SCHUNCK GROUP

Internationaler Assekuranz-Makler

Vorschlag
SCHUNCK Cyber Risk *Premium*
einfach logisch…

SCHUNCK GROUP

Internationaler Assekuranz-Makler

SCHUNCK GROUP
Cyber-Fachkompetenz in der Presse:


Business

Die Zahl der Cyberangriffe nimmt rasant zu. Eine Cyberattacke – initiiert von der KPMG [1] beschrieben, dass es nicht mehr die Frage ist, ob, sondern lediglich wann und wie ein Angriff gegen die eigene Unternehmung stattfinden wird. [1]. Dabei werden die Angriffe zunehmend professioneller und unter Einsatz neuester Technologien durchgeführt. Verschiedenste Länder, wenn neue Technologien oder Trends, wie beispielsweise Cloud Computing oder Bring-Your-Own-Device.

Zwar ist die Sensibilität auf die zunehmenden Gefahren gesellschaftlich gestiegen, doch haben acht von zehn Betriebe hinsichtlich ihres IT-Sicherheitsmanagements noch deutlichen Nachholbedarf. Eine aktuelle Studie der Risk Consultants von Corporate Trust 2014 ist vor allem der Mittelstand (5- Prüfer der Angreifer „in Deutschland wurden 59,5 % der mittelständischen Unternehmen, 33,3 % der Konzerne und 17,2 % der Kleinunternehmen geschädigt [2]. Dabei stellen Hacker nach dieser Studie überhaupt 41,8 % die größte Tätergruppe dar, gefolgt von Kunden und Lieferanten mit 16,8 %. Aber auch Voreure oder fahrlässiges Handeln eigener Mitarbeiter sind als erhebliche Schwachstelle zu sehen. «Unternehmen sind sich der finanziellen Auswirkungen von Cyberrisiken noch nicht ausreichend bewusst» [2].

Verschärfung der rechtlichen Rahmenbedingungen durch die Europäische Datenschutzverordnung. Durch die 2015 erwartete Verabschiedung der EU-Datenschutzrichtlinie wird eine teilweise drastische Verschärfung der Anforderungen an den Datenschutz einhergehen. Erwartet werden neben dem Wegfall der Begrenzung auf sensible Daten gem. § 42a BDSG und zeitgenaue Budgetfür sowie umfangreiche Mitteilungs- und Dokumentationspflichten innerhalb einer Zeitspanne von 24 Stunden ab dem Bekanntwerden des Verstoßes auf eine Datenschutzverletzung.

Strategien zur Risikobegrenzung. Rasant wachsende wirtschaftliche Risiken für Unternehmen und Manager bei versicherten rechtlichen Rahmenbedingungen stehen häufig einem unternehmerischen IT-Sicherheitsmanagement der Betriebe gegenüber. Dieses sollte neben technischen auch organisatorische und personelle Maßnahmen beinhalten. Zudem verfügen laut Studie von Corporate Trust derzeit noch nicht einmal jedes 20ste der Unternehmen über eine entsprechende Cyberversicherung.

Nur ein ganzheitliches Konzept aus angemessenen Sicherheitsstandards durch externe Spezialisten und Absicherung der Restrisiken über eine den individuellen Unternehmensrisikoprofilen angepassten Cyberversicherung bringen größtmögliche Sicherheit.

Cyberversicherung – ein geeignetes Mittel zum Risikotransfer? Auch eine gut funktionierende Cyber Security bietet keinen hundertprozentigen Schutz vor finanziellen Schäden infolge Cyberschocken.

Knapp fünf Prozent der Betriebe in Deutschland besitzen derzeit eine adäquate Cyberversicherung, während die große Mehrheit gegen Feuerschaden versichert ist. Die statistische Wahrscheinlichkeit durch eine Cyberattacke oder durch Fahrlässigkeit einen Datenverlust zu erleiden ist dagegen vielfach höher. Wie ist diese Diskrepanz zu erklären?

Die Gründe dafür sind vielschichtig. Diese sind beispielsweise...

- Mangelnde Transparenz und Information in den Produkten
- Geringe Vergleichbarkeit
- Intransparente Konzepte
- Mangelndes Bewusstsein im Umgang mit Cyberrisiken
- Fehlende Erfahrungswerte in versicherungstechnischen Summen

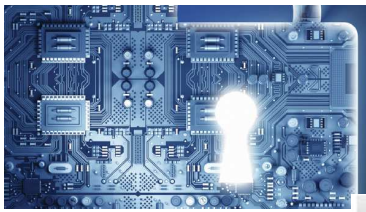
Gerade eine mittelstraft auf die Bedürfnisse zugeschnittene Cyberpolice kann existenzielle Unternehmensrisiken absichern und nachhaltig die Leistungsfähigkeit von persönlicher Insolvenzhaftung beispielsweise von Investoren oder Eigentümern schützen. Am Übermorgen ist es eine Cyberpolice daher schon deshalb fast notwendig, um im Extremfall nicht auf die D&O-Police zurückgreifen zu müssen.

SCHUNCK – we insure IT

Die SCHUNCK GROUP gehört zu den zehn größten deutschen Versicherungsmaklern, hat 1996 bereits als ein eigenes Competence Center Informationstechnologie und ist damit einer der größten unabhängigen Spezialisten der Branche. Die Cloud Computing, Risk Management, Softwarezertifizierung oder Datensicherheit mit eigenen IT-Spezialisten bietet das Unternehmen als weltweit erstes eigenes Bedingungswerk zu Standardrisiken. Flaggschiff ist die «SCHUNCK IT Police». Die Rundum-Versicherungslösung für IT-Unternehmen, in diesem Jahr wurden neben anderen Richtungsverbunden Versicherungen eine haftpflicht- und sachversorgte Cyber-Haftpflicht und eine optionale ausführliche Cyber-Eigenschadenversicherung für die Kunden erstellt.

EXPERTENMEETING ZUM THEMA CYBERSICHERHEIT UND CYBERVERSICHERUNG

Eine Standortbestimmung




Vorn: Michael Michael Dutz, Risikomanager, SCHUNCK GROUP (l.); Florian Delmaier, Leiter IT-Sicherheit & Computerkriminalität, Corporate Trust; hinten (v. l. n. r.): Peter Janson, Leiter Competence Center IT, SCHUNCK GROUP; Klaus Keus, Referatsleiter Analyse und Prognose, Bundesamt für Sicherheit in der Informationstechnologie (BSI); Friedrich Wimmer, Lead Consultant IT-Sicherheit, Corporate Trust; Underwriter Cyber Insurance, Zürich Gruppe Deutschland

RECHT + GELD 14.10.2015

Neuer Schutz vor Cyber-Risiken

Der Münchner Makler Schunck bietet eine Police an, mit der sich Logistikunternehmen gegen Störungen des IT-Systems und Datenverlust versichern können.

INTERVIEW

Tatort Computer

Das Internet birgt auch für Transportunternehmer ein großes Risikopotenzial. Michael Hauswirth, Geschäftsführer der Schunck Group Austria, im STRAGÜ-Interview über den Schutz gegen neue Gefahren der Cyberkriminalität.

STRAGÜ: **Nicht jeder Transportunternehmer ist sich offensichtlich des Risikos der Cyberkriminalität bewusst.**
Hauswirth: Richtig, trotzdem nehmen wir in jüngster Vergangenheit ein deutlich gesteigertes Bewusstsein dieser Gefahren gerade auch im Mittelstand und damit die Nachfrage nach einer

Logistik 4.0" wird auch die Cyberkriminalität weiter steigen. Allein die tägliche Presseberichterstattung gibt einen kleinen Überblick darüber, was heute schon möglich ist. So lassen sich mit einfachen Mitteln z.B. Steuerungsanlagen abschalten oder manipulieren. Auch ist es bereits (zwar nur zu Testzwecken) gelungen, Fahrzeuge während der Fahrt fremd zu steuern.

Jüngste sogar in Tageszeitungen veröffentlichte Vorfälle bei österreichischen Unternehmen zeigen eine sehr bedenkliche Entwicklung!

Welche Lösungen und Produkte bieten Versicherungen heimischen Transporteuren?

Der Versicherungsmarkt „Cyber" ist noch ein recht junger. Genau wie die derzeit am Markt erhältlichen Produkte mit ihren Stärken und Schwächen. Nach rund zwei Jahren Entwicklungs-

IT-Haftpflichtversicherung:
Kampf um Marktanteile sorgt für Innovationsfeuerwerk

Neue Vertragsklauseln

Eine Überprüfung der Haftpflichtversicherungen, die bis 2012 abgeschlossen wurden, lohnt sich auf jeden Fall. Denn

staatliche Stellen oder externe Risiken eingeschaltet, sodass hier genaue Zahlen kaum möglich sind. Berücksichtigt man, dass einzelne Unternehmen teilweise mit mehreren hundert (meist automatisierten)

HOHERE RISIKEN FÜR UNTERNEHMER AB 2015

Cyberrisiken – Gefahren aus dem Netz

IT-Attacken stellen die betriebliche Haftungssicherung vor immer neue Herausforderungen. Das Competence Center IT bei Schunck bereitet Unternehmen auf die neue Europäische Datenschutzrichtlinie 2015 vor.

Unabhängig von Größe oder Branche ist heute jedes Unternehmen mit Informationstechnologie konfrontiert. Kritisch wird es, wenn sensible Daten Teil der Geschäftsabläufe sind. Hackerangriffe, Unachtsamkeit oder auch vorsätzliche Schäden durch Mitarbeiter treffen Unternehmen empfindlich. Die Schäden erreichen schnell ungeahnte Höhen, doch sind nur wenige Unternehmen gegen solche Verluste abgesichert.

EUROPÄISCHE DATENSCHUTZVERORDNUNG VERSCHÄRFT HAFTUNGSRISIKEN

„Die Berücksichtigung der IT-Risiken gehört für jedes Unternehmen zum Risikomanagement. Ein funktionierendes Sicherheitsmanagement im

Unternehmen aller Branchen verabschiedet. „Laut einer KPMG-Cybercrime-Studie von 2013 sind in der Risikowahrnehmung der befragten

Systemhäuser und IT-Dienstleister. „Als wir uns mit dem Thema IT befassten, stellten wir große Defizite und Optimierungsmöglichkeiten bei

Sonderdruck aus Heft 9-10 2010 manage it

Versicherung von Haftpflichtrisiken von IT-/ ITK-Unternehmen

Grenzen werden überwunden

IT- und Telekommunikations- (ITK) Unternehmen sind einer Vielzahl von Haftungsrisiken ausgesetzt. Eine spezielle Haftpflichtversicherung für IT-/ ITK- Unternehmen verspricht dem Unternehmer Schutz bei Inanspruchnahme durch Kunden oder Dritte. Doch die Praxis sieht leider oft anders aus. Schließlich halten sich Schadenszenarien nicht an Versicherungsbedingungen ... und so bleibt Unternehmern ein ungutes Gefühl, ob Sie denn wirklich umfassend versichert sind ...

Allerdings gibt es kaum eine Zielgruppe, bei der sich einige Versicherer so weit in den Bereich der bisher nicht versicherbaren «Erfüllungsschäden» vorwagen. Ein Prozess, der sich in 2010 durch neue überarbeitete Haftpflichtbedingungen bei den führenden Branchenanbietern weiter beschleunigen dürfte.

Was bedeutet das für einen Unternehmer im Bereich IT- oder ITK? Eine Analyse der bestehenden Haftpflicht Versicherungspolice durch einen spezialisierten Versicherungsmakler lohnt heute mehr denn je – noch nie waren die Unterschiede in der Leistung im Schadenfall so gravierend wie heute. Einige konkrete Schadensbeispiele, – welche zweifelsohne versicherbar sind – sollen die Qualitätsunterschiede verdeutlichen.

Ausschlusstatbestand

Schaden wegen Betriebsunterbrechung (Erfüllungsfolgeschaden)
Ein IT-Unternehmen produziert Antivirensoftware. Das aktuelle Update der Computer-Version führte beim Kunden dazu, dass die PCs und Notebooks immer langsamer arbeiteten. (das

SCHUNCK CyberRisk *Premium*
Umfassender Cyber-Versicherungsschutz mit speziellen Anforderungen

„Unternehmen müssen sich künftig nicht mehr di
wann und wie eine Cyberattacke stattfindet" (Zita

Die Zahlen sind alarmierend: Rund 40 Prozent de
letzten 2 Jahren von Cyberkriminalität betroffen –
Studie 2015). Die Gesamtschäden für die Wirtsch

Stetig wachsende Cybergefahren, dazu weitreiche
für Unternehmen z.B. durch das IT-Sicherheitsges
Zudem rasante technische Entwicklungen (Stichw
Risiken zusätzlich. Viele Unternehmen in Deutsch
rungen unzureichend vorbereitet.

Es besteht akuter Handlungsbedarf – denn über
ten einig: Rein technisch ist das Problem der Cybersicherheit nicht mehr zu lösen"

SCHUNCK GROUP Internationaler Assekuranz-Makler

SCHUNCK Cyber Risk

DATENPANNE…

„Das kann uns nie passieren!“

(Antwort eines Systemadministrators bei einer Vielzahl von mittelständischen bis größeren Unternehmen)

„Unsere tägliche Ermittlungsarbeit (…) zeigt zwei Klassen von Unternehmen: Die, die bereits von e-Crime betroffen sind und die, die es sein werden oder dies nur noch nicht erkannt haben“ (Zitat: KPMG Cybercrime Studie 2015)

“Sie können tun, was Sie wollen. Sie werden vermutlich ein Opfer einer Cyberattacke werden”, (Zitat: Michael Picko vom Cybercrime Kompetenzzentrum des Landeskriminalamtes Nordrhein-Westfalen) “Sie müssen sich vorbereiten.” (Auszug: investigativ.welt.de 25.02.2016)

SCHUNCK GROUP Internationaler Assekuranz-Makler

SCHUNCK CyberRisk

Schlagzeilen....

LKA warnt vor Angriffen

Online-Kriminelle erpressen Computernutzer

17.02.2016, 19:51 Uhr | jhof, t-online.de

Ransomware macht Computerdaten unbrauchbar. (Quelle: t-online.de)

PC-Nutzer sollten dringend ihre Daten sichern. Der Grund: Zurzeit gibt es massiv Angriffe auf deutsche Internetnutzer und Firmennetzwerke, warnt das Landeskriminalamt in Nordrhein-Westfalen. Zum Teil gehen dabei Daten komplett verloren. Nur ein Backup hilft, denn einen verlässlichen Schutz gibt es nicht.

5300 Infektionen pro Stunde

Erpresser-Trojaner "Locky" wütet in Deutschland

20.02.2016, 14:08 Uhr | jhof, t-online.de

Der vorige Woche aufgeschlagene Erpressungs-Trojaner "Locky" verbreitet sich rasend schnell. Jetzt flattert der Schädling über Excel-Dateien auf den PC – doch Virenforscher warnen bereits vor einer nächsten, noch gefährlicheren Welle.

Neben dem Fraunhofer-Institut in Bayreuth zählte in dieser Woche noch ein weiteres Krankenhaus in Nordrhein-Westfalen zu den Opfern des Daten-Kidnappers. Großen Schaden soll Locky allerdings nicht angerichtet haben, da er sehr schnell entdeckt wurde. Die Schadsoftware verschlüsselt die Daten auf infizierten Computern und gibt diese erst nach Zahlung eines Lösegeldes wieder frei.

Immer dreister

Angebliche BKA-Warnung vor "Locky" ist ein Trojaner

03.03.2016, 14:41 Uhr | dpa, t-online.de

Online-Kriminelle nutzen weiterhin die Angst vor dem Trojaner "Locky". Ihre neuste Masche: Sie verschicken als gefälschte BKA-Mail getarnt ein angebliches Tool, das den gefährlichen Schädling aufspürt – wer die Mail ernst nimmt, installiert sich selbst einen Trojaner auf dem PC.

T Online

Schlagzeilen: 17.02.2016/ 20.02.2016/ 03.03.2016

SCHUNCK GROUP Internationaler Assekuranz-Makler

SCHUNCK CyberRisk

Schlagzeilen....

DVZ Seefracht

Gefahr für Ladung und Schiff

Ein Schlupfloch im Sicherheitskonzept kann rasch zu Ladungsverlust, langen Verzögerungen und im Endeffekt zu Einbußen in der Reputation der Logistikbranche führen. *(DVZ-Illustration: Melanie Köhn)*

Es ist ein Stoff, aus dem Thriller sind: Drogenschmuggler hacken sich in die Computersysteme des Hafens Antwerpen – verschaffen sich Zugang zu Sicherheitscodes und Passwörtern. So gelingt es ihnen, durch ihre Fahrer komplette Container vom Hafengelände, scheinbar ganz legal, abholen zu lassen. Deren Ladung – Bananen, T-Shirts, Tropenholz – ist vor der Verladung im Ursprungsland mit Drogen gespickt worden. Zwei Jahre dauerte es, bis das ausgefeilte System 2013 zufällig auffliegt, als ein Container auf den falschen Truck verladen wird und die Schmuggler versuchen, ihn mit Waffengewalt zurückzuholen.

HIN UND WEG

Cyber-Security: Logistikbranche im Visier von Hackern

in Transport und Tourismus, 31.03.2015

Es klingt wie das Drehbuch zu einem Action-Film: Hacker stehlen sensible Daten des Frachtverkehrs, sie manipulieren die IT-Systeme von Transportunternehmen – und schon werden physische Transportmittel wie Züge oder Flugzeuge ferngesteuert. Ein solches Szenario gibt es nicht nur auf der Leinwand. Tatsächlich ist der Transport- und Logistiksektor nicht vor den Gefahren von Cyber-Kriminalität gefeit. Und die gehen weit über den bloßen Datendiebstahl hinaus. Wirksame Schutzmaßnahmen gibt es dagegen bisher wenig.

Dr. Steffen Wagner

Partner, Head of Transport & Leisure

+49 69 9587-1507

KPMG

SCHUNCK CyberRisk

Schlagzeilen....

Süddeutsche Zeitung
SZ.de Zeitung Magazin

10. Juni 2015, 16:29 Uhr Cyberangriff

Sicherheitsfirma Kaspersky Lab gehackt

Die Zentrale von Kaspersky Lab in Moskau. (Foto: Bloomberg)

IT-Spezialisten ausspioniert

Die Sicherheitsfirma Kaspersky Lab ist erfolgreich von Hackern angegriffen worden. Die Attacke auf sein Netzwerk entdeckte das russische Unternehmen nach eigenen Angaben in diesem Frühjahr. Die Sicherheitsexperten gehen davon aus, dass die Angreifer an Informationen über neueste Technologien kommen wollten. Hinter den Angreifern soll ein Staat stecken. Die genauen Details hat das Unternehmen in einem 46-seitigen Bericht (hier das PDF) veröffentlicht. Im Interview mit dem US-Magazin *Wired* sagte Costin Raiu, Chef der IT-Forensik, dass die Angreifer mehrere Sicherheitslücken ausgenutzt haben. Das Besondere an diesen Lücken, die Zero Days heißen: Es sind Fehler in der Programmierung, über die selbst die Firma nicht Bescheid weiß. Solche Angriffe sind schwer abzuwehren.

SCHUNCK CyberRisk

Schlagzeilen....

Freitag, 19. Dezember 2014

Cyber-Angriff auf Stahlwerk

Hacker bringen Hochofen unter ihre Kontrolle

Die deutsche Industrie vernetzt sich immer stärker - und wird sensibler für Cyber-Attacken. Ein Beispiel zeigt, wie dramatisch die Folgen sein können: Hacker haben den Hochofen eines Stahlwerks unter ihre Kontrolle gebracht. Die Schäden sind massiv.

Die Anlage befand sich nach dem Angriff in einem "undefinierten Zustand". (Foto: REUTERS)

Hacker sind nach einem Bericht des Bundesamtes für Sicherheit in der Informationstechnik in das Netzwerk eines Stahlwerks eingedrungen, haben die Steuerung des Hochofens übernommen und die Anlage massiv beschädigt. Das geht aus dem Bericht "Die Lage der IT-Sicherheit in Deutschland 2014" hervor. Demnach führte der Einbruch der Hacker zum Ausfall ganzer Systeme der Anlage. Die Verantwortlichen in dem Stahlwerk seien nicht mehr in der Lage gewesen, den Hochofen herunterzufahren.

Dem Bericht zufolge haben sich die Angreifer zunächst mit auf Mitarbeiter zugeschnittene Fake-E-Mails Zugriff auf das Büro-Netzwerk der Anlage verschafft und sich von dort aus sukzessive bis in die Produktionsnetze vorgearbeitet. Das BSI bewertet die Kenntnisse der Hacker in diesem Fall als "sehr fortgeschritten" und geht davon aus, dass deren Wissen weit über die Kenntnisse der klassischen IT-Sicherheit hinaus ging und Fachwissen über die eingesetzten Industriesteuerungen und Produktionsprozesse mit einschließt.

Durch den Angriff fielen zunächst einzelne Komponenten aus, letztendlich war der Hochofen nicht mehr zu kontrollieren und befand sich in einem "undefinierten Zustand". Die Angestellten des Stahlwerks konnten den Hochofen nicht mehr herunterfahren und die gesamte Anlage wurde schwer beschädigt. Das BSI verrät in dem Bericht nicht, um welches Stahlwerk es sich gehandelt hat.

SCHUNCK GROUP Internationaler Assekuranz-Makler

Cyber Risiken

Bestandsaufnahme: Ausgewählte Ergebnisse einer Corporate Trust Studie 2014*

- **Nahezu jedes zweite der befragten Unternehmen war in den vergangenen zwei Jahren von e-Crime oder einem Verdachtsfall betroffen. Konkret waren dies in Deutschland 26,9%, weitere 27,4% hatten einen Verdachtsfall.**

- **77,5% der in Deutschland betroffenen Unternehmen hatten durch einen Spionageangriff einen finanziellen Schaden zwischen 10.000 € bis 100.000 € zu verzeichnen. Bei 4,5% betrug der Schaden über 1. Mio. €**

- **Der Mittelstand steht bei den Cyber Attacken besonders im Fokus der Angreifer. In Deutschland wurden 30,8% der mittelständischen Unternehmen, 23,5% Konzerne und 17,2% der Kleinunternehmen betroffen.**

- **Mit 41,5% stellen Hacker in Deutschland die größte Tätergruppe dar. Kunden und Lieferanten folgen mit 26,8% als zweitgrößte Gruppe, knapp gefolgt von den eigenen Mitarbeitern mit 22,8%. Damit entfallen rund die Hälfte aller Fälle auf das unmittelbare Umfeld des Unternehmens.**

- **Unternehmen versuchen Angriffe meist selbst zu lösen. Nur bei einem Viertel der Fälle in Deutschland (25,9%) wurden von den Unternehmen staatliche Stellen oder externe Spezialisten eingeschaltet.**

- **14,8% der Firmen in Deutschland haben keinen Verantwortlichen für die Belange des Informationsschutzes.**

- **Unternehmen setzen bislang kaum auf eine Cyber-Versicherung zum Risikotransfer. Nur 3,6% der Firmen in Deutschland verfügen über eine solche Police. 71,1% begründeten dies mit mangelnder Information zu verfügbaren Lösungen**

- **Studie: Industriespionage 2014 der Corporate Trust – business risk & crisis management**

Befragt wurden 300.000 Unternehmen in Deutschland & 42.000 Unternehmen in Österreich mit mehr als 10 Mitarbeitern und über 1. Mio. € Jahresumsatz

SCHUNCK GROUP Internationaler Assekuranz-Makler

Cyber Risiken

Bestandsaufnahme: Verschärfung der rechtlichen Rahmenbedingungen durch das IT-Sicherheitsgesetz/ § 13 Telemediengesetz...

Seit dem 24.07.2015 ist das **„Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“** (IT-Sicherheitsgesetz) in Kraft. Dieses bringt zunächst verschärfte Anforderungen für Serveradmins und Meldepflichten für Provider von Webservern sowie Kernkraftwerksbetreiber mit sich.
Geplant ist eine Rechtsverordnung, mit der eine Meldepflicht bei erheblichen IT-Sicherheitsvorfällen auch für Betreiber von „kritischen Infrastrukturen“ greift. Darunter fallen nach aktuellem Planungsstand die Bereiche

- Energie
- Informationstechnik
- **Transport und Verkehr**
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen

Parallel sollen gemeinsam mit der Wirtschaft Mindeststandards zur IT-Sicherheit erarbeitet werden *

Zeitgleich wurde das **Telemediengesetz** um einen **§ 13** ergänzt, der zusätzliche Pflichten für alle Betreiber einer Website trifft. Der Dienstanbieter wird zu zusätzlichen Sicherheitsmaßnahmen verpflichtet – ohne das der Gesetzgeber hierzu konkret wird. Allein das automatisierte Erfassen einer IP-Adresse beim Betreten einer Website kann als vorbereitende Maßnahme zur Identifikation einer Person gesehen werden. Eine SSL-Verschlüsselung dagegen wird als nicht ausreichende Maßnahme von Gesetzgeber gesehen. Bußgelder von bis zu € 50.000. drohen.

* Quelle: Heise Security

SCHUNCK GROUP Internationaler Assekuranz-Makler

Cyber Risiken

Bestandsaufnahme: Verschärfung der rechtlichen Rahmenbedingungen durch die neue EU-Datenschutzverordnung...

Am 15. Dezember 2015 wurde die Einigung über die Inkraftsetzung der Europäischen Datenschutz-verordnung erzielt. Diese ersetzt die europäische Datenschutzrichtlinie 95/46/EG vom 24.10.1995 mit dem Ziel einer Harmonisierung der nationalen EU-Datenschutzgesetze. Eine deutliche Verschärfung der Anforderungen an den Datenschutz sind nun Realität. Hier einige wesentliche Eckdaten der neuen Regelungen:

- Erhöhte Informationspflichten mit materiellen und zeitlichen Anforderungen
  - Informationspflichten innerhalb 72 Stunden, bzw. unverzüglich
  - Gesetzlich geregelter Mindestinhalt der Mitteilung
  - Dokumentationspflichten

- Erweiterung des Bußgeldrahmens auf bis zu 20 Mio. €, oder im Fall eines Unternehmens bis zu 4% seines weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist.

- Mögliche Schadensersatzverpflichtungen außerhalb des BDSG nach nationalem Recht bleiben bestehen

- Verschärfung der Datenschutzbestimmungen beim Informationsaustausch mit Drittländern. Damit soll z.B. einem Cloud-Anbieter mit Sitz in einem Drittland und Datenspeicherplätzen im EU-Raum die Einhaltung der EU-Datenschutzverordnung auferlegt werden können.

Cyber Risiken

Bestandsaufnahme: Haftung des Managements

§ 43 GmbHG

§ 93 AktG

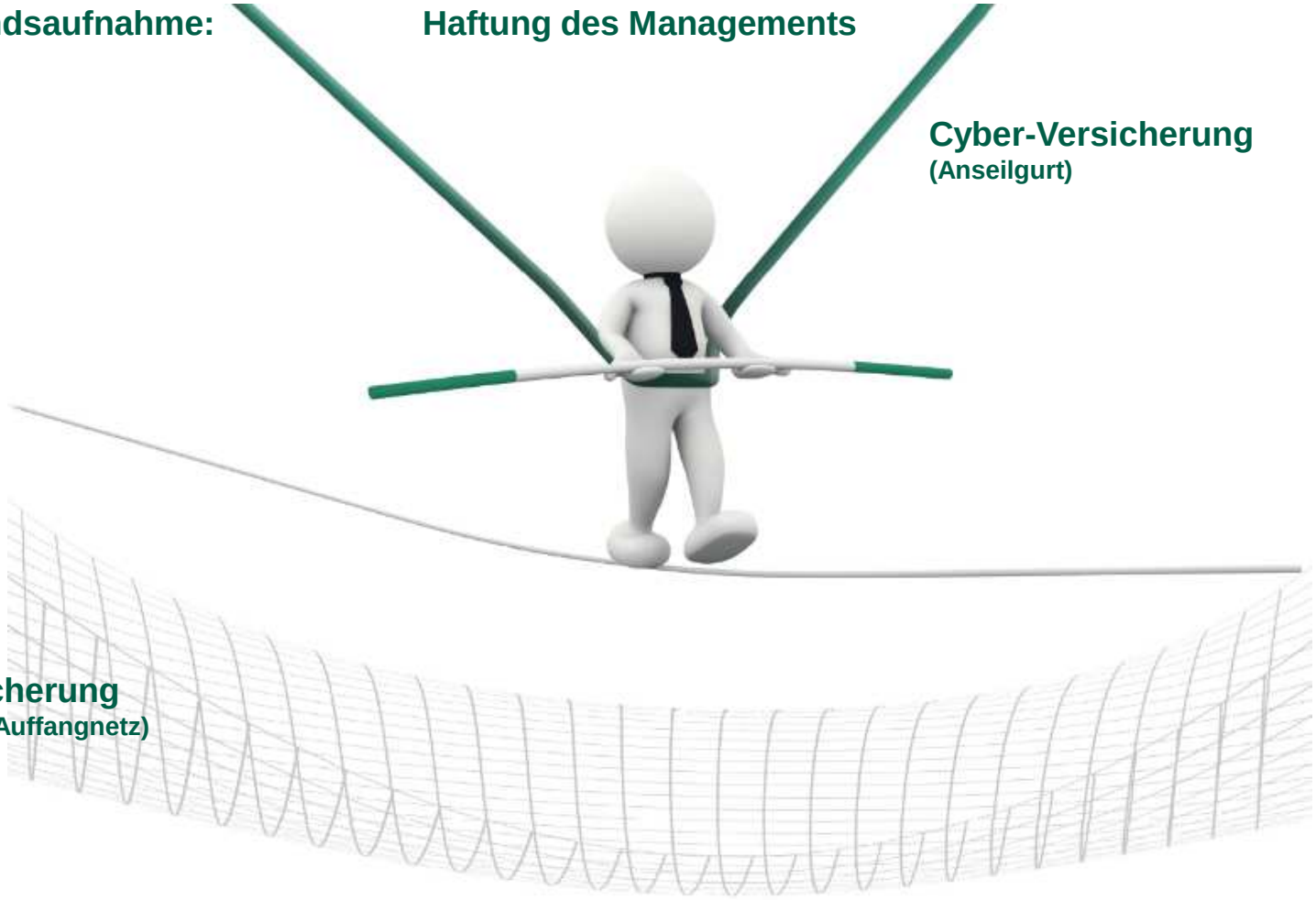
Ein funktionierendes Sicherheitsmanagement im Datenschutz ist Managerverantwortung. Trifft ein Unternehmen ein entsprechender Schaden, kann das Leitungsorgan persönlich und unbeschränkt mit seinem Privatvermögen in die Haftung genommen werden. Die Beweislast, wonach den Unternehmensleiter kein Verschulden trifft, liegt dabei beim Organ (umgekehrte Beweislast)

Cyber Risiken

Bestandsaufnahme:

Haftung des Managements

Cyber-Versicherung
(Anseilgurt)



D&O Versicherung
(„worst case“-Auffangnetz)

Cyber Risiken

Strategien zur Risikobegrenzung

- **Nur ein ganzheitliches Konzept eines IT-Sicherheitsmanagements bietet größtmögliche Sicherheit. Dazu gehören....**

SCHUNCK GROUP Internationaler Assekuranz-Makler

Vermögensabsicherung für das Unternehmen

SCHUNCK Cyber Risk *Premium* – einfach logisch…

Klare Poiicenstruktur….

Teil I: Versicherte Ereignisse (Definition Cybervorfall)

Teil II: Cyber-Assistance Leistungen (obligatorisch)

✓ Versicherungsfall ✓ Versicherungsleistung ✓ Ausschlüsse

Teil III: Cyber-Haftpflichtversicherung (optional)

✓ Versicherungsfall ✓ Versicherungsleistung ✓ Ausschlüsse

Teil IV: Cyber-Eigenschadenversicherung (optional)

✓ Versicherungsfall ✓ Versicherungsleistung ✓ Ausschlüsse

Teil V: Definitionen

SCHUNCK GROUP Internationaler Assekuranz-Makler

Vermögensabsicherung für das Unternehmen

SCHUNCK Cyber Risk *Premium* – einfach logisch…

Versicherte Ereignisse (Definition Cybervorfall)

Informationssicherheitsverletzung	Netzwerksicherheitsverletzung	Cyber Premium
Gesetzliche Bestimmungen zum Schutz von Daten	Übermittlung von Schadprogrammen an einen Dritten/ an VN durch einen Dritten	✓
Vertragliche Bestimmungen zum Schutz von Daten	DoS-/ DDoS-Attacken an einen Dritte/ an VN durch einen Dritten	
Geheimhaltungspflichten/ Vertraulichkeitsvereinbarungen zu geschäftlichen Informationen aller Art	Nicht autorisierte Nutzung, Vervielfältigung, Beschädigung, Zerstörung, Diebstahl von fremden elektronisch aufbewahrten Daten (incl. Persönlichkeitsverletzung)	
vertragliche Bestimmung, die ein dem BDSG o. vergleichbarer ausländischer Rechtsnorm entspricht	w.o. (nicht autorisierte Nutzung …) von eigenen elektronisch aufbewahrten Daten …	
Kreditkartenverarbeitungsvereinbarung mit Geschäftsbanken oder ähnl. Bezahlungssystemen	Blockade autorisierter Zugang Dritter auf VN-Systeme, sowie von VN auf Systeme Dritter	
	Unberechtigte Aneignung von Zugangscodes	
	Diebstahl von Hard- oder Software	

SCHUNCK GROUP Internationaler Assekuranz-Makler

Vermögensabsicherung für das Unternehmen

SCHUNCK Cyber Risk *Premium* – einfach logisch…

Cyber-Assistance Leistungen

	Cyber Premium
KRISENHOTLINE (24/365 Erreichbarkeit) bei Verdacht auf Datenschutzverletzung	✓
Kosten für Computer Forensik: € 500.000 zusätzliches Limit ohne Anrechnung Selbstbehalt)	
Kosten für Anzeige und Bekanntmachung von Datenrechtsverletzungen ▪ **Benachrichtigungskosten gegenüber Dateninhaber** ▪ **Kosten für behördliche Meldeverfahren** ▪ **Call-Center-Kosten**	
Kosten für Kreditüberwachungsdienstleistungen	
Kosten für Krisenmanagement und Public-Relations-Maßnahmen	
Vorgezogene Rettungskosten (Notfallmaßnahmen bis zur Schließung der Sicherheitslücke)	
Incident Response („Kammerjäger“ - Kosten zum Aufspüren und zur Behebung des Cybervorfalls)	

SCHUNCK GROUP Internationaler Assekuranz-Makler

Vermögensabsicherung für das Unternehmen

SCHUNCK Cyber Risk *Premium* – einfach logisch…

Cyber-Haftpflichtversicherung

	Cyber Premium
Prüfung der Haftpflichtfrage, Erfüllung begründeter, Abwehr unbegründeter Haftpflichtansprüche	✓
Inanspruchnahme durch Dritte auf Grundlage gesetzlicher– auch verschuldensunabhängige – Haftung bei Vermögensschäden	
Abwehrkosten bei behördlichen Verfahren (Rechtsschutz bei Straf-, Ordnungswidrigkeits- oder sonstiges behördliches Verfahren	
Inanspruchnahme durch Dritte auf Grundlage gesetzlicher und vertraglicher – auch verschuldensunabhängige – Haftung bei Vermögensschäden und (subsidiär) auch Personen- oder Sachschäden	
Rechtsverletzungen (Ausnahme: Patentrecht USA, Kanada, GB)	
Schäden infolge Diskriminierung (AGG)	
Intercompany Umsätze (von Dritten gegen mit dem VN verbundenes Unternehmen)	
Goodwill-Aktionen (Sublimit: € 100.000)	

SCHUNCK GROUP Internationaler Assekuranz-Makler

Vermögensabsicherung für das Unternehmen

SCHUNCK Cyber Risk *Premium* – einfach logisch…

Cyber-Eigenschadenversicherung

	Cyber Premium
Wiederherstellungskosten der Website, des Intranet, des Netzwerks, des Computersystems, der Programme, der Softwareanwendungen oder der elektronisch aufbewahrten Daten des VN	✓
Vertragsstrafen wegen Verletzung von Kreditkartenverarbeitungsvereinbarungen	
Cyber-Erpressung/ - lösegeld	
Vertragsstrafen wegen Verletzung von Geheimhaltungspflichten und Datenschutzvereinbarungen	
Unmittelbare Ertragsausfallschäden	
Deutlich erweiterte Definition der Ertragsausfallschäden (z.B. bei mittelbaren Ertragsausfallschäden über Service-Provider oder bei cyberbedingt vorausgehenden Sachschäden)	
Cyber-Diebstahl (z.B. Verlust, Umleitung von Geld/ Warenströmen, erhöhte Nutzungsentgelte (Stichwort: Voice-Over-IP)	

SCHUNCK GROUP Internationaler Assekuranz-Makler

Vermögensabsicherung für das Unternehmen

SCHUNCK Cyber Risk *Premium* – einfach logisch

Premium „HIGHLIGHTS“ im Überblick:

- Klare und einheitliche Begriffsdefinition des Cybervorfalls als Grundlage der Deckung
- Vorgezogene Rettungskosten & Incident Response
- Weitgehender Einschluss der vertraglichen Haftung
- Subsidiäre Erweiterung auf Personen- & Sachschäden in Haftpflicht
- Unmittelbare Ertragsausfallschäden – auch infolge Cyber-Sachschaden „Stichwort: Industrie 4.0“
- Mittelbare Ertragsausfallschäden – auch als Folge eines Cybervorfalls beim Service Provider

Cyber Risk von SCHUNCK – Die Feuerversicherung des 21. Jahrhunderts

u.a.m.

SCHUNCK-Kompetenz

Ihre Ansprechpartner bei der SCHUNCK GROUP

Peter Janson
OSKAR SCHUNCK GmbH & Co. KG

Schunckhaus München
Elsenheimerstraße7; D-80687 München
Telefon : +49 /89/ 38177 456
Mobil: +49/172/8908475
JansonP@schunck.de

Urheber- und Nutzungsrechte

Alle Urheber- und Verwertungsrechte am Versicherungskonzept, der Präsentation und den Inhalten liegen bei der SCHUNCK GROUP oder den jeweiligen Urhebern. Jegliche Verwertung und Verwendung des Konzepts, der Präsentation und der Inhalte oder Auszüge davon – auch in abgeänderter Form – sowie die Weitergabe an Dritte ist nicht gestattet.

SCHUNCK GROUP Internationaler Assekuranz-Makler

Information
gemäß § 11 VersVermV

OSKAR SCHUNCK GmbH & Co. KG,

Leopoldstraße 20, 80802 München, vertreten durch die Geschäftsführer, Herrn Albert K.O. Schunck und Rainer Witzel ist zugelassener Versicherungsmakler mit Erlaubnis gemäß § 34 d Abs. 1 Gewerbeordnung (GewO). Dies ist unter der Registrierungsnummer D-NTHO-9X9YY-41 überprüfbar unter www.vermittlerregister.info

Die OSKAR SCHUNCK GmbH & Co. KG besitzt keine direkte oder indirekte Beteiligung von über 10 % an Stimmrechten oder Kapital eines Versicherungsunternehmens noch besitzen Versicherungsunternehmen eine direkte oder indirekte Beteiligung von über 10 % an den Stimmrechten oder am Kapital der OSKAR SCHUNCK GmbH & Co. KG.

Gemeinsame Registerstelle:

Deutscher Industrie- und Handelskammertag (DIHK) e.V., Breite Straße 29, 10178 Berlin (Tel. 0180-500 585-0 (14 Cent/Min aus dem dt. Festnetz, höchstens 42 Cent/Min aus Mobilfunk-netzen); www.vermittlerregister.info.

Die Aufsichtsbehörde lautet:

Industrie- und Handelskammer für München und Oberbayern, Max-Joseph-Straße 2, 80333 München, Tel.: 089 51116-150

Schlichtungsstellen:

Bei Streitigkeiten zwischen Versicherungs-vermittlern und Versicherungsnehmern können folgende Schlichtungsstellen kontaktiert werden:
Versicherungsombudsmann e.V., Postfach 08 06 32, 10006 Berlin
Ombudsmann für die Private Kranken- und Pflegeversicherung, Kronenstraße 13, 10117 Berlin