DEFCON 2

für Manager- und Unternehmenshaftung

Foto: alamy

Streng Geheim +++ Neuer Kurs +++ 50° 51 N, 4° 21´0 +++ IT Maschinen AK voraus +++ Firewall-Sonar aktivieren +++ Kommunikationscode https-URLs-Datenverschlüsselung verwenden +++ auf Cyber-Sicherung fahren +++ Boot und Mannschaft sicher durch Daten- und Cybersee in den Erfolgshafen unversehrt steuern +++ Kapitän hat alle Vollmachten zur Auftragserfüllung +++ gez.: die Gesellschafter

„IT-Sicherheit und EU-Datenschutz-Grundverordnung sind das Thema Nummer 1. Die Metapher der Funknachricht erfüllt ihren Zweck, wenn die Leser dadurch die Brisanz für sich und ihr Unternehmen lokalisieren. Die Modernisierung der EU-Datenschutz-Grundverordnung fordert von allen Unternehmen eine Anpassung der bisherigen in- und externen Verfahren. Doch nicht genug. Die Unternehmens-Achillesferse ist nun die IT-Sicherheit, wenn sie es nicht schon vorher war. Diese Broschüre soll die Zusammenhänge und Lösungsansätze kurz und knapp vorstellen.“

Detlef Tauscher – Geschäftsführer der Centberg GmbH –

Einführung EU-Datenschutz-Grundverordnung (EU-DSGVO)

Historie. Das EU-Parlament hat am 14.04.2016 die EU-Datenschutz-Grundverordnung verabschiedet. 20 Tage nach Veröffentlichung im EU-Amtsblatt ist die Verordnung in Kraft getreten und seit dem 25. Mai 2018 ist die Anwendung europaweit verpflichtend.

Die Verordnung. Die umfangreichen – und teilweise unklaren – Neuregelungen führen zu Rechtsunsicherheiten. Unbestimmte Rechtsbegriffe sollten durch die Aufsichtsbehörden und die Artikel-29-Gruppe, die am 25.05.2018 durch den Rechtsnachfolger, den Europäischen Datenschutzausschuss (Art. 68 DSGVO) abgelöst wurde, konkreter erläutert werden. Es ist nicht sicher, dass sich der Datenschutzausschuss die Aussagen seines Rechtsvorgängers zu Eigen macht.

Die Folgen. Wirtschaftsunternehmen müssen einen erheblichen organisatorischen und finanziellen Aufwand betreiben, um die Anforderungen der EU-DSGVO zu erfüllen. Dies führt zudem zu weitreichenden Zusatzanforderungen an die elektronische Datenverarbeitung (EDV).

Ziel der Verordnung

Ziel der Verordnung ist es, den Schutz personenbezogener Daten zu garantieren und einen einheitlichen und freien Datenverkehr innerhalb der EU zu gewährleisten. Die Speicherung und Verarbeitung dieser Daten ist nur zulässig, sofern eine ausdrückliche und schriftliche Erlaubnis der betroffenen Person vorliegt.
Die Definition einer betroffenen Person im Sinne der EU-DSGVO ist alleine durch eine E-Mail möglich.
Beispiel: detlef.tauscher@centberg.de.

Unternehmens-Sicherheitsarchitektur 2018

Die Datensicherheit wird von drei Faktoren bestimmt. Moderner EDV-Technik, sorgfältigen Mitarbeiter/innen im Umgang mit Daten und Cyber-Management.

Sicherheitsfaktor EDV

Die EDV ist das Rückgrat von Unternehmen. Störungen sind nicht vorgesehen. Kundenverwaltung, Auftragsannahme, Bestellungen, Auslieferung, Werbung und Kommunikation werden heute zu 90 % durch den Einsatz der EDV gesteuert.

Der reibungslose Ablauf aller Betriebsprozesse ist nur durch ein modernes und störungsfreies EDV-System sicherzustellen.

Ernsthafte Störungen oder ein Komplettausfall führen unmittelbar zur Betriebsunterbrechung. Nur wenige Tage ohne EDV können hohe Kosten auslösen, zu Betriebsstillstand führen und die Wiederherstellung der firmeneigenen Daten nach sich ziehen. Im günstigsten Fall wird das Bilanzergebnis beschädigt, im ungünstigsten Fall kann der entstandene Schaden zur Zahlungsunfähigkeit eines Unternehmens führen.


Foto: pixabay

Lösung

Der Einsatz einer dem Stand der Technik entsprechenden Hard- und Software. Lizenzierte Softwareprogramme, regelmäßige Datensicherung, Firewall und Virenscanner reduzieren die Ausfallrisiken.

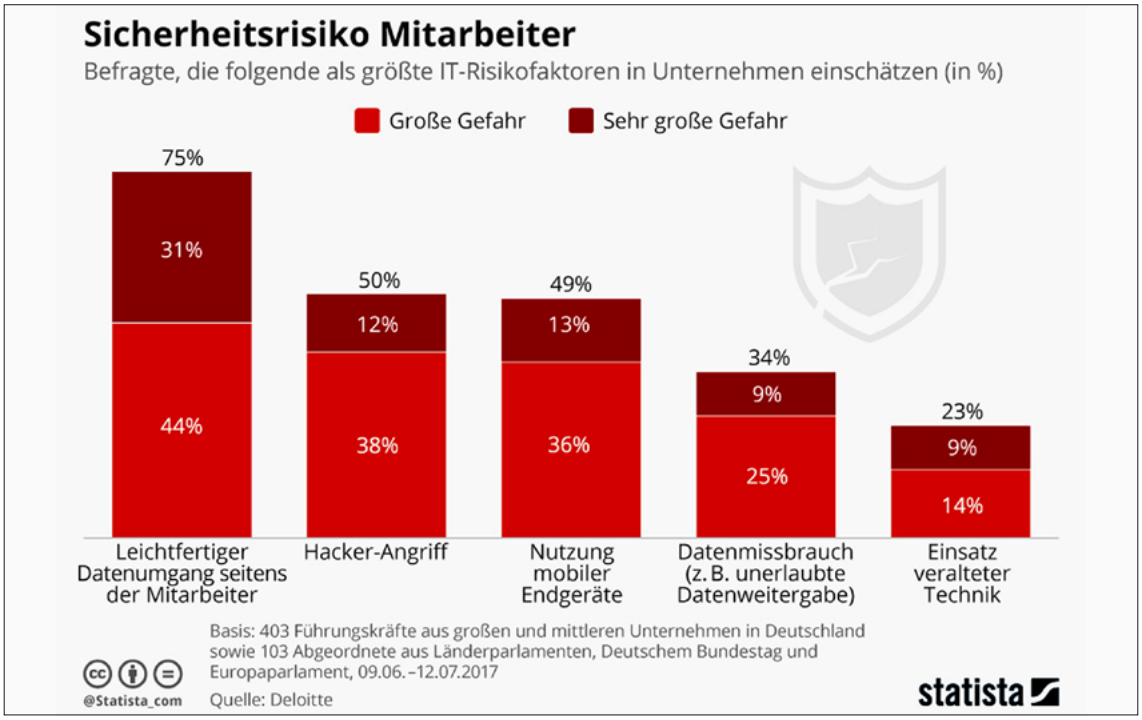
Faktor IT-Sicherheit 2018

Die IT-Sicherheit eines Unternehmens ist verantwortlich für
a) die Verfügbarkeit der EDV,
b) den Schutz vor Datenzerstörung und/oder Datendiebstahl.

Eine wahre Herkulesaufgabe bei den immer komplexer werdenden Netzwerken. Permanent steigen die erzeugten Datenströme durch erweiterte Anwendungen. E-Mails mit Dokumentenanhängen ersetzen größtenteils die traditionelle Briefpost und die Kommunikationserweiterungen zwischen Firmennetzwerken, Smartphones, Laptops und anderen mobilen Geräten kann über Funkverbindungen und offene WLAN-Netze jederzeit von überall genutzt werden. Komprimierte Datenübergaben und Geschäftspräsentationen durch nicht auf Schadsoftware geprüfte USB-Sticks und SD-Speicherkarten sind oft an der Tagesordnung.
Die Vielzahl an Datenbewegungen bietet Viren, Würmern, Trojanern, Spionage- und Zerstörungssoftware ein ideales Transportband, auf dem sich die „Schädlinge“ unerkannt in die IT-Infrastruktur eines Unternehmens befördern lassen können. Einmal eingedrungen, können sie zur Tat schreiten.

Faktor Mitarbeiter / Geschäftspartner

Mitarbeiter werden als größtes Sicherheitsrisiko eingeschätzt. Sorglose Nutzung des Internets, das übereilte Öffnen von Anlagen einer empfangenen E-Mail mit ausführbaren Dateien, reger Datenaustausch über soziale Netzwerke oder Datenübernahme von ungesicherten USB-Sticks in das Firmennetzwerk bergen ein hohes Gefahrenpotenzial.



Lösung

Erhöhung der IT-Sicherheitsstandards und Sensibilisierung und Schulung aller Mitarbeiter/innen auf potentielle Gefahren. Mitarbeiter informieren, dass der Gebrauch von Wechseldatenträgern zu vermeiden ist. Nutzung von sozialen Netzwerken ist grundsätzlich mit der Geschäftsführung und IT-Sicherheit abzustimmen. Gleiches gilt für die Genehmigung von privaten Nutzungen des Netzwerkes und mobiler Geräte.

Hacker-Angriffe und Cyber-Schädlinge

Segen und Fluch liegen nahe beieinander. Die rasante Entwicklung der elektronischen Datenverarbeitung und Datenvernetzung eröffnen Unternehmen Möglichkeiten, die vor 10 oder 20 Jahren undenkbar gewesen wären. Vieles geht kostengünstiger und schneller: Kommunikation, Ein- und Verkauf und das Auswerten von betriebswirtschaftlichen Kennzahlen.


Foto: pixabay

Fluch deshalb, weil der Technikeinsatz nicht ohne Risiko ist. Prozessoren mit Sicherheitslücken, infizierte USB-Sticks oder ein empfangenes Dokument mit Schadsoftware über E-Mail oder mobile Geräte gehören zu der Vielzahl an Krankheitserregern der EDV.

„… Wir überwachen und schützen unsere IT-Infrastruktur perfekt …“
Unternehmenssprecher eines Unternehmens mit 50 Mitarbeitern 2018

Nun, Sicherheit ist relativ. Industriekonzerne, Bundesministerien, Regierungen weltweit und Stromversorger verfügen über sehr moderne IT-Ausstattungen, kompetente IT-Fachleute und einige sogar über eigene Hacker-Abteilungen. Deren Aufgabe ist es, die eigenen Systeme zu hacken, um Sicherheitslücken zu entdecken, bevor es Hacker tun.

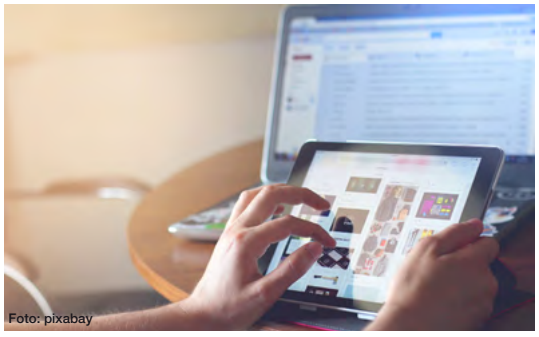


Foto: pixabay

Aber selbst diese teuren und professionellen Sicherheitsmaßnahmen schützen die Schwergewichte der IT-Sicherheit nicht.

Bundestag: In das hoch gesicherte Netz des Bundestages ist ein Hacker 2017 eingedrungen.
Kiew, Dezember 2016: Strom-Blackout. Eine gezielte Hacker-Attacke auf die 3-Millionen-Metropole hat die Stromversorgung weiter Teile der Stadt für Stunden unterbrochen.
Deutsche Banken, August 2016: Von dem Online-Banking-Trojaner Goznym sind Kunden von 13 deutschen Banken betroffen. Nach dem Diebstahl der Zugangsdaten von Konten wurden Guthaben leer geräumt.

Foto: pixabay

Lösung

Eine 100%ige Sicherheit gibt es nicht. Mit moderner Hard- und Software in Verbindung mit den klassischen Schutzfunktionen plus Sensibilisierung der Mitarbeiter und einem wirtschaftlichen Schutzschild ist alles getan, was getan werden kann. Und: Eine Cyber-Versicherung ist die dritte Fundamentversicherung moderner Unternehmen.

Cyber-Schutz für den Fall der Fälle

Wenn alle Sicherheitsvorkehrungen die Schädigung, Zerstörung oder den Datendiebstahl nicht verhindern konnten, geht es um die Schadensbehebung und die Abwehr von Haftungsansprüchen. Alleine im Bereich der Cyber-Haftpflicht wird das Kostenrisiko im mittelständischen Bereich zwischen 250.000 € und 1 Million als Orientierungsgröße angesetzt.
Ertragsausfall durch Betriebsstillstand, Wiederherstellung der Daten, Nichtzugriff auf Steuer- und Gehaltsdaten sind eine weitere Kostenposition.
Dann gilt es die Maßnahmen, die durch die EU-DSGVO verpflichtend sind, durchzuführen und in Zusammenarbeit mit PR-Beratern den eingetretenen Imageschaden so gering wie möglich zu halten.


Foto: pixabay

Lösung
Individuelle Absicherung für Cyber-Haftpflichtschäden und Mitarbeitereigenschäden.

Umfang einer CYBER-VERSICHERUNG

Auslöser	
Versicherte Mitarbeiter-Eigenschäden	**Versicherte Haftpflichtschäden**
Vorsatz von bösartigen Mitarbeitern	Verlust von elektronischen Daten
Betrug	Veränderung von elektronischen Daten
Unterschlagung	Blockade von elektronischen Daten
Diebstahl von Firmengeldern	Verletzung von vertraulichen Daten
Diebstahl von Kundendaten	Weitergabe von Schadsoftware (DoS)
Sachbeschädigung an den IT-Systemen	Datenmissbrauch / Datensabotage
Social-Engineering-Schäden	CEO-Betrug

Leistungs- und Kostenübernahme des Versicherers für/bei:
❑ Soforthilfe bei Cyber-Angriff-Entdeckung / Forensik
❑ Kosten für IT-Sicherheitsberater
❑ Eventuelle Übernahme von Geldforderungen zur Aufhebung von IT-Blockade(n)
❑ Übernahme von Vermögensschäden aus Malware (DoS-Attacken)
❑ Übernahme von Ansprüchen aus Verletzung des Datenschutzes (EU-DSGVO)
❑ Betriebsunterbrechung/Ertragsausfall – in der Regel 12 Stunden Selbstbeteiligung –
❑ Wiederherstellung von Daten, Programmen und Netzwerken
❑ Unerlaubte Medienaktivitäten durch unbeabsichtigte Veröffentlichungen
❑ Benachrichtigung der Kunden/Mandanten zur Datenschutzverletzung
❑ Kosten für Rechtsanwalt und PR-Berater zum Schutz der Firmenreputation
❑ Übernahme von Vertrauensschäden durch Mitarbeiter
❑ IT-Sicherheitsverletzungen durch ein Eindringen, Einwirken, Blockieren der Firmendaten
❑ Übernahme von Bußgeld- und Strafverfahren
❑ Kosten der außergerichtlichen und gerichtlichen Abwehr eines Haftpflichtanspruchs
❑ Beschädigung, Zerstörung, Veränderung, Blockierung oder Missbrauch des IT-Systems durch Dritte

Haftung von Geschäftsführer und Vorstand

Jahrelang wurden allein die IT-Leiter für folgenschwere Cyberangriffe verantwortlich gemacht. Doch diese Zeiten sind vorbei. Inzwischen stehen auch Konzernchefs nach einem Hackerangriff im Kreuzfeuer der Kritik. Der Konzernchef der US-Warenhauskette Target hat auf Warnungen der IT-Sicherheitsabteilung nicht unmittelbar, sondern erst vier Wochen zeitversetzt reagiert. Nach einer folgenschweren Panne für das Unternehmen musste der Vorstandsvorsitzende seinen Chefsessel räumen.

Foto: pixabay

Führungskräfte werden heute für Fehler zur Verantwortung gezogen. Die Managerhaftung ist daher nicht nur in Krisenzeiten eine reale Gefahr für Geschäftsführer und Vorstände. Nur die Weisung der Gesellschafter, es sei jederzeit sicherzustellen, dass die gesetzlichen Vorgaben der EU-Datenschutz-Grundverordnung (EU-DSGVO) einzuhalten seien, kann bei einer Datenpanne eine Managerhaftung auslösen. Ein lückenhafter Versicherungsschutz der Gesellschaft kann schnell den Chefsessel oder gar die eigene wirtschaftliche Existenz kosten.

Lösung

Wenn Vorstand und Geschäftsführung nicht selbst die Majorität der Gesellschaftsanteile halten, ist eine Directors-and-Officers-Versicherung (kurz D&O) der letzte mögliche Schutzschirm in der Schadenabwehr.

Sicherheit ist kein Glücksspiel

Betriebs- und Managerversicherungen sind keine 08/15-Themen. Deshalb investieren wir zunächst Gesprächszeit mit Ihnen.


Foto: fotolia

Unser Angebot Profi$^{60\text{-}DUO}$

Wir vereinbaren zwei 60-Minuten-Termine mit Ihnen.

In der ersten Runde haben Sie die Möglichkeit, Ihre Fragen zu stellen und die Besonderheiten Ihrer Gesellschaft vorzustellen.

Diese Informationen geben uns einen zielgenauen Arbeitsauftrag. Je nach Unternehmensart und -größe entwickeln und verhandeln wir innerhalb von 7 bis 14 Tagen passgenaue und wirtschaftliche Lösungsvorschläge.

Im zweiten Gespräch stellen wir Ihnen konkret den ausgearbeiteten Vorschlag vor.

36.000 € durchschnittliche Kosten pro Cyber-Angriff

Die Folgekosten für Unternehmen nach einem Cyber-Angriff (Schadenhöhe) steigen jährlich an. 2014 mussten Großunternehmen (ab 1.500 Mitarbeitern) durchschnittlich 560.000 € und klein- und mittelständische Unternehmen 41.000 € aufbringen. Mit Einführung der EU-DSGVO werden die Kosten nochmals deutlich steigen.

Bilanz von Kosten und Risikoschutz

Ein Unternehmen mit 1.000.000 € Jahresumsatz bezahlt jährlich 856,80 € (inkl. Versicherungssteuer) für eine exklusive Absicherung von bis zu 500.000 €.
Cyber-Schäden sind weder zeitlich noch in der Höhe kalkulierbar. Wenn sie eintreten, hat es auf alle Fälle wirtschaftliche Folgen. Die Kosten belasten sofort die Jahresbilanz des Schadenjahres und können in ungünstigen Situationen sogar die Zahlungsfähigkeit der Unternehmung überfordern. Zur Absicherung des Unternehmens ist eine Cyber-Versicherung notwendig. Für angestellte Unternehmensleiter (GmbH-Geschäftsführer, Vorstand einer AG) ist die Cyber-Versicherung zusätzlich ein wichtiges Instrument zur Vermeidung persönlicher Haftungsansprüche durch die Gesellschafter.

Cyber-Schäden: Kosten- und Nutzenbilanz:

Jahresumsätze bis	Versicherungssumme / Beiträge				
	100.000 €	250.000 €	500.000 €	750.000 €	1.000.000 €
100.000 €	380 €	475 €	595 €	690 €	785 €
250.000 €	420 €	520 €	650 €	755 €	860 €
500.000 €	460 €	575 €	720 €	835 €	950 €
1.000.000 €	555 €	695 €	870 €	1.010 €	1.150 €
1.500.000 €	670 €	835 €	1.045 €	1.150 €	1.250 €
2.500.000 €	770 €	880 €	1.160 €	1.235 €	1.310 €
5.000.000 €	880 €	950 €	1.255 €	1.420 €	1.580 €

Annahme: Schadenereignis im 10. Absicherungsjahr	
Cyber-Folgekosten gering	41.000 €
./. Beitragsprämie in 10 Jahren	– 8.568 €
Kosten- und Nutzenbilanz für das Unternehmen	32.432 €


Foto: fotolia

„Die Datenverarbeitung in Dienstleistungs- und Produktionsprozessen wird immer komplexer und verletzbarer. Datenpannen oder kriminelle Cyber-Attacken sind im Bereich des Möglichen. Die erfolgreichen Cyber-Angriffe auf hochgesicherte Regierungs- und Konzern-Netzwerke sind ein eindeutiger Beleg dafür. Der Schutz für die Centberg GmbH ist durch eine Kombination von IT-Sicherheit, Umsetzung der Datenschutzrichtlinie gemäß EU-DSGVO, Mitarbeiterschulungen und Cyber-Versicherung hergestellt."

Detlef Tauscher – Geschäftsführer der Centberg GmbH –

Wir chauffieren Sie jederzeit sicher durch die Straßen der deutschen und europäischen Versicherungswirtschaft, damit Sie sich auf das konzentrieren können, was Ihr Unternehmen nach vorne bringt.

CENTBERG
LEBEN | KRANKEN | UNFALL | SACH | GEWERBE

Centberg GmbH · Sophie-Charlotten-Straße 31/32 · 14059 Berlin
kontakt@centberg.de · Tel.: 030 339 889 50 · Fax: 030 339 889 40
www.centberg.de · Registrierungsnummer: D-YEFT-VYG9V-14