Digitalgespräch Folge 27

Sterben, Trauern und Vermächtnis: Was ändert sich durch Digitalität?

Mit Florian Salm von der Gothaer Allgemeine Versicherung AG und Ulrich Greveler von der Hochschule Rhein-Waal, 27. September 2022
https://zevedi.de/digitalgespraech-027-florian-salm-ulrich-greveler/

[Der Vorspann mit Musik und Ausschnitten aus dem Gespräch beginnt.]

Marlene Görger [mg]: Herr Greveler, Sie sind Professor für angewandte Informatik, insbesondere für IT-Sicherheit. Mit Ihnen haben wir einen Experten für die technischen Aspekte bei der Frage nach Cyberrisiken zu Gast.

Ulrich Greveler [Greveler]: Wenn schon eine Versicherung sagt: "Wir versichern euch nicht, das ist ja Kraut und Rüben eure IT", dann hat das ja auch eine gewisse Aussagetiefe. Wir müssen grundsätzlich davon ausgehen, dass wer Software einsetzt, setzt auch fehlerhafte Software ein.

Petra Gehring [pgg]: Wir sind heute zum ersten Mal zu viert im Digitalgespräch.

[mg]: Herr Salm, Sie sind Senior Underwriter für den Bereich Cyber bei der Gothaer Versicherung.

[pgg]: Kann man Betroffene, gerade von so einer erpresserischen Attacke, beraten und machen Sie das auch?

Florian Salm [Salm]: Es gibt jetzt keinen Königsweg. Ist denn die Zahlung des Lösegeldes der bessere oder der schlechtere Weg? Das ist immer wieder eine einzelfallbasierte Entscheidung. Das kann man sich vorstellen wie bei einer Personenentführung. Da haben die wenigsten Erfahrungswerte: Wie gehe ich denn mit einem Entführer um?

[Greveler]: Dann holen wir so einen Hacker, der soll uns hier mal auseinandernehmen und uns sagen, wo die Schwächen sind. Dann schließen wir die Schwächen und dann haben wir das Thema abgehakt. Das funktioniert nicht.

[Der Vorspann endet, das Gespräch beginnt.]

[mg]: Wenn etwas nicht so läuft, wie es soll, und dadurch finanzielle Schäden entstehen, hat man hoffentlich in besseren Zeiten eine passende Versicherung abgeschlossen. In unserer vom Finanziellen durchdrungenen Welt sind praktisch keine Lebensbereiche von wirtschaftlichen Abwägungen ausgeschlossen. Und so gibt es auch zahlreiche Versicherungen, die mehr oder weniger viel Sinn machen. Zu manchen Abschlüssen sind wir als BürgerInnen und Unternehmen in Deutschland

verpflichtet. Man denke z.B. an die Kfz -Versicherung. Der individuellen Risikofreudigkeit sind hierzulande also ein paar Grenzen gesetzt. Auch wenn die meisten freiwilligen Versicherungen, der No-Brainer-Haftpflicht eingeschlossen, eine Frage des individuellen Typs und Lebensstils sind. Wir haben das Gefühl, die Gefahren, in die wir uns begeben, oder eben nicht gut genug abzuschätzen, um für uns selbst und unser Handeln Verantwortung übernehmen zu können, auch gegenüber anderen Menschen. Wir vertrauen unserer Urteilskraft und vielleicht auch darauf, dass schon alles gut gehen wird. Das heißt auch, dass wir im Zweifelsfall bereit sind, unangenehme Konsequenzen zu tragen. Wie sieht das aber aus in der digitalen Welt, deren technische Basis, ein System von Systemen, niemand überschaut? Unsere Sinne liefern an den auditiven, visuellen und mittlerweile auch haptischen Schnittstellen der allermeisten EndnutzerInnen wenig Aussagekräftiges darüber, wie sicher die IT dahinter läuft. Kleine Fehler und jahrelang unentdeckte Schwachstellen können plötzlich und in rasender Geschwindigkeit enorme Auswirkungen haben. Je vernetzter wir werden, desto umfassender sind die Schäden. Und eine besonders große, vielleicht die größte Gefahr für IT-Systeme geht von Kriminalität aus. Die Zahl der Cyberattacken auf Unternehmen, staatliche Einrichtungen, kritische Infrastruktur und auch Privatpersonen nimmt von Jahr zu Jahr zu. Wie ist es möglich, solche IT-Risiken zu kalkulieren, die für den Laien überwältigend komplex scheinen? Und dann auch noch so präzise, dass man dagegen Versicherungen anbieten kann. Darüber sprechen wir heute im Digitalgespräch. Mein Name ist Marlene Görger, ich bin Physikerin und Technikphilosophin am Zentrum verantwortungsbewusste Digitalisierung.

[pgg]: Und ich bin Petra Gehring, Professorin für Philosophie an der TU Darmstadt. Wir sind heute zum ersten Mal zu viert im Digitalgespräch. Denn bei uns in der Videokonferenz und im Gespräch ist zum einen Florian Salm, zugeschaltet aus Köln, und zum anderen Professor Ulrich Greveler aus Essen. Hallo und herzlich Willkommen an Sie beide beim ZEVEDI-Podcast in dieser Runde!

[Greveler]: Hallo.

[Salm]: Hallo auch von meiner Seite. Freue mich, hier zu sein.

[mg]: Herr Salm, Sie sind Senior Underwriter für den Bereich Cyber bei der Gothaer Versicherung. Was genau sich hinter dieser Berufsbezeichnung verbirgt, lösen wir gleich auf. Zudem sind Sie Dozent für Versicherungsrecht an der Uni Hamburg. Dort lehren Sie zum Thema Cyber-Risk-Insurance. Was es mit der Cyber-Risikobewertung auf sich hat und wie man als Versicherer damit umgeht, darüber werden wir heute ausführlich sprechen. Vorher möchte ich aber noch unseren zweiten Gast vorstellen. Herr Greveler, Sie sind Professor für angewandte Informatik, insbesondere für IT-Sicherheit. Sie forschen und lehren an der Hochschule Rhein-Waal und befassen sich mit der Bewertung und Minimierung von IT-Risiken. Zu Ihren Arbeitsfeldern gehören außerdem Datenschutz und Digitalisierung von Verwaltung. Zudem sind Sie als Gutachter und Berater für IT-Sicherheit tätig. Mit Ihnen haben wir also einen Experten für die technischen Aspekte bei der Frage nach Cyberrisiken zu Gast. Vielleicht steigen

wir gleich mal ganz konkret ein. Herr Greveler, hätten Sie mal ein Beispiel für die Fälle, in denen Sie in letzter Zeit hinzugezogen wurden?

[Greveler]: Ja, ich habe diese Woche tatsächlich mit einem IT-Leiter eines Unternehmens gesprochen. Also ich hatte auch vorher schon mit ihm Kontakt, aber er hatte sich wieder mal gemeldet mit aktuellen Informationen. Der hat so einen richtig heftigen Cyber-Vorfall durchlitten, also er und auch das gesamte Unternehmen. Das kann man sich hier so vorstellen: Also ein kunststoffverarbeitendes Unternehmen, und mitten in der Woche, die Mitarbeiter kommen morgens zur Arbeit und melden sich bei der IT, dass einige PCs nicht mehr so responsiv sind, dass die Anwendungen nicht mehr funktionieren oder dass Dateien zu fehlen scheinen, der Zugriff zu lange dauert. Und das führt schon zu einer enormen Stresssituation, wenn sich mehrere Nutzer auf einmal melden, darunter vielleicht auch Entscheidungsträger, die dann noch mit mehr Druck dahinter eine Lösung verlangen. Und das führte, wie gesagt, zu einem steigenden Stresslevel. Er hatte auch einen Verdacht, leider eine falsche Fährte. Schließlich meldeten sich sogar Kollegen aus der Produktion und sagten, die Daten laufen nicht mehr ein. Wir wissen gerade gar nicht, was wir produzieren, welche Stückzahlen noch da sind. Und so wurde eine Baustelle nach der anderen aufgemacht, er konnte kaum noch priorisieren. Und erfuhr dann, und da war es noch nicht mal mittags, dass die ersten Produktionsmaschinen sogar stehen geblieben sind und dass gerade die Produktionslogistik zusammenbricht. Das heißt, dann fehlen die Teile für den nächsten Prozess. Das heißt, das Unternehmen erlitt an diesem Tag eine Betriebsunterbrechung. Wie man später erfahren hat, war das eben eine Cyberattacke. Es hatte sich eine Malware ausgebreitet, die kam über eine E-Mail rein. Aber das wusste er natürlich in dem Moment noch nicht. Das heißt, er brauchte erst mal einige Stunden, um überhaupt auf die Idee zu kommen, dass es sich um eine Attacke handelt, und dann auch sich zu überlegen, welche weiteren Schritte nötig sind. Und jetzt in der Retrospektive hat man natürlich da so in aller Ruhe einen entspannten Blick wieder da drauf. Gerade als Außenstehender ist das viel einfacher, als wenn man davon betroffen ist, und kann jetzt feststellen: Es ist wirklich hier ein Millionenschaden entstanden, weil eben über einen Zeitraum von – es waren so gute zwei Wochen bis die Produktion auch wieder lief und die vertrieblichen und logistischen Prozesse wieder angelaufen sind, weil so lange eben im Unternehmen fast nichts richtig funktioniert hatte. Und jetzt ist man aber auch immer noch einige Wochen später mit Aufräumarbeiten beschäftigt. Das ist so ein typischer Fall, diese Malware, also sprechen wir über bösartige Software, die eben in ein Unternehmen ja eingebracht wird, meistens mit dem Ziel von Erpressung oder auch manchmal Sabotage. Die kann eben heutige Industrie, aber auch kaufmännische, auch Handelsunternehmen, auch öffentliche Verwaltungen vollständig oder auch zu einem großen Teil außer Gefecht setzen.

[mg]: Herr Salm, Sie sind Senior Underwriter. Ich gebe zu, ich musste nachschauen, was das bedeutet, bin aber fündig geworden. Wenn ich richtig verstanden habe, zeichnen Sie Vertragsabschlüsse, für die es keine Standardvereinbarungen gibt. Das heißt, Sie müssen für diese besonderen Situationen auch die Risiken bewerten. Wenn

wir uns jetzt anhören, das Szenario, das Herr Greveler gerade geschildert hat, ist das ganz typisch oder wäre das schon ein Fall, bei dem Sie als Versicherer eine Rolle spielen würden?

[Greveler]: Ja, also das ist ein typisches Szenario, was wir als Versicherer häufiger sehen. Also die von Herrn Greveler geschilderte Attacke in Bezug auf eine Ransomware-Attacke gegenüber einem Versicherungsnehmer ist aktuell auch der Versicherungsfall oder die Meldung bei einer vorhandenen Police, welche am häufigsten vorkommt. Wie insgesamt die Versicherungspolice gestaltet ist, welche auslösenden Prozesse oder Faktoren eintreten können, damit diese greift, kommen wir mit Sicherheit im späteren Zeitpunkt noch dazu. Aber der geschilderte Fall von Herrn Greveler ist durchaus ein Fall, mit dem wir uns bei der Versicherungsgesellschaft beschäftigen würden, sofern denn eine Versicherungspolice besteht.

[pgg]: Ich nehme jetzt erstmal mit: Man kann sich dagegen versichern. Das ist ja schon eine eindrucksvolle Vorstellung, wenn es so ist, wie Herr Greveler sagt, dass da über mehrere Wochen das Unternehmen stillliegt, also Produktionsausfälle und so weiter. Das sind ja große Risiken, nicht nur jetzt für das Unternehmen, sondern auch für den Versicherer.

[Greveler]: Absolut. Also wie das Cyberrisiko, gibt es ja für Unternehmen viele Risiken, die zu bewerten gelten. Also innerhalb meines Riskmanagements habe ich ja beispielsweise das Risiko auch eines Feuers, was ich absichern muss. Und als Risiko dazu kann ich auch die Cybergefahr nennen. Das heißt natürlich, infolgedessen kann ein Unternehmen mehrere Tage, mehrere Wochen stehen, entweder komplett oder in Teilen seiner Produktion beispielsweise. Und das kann natürlich dann, neben den Sachwerten, die vielleicht kaputtgehen können, auch zu Produktionsausfällen führen. Und diese müssen oder können dann durch eine Cyberversicherung, in dem Fall, wenn es ein Cyberversicherungsfall war, ersetzt werden.

[mg]: Wie grenzt man das denn gegeneinander ab? Generell IT-Risiken gegen Cyberrisiken?

[Greveler]: Jetzt hoffe ich, dass ich die Frage einigermaßen richtig verstehe. Also ein IT-Risiko kann ja unterschiedlich sein. Es kann eine Hardware versagen, es kann vielleicht auch ein physischer Angriff sein, es kann ein Hackerangriff sein, es kann menschliches Versagen sein. Also all das sind ja Risiken. Wir sprechen jetzt erst mal noch über Risiken, die ein Unternehmen treffen können. Im zweiten Schritt, wenn die Versicherung ins Spiel kommt, geht es eben um die Risiken, die auch innerhalb der Police oder innerhalb der Deckungsbausteine versichert wären oder versichert sind. Wenn ich jetzt den Blickwickel habe eines Risikomanagers eines Unternehmens, muss ich natürlich alle Risiken betrachten. Im zweiten Schritt kann ich gucken, kann ich diese auch transferieren, beispielsweise über eine Police. Das ist bei jedem Risiko, deswegen eingangs auch das Beispiel über das Feuer, das Gleiche. Da könnte ich auch sagen: Mensch, ich erkenne das Risiko Feuer, ich will das transferieren, oder ich

verlasse mich darauf, dass keins passiert oder die Feuerwehr oder wie auch immer, als wenn man das als Risikomanager dann sieht.

[mg]: Gibt es Schäden, bei denen unklar ist, ob es ein Cyberfall ist oder was anderes?

[Greveler]: Ja, kann es natürlich durchaus geben. Also der klassische Fall, dass ich natürlich in der Früh jetzt ins Unternehmen komme und beispielsweise kein Bildschirm mehr geht, kann natürlich sein: Es ist die Hacker-Attacke. Es kann aber auch sein, dass es ein Stromausfall ist oder das Internet funktioniert nicht. Es kann vielleicht aber auch von den Reinigungskräften am Wochenende etwas schiefgegangen sein. Es kann aber vielleicht auch irgendwo ein Server überhitzt gewesen sein oder es kann vielleicht irgendwo ein Rohrbruch gewesen sein. Also es gibt unterschiedliche Themen. Trotz alledem wollen wir natürlich sagen, wenn ich einen Verdachtsfall habe, dass beispielsweise ein Cyberangriff vorliegen könnte, also das heißt, ein auslösender Versicherungsfall. Halten wir unsere Kunden dazu an, uns anzurufen, uns zu kontaktieren, damit wir der Sache näher auf den Grund gehen können.

[pgg]: Herr Greveler, Sie hatten auch gerade wissend genickt, als es um die Frage der Unterscheidbarkeit geht. Werden Sie da als Sachverständiger auch manchmal gefragt: War es jetzt ein Angriff oder war es einfach was anderes, ich sage jetzt mal, rein Technisches?

[Greveler]: Ja, das gehört tatsächlich zu meinem Aufgabenspektrum, dass dann eben plausibilisiert wird, inwieweit die Darstellung eines Schadens dann eine eindeutige oder wahrscheinliche überhaupt technische Ursache hat. Es kann ja auch ein menschliches Versagen oder ein menschlicher Fehler sein. Und inwieweit es einem absichtlichen Angriff, also das, was so langläufig so als Hacker-Attacke oder so bezeichnet wird, zuzuordnen ist. Oder vielleicht auch, wie es eben Herr Salm auch beschrieben hat, eine andere Schadensursache hatte, wie zum Beispiel jetzt Strom, Wasser, Feuer und so weiter. Zudem gibt es natürlich auch Grenzfälle. Also wir sprechen auch von Cybergefahren, wenn Rechner Tatmittel sind. Da geht es zum Beispiel auch oft um finanzielle Überweisungen. Man täuscht einen Menschen mithilfe einer gefälschten E -Mail und dann wird Geld auf ein falsches Konto überwiesen. Einen solchen Angriff kann ich mit gefälschten E-Mails machen, aber auch mit dem Telefonhörer oder mit anderen trickreichen Maßnahmen. Und dann verschwimmt das natürlich. Mir ist natürlich jetzt mit meiner technischen Brille dann fast egal, welche der Versicherungen eines Kunden zahlt, Hauptsache ihm wird geholfen. Aber jetzt für die beteiligten Parteien ist natürlich wichtig zu wissen: Haben wir jetzt hier einen Cyberschaden oder etwas anderes oder möglicherweise auch ein Fehlverhalten auf der einen oder anderen Seite. Und dann werden eben Gutachter benötigt, die dort auch eine Zuordnung treffen und vielleicht überhaupt auch die Tatschilderung plausibilisieren können, verschiedene Fälle auseinanderhalten können, weil das doch eine hohe Komplexität erreichen kann.

[pgg]: Herr Salm, Sie sind ja seitens der Versicherer sicherlich auch daran interessiert zu sehen, welcher Typ von Schaden oder welcher Typ von Risiko ist wie wichtig für Unternehmen, insbesondere die Sie versichern wollen. Und da haben Sie doch sicher einen Eindruck. Also was kommt wie häufig vor, grob gesagt?

[Salm]: Ja, also natürlich, wie eingangs schon mal kurz erwähnt, ist die Ransomware-Attacke die aktuell häufigste Attacke, die wir sehen. Also sprich, es passiert ein Angriff auf das System des Versicherungsnehmers und dort werden Systeme verschlüsselt und gleichzeitig werden auch Lösegeld-Forderungen eines Unternehmens weitergegeben, die dann häufig auch bewiesen werden, Mensch, ich zeig dir, ich habe wirklich von dir Daten entwendet, die könnte ich benutzen, ich könnte die betroffenen Personen kontaktieren, ich könnte die veröffentlichen und so weiter. Gleichzeitig habe ich eben mit dieser Ransomware-Attacke dann auch Nebeneffekte, das heißt, die von Herrn Greveler da beispielsweise skizzierte Betriebsunterbrechung oder Betriebseinschränkung von den Abläufen her. Gleichzeitig habe ich dazu Wiederherstellungskosten und, und, und. Also das ist beispielsweise ein Szenario, was wir sehr, sehr häufig sehen. Darüber hinaus gibt es Denial-of-Service-Attacken, beispielsweise häufig bei Unternehmen, die einen Internet-Online-Handel, beispielsweise in einem Web-Shop, betreiben. Diese Szenarien ist das, was wir häufiger sehen. Ein bisschen exotisch ist vielleicht auf der anderen Seite auch ein übermotivierter Mitarbeiter, das heißt, ein Innentäter, der dort quasi sein Unwesen treibt von innen heraus und das Unternehmen sabotiert und dort eben auch Kosten oder Betriebsunterbrechungen auslöst.

[mg]: Was bieten Versicherungen denn dann an? Also gerade diese Ransomware-Attacken, das ist natürlich extrem bedrohlich und ganz unterschiedliche Ausgänge der Situation sind denkbar. Was greift dann?

[Salm]: Also die Police oder die Leistung des Versicherers in der Cyberversicherung kann man grob in drei Kategorien teilen. Auf der einen Seite habe ich die Haftpflicht-Komponente. Das heißt, ich habe beispielsweise Daten Dritter gespeichert, für die ich verantwortlich bin. Die werden entwendet. Und danach kommen Schadensersatzansprüche auf mich zu als Unternehmen. Und gleichzeitig habe ich neben den Schadenersatzansprüchen beispielsweise auch noch die Prüfung derer, ob denn überhaupt rechtens sind. Auf der anderen Seite habe ich beispielsweise eine große Eigenschadenkomponente. Sprich, die Betriebsunterbrechung steht da ganz im Vordergrund, aber vielleicht auch die Lösegeldzahlung, die an mich gerichtet wird. Wiederherstellungskosten beispielsweise. Und die dritte große Säule bei der Cyberpolice ist die Assistenzdienstleistung. Das heißt, hier wird beispielsweise Stichwort Forensik kommen. Das heißt, externe Mitarbeiter oder Forensiker gehen dann auf den Versicherungsnehmer zu, suchen dort den Patienten Null beispielsweise oder aber auch rechtliche Beratung. Ich habe einen Datenschutzvorfall. Wie ist der zu bewerten? Muss ich auf die Behörden zugehen? Ich habe eine Meldepflicht gegebenenfalls und werde dorthin gehend beraten. Oder auch das PR-Thema. Wie gehe ich denn überhaupt mit einem Cyberangriff um innerhalb des Netzes, innerhalb

der Öffentlichkeit? Wie gehe ich mit meinen Mitarbeitern um, mit meinen Kunden, meinen Dienstleistern und so weiter. Also es ist ein großes Portefeuille an auf der einen Seite Entschädigungsleistungen und Prüfungen, aber auch an Dienstleistungen, die die Versicherer in dem Fall bieten.

[pgg]: Kann man Betroffene, gerade von so einer erpresserischen Attacke, beraten? Machen Sie das auch? Also die werden sich ja dann auch fragen, wie verhalten wir uns denn jetzt? Sollen wir da, keine Ahnung, zahlen? Sollen wir das ignorieren oder was auch immer?

[Salm]: Das ist eine sehr interessante Frage, weil das natürlich für die meisten Unternehmen absolutes Neuland ist. Also das kann man sich vergleichsweise vorstellen, wie wirklich bei einer Personenentführung. Da haben die wenigsten Erfahrungswerte: Wie gehe ich denn mit einem Entführer um? Also in der Kommunikation jetzt. Hier ist es ähnlich. Es gibt quasi Dienstleister, die die Kontaktaufnahme oder die Verhandlungen mit einem Erpresser auf der anderen Seite, also in dem Fall dem, ich sage mal, Täter, der hinter dieser Ransomware-Attacke steht, führen und dort dann eine Verhandlungsposition einnehmen. Und die zum Wohle des Unternehmens, sage ich jetzt einfach mal so, denn, Klammer auf, es gibt jetzt keinen Königsweg, ist denn die Zahlung des Lösegeldes der bessere oder der schlechtere Weg? Das ist immer wieder eine einzelfallbasierte Entscheidung. Aber sowohl die Verhandlung als auch natürlich am Schluss, beispielsweise die Zahlung, Stichwort Bitcoin, erfolgt über einen Dienstleister, der in diesem ganzen Versicherungspaket enthalten ist.

[pgg]: Herr Greveler, hat das auch eine technische Komponente? Diese Ransomware-Fälle sind natürlich, regen die Fantasie an. Kann man da auch technisch irgendwie dagegenhalten als Unternehmen, oder können Sie allenfalls klassifizieren, was für ein Typ von Angriff das ist?

[Greveler]: Sie meinen, wenn es schon passiert ist? Die technische Komponente wird meistens durch einen sogenannten Forensik-Dienstleister dann abgebildet. Der übernimmt dann eine ähnlich wichtige Rolle wie der andere Krisenberater, den gerade auch Herr Salm umschrieben hat. Der kommt dann auch eben notfalls mit einem ganzen Team von Spezialistinnen und Spezialisten, die dann wirklich vor Ort Systeme sich anschauen, vielleicht auch Netzwerke unterbrechen, schnelle Hilfe geben, umschalten können, vielleicht auf nicht infizierte Systeme. Dazu ist ein spezielles Wissen notwendig, auch Beweise richtig zu sichern, und um keine Fehler in der ersten Reaktion zu machen. Die meisten IT-Abteilungen hatten ja noch gar keine Erfahrung mit dieser Art von Ereignis. Und schon aus diesem Grunde ist es sehr gut, sich dann spezialisierter Hilfe zu bedienen. Gerade die Unternehmen, die jetzt auch dort beraten sind, auch eine Cyberversicherung haben, haben natürlich auch dann eine feste Kontaktliste von solchen Ansprechpartnerinnen und Ansprechpartnern, die dann auch vor Ort erscheinen. Was ich hier auch gerne noch dazusagen möchte, ist: Sprechen Sie auch mit der Polizei, also wenn Sie mal betroffen sind. Da gibt es komischerweise eine

gewisse Scheu, sowohl bei Privatpersonen als auch bei betroffenen Unternehmern. Es ist aber nicht mehr so, falls es überhaupt mal in jüngerer Vergangenheit so war, also es ist, glaube ich, schon 20 Jahre her, aber heute ist es nicht mehr so, dass es da keine Spezialisten gäbe. Das heißt, es gibt auch bei jedem Landeskriminalamt Ansprechpartner für solche Cyberinzidenz. Und es kann überhaupt nicht schaden, eine polizeiliche Anzeige zu stellen. Es ist übrigens auch nicht verboten, ein Lösegeld zu zahlen. Das ist manchmal auch so ein Gerücht, was da schnell aufkommt. Also, die Polizei wird Ihnen das nicht verbieten, den Täter auch noch zu bezahlen. Aber aus fachlich-ethischer Sicht würde ich generell davon abraten, also im Zweifel kein Lösegeld bezahlen. Nur unter ganz bestimmten Umständen ist das eine sinnvolle Entscheidung.

[Salm]: Genau, vielleicht ganz kurz als Ergänzung. Wir haben eben auch schon erfahren, dass das eine oder andere Unternehmen genau aus diesen ethischen Gründen, wie Herr Greveler das genannt hat, gesagt hat: Auf keinen Fall würden wir ein Lösegeld bezahlen. Und das kommt immer wieder häufig vor. Und es ist eben wie gesagt jedes Mal eine Entscheidung. Und es gibt, glaube ich, da auch noch keinen Königsweg, dass man sagt, wenn der Versicherer sagt, zahle auf jeden Fall das Lösegeld. Oder der Unternehmer sagt, ich zahle es auf jeden Fall. Und der Versicherer sagt nein. Also es ist jedes Mal ein in die Hand geben und sich auch für die bestmögliche Lösung entscheiden. Denn man muss ja auch so ein bisschen dann weitergucken: Wie kann das Unternehmen denn damit mit seiner Entscheidung weitermachen oder auch weiter gut leben, auch in seiner moralischen Vorstellung.

[mg]: Herr Greveler, Ihr Fachgebiet ist ja nicht nur die Bewertung beziehungsweise die Begutachtung im Schadensfall, sondern auch die Minimierung von IT-Sicherheitsrisiken. Was hätten Sie da für Hinweise? Was sind die häufigsten Fehler, sage ich jetzt mal, die Unternehmen machen?

[Greveler]: Ja, da gibt es ganz unterschiedliche Dinge. Also wenn wir Sicherheitsrisiken in Unternehmen zu bewerten versuchen, schaut man sich natürlich auch an: Wie groß ist erstmal die Abhängigkeit vom Digitalen an sich? Das ist ja schon mal sehr unterschiedlich ausgeprägt. Also wenn Sie jetzt an einen kleinen Unternehmer denken, vielleicht bei Ihnen an der Ecke, der etwas verkauft oder etwas zubereitet, Lebensmittel zum Beispiel, der hat vielleicht nur eine Kasse oder vielleicht ein Bestellsystem dahinter, der würde vielleicht zurecht sagen, also wenn die Rechner hier alle ausfallen, dann komme ich mit Papier nochmal hin. Das ist zwar umständlich, aber ich habe hier keine Betriebsunterbrechung. Meine Kunden finden mich auch so. Das ist so das eine Extrem, da gibt es fast kein Cyberrisiko. Das ist aber nicht die Regel. Und bei mittelständischen Unternehmen, bei produzierenden Unternehmen und ab einer gewissen Größenordnung ist es eben so, dass digitale Systeme einen wesentlichen Teil der Wertschöpfung bilden. Zum Beispiel im Logistiksektor. Sie können dann besonders effizient, also auch kostengünstig etwas liefern, wenn alle IT-Prozesse sehr schön ineinandergreifen, wenn da kein Mensch nochmal dazwischen muss, wenn das alles so automatisch funktioniert. Und diese Unternehmen haben natürlich eine hochgradige

Abhängigkeit von allen Systemen. Und dann schaut man sich eben genau an. Zum einen gibt es hier eine organisatorische Zuweisung. So, fühlt sich jemand hier auch verantwortlich für die IT und deren Sicherheit? Je größer ein Unternehmen, desto eher sollte das auch eine hauptberufliche Person sein. Dann schaut man sich eben an: Wie ist die Technik aufgestellt und welche Vorgaben gibt es dafür. Einige Unternehmen haben leider so eine einfache Vorstellung. Also oft so Familienunternehmer, die noch sehr autoritär regieren. Die sagen: Dann holen wir so einen Experten, so einen Hacker, der soll uns hier mal auseinandernehmen und uns sagen, wo die Schwächen sind. Dann schließen wir die Schwächen und dann haben wir das Thema abgehakt. Das funktioniert nicht. Also wir sehen IT-Sicherheit oder Informationssicherheit allgemein heute so als Prozess an, bei dem man eben so einen Zustand erreicht, wo man ständig in der Lage ist, solche Risiken zu erkennen, zu dämpfen. Und insbesondere Vorgaben hat es bis hin zu solchen ganz konkreten Richtlinien. Zum Beispiel werden Systeme ans Netzwerk angeschlossen. Wer darf welche Rechte zuweisen? Und das im Unternehmen eben zu einem Zustand führt, der allgemein risikodämpfend wirkt. Und je mehr von diesen organisatorischen Prozessen vorhanden sind und je mehr auch aktuelle technische Themen betrachtet werden, je schneller man auch reagieren kann, zum Beispiel neue Software verwendet und alte anfällige Versionen sehr schnell danach austauschen kann, desto besser ist eine Risikosituation. Und eine gute Risikosituation, ein geringes Risiko, ist auch eine gewisse Voraussetzung überhaupt, dass eine Cyberversicherung sich für ein Unternehmen interessiert.

[pgg]: Das wollte ich jetzt auch gerade fragen. Wird die Versicherung günstiger, wenn man als Unternehmen nachweisen kann, dass man eine sehr gute Sicherheitskultur vor Ort hat? Gucken Sie sich das an? Haben Sie dann sozusagen ein maßgeschneidertes Angebot, mit dem Sie honorieren können, wenn Unternehmen da Energie reinstecken?

[Salm]: Absolut ist es so, dass wir nicht jedes Unternehmen gleich bewerten. Vielleicht sollte man am Anfang ganz kurz auch den, wie soll man sagen, den Reifegrad vielleicht einer IT so ein bisschen klassifizieren. Also wir haben ja auch mitunter Gewerbekunden, die Versicherungswirtschaft, oder wir sagen jetzt in dem Fall Unternehmen bis 10 Millionen Euro Umsatz, beispielsweise um mal eine Größenordnung einzubringen. Und dann auch Industriekunden, das sind Unternehmen, die natürlich jetzt darüber liegen, wirklich Ende oben offen, bis hin zu den DAX-Unternehmen, die natürlich eine ganz, ganz andere IT-Ausstattung auch in der IT-Sicherheit vorweisen können – logischerweise, und das ist ja auch gut so. Deswegen sind auch von uns, von den Versicherungen her, die Anforderungen hinsichtlich der Mindestvoraussetzungen unterschiedlich. Mittlerweile, und ich benutze das Wort mittlerweile, ist es so, dass wir natürlich uns dafür interessieren, das auch honorieren, aber auch schon etwas als Mindestvoraussetzung dem Versicherungsnehmer gegenüberstellen. Das heißt, zu den Anfängen der Cyberversicherung in Deutschland, ich sag mal 2017, 2018, war es so, dass logischerweise der Prüfungsprozess ebenfalls vorhanden war, jedoch die Mindestvoraussetzungen noch nicht so streng gelegt worden sind, wie sie heute gelegt werden. Hat einfach den Hintergrund, dass wir von der Schadenfallentwicklung

sehen, dass diese Mindestvoraussetzungen, Herr Greveler hat eben einige davon genannt, sehr, sehr stark in den Fokus rücken. Und deswegen wollen oder möchten wir auch bei unterschiedlichen Unternehmensgrößen unterschiedliche Voraussetzungen sehen. Als Beispiel ist das Patch-Management schon eben genannt worden von dem Herrn Greveler, aber auch Awareness, Backup, Notfallmanagement. Es gibt einige Punkte, die man dort nennen kann und die von einigen Versicherern als absolutes Must-Have mittlerweile bewertet oder gesehen werden, dass eine Versicherung überhaupt zustande kommt. Und Ihre Eingangsfrage war ja, ob es dann günstiger wird. In dem Fall muss ich das günstiger streichen. In dem Fall muss ich sagen, dass wir überhaupt eine Versicherung darstellen können.

[mg]: Wie gehen Sie denn dann im weiteren Verlauf vor, wenn Sie jetzt wirklich ein Risiko abschätzen und auch eine Police festlegen wollen?

Florian Salm [Salm]: Also in der Praxis ist es so, dass wir uns natürlich erstmal Gedanken machen: Können wir das Risiko, und damit meine ich wirklich, ich kenne nur Name, Adresse, Umsatz, Branche, überhaupt versichern? Also das heißt, jeder Versicherer hat in der Regel Zeichnungsrichtlinien, mit denen er auf Risiken zugeht in der Bewertung. Wenn also das Risiko beispielsweise all diese Zeichnungsrichtlinien im positiven Sinne erfüllt, gehen wir in der Praxis so vor, dass wir dann über einen Risikofragebogen verschiedene Fragen aus dem Bereich Datenschutz als auch IT-Sicherheit abprüfen. Und im zweiten Schritt beispielsweise auch in einem Risikodialog mit dem Versicherungsnehmer zusammen weitere Fragen aus dem Fragebogen näher definieren. Und danach machen wir uns ein Bild, wie wir das Risiko einschätzen auf diese einzelnen Punkte hin und ob wir das versicherbar halten, und dann natürlich auch die Kalkulation der Prämie vornehmen. Und die beispielsweise dann fußt auf eben nochmal Branche, Versicherungssumme, der Selbstbehalt, der beispielsweise genommen wird, Standorte, aber auch Abhängigkeit von der IT an sich. Unsere Aufgabe ist es, die Versicherungsfälle, die denn dort passieren können, die Szenarien, sich eben vorzustellen. Also als Beispiel: Ist natürlich so, wenn ich sage, ich habe ein Unternehmen mit einer, ich sage mal, schlechten IT-Sicherheit, aber mit einem geringen Risiko, wie kann ich das bewerten? Oder habe ich ein Unternehmen mit einer wahnsinnig tollen IT-Sicherheit, aber einem enorm hohen Risiko? Also von der Eintrittswahrscheinlichkeit her: Wie gehe ich dann damit ran und kommt dann eben am Schluss die ganze Prämiengestaltung oder auch Angebotsgestaltung zur Geltung?

[pgg]: Jetzt ist das Ganze gleichzeitig aber auch ein dynamisches Feld. Sie haben das gesagt. Also das wird mehr. Zum Beispiel diese Ransomware-Konstellation. Möglicherweise spielt sogar die politische Weltlage dabei eine Rolle. Da müssen Sie dann vermutlich auch reagieren. Entweder auf die Gesamtentwicklung der Vorfälle oder vielleicht auch auf die Situation bei einem konkreten, bei Ihnen versicherten Unternehmen?

Florian Salm [Salm]: Absolut. Also, Sie sprechen es an. Die politische Situation ist natürlich jetzt seit Anfang des Jahres ein Thema, was uns alle bewegt und was

natürlich auch jetzt in der Cyberversicherungswelt die Spuren hinterlassen hat. Man hat ja die Vermutung geäußert, dass natürlich auch politisch motivierte Angriffe auf Unternehmen oder Infrastrukturen in den westlichen Ländern vor allem eintreten können. Dem hat man natürlich dann auch höheren Nachdruck geschenkt, dass man das so verfolgt. Als weiteren Punkt zum Beispiel dort zu nennen ist die Warnung vom BSI gegenüber dem Hersteller Kaspersky, der ja auch Programme anbietet, die viele Unternehmen auch einsetzen in der IT-Sicherheit. Und auch hier reagieren wir beispielsweise als Versicherer und nehmen das natürlich ernst und gehen dann auf die Versicherungsnehmer zu, die aktuell Kaspersky eingesetzt haben. Jetzt, um bei dem Beispiel zu bleiben, ist es natürlich so, dass dann der Unternehmer nicht von heute auf morgen sämtliche Produkte von Kaspersky austauschen kann. Aber gemeinsam mit dem Unternehmen möchten wir natürlich dann eine Lösung finden, damit wir auch für die Zukunft gut aufgestellt sind. Da ist jedes Versicherungsunternehmen unterschiedlich in der Herangehensweise, aber auch wir haben das Thema natürlich im Fokus und verfolgen das.

[mg]: Herr Greveler, wie würden Sie denn aus der technischen Sicht da draufgucken? Kann man sagen, dass wenn sich keine Versicherung findet für ein bestimmtes Setup oder eine bestimmte Systemarchitektur, dann hat das auch gute Gründe, denn diese Architektur ist so unsicher, dass man sie gar nicht realisieren sollte? Also kann man das so nebeneinanderlegen?

[Greveler]: Es gibt zumindest Unternehmen, die eine interne Vorgehensweise haben, die einem Versicherer nicht gefällt und die aber auch aus organisatorisch-technischer Sicht vorsichtig gesagt nicht dem Stand der Technik entspricht, oder wo ich eben auch als Informatiker sagen würde: Die verhalten sich einfach fahrlässig. Und dann stimmt das natürlich überein, dann wird ein Versicherer das nicht wollen und ich mit meiner fachlichen Brille kann dann auch nur sagen: Liebe Leute, ihr müsst da was ändern, ihr habt auch eine Verantwortung eurem Unternehmen gegenüber. Mir ist es ja fast egal, ob die versichert sind oder nicht, aber wenn die mich fragen, ob sie Risiken haben, dann würde ich die entsprechend auch benennen. Das sind zum Teil sogar auch gesetzliche Anforderungen an die Unternehmensleitung, an die Geschäftsführung. Also: Die müssen in der Lage sein, Risiken zu erkennen und auch solche zu beseitigen, die den Fortbestand des Unternehmens beispielsweise gefährden. Das gibt es hin und wieder. Das ist dann ein Vorgespräch, vielleicht für ein eigentliches Fachgespräch, auch mit IT-Leitung und anderen, vielleicht auch IT-Dienstleistern. Es gibt auch Unternehmen, die haben gar keine eigene IT, die haben es irgendwie verteilt auf verschiedene Dienstleister, haben auch keinen Überblick mehr darüber. Und dann kann ich auch manchmal unterstützen, da vielleicht etwas Grund reinzukriegen und mal zu fragen: Welcher Dienstleister macht was und wo ist hier die Verantwortung auch verteilt? In der Regel schafft man es, mit guten fachlichen Argumenten dann auch Unternehmer zu überzeugen, dann vielleicht auch etwas zu tun. Aber man muss auch offen sagen, es gibt natürlich Unternehmen, die haben andere Baustellen, die schreiben rote Zahlen, die haben vielleicht kein Investvolumen mehr übrig und die sparen dann auch an der Sicherheit. Kann ich Ihnen auch nicht immer verdenken, weil

ja, wie gesagt, das Unternehmen ist sowieso schon vielleicht in Schieflage. Und dann werden dort auch entsprechend höhere Risiken einfach hingenommen. Dass die dann keine Versicherung mehr kriegen, ist dann für ein solches Unternehmen vielleicht aber auch zweitrangig. Dann ist irgendwann so ein Moment erreicht, wo man erstmal nicht helfen kann. Dann ist vielleicht eher ein Unternehmensberater gefragt, der insgesamt das Schiff dort wieder auf Kurs bringt. Also da gibt es eine sehr große Bandbreite, sowohl an vorhandenen Risiken als auch an Fähigkeiten und Bereitschaften, daran etwas zu tun.

[Salm]: Vielleicht noch als Ergänzung, aus Versichererbrille: Die eher schwer versicherbaren Risiken, die ja auch angesprochen sind. Das Cyberrisiko an sich ist deswegen halt auch so schwer für uns, zu greifen, in der Assekuranz, weil man natürlich zwei Faktoren hat, die man hier beachten muss, die bei vielen anderen Risiken nicht da sind. Also auf der einen Seite ist diese fehlende Erfahrung bei uns über die letzten Jahrzehnte. Also bei anderen Risiken ist das da, bei der Cyberversicherung eben erst seit kurzer Zeit. Und das Zweite ist eben diese Dynamik, die Herr Greveler eben auch beschrieben hat, dass man sagt, gestern oder vorgestern ist definitiv nicht morgen. Das ist vielleicht bei dem Feuerbegriff ein bisschen anders zu sehen. Da kann ich mich eher darauf einstellen, was auf mich zukommt oder zukam. Und das ist in der IT-Sicherheit oder in diesen unterschiedlichen Angriffssektoren gar nicht mehr der Fall. Und das macht eben diese Kalkulation für den Versicherer extremst anspruchsvoll, dass man sagt: Finde ich wirklich die richtigen Stellschrauben in Bezug auf die richtige Branche, Mindestvoraussetzungen, Versicherungssumme, Selbstbehalte, versicherte Leistungen (und, und, und), also alles, was zu diesem Paket dazukommt, oder ist das im Zweifel sogar unversicherbar? Und am Schluss ist es bei den Versicherern eben so, dass auch eine große Mathematik dahintersteht und diese Eintrittswahrscheinlichkeit eine hohe Rolle spielt und dieses Verständnis von dem Risiko. Und das ist bei Cyber sehr, sehr anspruchsvoll.

[pgg]: Sie haben eben mit dem BSI noch einen dritten Player genannt, jetzt neben der Technik und der Versicherungsseite, die sozusagen auf die Unternehmen blicken, nämlich die Behörden, die sich auch darum kümmern. Also Bundesamt für Informationssicherheit, vielleicht auch Polizei, Staatsanwaltschaft, wie auch immer. Wie ist da Ihr Blick als Versicherung drauf? Finden Sie, dass die genug tun? Oder gibt es da auch noch Baustellen, wo Sie sagen, die Politik müsste eigentlich mehr machen oder die Administration in Deutschland?

[Salm]: Ich weiß es nicht, ob ich sofort den Staffelstab irgendwie in Richtung Politik übergeben wollen würde. Das ist immer eine schwierige Aussage. Aber es ist so, dass ich finde, die Eigenverantwortung von den einzelnen Unternehmen müsste natürlich wachsen. Und die Politik kann dort ein großes Verständnis schaffen. Also wie schon häufig erwähnt, ist eben die Auffassung der IT-Sicherheit in den einzelnen Unternehmen sehr, sehr unterschiedlich gelagert. Die einen setzen das Thema sehr, sehr hoch an, nicht nur von einer einmaligen Aktion, sondern als laufendes Projekt, nehmen auch verantwortliche Personen mit in die Pflicht und haben dieses Thema

immer auf dem Schirm, immer auf dem Radar, also angefangen von der Geschäftsführung bis hin zu den auswählenden Organen. Die anderen Unternehmen oder die Unternehmen, die vielleicht das Ganze natürlich irgendwo wahrgenommen haben, tun vielleicht noch nicht das, was man ausreichend dafür schaffen könnte, und haben auch ein falsches Verständnis von der gesamten Situation. Also wir sehen es auch immer wieder in der Kommunikation, auch direkt mit Versicherungsnehmern, als auch beispielsweise in diversen Umfragen, dass natürlich diese Eigenverantwortung für das Unternehmen nicht so ausgeprägt ist in der Form, dass man denkt, man ist selbst betroffen. Also man weiß um die Gefahr und auch ein Mitbewerber, die AGCS beispielsweise, die fragt jedes Jahr auch viele, viele Unternehmen an nach den größten Risiken weltweit, und da ist die Cybergefahr ganz, ganz oben mit dabei. Also sprich, alle Unternehmenslenker und Entscheider wissen eigentlich um diese Gefahr. Trotzdem ist sie noch nicht ganz oben angekommen in der Umsetzung, und das ist, glaube, ich ein Thema. Und wenn die Behörden, die Politik in diese Kerbe einsteigt, dann würde das mit Sicherheit allen weiterhelfen, denn eins ist klar: Wenn die Versicherungswirtschaft quasi hier einen Risikotransfer schaffen will und schaffen soll, ist es vonnöten, dass natürlich die Schäden nicht ins Unermessliche irgendwann abdriften, und das passiert oder kann nur passieren, wenn natürlich die Unternehmen auch dahingehend die Sicherungsmechanismen hochfahren.

[pgg]: Das heißt, es wäre eine klassische Erwartung, die Aufklärungsarbeit noch zu verstärken und das Bewusstsein zu verstärken?

[Salm]: Genau.

[mg]: Herr Greveler, Herr Salm hat ja vorhin schon mal angesprochen, dass ein Teil der Versicherungsleistung eben auch ist, zu prüfen, ob das Unternehmen überhaupt haftbar ist für Schäden, die entstehen. Kann man das in so Cyberzusammenhängen immer so genau sagen oder im Regelfall so genau sagen? Ich denke zum Beispiel an Angriffe, die möglich wurden im letzten Jahr durch Lock4Shell, wo dann natürlich Schwachstellen entstehen in ganz vielen Systemen. Da gibt es eine kleine Gruppe von Programmierern, die haben irgendein Modul bereitgestellt mit dem arbeiten dann alle. Wer ist dann letztendlich verantwortlich?

[Greveler]: Also verantwortlich jetzt zum Beispiel für einen Fehler in einer Software ist nicht jetzt notwendigerweise der- oder diejenige, die jetzt diesen Fehler programmiert hat, um Beispiele wie Lock4Shell oder andere heranzuziehen, sondern wir müssen grundsätzlich davon ausgehen, dass wer Software einsetzt, setzt auch fehlerhafte Software ein. Das ist so quasi schon ein Paradigma in der Softwareentwicklung. Es gibt keine fehlerfreie Software. Das heißt, auch hier ist erstmal ein Prozess vonnöten: Wie werde ich informiert, wenn eine Schwachstelle in der Software gefunden wird? Wie schnell kann ich darauf reagieren? Und wenn ich zum Beispiel jetzt noch keine neue Version habe, die einen Fehler beseitigt, dann sprechen wir von solchen Zero-Day-Attacken zum Beispiel. Also das ist dann der Tag 0 gerade. Ich erfahre, es gibt eine Sicherheitslücke, aber es gibt noch keinen Patch. Ich kann sie noch nicht schließen.

Dann brauche ich so einen Plan B. Da sprechen wir so ganz allgemein von einem Workaround, dass ich vielleicht etwas machen kann, was das Problem so weit entschärft, dass der Angreifer nicht mehr zugreifen kann, aber meine Produktion, mein System, mein Webserver oder so läuft noch im Notbetrieb weiter. Das sind wichtige Maßnahmen. Was überhaupt nicht hilft, ist, jetzt einem sowieso dann meistens nicht bekannten Programmierer, Programmiererin da eine Schuld zuzuweisen. Gerade solche Software aus dem Bereich Open Source wird letztlich von so einer Art Kollektiv erstellt. Das ist dann eine Partei, die aus sehr vielen Menschen besteht, wo einige programmiert, andere getestet, andere weiterentwickelt haben. Und wie gesagt, da sowieso keine fehlerfreie Software existiert, wäre es dort jetzt auch nicht sinnvoll, Verantwortlichkeiten zuzuweisen. Also verantwortlich ist der- oder diejenige, die die Software einsetzt, und dann eben dafür, auch Prozesse dafür in Kraft zu setzen, um notfalls zu reparieren, um die Software zu tauschen oder auch das ganze System erstmal außer Betrieb zu nehmen. Wenn es jetzt wirklich so eine sehr schwerwiegende Sicherheitslücke, wie das jetzt von Ihnen angesprochene Lock4Shell-Problem betrifft.

[mg]: Entstehen dann nicht auch neue Risikotypen, gerade wenn so vernetzte Produktions- oder Entwicklungsprozesse zum Einsatz kommen, auch vielleicht mit Blick auf große staatliche Infrastrukturen, wo dann Unternehmen beteiligt sind?

[Greveler]: Es entstehen hier tatsächlich so neue Typen von Risiken und da gibt es auch einige davon, die sind nicht versicherbar – oder jedenfalls passt da auch die Cyberversicherung als Typus nicht. Das ist auch etwas, das fragen auch Behörden oder manchmal auch Unternehmer: Wie kann ich mich eigentlich davor absichern, dass etwas nicht richtig funktioniert? Also die schaffen vielleicht ein neues Warenwirtschaftssystem an, und das ist heutzutage so ein Prozess, der zieht sich oft über Jahre von der Anforderung bis zur Lieferung, Integration und so weiter. Manchmal stellt sich heraus: Es geht nicht. Irgendeiner hat Fehler gemacht, meistens mehrere Personen, vielleicht wurden die Anforderungen nicht richtig erhoben, vielleicht wurde die Software tatsächlich nicht richtig programmiert oder falsch angepasst an das Unternehmen oder vielleicht sind die betriebswirtschaftlichen Prozesse von Anfang an dort auch nicht so richtig durchgeführt oder erfasst worden. Also kurzum: Am Ende hat man eine Softwarelösung, die nicht die Funktionalität hat, die das Unternehmen braucht, und ein großer Schaden ist da. Vielleicht muss man alles wieder zurückrollen, vielleicht verliert man alleine deswegen Aufträge. Da sehen Sie, das ist kein Schaden, der durch einen Angreifer ausgelöst wurde, sondern im Zweifel durch Pech beim Denken, oder vielleicht hat man auch einfach mal Pech bei so komplexen Projekten, die können gelingen oder auch schiefgehen. Also im Behördenbereich haben wir Projekte, die sind zehn Jahre gelaufen und dann wurden sie zurückgerollt. Diese Art von Risiken, die ist sehr real. Das ist Teil einer Digitalisierungsstrategie einfach, dass man solche Risiken eben auch kennenlernt. Für diese braucht man dann eben auch eine Lösung, und die lautet aber nicht unbedingt Versicherung. Also da muss man auch ein weiteres Riskmanagement betreiben. Daran arbeiten wir noch so ein bisschen, zu verstehen und auch Lösungsstrategien zu finden für solche Fälle.

[Greveler]: Gibt es so ganze Innovationspfade, die nicht verfolgt werden, weil sie nicht versicherbar sind?

[Greveler]: Das glaube ich nicht. Also es wird manchmal so vermutet, dass bestimmte Technologien nicht vorankommen, weil man nicht so genau weiß, wer haftbar gemacht wird oder wer versichert werden muss. Zum Beispiel beim autonomen Fahren ist das so ein häufig genannter Hinderungsgrund. Das halte ich aber eher für ein Gerücht. Also tatsächlich ist es so, also wenn etwas technologisch interessant ist, wenn es Fortschritte, mehr Effizienz oder mehr Funktion, mehr in dem Fall vielleicht auch Fahrvergnügen oder Ähnliches mit sich bringt, dann wird man dem schon erstmal nachgehen und auch in Forschung und Entwicklung versuchen, dort eben etwas Neues zu finden, ein neues Produkt oder eine neue Idee voranzubringen. Und dann hinterher zu sehen, natürlich gibt es irgendwann einen Punkt, wo man mal überlegen muss: Ist jetzt noch die Fahrerin verantwortlich oder der Hersteller oder vielleicht ein Dritter, der dort ein Telematiksystem bedient? Das ist eine komplexe Frage, auch mit vielen Akteuren, auch hier wieder so Ethiker, Juristen, Techniker und sicherlich auch irgendwann die Versicherungsexperten. Aber daran scheitert nicht die Innovation. Das kann man irgendwie schon hinkriegen, da auch eine Aufteilung zu finden. Dann ist es vielleicht am Ende auch 50-50 oder so. Aber dass deswegen eine Innovation behindert wird, ist mir nicht wirklich irgendwo mal aufgefallen.

[pgg]: Zum Stichwort Forschung, Herr Salm, natürlich wissen Sie als Versicherer unheimlich viel über Risiken, über konkrete Schadensszenarien, auch über die Dynamik in diesem Feld, also was verändert sich wie und so weiter. Ist für Sie Wissenschaft interessant? Also liefert die Wissenschaft Ihnen auch Wissen über Ihr Gebiet oder sind Sie als Versicherer so nah dran, dass Sie im Grunde mehr wissen als jeder Forscher oder jede Forscherin wissen könnte?

[Salm]: Das glaube ich nicht, dass wir da mehr wissen als andere. Ich würde es vielmehr so sagen, dass wir uns gerne dem Wissen anderer bedienen. Man muss ja so sehen, ich glaube, die IT-Sicherheit war natürlich bei den Versicherern schon seit vielen Jahren ein Thema, aber ich glaube eher für die eigene Gesellschaft und nicht auf Grund von einer Versicherungspolice, die dort irgendwo war. Und als dann die Cyberversicherung, in Deutschland war sie zum ersten Mal 2011 aktiv, nach Deutschland eben gekommen ist, also Ursprung ist eben USA und UK, da hat man sich natürlich auch mit diesem Thema IT-Sicherheit immer mehr und mehr befasst. Aber deswegen sage ich es: Von der Historie her hatte man natürlich jetzt nicht das Know-how oder die Fachkräfte, die dort einen weiterbringen können. Das heißt, mittlerweile sind die Versicherer besser aufgestellt als noch vor 10 Jahren, logischerweise. Haben auch eigenes Know-how aufgebaut und haben jetzt auch schon neben dem eigenen Wissen logischerweise auch noch externe Dienstleister mit im Boot. Wenn ich zum Beispiel jetzt an den Herrn Greveler denke, der eben auch im Audit-Bereich tätig ist, auch für die Bewertung eines Versicherungsrisikos, dann bedienen wir uns eben sehr gerne den Fachleuten, weil diese aus der Praxis, aber auch aus der Forschung mit

diesem Thema IT-Sicherheit und natürlich auch mit den Angriffsszenarien viel, viel länger schon zu tun haben. Und das Ziel sollte es natürlich schon sein, dass wir bei der Assekuranz immer mehr und mehr Fach-Know-how, eigenes Fach-Know-how aufbauen. Trotzdem denke ich aber, dass man niemals sagen sollte: Wir in unseren eigenen Vier Wänden haben das Wissen gepachtet, und jetzt verschließen wir uns dort dem Wissen von draußen. Das wird hoffentlich nicht passieren.

[mg]: Eine Frage nochmal mit Blick in die Statistik. Wir hatten es vorher schon mal gestreift, aber vielleicht können wir es einfach mal so ganz konkret an den Zahlen besprechen. Die Gothaer hat im Juni 2022 die KMU-Studie 2022 veröffentlicht. Und daraus geht hervor, dass Cyberangriffe die größte Bedrohung für Mittelständler darstellen, also auch in deren eigener Bewertung, Sie hatten das erwähnt, und dass aber trotzdem nur 21 % eine Cyberversicherung abgeschlossen haben. Also wir haben jetzt heute schon zwei Gründe gehört, woran das liegen kann. Also einer ist, ich kümmere mich einfach nicht drum, der andere ist, ich werde nicht versichert. Ist das signifikant, dieser zweite Fall, also dass Unternehmen eigentlich eine Versicherung abschließen wollten, aber keine Versicherung finden, weil ihre IT nicht geeignet ist oder nicht up to date ist? Oder ist es doch meistens so, dass man sich einfach nicht bemüht?

[Salm]: Wir versuchen natürlich auf Seiten der Versicherung eine Lösung zu finden, wenn ein Unternehmen eine Police haben möchte. Sprich, wenn dort die Prüfung passiert, nachdem wir beispielsweise einen Fragebogen aufgenommen haben, und wir sehen, dass dort noch erhebliche Lücken bestehen, gehen wir auf den Versicherungsnehmer zu oder auf das Unternehmen und schildern, wo wir Nachholbedarf sehen. Und wenn das nicht in einem kurzen Abstand passieren kann, dann würden wir sagen: Lasst uns doch bitte in einem Jahr noch mal sprechen. Andererseits könnten wir vielleicht aber auch mit sogenannten Auflagen arbeiten, dass wir sagen: Mensch, wir können schon mal mit der Versicherung starten, aber im Bereich XY hättest du Nachholbedarf, du müsstest dort was innerhalb der nächsten drei oder sechs Monate aufsetzen, damit wir dann auch ein vernünftiges Risiko aus unserer Sicht für die Cyberversicherung haben. Das Zweite ist, glaube ich, wirklich, dass es an einem Wissensdelta liegt, bei dem wir alle so ein bisschen Mitschuld tragen. Also ich glaube, auf der einen Seite eben die Assekuranz mit den Vermittlern und den Versicherern macht vielleicht noch nicht genügend Werbung an der richtigen Stelle für die Cyberversicherung. Das heißt, die Aufklärungsarbeit, da sind wir noch nicht am Ende angelangt. Wir sehen immer häufiger, dass bei vielen Versicherungsnehmern das Thema eben ausgespart wurde oder wird. Teilweise, weil man es einfach vergessen hat oder vielleicht noch nicht darüber gesprochen hat, teilweise aber auch weil es zu komplex ist und alle Gesprächsteilnehmer das Thema noch nicht aufgenommen haben. Also auch hier müssen wir als Versicherer beispielsweise die Vermittler noch besser schulen und besser mit dem Thema vertraut machen. Und auf der anderen Seite ist eben das Thema, was ich vorher angesprochen habe, dass die Versicherungsnehmer auch diese falsche Wahrnehmung haben, dass ich eben das Thema quasi auf meiner Risikoagenda habe, aber noch nicht denke, dass es mir selbst

auch passiert. Und das ist mitunter ein sehr, sehr hohes Problem, weil man dort natürlich im Kopf des Entscheiders ansetzen muss, und in den können wir alle nicht reingucken und den kann man quasi nur durch kommunikative Bestleistungen erreichen.

[mg]: Herr Greveler, was würden Sie denn sagen? Stimmt die Behauptung, dass früher oder später jedes Unternehmen mal betroffen sein wird von der Cyber-Attacke oder sagen Sie aus Sicht des IT-Experten, man kann sich da ausreichend absichern?

[Greveler]: Weder noch. Also eine Cyberattacke passiert einem Unternehmen tatsächlich ständig. Deswegen lassen sich solche Aussagen auch immer sehr leicht widerlegen als auch beweisen. Dann ist auch die Frage: Ab wann zählt man das denn? Wann wäre es so ein *major incident*, wie wir es sagen? Wie ein Millionenschaden für ein mittelständisches Unternehmen. Das wird nicht jedem passieren, also auch nicht in den nächsten zehn Jahren. Je kleiner man diese Hürde setzt, aber dann kann man irgendwann sagen: Ja, da passiert es eigentlich jedem und auch jedes Jahr. Die Frage: Was kann man dagegen tun? Wir hatten ja vorhin schon darüber gesprochen, diese Risikominimierung ist ja oft eine Voraussetzung, dass jemand überhaupt ein Angebot für eine Versicherung erhält. Danach muss er natürlich immer noch eine kaufmännische Entscheidung treffen, ob er das dann annimmt oder nicht. Wir sprechen also letztlich von Restrisiken, die er auf einen Versicherer überträgt. Und solche Restrisiken werden immer verbleiben. Also ab einer gewissen Unternehmensgröße, wenn eine vollständige Digitalisierung durchgeführt wurde, können wir solche Restrisiken einfach nicht mehr komplett eliminieren, weil natürlich machen Menschen Fehler. Natürlich kann es auch mal sein, dass ich zu spät reagiere mit einem Softwarepatch, oder weil es eben diesen Patch noch nicht gab, wie bei dem vorhin genannten Beispiel. Also kurzum, das ist dort letztlich so ein Balanceakt, dass man überlegt, wie viel Risiko kann ich hier ertragen, kann ich das überhaupt abschätzen und wie viel davon kann ich auf einen Versicherer übertragen oder möchte ich, jetzt auch bezogen dann auf die Kosten, die damit einhergehen, auf einen Versicherer übertragen? Die Vergangenheit hat allerdings gezeigt, dass hier die Versicherungswirtschaft auch so eine positive, normative Kraft bewirkt hat, dass eben bei vielen Unternehmen inzwischen die Bereitschaft dadurch auch gestiegen ist, sich so Standards zu unterwerfen, sich vielleicht auch zertifizieren zu lassen, weil man eben auch eingesehen hat, dass gewisse Dinge einfach erwartet werden, also nicht nur zum guten Ton gehören, sondern auch zu einem verantwortlichen Handeln als Manager einfach dazu gehören. Denn wenn schon eine Versicherung sagt, "wir versichern euch nicht, das ist ja Kraut und Rüben, eure IT", dann hat das ja auch eine gewisse Aussagetiefe. Also dann ist das ja auch erstmal ein Feedback für die Leistung der bisherigen IT beziehungsweise für das Budget, das man vielleicht auch seinen Mitarbeitern zur Verfügung gestellt hat für IT-Sicherheit. Das sehe ich tatsächlich ganz positiv. Dafür habe ich ein paar Jahre gebraucht. Ich war zu Beginn auch sehr skeptisch, weil ich nun mal Informatiker bin, und dann dachte ich, die sollen Sicherheit machen, aber nicht sich gegen Sicherheitsverletzungen versichern. Das ist ja quasi unsportlich. Also bitte an der IT arbeiten und nicht einfach dann so eine Art Los kaufen.

Aber wie gesagt, da musste ich meine Meinung revidieren, weil es tatsächlich dazu geführt hat, dass gerade so diese Grundmaßnahmen, das Paket, das eigentlich alle Unternehmen umsetzen sollten, dass diese jetzt eine sehr weite Verbreitung gefunden haben. Und dazu haben eben Cyberversicherungen beigetragen, und dazu hat auch das BSI beigetragen durch ein sehr großes Papierwerk, was man eben auch vielen Unternehmen in die Hand drücken kann. Und das führt insgesamt letztlich auch zu einer Absicherung der wirtschaftlichen Gesamtleistung. Sie sprachen ja auch schon an, diese politischen Risiken an der Stelle oder auch diese geopolitischen Auseinandersetzungen. Und gerade unter der Betrachtung solcher Risiken ist es natürlich erstmal ein gutes Gefühl, um es vorsichtig zu sagen, dass doch zumindest viele große Unternehmen inzwischen in ihre IT-Sicherheit investiert haben und ihre Risiken zumindest einmal betrachtet haben. Aber auch dann bleiben immer noch Restrisiken.

[Das Gespräch endet, der Abspann beginnt.]

[mg]: Und damit sind wir für diesmal wieder am Ende des Digitalgesprächs angekommen und bedanken uns bei Florian Salm von der Gothaer Allgemeine Versicherung AG und bei Ulrich Greveler von der Hochschule Rhein-Waal für die interessanten Einblicke und die spannende Diskussion. Viele Grüße nach Köln und nach Essen. Vielen Dank auch an Sie, liebe Zuhörerinnen, liebe Zuhörer, fürs Interesse und die Aufmerksamkeit. Und wie immer, wenn Sie mögen, in drei Wochen wieder zur nächsten Folge des Digitalgesprächs, dem Podcast von ZEVEDI, dem Zentrum verantwortungsbewusste Digitalisierung.