

Blockchain macht Lieferketten sauber und effizient

Mathematisch abgesicherte Daten bringen Vertrauen in die Lieferkette

Saubere Lieferketten, Schonung von Umwelt und Klima, extrem hoher Schutz vor Wirtschaftsspionage und Hackern sowie Kollaboration, ohne Geschäftsgeheimnisse zu verraten. Das, was so klingt als seien wir in einer paradisiatischen Wirtschaftsordnung angekommen, kann die Blockchain tatsächlich leisten. Eine Technologie als Antwort auf drängende Probleme unserer Zeit.

Dabei muss gleich zu Anfang mit einem weit verbreiteten Missverständnis aufgeräumt werden. Blockchain ist nicht Bitcoin, jene digitale Münze, die immer dann von sich reden macht, wenn Hacker Unternehmen erpressen oder dramatische Kursverläufe die Anleger in Atem halten. Zwar benötigt der Bitcoin die Blockchain-Technologie, doch Bitcoin ist nur eine unter vielen möglichen Kryptowährungen. Eins aber haben alle Kryptowährungen gemeinsam: Sie benötigen die Blockchain, denn ohne die Blockchain gäbe es sie nicht.



Bettina Uhlich,
Evonik



Heinz-Günter Lux,
Evonik



Datenregister mit großem Fassungsvermögen

Der Blockchain hingegen ist es völlig egal, ob auf ihr Zertifikate, Rechnungen oder eben digitales Geld eingestellt werden. Doch was ist die Blockchain eigentlich? Kurz gesagt: Bei der Blockchain handelt es sich um eine Art Datenregister mit einem sehr großen Fassungsvermögen. Dabei werden die Daten erst dann an die digitale Kette als Block angedockt, wenn deren Korrektheit von allen beteiligten Geschäftsteilnehmern anerkannt wurde. Diese Daten werden in Kurzform in „Hashs“ verschlüsselt, was sie vor unberechtigter Neugierde schützt und zugleich das Datenregister entlastet. Sie werden nicht mehr wie bisher an einer zentralen Stelle gespeichert, sondern dezentral auf viele Rechenzentren verteilt. Das

tiert – nur geändert oder gelöscht werden, wenn alle Teilnehmer auf der Blockchain einverstanden sind. Aber selbst dieser Akt wird registriert. Die Blockchain vergisst nichts. Alles wird protokolliert. Deswegen bezeichnen manche die Blockchain auch als ein riesiges Datenprotokoll.

Warum aber ist eine solche dezentrale digitale Infrastruktur für die Industrie so interessant? Die Gründe sind schnell genannt: Die Blockchain steigert die Effizienz innerhalb der Lieferkette enorm und eröffnet signifikante Automatisierungs- und Effizienzpotenziale. Im Themis-Pilotprojekt, das von Evonik, BASF und Commerzbank initiiert worden ist, wurde der Zahlungsprozess über die Blockchain in einem geschlossenen Datenkreislauf mittels programmierbaren Geldes entlang der bereits existenten Prozessketten transparenter, schneller und verlässlicher. Ein Geschäftsvolumen von mehreren Millionen Euro wurde so bereits abgewickelt. Der auf der

le Anwendungen prädestinieren. Einer der wichtigsten Gründe ist, dass alle Geschäftsteilnehmer die Daten in Echtzeit bekommen, und zwar gleichzeitig. Das gab es noch nie. Das schafft eine Transparenz vom Anfang der Lieferkette bis an ihr Ende. Das hat weitreichende Folgen. Statt Expeditionen individuell für einzelne Transporte beauftragen zu müssen, was zur Folge hat, dass der Lkw nach Entladung zunächst leer zum nächsten Einsatzort fahren muss, erhält der Spediteur nun Zugriff auf alle anstehenden Transporte. Das gilt auch für die Transporte des Warenempfängers. So kann die Logistik aktiv Folgetransporte, die in der Blockchain aufgeführt werden, gleich mitbuchen. Leerfahrten können so deutlich minimiert werden. So kann die Blockchain dabei helfen, die CO₂-Belastungen deutlich zu reduzieren. Doch die digitalen Blöcke können noch mehr. Sie verschaffen der Kreislaufwirtschaft eine nie gekannte Verlässlichkeit und ermöglichen neue Lösungen.

Arbeits- und Menschenrechte eingehalten wurden – die Blockchain verrät es ihnen. Das nennt man eine saubere Lieferkette. Genau danach verlangt der Verbraucher. Diese Chance durch die Blockchain will die Chemie auch nutzen, um die Kunststoffkreislaufwirtschaft lückenlos belegen zu können. So arbeitet Covestro an dem Aufbau einer Kunststoffkreislaufwirtschaft auf Blockchain-Basis. Ähnliches tut BASF in Brasilien und Kanada. Noch geschieht dies im Rahmen von Pilotprojekten. Ziel jedoch ist es, die Kunststoffkreislaufwirtschaft weltweit zu etablieren. Schließlich gilt: Wenn sich die Kunststoffe im Kreise drehen, sie mehrfach genutzt werden, landen sie nicht in der Umwelt und verursachen hier keine Schä-

ZUR PERSON

Bettina Uhlich, Betriebswirtin und promovierte Wirtschaftsingenieurin, ist seit 2014 CIO und Leiterin der weltweiten IT-Services von Evonik. Sie wurde 2016 unter die besten drei CIO des Jahres gewählt, weil sie auf vorbildhafte Weise die Digitalisierung im Evonik-Konzern weltweit vorantreibt.

ZUR PERSON

Heinz-Günter Lux, gelernter Industriefachwirt mit einem MBA von der Lubin School of Business an der Pace University, New York, trat 1988 in die Degussa ein und hat seitdem in verschiedenen Leitungspositionen im Evonik-Konzern gearbeitet. Seit 2017 ist er Senior Digital Strategist bei Evonik Digital.

schwunghaften Handel betreiben, aber auch Staaten wollen Daten, Daten und nochmals Daten. Noch ist der Diebstahl nicht allzu schwer, doch die Europäische Kommission ist entschlossen, dem in Zukunft mit Unterstützung der Blockchain einen Riegel vorzuschieben. Deswegen baut Brüssel an einer Euro-

isch gegenüberstehen, denn die Daten können durch verschiedene mathematische Bestätigungsverfahren auf ihre Korrektheit geprüft werden, ohne jedoch Geschäftsgeheimnisse preisgeben zu müssen, schließlich sind die Daten in Hashs verschlüsselt.

Die Chemieindustrie will die Chancen der Blockchain nutzen. Da sie am Anfang vieler Lieferketten steht und mit der gesamten produzierenden Industrie weltweit verbunden ist, wird dies der Blockchain zum Durchbruch verhelfen. So wird die Chemie zum wichtigsten Treiber dieser revolutionären Technologie.

Die Chemieindustrie wird der Blockchain zum Durchbruch verhelfen.

macht es Hackern enorm schwer. Ein Computer lässt sich vielleicht hacken, aber nie alle. Die korrekten Daten lassen sich immer identifizieren, die falschen ebenso.

Sind die Daten einmal auf einer privaten Blockchain eingestellt, können sie – im Unterschied zu einer öffentlichen Blockchain, die nachträgliche Veränderung nicht akzeptiert

Blockchain basierende Zahlungsprozess ist ein wichtiger Baustein hin zur Entwicklung vollautonomer Lieferketten.

Alle Teilnehmer bekommen alle Daten in Echtzeit

Doch die Blockchain hat weitere Vorteile, die sie für die industri-

Vom Vertrauen zum Wissen

Mussten Verbraucher bisher Siegel, wie etwa Fairtrade, vertrauen, können sie in Zukunft wissen. Denn die Wahrheit über die Lieferkette liegt auf der Blockchain. Dort ist sie vor Manipulationen sicher. Im Supermarkt kann mit Hilfe eines QR-Codes diese Wahrheit über Waren, Materialien und Rohstoffe zu jeder Zeit abgerufen werden, prinzipiell von jedem Kunden. Damit sind die Siegel obsolet. Ob der Fisch vegan gefüttert wurde, ob

den. Wer sich als Verbraucher genau informieren will, kann dies tun. Mit Hilfe der Blockchain erhalten kritische Kunden eine befriedigende Antwort.

Die Gier nach den Daten

Da Daten in der Industrie 4.0 die wichtigsten Werte sind, ohne sie nichts geht, sind Hackerangriffe und digitale Wirtschaftsspionage an der Tagesordnung. Alle wollen an die Daten ran. Kriminelle, die im Darknet mit den Daten einen

päischen Blockchain-Infrastruktur (EBSI), um die Daten europäischer Unternehmen sowie die Daten der Bürger in Zukunft besser schützen zu können. Denn die digitale Kette mit ihrer Verschlüsselung via Algorithmus ist schwer zu durchdringen, selbst Quantencomputer sind nach wie vor nicht in der Lage, diesen Schutzwall zu durchbrechen.

Trotzdem ist die Blockchain nicht von der Außenwelt abgeschirmt. Im Gegenteil: Sie ermöglicht Kollaborationen selbst dann, wenn sich Staaten oder Geschäftspartner misstrau-

Bettina Uhlich, CIO,
Evonik Industries AG,
Essen

Heinz-Günter Lux,
Senior Digital Strategist,
Evonik Digital GmbH,
Essen

■ bettina.uhlich@evonik.com
■ heinz-guenter.lux@evonik.com
■ www.evonik.de

Risiko Cyberkriminalität

Schutz und Versicherung für mittelständische Chemiehändler

Das jedes Unternehmen bei einem Ausfall seiner IT unmittelbar zum Stillstand kommt, ist traurige Realität, ebenso, dass der Verlust von Daten nicht nur zu Verzögerungen führt, sondern die Existenz konkret bedroht. Auch dass bei kurzen Lieferzeiten der Ausfall eines Chemiehändlers rasch die Arbeitsfähigkeit der Kunden bedroht, ist eine gefährliche Realität. Gezielte Angriffe auf bekannte Organisation erfolgen zunehmend mittels Bots, die im Netz Angriffsobjekte suchen, wahllos vorgehen und praktisch jeden treffen können. Ein aktueller Cyberangriff auf einen großen Chemikalienhändler zeigt die Gefahren aus dieser Richtung auf. Wie können insbesondere Mittelständler die Gefahrenabwehr organisieren?

Der weitere Text macht den Leser nicht zu einem IT- oder Cyberexperten, ermöglicht aber die konstruktive Prüfung der aktuellen

Schutzmaßnahmen, um darauf aufbauend Schwachstellen zu beseitigen. Dazu gehört eine Versicherung für den Fall der Fälle.



Thomas Schneider,
Compliance-Experte

Voraussetzungen für den Abschluss einer Cyberversicherung

Die Mindestsicherheitsvorkehrungen, welche von den Versicherern verlangt werden, sind sowohl abhängig vom Umsatz des Unternehmens als auch der gewünschten Versicherungssumme. Bis zu einem Jahresumsatz von 10 Mio. EUR sind zumindest Antivirenprogramme mit aktuellen Virendatenbanken, regel-



Frank Geuer,
Fülling & Meysenburg

mäßige Datensicherung auf Datenträgern oder separierten Systemen und Firewalls an allen Übergängen in das Internet für stationäre IT-Systeme zu gewährleisten. Im Einzelfall erfolgt die Abstimmung der Sicherheitsvorkehrungen zwischen den eigenen IT-Spezialisten und dem Versicherer.

Aktuell beträgt der Beitrag für ein Unternehmen mit einem Umsatz von 2,5 Mio. EUR und einer

Absicherung gegen Eigenschäden, Betriebsunterbrechungen, Erpressung sowie einer Cyberhaftpflicht und einer vereinbarten Selbstbeteiligung von 500 EUR jährlich rund 1.000 EUR. Darüber hinaus fordern Versicherer weitere Sicherheitsstandards wie:

- Rasches Einspielen von Updates und Sicherheits-Patches. Betriebssysteme oder Programme fordern häufig dazu auf, ein Update einzuspielen.
- Sparsame Nutzung und Einrichtung von IT-Administratorenzugängen. Wer einen Computer einrichtet, sollte ein Administratorprofil mit gesondertem Kennwort anlegen und dieses

Profil nur benutzen, wenn neue Programme eingerichtet oder das Betriebssystem konfiguriert werden.

- Einrichtung individueller Mitarbeiterzugänge. Jeder Mitarbeiter sollte ein eigenes Benutzerkonto mit eigenem Passwort besitzen. Darüber definieren Administratoren, welche Berechtigungen bestehen und welche nicht. Bei einem Angriff kann über einzelne Nutzer-Accounts besser nachvollzogen werden, wie der Eindringling in das Netzwerk gelangte.

Fortsetzung auf Seite 22 ►

Wo liegt die Zukunft der chemischen Industrie?

New Business Development im (Klima-)Wandel

Das Geschäft läuft. Ja, es brummt sogar. Der Rohstoff Öl ist billig und wird uns in den nächsten 165 Jahren weder ausgehen noch so teuer werden, dass wir uns jetzt schon ernsthaft um Alternativen kümmern müssten. Die Menschheit wächst und die Nachfrage nach Farben, Additiven, Pestiziden, Herbiziden, Düngern sowie Kunst-, Treib- und Wirkstoffen wächst mit ihr. Ein Traum für Unternehmer und Shareholder. Und doch bleibt ein ungutes Gefühl zurück. Irgendwie spüren wir, spätestens wenn wir die Werkstore unserer Unternehmen hinter uns gelassen haben, dass etwas nicht stimmt.

Die Wälder um uns herum vertrocknen, die Sommer sind so heiß wie noch nie, und der Schnee, der diesen Winter fiel, wurde zur Sensation. Als Bürger wissen wir auf eine diffuse Art, dass es so nicht weiter gehen kann. Dass die Erde wohl nicht mehr von dem aufnehmen kann, was wir als Abfall in Meere, Flüsse, Landschaft und Atmosphäre entlassen. Auf eine diffuse Art haben wir längst verstanden, was die meisten Ökonomen immer noch vehement negieren: mehr Wachstum, mehr Stoffstrom wird wohl nicht gehen.

Chancen für die chemische Industrie

Für die chemische Industrie birgt diese Situation große Chancen. Als Schlüsselindustrie, die an mehr als 90% aller Stoffströme indirekt oder direkt beteiligt ist, hat sie die Chance, umweltverträgliche und recyclebare Stoffe zu entwickeln, Altstoffe in Rohstoffquellen zu verwandeln oder Energiespeicher zu entwickeln, die ein Schlüssel zur Versorgung mit al-



Stephan Haubold,
SDH-Consult

ternativen Energiequellen sind. Sie kann damit zum großen Gewinner einer veränderten Wirtschaft werden.

Risiko: Sudden Regulatory Death

Als größtes Risiko kann der Sudden Regulatory Death (SRD) gesehen werden. Wie bereits in anderen Industriezweigen zu beobachten ist, ist es nicht unwahrscheinlich, dass Gesellschaft und Gesetzgeber sich der chemischen Industrie emotional aufgeladene zuwenden und mit steigenden Außentemperaturen und zunehmenden Naturkatastrophen verstärkt radikalere Regularien implementieren. Dies ist kein Szenario, das mit „CO₂-Neutralität bis 2050“ zu bekämpfen ist, bedenkt man, dass uns laut Deutschem Zentrum für



ZUR PERSON

Stephan Haubold ist Studiendekan für Wirtschaftschemie und MINT-Entrepreneurship der Hochschule Fresenius in Idstein (HSF). Zudem hat er die wissenschaftliche Leitung des Competence Centers für Entrepreneurship Frankfurt Rhein/Main der HSF inne. Der promovierte Chemiker wurde im Dezember 2018 zum Professor im Fachbereich Chemie und Biologie der HSF berufen. Haubold entwickelte bereits neue Produkte zur Marktreife und führte sie ein, gründete ein Unternehmen im Bereich der Nanomaterialien, die Unternehmensberatung SDH-Consult und übernahm eine Agentur für medizinische Fachkommunikation mittels Management Buy Out.

Luft- und Raumfahrt (DLR) noch ca. sieben Jahre (2028) bleiben, bis unser (weltweites) CO₂-Kontingent, das den Temperaturanstieg unterhalb von 1,5 °C hält, aufgebraucht ist. Die Zeit wird knapp – sehr schnell.

Stärken der Industrie

Dabei besitzt die Industrie erhebliche Stärken. Sie besitzt Prozess-Know-how, eigene Wissenschaftler und Forschungskooperationen und Erfahrung mit dem Auf-, Um- und Neubau von Großanlagen und produzierenden Unternehmen.

Mangel an Veränderungswillen als Schwäche

Als Schwäche könnte sich der mangelnde Wille zur Veränderung herausstellen. „Wir verbrauchen doch nur 8% des weltweiten Ölverbrauchs“, „wir werden doch immer effizienter“, „ohne uns würde das Leben in vielerlei Hinsicht wesentlich unbequemer werden“ etc. Das ist alles richtig und doch ist es grundlegend falsch zu

glauben, man könne sich als Unternehmen aus diesem Wandel, der alle Regionen und alle Menschen der Welt erfasst hat, raushalten.

Erstmals in der Geschichte der Industrialisierung wird der Markt nicht von Nachfrage und Angebot getrieben, sondern von der Erkenntnis, dass die Welt „voll“ ist und unseren Abfall nicht mehr aufnehmen kann. Wir werden uns ebenso daran gewöhnen müssen, dass physikalisches oder stoffstromgetriebenes Wachstum nicht mehr das primäre Ziel von Gesellschaften oder Unternehmen sein kann. Wir werden uns ebenso daran gewöhnen müssen, dass unsere strategischen Überlegungen zum New Business Development ausschließlich Problemgetrieben sein sollten. Wir werden es uns nicht mehr leisten können eine im Labor entwickelte Lösung in Märkte zu drücken, die dazu kein korrespondierendes Problem hat und/oder die nicht konform mit der Forderung nach Abfallneutralität einschließlich CO₂-Emissionen ist. Wir werden uns daran ge-

wöhnen müssen, dass es keine einfachen Antworten, wie „Dann machen wir alles circular oder biobased.“ mehr gibt, wenn es darum geht, den CO₂-Fußabdruck nicht nur stabil zu halten, sondern radikal zu senken oder darum, persistente und/oder toxische Stoffe durch ihr Gegenteil auszutauschen oder wegzulassen. Manches Produkt wird es vielleicht auch ersatzlos nicht mehr geben.

Fazit

New Business muss in Zukunft „von hinten“ gedacht werden. Wie in einer Retrosynthese wird das Problem in seine Einzelteile und Eigenschaften zerlegt, bis man die Eigenschaften der Lösung vor sich hat. Erst dann geht es in die Entwicklung. Dabei stehen einige Eigenschaften grundsätzlich fest. Der CO₂-Fußabdruck des neuen Produkts muss entlang seiner gesamten Lieferkette, von der Rohstoffgewinnung bis zur Entsorgung bekannt sein. Dabei darf in Zukunft nicht mehr vernachlässigt werden,

dass Rohstoffe bei ihrer Gewinnung z.B. Fläche, Wasser und Atmosphäre verbrauchen, ganz unabhängig davon, ob sie bio- oder ölbasiert sind. Dass Sie teilweise viele tausend Kilometer um die Erde reisen, bevor sie verarbeitet werden und dass sie am Ende ihres Lebenszyklus nicht einfach auf einer Müllhalde, in der Landschaft oder einer Verbrennungsanlage landen, ohne, dass das zu ihrem CO₂-Fußabdruck hinzuzurechnen wäre. Zusätzlich müssen bei der ökonomischen Betrachtung einer neuen Idee nicht nur Rohstoff- und Produktionskosten, sondern auch Folge- und Entsorgungskosten mit eingerechnet werden, auch wenn diese möglicherweise noch nicht eingepreist werden müssen. New Business Development entwickelt sich also aus der Nische zur Grundlage des strategischen Managements.

Stephan Haubold, Geschäftsführer, SDH-Consult, Bonn

■ s.haubold@sdh-consult.de
■ www.sdh-consult.de

GDCh-Kurs

New Business Development im (Klima-) Wandel

- 11. Oktober 2021, Online-Kurs
- GDCh-Kurs: 420/21
- Leitung: Stephan Haubold

Weitere Informationen und Anmeldung über:

- Gesellschaft Deutscher Chemiker (GDCh), Fortbildung
- Tel.: +49 69 7917 291
- fb@gdch.de
- www.gdch.de/fortbildung

Risiko Cyberkriminalität

◀ Fortsetzung von Seite 20

- Erzwingen komplexer Passwörter. Mindeststandards sollten eine bestimmte Passwörterlänge und die Verwendung eines Sonderzeichens und einer Zahl vorschreiben.
- Sicherung von Mobilgeräten. Nicht auszuschließen ist, dass ein Laptop im Zug vergessen oder das Smartphone aus der Tasche gestohlen wird. Wenn diese Geräte ungeschützt sind, können Diebe Passwörter oder sensible Firmendaten abfischen. Deshalb sollten mobile Datenträger vollverschlüsselt und mithilfe eines Passworts geschützt sein. Daten auf Laptops oder Handys sollten aus der Ferne gelöscht werden können.
- Verhinderung der Manipulation von Sicherungskopien. Die Datensicherung sollte physisch getrennt vom Server aufbewahrt werden.
- Von Zeit zu Zeit sollte geprüft werden, ob mithilfe der Sicherungskopien die Daten tatsächlich wiederhergestellt werden können.

Leistungen einer Cybersicherung

Versichert sind Eigenschäden (insbesondere die Beschädigung, Zerstörung, Blockierung, Veränderung oder der Missbrauch der IT-Systeme, Programme oder elektronischen Daten infolge eines Hacker-Einbruchs) sowie Haftpflichtansprüche (Drittsschäden), die aus dem Missbrauch der Daten entstehen, die im Betrieb gespeichert waren. Die Haftpflicht deckt u.a. Schäden für die Folgen aufgrund von Verstößen gegen die Cybersicherheit, den Datenschutz sowie gegen Datenvertraulichkeitserklärungen und Geheimhaltungspflichten.

Der Leistungsumfang einer „Cyber-Risk-Versicherung“ erstreckt sich primär auf Kosten, die aufgrund einer Attacke entstehen und auf Vermögensschäden, die durch das eigene Handeln/Verschulden Dritten zugefügt werden. Darunter können z.B. Kosten für IT-Forensik, Informationskosten, Kosten für Krisenmanagement und PR-Beratung, Kreditüberwachungsdienstleistungen, Betriebsunterbrechungsschäden, Rechtsberatung, Vertragsstrafen (PCI), Lösegeldzahlungen, Wiederherstellungskosten und Sicherheitsverbesserungen fallen.

Aufbau der Cybersicherung

Versicherungskonzepte sind modular aufgebaut und auf die Anforderung des Versicherungsnehmers abgestimmt. Bei der folgenden Aufstellung werden durchschnittliche Kosten mittelständischer Chemiehändler aufgeführt:

Dateneigenschäden

Grundbaustein für die Datenforensik, Wiederherstellung und die weiteren Cyberschäden. Ein Mitarbeiter öffnet den Anhang einer E-Mail, welcher einen Verschlüsselungstrojaner beinhaltet. Die Daten auf den Systemen werden somit unlesbar gemacht. Die Kosten für die IT-Forensik sowie die Entfernung der Schadsoftware und Installation neuer Sicherheitssoftware betragen 25.000 EUR.

Betriebsunterbrechung

Greift bei Stillstand oder Ertragsausfall des Betriebs durch einen Hackerangriff. Das Unternehmen



wird mit einer Denial-of-Service (DoS)-Attacke angegriffen. Die Plattform und damit verbundene Dienste sind zwei Tage für Geschäftspartner nicht erreichbar. Die Kosten für Anmietung zusätzlicher Serverkapazitäten sowie für die Betriebsunterbrechung und Wiederherstellung der ursprünglichen Homepage belaufen sich auf ca. 70.000 EUR.

Erpressung

Ein Zugriff auf den Computer ist unmöglich, weil Hacker diesen bis zur Zahlung einer Geldsumme gesperrt haben. Ein Hacker verschafft sich Zugriff auf die IT-Systeme und verschlüsselt wichtige Kundendaten. Später kommt eine E-Mail mit der Forderung, den Betrag in Höhe von

28.000 EUR in Form von Bitcoins zu zahlen. Beim Umgang mit den Erpressern unterstützt die Versicherung auch.

Vertrauensschaden

Wenn Mitarbeiter/Dritte z.B. Unterschlagung von Geld oder Erschleichung von Zahlungen im Betrieb durchführen. Ein Mitarbeiter hat Zugang zu Konten des Chemiehändlers. Dies nutzt er, um sich Beträge auf sein Privatkonto zu überweisen. Der über ein Jahr entstandene Schaden beträgt insgesamt 30.000 EUR.

Cyberhaftpflicht

Wenn z.B. versehentlich Viren an Kunden oder Dritte weitergegeben werden.

Ein Chemiehändler stellt seinen Kunden kostenlose Dienstleistungs-/Produktinformationen zum Download zur Verfügung. Eine Datei zum Download ist infiziert. Die IT-Systeme mehrerer Kunden werden infiziert. Der entstandene Gesamtschaden beläuft sich auf 28.000 EUR.

Cybersicherungen sollten außerdem die folgenden Leistungen beinhalten:

- Soforthilfe durch eine 24-Stunden-Hotline ohne Anrechnung auf die Versicherungssumme und auf den Selbstbehalt
- Mitversicherung aller Unternehmensdaten, aller Arten von Cyberangriffen (z.B. DoS, DDoS) und aller Arten von Cyberangriffen (z.B. Golden-Tickets, Zero-Day-Lücken)

- Vertragsstrafen bei Verletzung von Geheimhaltungspflichten und Datenvertraulichkeitserklärungen
- Mitversicherung aller Arten von Schadsoftware-Infektionen (Viren, Würmer, Trojaner), von Bedienfehlern sowie von gezielten und ungezielten Angriffen
- Verstöße bei Marken- und Urheberrechten durch Werbung und Marketing
- Kosten für Sicherheitsanalyse und Sicherheitsverbesserungen nach einem Schadenfall
- Absicherung aller IT-Systeme, Programme und Daten (auch auf mobilen Geräten)
- Straf- und Ordnungswidrigkeiten-Rechtsschutz bei Cyberverstößen
- Abwehrkosten in Bezug auf behördliche Verfahren
- Bei internationalen Aktivitäten: weltweiter Versicherungsschutz ohne Einschränkungen für die USA

Zusätzliche Leistungen

Gute Cybersicherer bieten darüber hinaus weitere Leistungen, und viele Versicherer stellen kostenlose Trainings- und Präventionsmaßnahmen zu Daten- und Cybersicherheit zur Verfügung.

Thomas Schneider, Compliance-Experte, Essen

Frank Geuer, Geschäftsführer, Fülling & Meysenburg, Essen

■ s_tommy@web.de
■ frank.geuer@f-u-m.de
■ www.f-u-m.de