdecken. Ebenso den Fall, dass Kundendaten durch einen Hackerangriff an die Öffentlichkeit gelangen und Ansprüche gegen den Handwerksbetrieb geltend gemacht werden, weil ein Verstoß gegen die Datenschutzgrundverordnung vorliegt. Die dritte Säule sind die Kosten, die im Zusammenhang mit der Aufarbeitung des Hackerangriffs entstehen. Darunter fallen Forensikkosten für IT-Experten, die den Cyberangriff untersuchen. Optional ist es aus meiner Sicht auch die Kosten für Krisenkommunikation oder Reputationswiederherstellung durch die Versicherung abdecken zu lassen. Dies ist abhängig vom Einzelfall zu entscheiden.

**Sind Fehler der Mitarbeiter, etwa durch das Öffnen eines E-Mail-Anhangs, mitversichert?**

Solche Vorfälle sind üblicherweise abgedeckt. Zwar sollten Mitarbeiter geschult werden, damit sie eine verdächtige E-Mail erkennen können, aber ganz vermeiden lässt sich ein solches Risiko in der Praxis nicht. Die Phishing-Angriffe sind inzwischen so professionell, dass sich gefälschte Nachrichten teilweise kaum noch als solche erkennen lassen.

**Darf ich meine Mitarbeiter auch Zuhause arbeiten lassen, ohne den Versicherungsschutz zu riskieren?**

Remote zu arbeiten ist von den Versicherungen abgedeckt, alles andere wäre in unserer heutigen Zeit auch lebensfremd. Aber natürlich gelten die Obliegenheiten genauso für den privaten Bereich, in dem sich die Mitarbeiter befinden. Deshalb sollten im Homeoffice nur Arbeitsgeräte der Firma zum Einsatz kommen. Üblicherweise greifen die Mitarbeiter über eine abgesicherte VPN-Verbindung auf die Firmendaten zu. Der Zugriff über Privatrechner oder ein offenes WLAN sind zu vermeiden, um den Versicherungsschutz nicht zu verlieren.

**Zahlt die Versicherung auch für einen Ausfall bei meinem IT-Dienstleister?**

Wenn der Dienstleister die vereinbarte Leistung nicht in vertraglich festgelegter Form erbringt, weil etwa die Integrität der Daten nicht mehr gesichert ist, diese verändert wurden oder an die Öffentlichkeit geraten, besteht Versicherungsschutz. Anders sieht das aus, wenn die Leistung komplett ausfällt, weil es zum Beispiel einen Brand beim IT-Dienstleister gibt. In diesem Fall ist er gegenüber dem Handwerksbetrieb schadensersatzpflichtig. Der Versicherungsschutz des Handwerksbetriebs greift hier nicht mehr.

**Cyberangriffe werden häufig von Staaten organisiert. Bin ich auch dagegen geschützt?**

Grundsätzlich enthalten alle Policen einen Kriegsausschluss. Auch wenn Angriffe ohne Kriegserklärung stattfinden, handelt es sich um einen kriegsähnlichen Zustand, sobald kritische Infrastruktur angegriffen wird. Hier greift deshalb kein Versicherungsschutz. In der Praxis lässt sich allerdings oftmals schwer feststellen, ob der Angriff tatsächlich von einem Staat verübt wurde.

**Cybersicherheit im Check**

Es vergeht wohl kaum ein Tag ohne einen erfolgreichen Hackerangriff auf Unternehmen in Deutschland. Um sich darauf vorzubereiten, bietet der Gesamtverband der Deutschen Versicherungswirtschaft ein Online-Tool, das die IT-Sicherheit auf den Prüfstand stellt. Zudem gibt es eine Übersicht zu Anbietern von Cyberversicherungen sowie ein Video, das verständlich erklärt, wie die Versicherung im Schadensfall hilft. Mehr Informationen unter www.gdv.de/gdv/themen/digitalisierung/cybersicherheit

**So steht es um die IT-Sicherheit**

Entwicklung in Deutschland 2023