DataGuard

WHITEPAPER

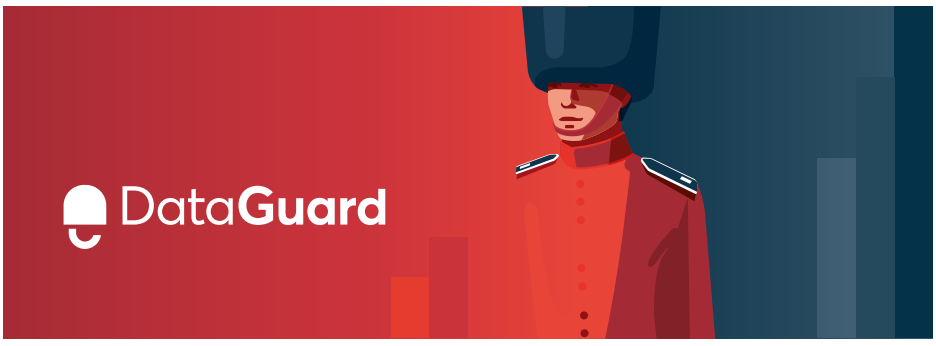
INFORMATIONS-SICHERHEIT 1x1

Alles, was Sie über Informations-sicherheit wissen müssen

- Was ist Informationssicherheit?
- Wie können Informationswerte vor Cyber-Attacken und Datenlecks geschützt werden?
- So schützen Sie Ihr Unternehmen durch ein Informationssicherheits-Managementsystem

ÜBER DATAGUARD

DataGuard ist ein Compliance-Software-Unternehmen mit mehr als 200 Mitarbeitenden in München, Berlin, London und Wien. Als ISO-27001-zertifiziertes Unternehmen und einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard über 2.500 Unternehmen die unkomplizierte Automatisierung und Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance („PIC"). Die Komplettlösungen von DataGuard reduzieren die Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001.



2.500+

KUNDEN

40 TAUSEND

ZUM DATENSCHUTZ GESCHULTE MENSCHEN

30 MILLIONEN

GESCHÜTZTE MENSCHEN

INHALT

EINLEITUNG

Ein durchschnittliches Unternehmen verwaltete 2019 rund 13,53 Petabytes (1 Petabyte = 1.000 Terabyte) an Daten – und damit 39 % mehr als noch in 2018 (Dell). Mittlerweile hängt jeder Prozess von der Verfügbarkeit der richtigen Daten ab. Und genau diese sind zunehmend komplexen Risiken ausgesetzt, darunter physischen Gefahren wie Bränden und Überschwemmungen, unautorisierten Zugriffen, Cyber-Attacken und Datenlecks, aber auch Gefahren durch fehlerhafte Datenverarbeitung.

Wenn Daten verloren gehen, nicht abrufbar sind oder in falsche Hände geraten, müssen Unternehmen mit finanziellen Schäden, Imageverlusten und ggf. rechtlichen Konsequenzen rechnen. Mit der Datenmenge und dem technischen Fortschritt steigen auch die Anforderungen an deren Schutz.

Hinzu kommt, dass immer mehr Arbeitnehmer von zu Hause aus arbeiten, also über das private WLAN auf das Intranet zugreifen. Obendrein nutzen sie vielleicht das eigene Mobiltelefon für Business-Anwendungen. Die Angriffsfläche vergrößert sich dadurch weiter.

In einer Studie von Dell gaben 82 % der befragten Unternehmen an, 2019 einen Störungsfall (z. B. Datenverlust, Systemausfall) erlebt zu haben. 2018 waren es noch 76 %. Außerdem befürchtete die Mehrheit (68 %) der Befragten einen Störfall in den nächsten zwölf Monaten.

In der Informationssicherheit geht es darum, die Daten und Unternehmenswerte bestmöglich zu schützen – damit es weder zu ungewollten, selbst verschuldeten Störfällen noch zu erfolgreichen Hackerangriffen von außen kommen kann.

KAPITEL 1

EINFÜHRUNG IN DIE INFORMATIONSSICHERHEIT

Informationssicherheit (auch als InfoSec bezeichnet) umfasst alle Maßnahmen, die Unternehmen zum Schutz von Informationen ergreifen. Dazu gehören Richtlinien und Maßnahmen, die den Zugriff Unbefugter auf geschäftliche Informationen verhindern.
Die Informationssicherheit ist ein wachsender und sich weiterentwickelnder Bereich, der ein breites Spektrum an Themen abdeckt. Neben der technologischen Ausstattung stehen auch die Sicherheit sämtlicher Prozesse und Geschäftsaktivitäten eines Unternehmens im Fokus sowie die Qualifikation und Vertrauenswürdigkeit der involvierten Menschen aus Belegschaft und Geschäftsführung, aber auch Lieferanten.

IN DIESEM KAPITEL

- Die Informationssicherheit beschreibt den Schutz von Unternehmenswerten nach mindestens drei Schutzzielen.
- Informationssicherheit gewinnt an Bedeutung, da der Schutz von Unternehmenswerten zugleich immer wichtiger und immer schwieriger wird.
- Informationssicherheit spielt für alle Branchen eine Rolle. Ganz besonders wichtig ist sie für stark softwaregetriebene und digital arbeitende Unternehmen. Hinzu kommen Firmen aus Industrien mit hoher Regulierungsnotwendigkeit.

Definitionen: Begriffe in der Informationssicherheit

Informationssicherheit beschreibt den Schutz von Informationswerten nach mindestens drei Schutzzielen:

- Vertraulichkeit → Informationen sind nur berechtigten Personen zugänglich
- Integrität → Informationen sind vor unrechtmäßiger oder außerplanmäßiger Veränderung gesichert
- Verfügbarkeit → Informationen sind zu jeder Zeit verfügbar und können bei Problemen wiederhergestellt werden

Zwar gibt es internationale Standards und Normen, die Anforderungen an die Informationssicherheit und Maßnahmen zur Umsetzung definieren, allerdings existiert kein festgelegter rechtlicher Rahmen.

Als Informationswerte (im Kontext der Informationssicherheit) wiederum gelten alle Daten, Informationen und Gegenstände, die einen Mehrwert für die Funktionen einer Organisation darstellen und dadurch die Erfüllung der Geschäftsanforderungen ermöglichen. Informationswerte haben einen geschäftlichen Wert – daher auch ihr Name.

Beispiele sind:

- Hardware, Software, Daten, Datenbanken, Prozesse und Anwendungen innerhalb eines Informationssystems
- Geräte, Clouds und andere Komponenten der IT-Umgebung, die Informationen verarbeiten
- Anwendungen, ein GSS (General Support System), Personal, Ausrüstungen und kollektive Gruppen von Systemen

Um den Begriff der Informationssicherheit sauber zu definieren, lohnt sich außerdem ein Blick auf die Begriffe der *Daten, Informationen und Wissen.*

Daten: Ob analog oder digital, als Datum (im Plural: Daten) wird ein Symbol, Zeichen, Wert oder eine Zahl bezeichnet. So wäre zum Beispiel *175,98 cm* ein Datum. Daten sind die Grundlage von Informationen und Wissen. Daher sprechen wir in der Informationssicherheit auch oft von dem Aspekt der Datensicherheit. Denn: Ohne sichere Daten keine sicheren Informationen.

Informationen: Verleiht man den Daten Kontext, zum Beispiel durch Syntax oder Verknüpfungen, so ergeben sich Informationen. Aus dem Datum *175,98 cm* wird eine Information, wenn sie in einer Tabelle in der Spalte „Körpergröße" auftaucht. Die Information wäre also: *Die Körpergröße beträgt 175,98 cm.*

Wissen: Zu Wissen werden Informationen dann, wenn sie weiter mit Sachverhalten verknüpft und verarbeitet werden. Zum Beispiel wäre *„Hans Peter Müller hat eine Körpergröße von 175,98 cm"* Wissen zu einer bestimmten Person.

Geht es also im Folgenden um Begriffe wie Datenverfügbarkeit oder Wissensmanagement, so betrachten wir dabei einfach unterschiedliche Abstraktionsebenen von Informationen.

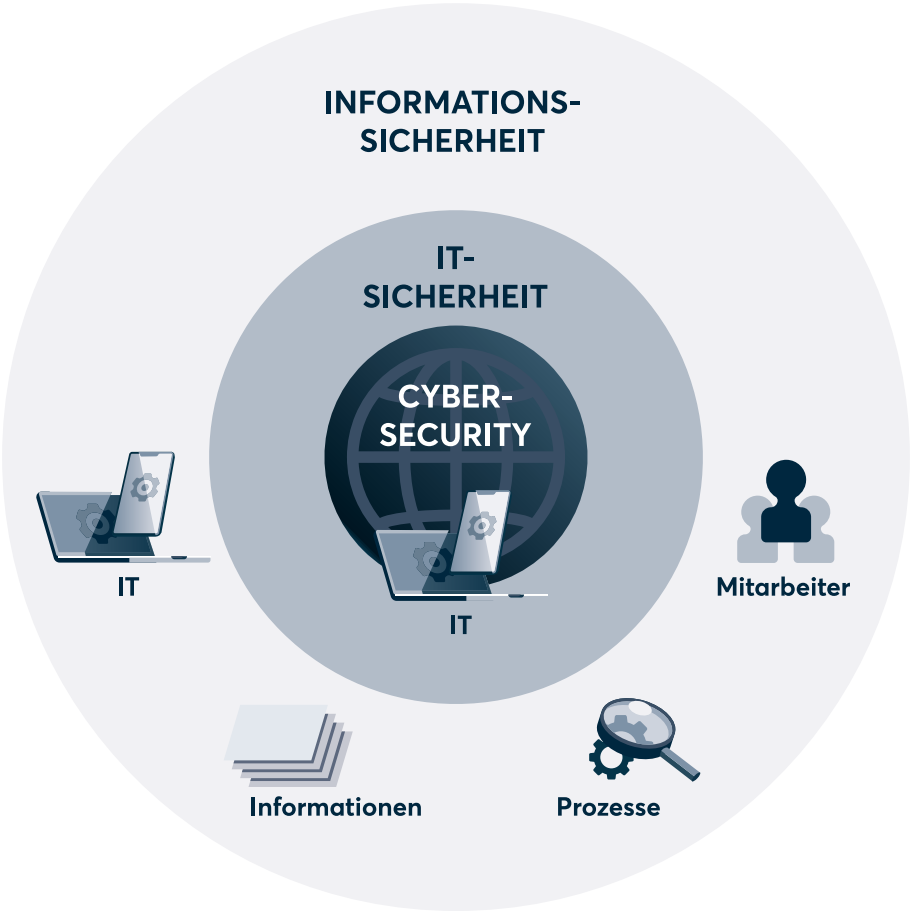
Eine Abgrenzung: Informationssicherheit vs. Cybersecurity vs. IT-Sicherheit

Der Begriff der **IT-Sicherheit** wird hin und wieder irreführenderweise mit dem der Informationssicherheit oder Cybersecurity gleichgesetzt. Hier eine Abgrenzung: In der **Informationssicherheit** geht es um den Schutz von Informationen. Die Information selbst ist der eigentliche Wert, sie existiert unabhängig von der IT oder dem Cyberspace und muss in allen Erscheinungsformen geschützt werden.

Zum Beispiel in Form einer Akte voller bedruckter Seiten oder in Form unternehmensspezifischen Wissens in den Köpfen der Mitarbeitenden. **IT-Sicherheit** bezieht sich auf die IT-Infrastruktur: Computer, Server, Clouds, Leitungen usw. müssen sicher und vor Zugriffen durch unberechtigte Dritte geschützt sein. Die IT transportiert und verarbeitet Information, das ist ihr Zweck.

Cybersecurity ist als Teilbereich der IT-Sicherheit zu verstehen. Es geht um den Schutz von Informationen im Cyberspace, also um Informationssicherheit in Verbindung mit dem Internet.

→ Jede Maßnahme der IT-Sicherheit trägt zur Informationssicherheit bei, aber nicht jeder Aspekt der Informationssicherheit hat etwas mit IT-Sicherheit zu tun



Informationssicherheit gewinnt an Bedeutung

In den letzten Jahren wurden zahlreiche Gesetze auf den Weg gebracht bzw. aktualisiert, die sich direkt mit der Informationssicherheit befassen. Das liegt mitunter an dem rasanten technischen Fortschritt, der Digitalisierung und den damit einhergehenden Risiken.

Zu den wichtigsten Gesetzen gehören: das IT-Sicherheitsgesetz bzw. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), die Verordnung zur Bestimmung Kritischer Infrastrukturen (**KRITIS-Verordnung**), das Geschäftsgeheimnisschutzgesetz und das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG).

Auch das Bewusstsein von Verbrauchern, B2B-Kunden, Investoren, Mitarbeitern und anderen Stakeholdern wächst. Investoren unterziehen Unternehmen eingehenden **Due-Diligence-Prüfungen**, bei denen die Informationssicherheit genau unter die Lupe genommen wird. Vermehrt spielen auch Zertifizierungen – zum Beispiel nach ISO 27001 und TISAX®* – eine große Rolle im Kampf um Vertriebspartner und Kunden.

Anmerkung: Fachumgangssprachlich spricht man meist nur von der ISO 27001. Die fachlich korrekte Schreibweise ist aber ISO/IEC 27001.

Für diese Branchen spielt Informationssicherheit eine Rolle

Jedes Unternehmen sollte sich mit Informationssicherheit auseinandersetzen – unabhängig von der Branche, unabhängig von der Betriebsgröße. Besonders wichtig ist das Thema für stark softwaregetriebene und digitale Unternehmen. Hinzu kommen Firmen aus Industrien mit hoher Regulierungsnotwendigkeit. Beispiel Gesundheitsmarkt: Hier sind bei der Informationssicherheit von Haus aus strenge Mindeststandards einzuhalten – etwa um die ärztliche Schweigepflicht zu gewährleisten.

In der Automotive-Branche liegt der besondere Fokus auf Informationssicherheit eher am Produkt: Es ist so komplex und wird von so vielen Beteiligten hergestellt, dass stark regulierte Freigabeprozesse zu absolvieren sind, bis ein Fahrzeug auf die Straße darf. Deshalb müssen alle an der Supply Chain beteiligten Player die Anforderungen erfüllen: der Konzern genauso wie ein mittelständischer Teilezulieferer, die Werbeagentur oder ein beratender Freiberufler. Wer Anteil an der Lieferkette hat, muss die in der Branche gültigen Anforderungen an die Informationssicherheit erfüllen – ohne Ausnahme. Bei der Datenschutzgrundverordnung (DSGVO) ist das zum Beispiel ganz anders, die gilt erst für Betriebe mit mehr als 20 Mitarbeitern.

* TISAX® ist eine eingetragene Marke der ENX Association

KAPITEL 2

DIE SCHUTZZIELE DER INFORMATIONSSICHERHEIT

Die drei Schutzziele der Informationssicherheit sind:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Wenn Unternehmen Maßnahmen zur Informationssicherheit implementieren, sollten diese immer mindestens eines dieser Ziele verfolgen.

IN DIESEM KAPITEL

- Die drei Hauptschutzziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit.
- Verbindlichkeit, Zurechenbarkeit und Authentizität gelten als erweiterte Schutzziele.

Vertraulichkeit

„Ich erzähle dir jetzt was, aber behandle es bitte vertraulich." Uns allen wäre sofort klar, was damit gemeint ist: Erzähle es nicht einfach so weiter. Die Vertraulichkeit von Informationen bedeutet genau das. Informationen müssen vor dem unbefugten Zugriff Dritter geschützt werden. Dafür muss klar sein, wer zu dem Kreis befugter Personen gehört.

Zu Maßnahmen, die der Vertraulichkeit von Informationen dienen, gehören:

- Verschlüsselung von Daten
- Zugangssteuerung
- Physische Sicherheit und Umgebungssicherheit
- Betriebssicherheit
- Kommunikationssicherheit

Integrität

Ein Mensch, der als integer gilt, ist verlässlich. Wenn wir von der Integrität von Daten und Informationen sprechen, meint das, dass sie sich nicht unbemerkt oder unzulässig verändern lassen und somit immer korrekt und verlässlich vorliegen. In gewisser Weise spielt auch hier die Vertraulichkeit mit hinein – also der Schutz vor unbefugtem Zugriff. Doch Integrität meint vor allem den Schutz vor unbemerkten Veränderungen. Oft passieren diese weniger durch Menschen und mehr durch fehlerhafte Systeme und Prozesse.

Zu Maßnahmen, die der Integrität von Informationen dienen, gehören:

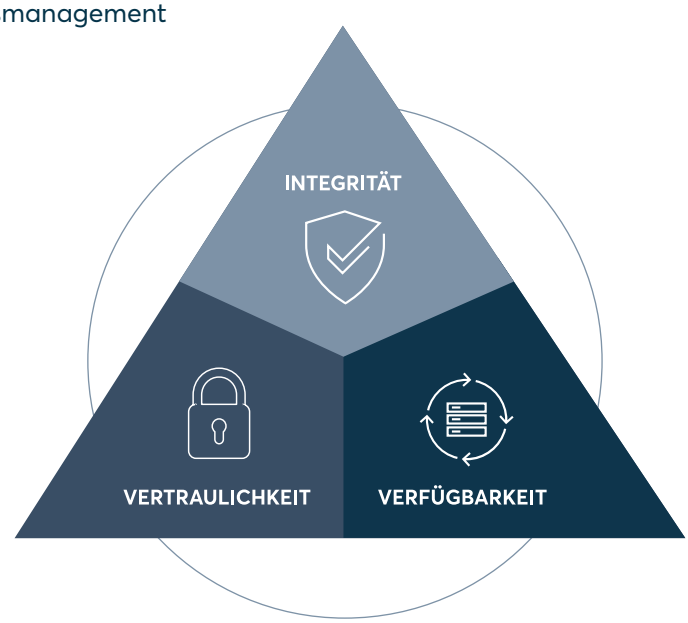
- Zugangssteuerung
- Management der Werte
- Anschaffung, Entwicklung und Instandhaltung von Systemen

Verfügbarkeit

Was nutzen vertraulich behandelte, integre Daten, wenn Nutzer nicht in dem Moment an sie herankommen, in dem sie benötigt werden? Beim Schutzziel der Verfügbarkeit geht es darum, die technologische Infrastruktur aufzubauen, die Daten und Informationen verfügbar machen. Oder deutlicher ausgedrückt: Systemausfälle zu verhindern. Gehen Daten doch einmal verloren, ist es ebenfalls Aufgabe der Informationssicherheit, den Betriebszustand so schnell wie möglich wiederherzustellen – zum Beispiel durch Back-ups.

Zu Maßnahmen, die der Verfügbarkeit von Informationen dienen, gehören:

- Risikoanalyse
- Anschaffung, Entwicklung und Instandhalten von Systemen
- Management von Informationssicherheitsvorfällen
- Betriebliches Kontinuitätsmanagement



Erweiterung der drei Schutzziele um Verbindlichkeit, Zurechenbarkeit und Authentizität

Werden Daten geändert, muss es nach den Schutzzielen der Verbindlichkeit und Zurechenbarkeit möglich sein, die Änderungen eindeutig und unanfechtbar einer Identität (im besten Fall einer natürlichen Person) zuzuordnen. Das kann nur durch ein vollständiges Identitätsmanagement und Änderungshistorien gewährleistet werden – zum Beispiel zeichnen die meisten CRM-Systeme auf, wann und von wem Angaben zu einem Kontakt geändert wurden. Teilen sich nun mehrere Nutzer eine Lizenz, führt das dazu, dass die Verbindlichkeit und Zurechenbarkeit nicht gegeben sind.

Authentizität steht für die Echtheit von Informationen, die sich anhand ihrer Eigenschaften überprüfen lassen muss.

KAPITEL 3

GEFAHREN FÜR DIE INFORMATIONSSICHERHEIT

Geht es um Gefahren, denen Informationswerte ausgesetzt sind, denken die meisten zuerst an Cyber-Attacken, organisierte Kriminalität und Spionage. Und es stimmt: Kriminelle Attacken – gerade auf digitale Systeme – sind eine große Gefahr mit weitreichenden Folgen:

Im Jahr 2020/2021 entstanden deutschen Unternehmen Schäden von 223 Milliarden Euro durch Diebstahl, Spionage oder Sabotage. 2018/2019 waren es noch 103 Milliarden Euro. Neun von zehn Unternehmen waren nach Angaben der Bitkom direkt von Cyber-Angriffen betroffen.

Und Informationen werden nicht ausschließlich von Angreifern mit böswilligen Absichten bedroht. Auch die eigenen Mitarbeiter können – mutwillig oder versehentlich – eine Gefahr für die Informationssicherheit darstellen, genauso wie fehlerhafte Systeme, Prozesse und physische Bedrohungen durch Naturgewalten.

IN DIESEM KAPITEL

- Die Informationssicherheit kann durch Naturgewalten, eigene Mitarbeiter, Systeme und Prozesse sowie Cyberkriminalität gefährdet werden.
- Bei Hacker-Angriffen geht es meist um die Erpressung von Lösegeldern oder den Diebstahl von Daten, die für weitere Angriffe benötigt werden. Geistiges Eigentum für sich zu gewinnen, gehört nur selten zu den Zielen von Cyberkriminellen.
- Die gängigsten Einfallstore für Hacker-Angriffe sind Social Engineering, unsichere Passwörter, standortunabhängiges Arbeiten, Schatten-IT und unsichere Cloud-Lösungen.

Physische Gefahren

Im März 2021 brach in einem fünfstöckigen Rechenzentrum in Straßburg ein Feuer aus. 12.000 Server standen in Flammen, über 100.000 Webseiten wurden lahmgelegt und viele der zerstörten Daten waren für immer verloren – mit verheerenden wirtschaftlichen Folgen. Warum? Viele Unternehmen hatten nicht beachtet, dass Daten redundant gespeichert werden müssen. Sie hatten keine Kopien und standen genauso verdutzt da, wie so mancher Privatanwender im Computer-Geschäft, wenn die typische Frage kommt:
„Sie haben doch regelmäßig Back-ups durchgeführt, oder? Wo finden wir die denn?"

Dass ein Rechenzentrum durch Feuer, Wasser und andere Naturgewalten beschädigt wird, kann nicht ausgeschlossen werden. Eine der Aufgaben der Informationssicherheit besteht deshalb im betrieblichen Kontinuitätsmanagement. Gehen Daten in einem Rechenzentrum verloren – ein Risiko, das im Rahmen einer Risikoanalyse aufgedeckt werden sollte – muss sich der Betriebszustand trotzdem aufrechterhalten lassen können. Bei der Auswahl eines Rechenzentrums oder einer Cloud-Lösung, die geschäftskritische Informationen verarbeiten, ist aus Sicht der Informationssicherheit auf eine hohe Betriebszeitgarantie zu achten.

Gefahren durch eigene Mitarbeiter

Unachtsamkeit und unzureichend geschulte Mitarbeiter zählen laut einer Studie von **KPMG (2019)** zu den meistgenannten Faktoren, die Cyberkriminalität begünstigen. Und auch, wenn Angriffe sich mehrheitlich externen Unbekannten zuweisen lassen, erkennen 48 % der befragten Unternehmen in der Studie ihre eigenen Mitarbeiter als potenzielle Gefahr.

An die Öffentlichkeit gelangt Datenklau durch (ehemalige) Mitarbeiter so gut wie nie. Zum einen lässt er sich schwer nachweisen. Zum anderen liegt es im Interesse eines Unternehmens, derartige Informationen nicht publik zu machen – es sei denn natürlich, es besteht eine Meldepflicht laut DSGVO.

Typischerweise sind besonders der Ein- und Austritt in und aus dem Unternehmen riskante Zeitpunkte. Neue Mitarbeiter, die besonders umfangreichen Zugang zu sensiblen Unternehmensdaten bekommen (z. B. IT-Leiter oder höheres Management), sollten durch einen Background-Check überprüft werden. Wer das Unternehmen verlässt, sollte alle Informationswerte zurückgeben. Ob es jedoch letztendlich Kundendaten auf einem USB-Stick aus dem Unternehmen schaffen, lässt sich in der Realität kaum überprüfen.

Oft ist es aber gar nicht der mutwillige Datenklau, der Mitarbeiter zu einer Gefahr für die Informationssicherheit macht. Vielmehr ist der „Faktor Mensch" besonders bei unzureichenden Schulungen oder schlichtweg durch Nachlässigkeit eine große Schwachstelle.

Gefahren durch Systeme und Prozesse

Damit die Schutzziele der Informationssicherheit auch wirklich erreicht werden können, müssen die Systeme, in denen sie gespeichert und verarbeitet werden, mitspielen. Nehmen wir das Schutzziel der Integrität: Unerkannte Datenmanipulationen dürfen zur Erreichung dieses Schutzzieles IT-seitig nicht möglich sein.

Verwendet ein Unternehmen beispielsweise ein Tool, das ein Abändern der Rechnungsnummer auf einer Ausgangsrechnung nachträglich zulässt, kann das dazu führen, dass eingehende Zahlungen falsch zugewiesen werden. In diesem Fall sollte also eine Manipulation des Datums „Rechnungsnummer" nach Versenden der Rechnung nicht mehr möglich sein.

Auch bei selbstprogrammierten Lösungen kann es durch kleine Fehler passieren, dass Daten fälschlicherweise überschrieben, dupliziert oder anderweitig verändert werden. Dann ist die Datenintegrität nicht mehr gegeben. IT-Systeme müssen also durchgängig und in ihrem Zusammenspiel einwandfrei funktionieren.

Gefahren durch Cyberkriminalität

„Oops, your files have been encrypted!"

Diese Nachricht begrüßte zahlreiche Nutzer auf ihren Computerbildschirmen, als sie im Frühjahr 2017 Opfer der Ransomware-Attacke **„WannaCry"** wurden. Am linken Bildschirmrand zählte ein Timer die Stunden und Minuten bis zur endgültigen Löschung der Daten, die sich auf dem Gerät befanden. Freikaufen konnten Nutzer ihre Daten angeblich durch eine Bitcoin-Zahlung von 300 bis 600 €.

Durch WannaCry wurden innerhalb von drei Tagen in über 150 Ländern mehr als 200.000 Rechner von Privatpersonen und Unternehmen befallen. Der Betrieb der Deutschen Bahn war stundenlang eingeschränkt, weil Anzeigetafeln auf Bahnhöfen nicht mehr richtig funktionierten. Beim National Health Service (NHS) in England wurden Gesundheitsdaten von Patienten verschlüsselt und Krankenwagen fehlgeleitet, wodurch lebensbedrohliche Situationen entstanden.

WannaCry nutzte eine Schwachstelle in der Datei- und Druckerfreigabe von Windows und befiel Rechner, die das letzte Update von Windows noch nicht installiert hatten.
Ob Unternehmen das Lösegeld bezahlten oder nicht – der Großteil sah seine Daten erst wieder, als Microsoft durch einen Notfallpatch per „Killswitch" die Schadsoftware auf allen Systemen stoppen konnte.

Die Schadsoftware hatte nur auf Endgeräten mit veraltetem Betriebssystem eine Chance. Hätten Nutzer das neuste Update von Microsoft durchgeführt, wäre die bereits bekannte Schwachstelle behoben worden. Eine der Aufgaben der Informationssicherheit besteht in der Anschaffung, Entwicklung und Instandhalten von Systemen. Dazu gehört es auch, sicherzustellen, dass alle Mitarbeiter eines Unternehmens die aktuelle und sicherste Version eines Betriebssystems installieren.

Diese Ziele verfolgen Hacker

Ransomware-Attacken wie die von WannaCry erfreuen sich bei Cyberkriminellen einer besonderen Beliebtheit (+358 % seit 2018/19). Der Verlust von Informationen wie Kunden- oder Unternehmensdaten durch Ransomware-Angriffe kann Unternehmen Stunden, Tage oder gar Wochen beeinträchtigen und bedroht neben der Wettbewerbsfähigkeit auch ihre Reputation.

Das Ziel eines Cyber-Angriffs besteht meist darin, Lösegeld für gestohlene/verschlüsselte Datensätze zu erpressen. Login-Daten zu E-Mail-Postfächern ermöglichen es Hackern zudem, ausgehend von diesen weitere Phishing-Attacken zu starten (und zum Beispiel von Kollegen oder Geschäftspartnern vertrauliche Informationen zu erbeuten). Immer populärer wird eine Strategie namens Cryptojacking – das Mining von Kryptowährungen durch die Nutzung von Rechenkapazität, ohne dass der Nutzer davon etwas mitbekommt.

Auch auf geistiges Eigentum haben Hacker es laut Bitkom-Studie abgesehen. So heißt es in einem Pressebericht: „Geistiges Eigentum wie Patente oder Forschungsinformationen wurden bei 18 Prozent gestohlen – ein Plus von 11 Prozentpunkten gegenüber den Jahren 2018/2019." Für den innovationsgetriebenen deutschen Markt führt der Verlust geistigen Eigentums zu potenziell besonders hohen Schäden.

Typische Einfallstore für Hacker-Angriffe

#1 Social Engineering – der „Faktor Mensch"
Beim Social Engineering geht es nicht um ausgefeilte Technik, sondern um die größte Schwachstelle eines jeden Sicherheitssystems: den Nutzer. Hacker bauen zu Mitarbeiter*innen eines Unternehmens entweder Vertrauen auf oder setzen diese unter Druck, um an vertrauliche Informationen wie beispielweise Passwörter oder Kreditkartendaten zu kommen. In der Regel läuft die Kommunikation digital ab. Ein Cyberkrimineller könnte sich als IT-Support-Mitarbeiterin ausgeben oder sogar als CEO und auf die Zusendung dringender, wichtiger Informationen pochen (hier ein detaillierter Artikel von heise online zu CEO-Betrügern).

Haben die Cyber-Kriminellen erst einmal eine Stresssituation geschaffen, gucken Mitarbeiter oft nicht mehr genau hin und übersehen vielleicht, dass mit der E-Mail-Adresse des Absenders etwas nicht stimmt oder das Gegenüber seltsame Daten anfordert.

#2 Unsichere Passwörter
„Labrador123", „Beate" oder „Sylt" sind typische Beispiele für beliebte, schwache Passwörter. Denn Hacker probieren beim sogenannten Password-Spraying mit Hilfe einer Software gängige Buchstabenkonstellationen aus. Ist ein Passwort persönlich mit einem Nutzer verbunden (zum Beispiel der Name des Partners, Haustiers oder Lieblings-Urlaubsorts), können Cyberkriminelle mit Wissen über die Person noch leichter an dieses Passwort kommen.

Und Passwörter sind der Schlüssel zu persönlichen Daten sowie Unternehmensdaten wie CRM-Datenbanken, E-Mail-Postfächern, etc.

#3 Schatten-IT
Als Schatten-IT wird die Hard- und Software bezeichnet, die Mitarbeiter für ihre Arbeit nutzen, ohne dass die IT-Abteilung davon weiß. Typische Beispiele sind Browser-Plug-ins und Messaging-Clients. Die Lösungen tauchen offiziell nirgendwo auf und können daher auch nicht im IT-Sicherheitskonzept berücksichtigt werden.
So schaffen unsichere Lösungen es in die tägliche Anwendung und stellen einen Angriffsvektor für Malware oder Cryptojacking dar.

#4 Homeoffice/standortunabhängiges Arbeiten

Es ist kein Zufall, dass 2020 das absolute Rekordjahr für Cyber-Attacken war. Viele Unternehmen waren von ihren Prozessen und Systemen her nicht darauf vorbereitet, die gesamte Belegschaft recht plötzlich zum Arbeiten nach Hause zu schicken. Wie eingangs erwähnt, waren besonders Ransomware-Attacken erfolgreich. Typische Angriffsvektoren für **Ransomware-Attacken** sind infizierte E-Mail-Anhänge, infizierte Downloads und Social-Engineering-Angriffe.

#5 Mangelnde Due Diligence beim Einführen von Cloud-Services

In einer Studie der IDG Research Services von 2019 gab knapp die Hälfte (47 %) der befragten Unternehmen an, Cyber-Angriffe auf ihre Cloud-Services festgestellt zu haben. Und die Anzahl dieser Art von Angriffen steigt seit Jahren konstant. Man könnte also meinen, dass Cloud-Lösungen ein erhöhtes Sicherheitsrisiko darstellen. So ganz stimmt das allerdings nicht. Die steigende Anzahl der Attacken hat ganz einfach etwas mit der zunehmenden Beliebtheit und steigenden Nutzung von Cloud-Lösungen und -Services zu tun. Oft sind Cloud-Lösungen sogar sicherer als intern gehostete IT, da sie automatisch regelmäßige Sicherheits-Updates erhalten.

Doch Cloud ist nicht gleich Cloud. Es gibt durchaus Anbieter und Lösungen mit gravierenden Lücken in Informationssicherheit und Datenschutz. Unternehmen kommen an einer Prüfung neuer Cloud-Dienstleister nicht vorbei: Liegt eine eigene Zertifizierung des Informationssicherheits-Managementsystems vor? Gibt es Ergebnisse von Sicherheitstests (sogenannten Penetrations-Tests)? Welche vertraglichen Zusicherungen gibt der Dienstleister?

KAPITEL 4

AUFBAU EINES INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEMS (ISMS)

Ein ISMS sorgt in puncto Informationssicherheit für Transparenz sowie vorhersagbare Prozesse und KPI-Ergebnisse. Sprich: Mit einem gut umgesetzten ISMS gibt es in Fragen der Informationssicherheit keine Überraschungen. Benjamin Franklin wird ein Ausspruch zugeschrieben, der den Nutzen eines ISMS im Umkehrschluss auf den Punkt bringt: „When you fail to prepare, you prepare to fail."

Ein ISMS lässt sich nur erfolgreich umsetzen, wenn es von der Unternehmensleitung wirklich gewollt und mit den nötigen Ressourcen ausgestattet wird. Lippenbekenntnisse reichen nicht. Der Informationssicherheitsbeauftragte (ISB) braucht das Vertrauen der Geschäftsleitung und muss handlungsfähig gemacht werden. So, dass er ein funktionierendes Zusammenspiel von Menschen, Tools und Prozessen für die Informationssicherheit gewährleisten kann.

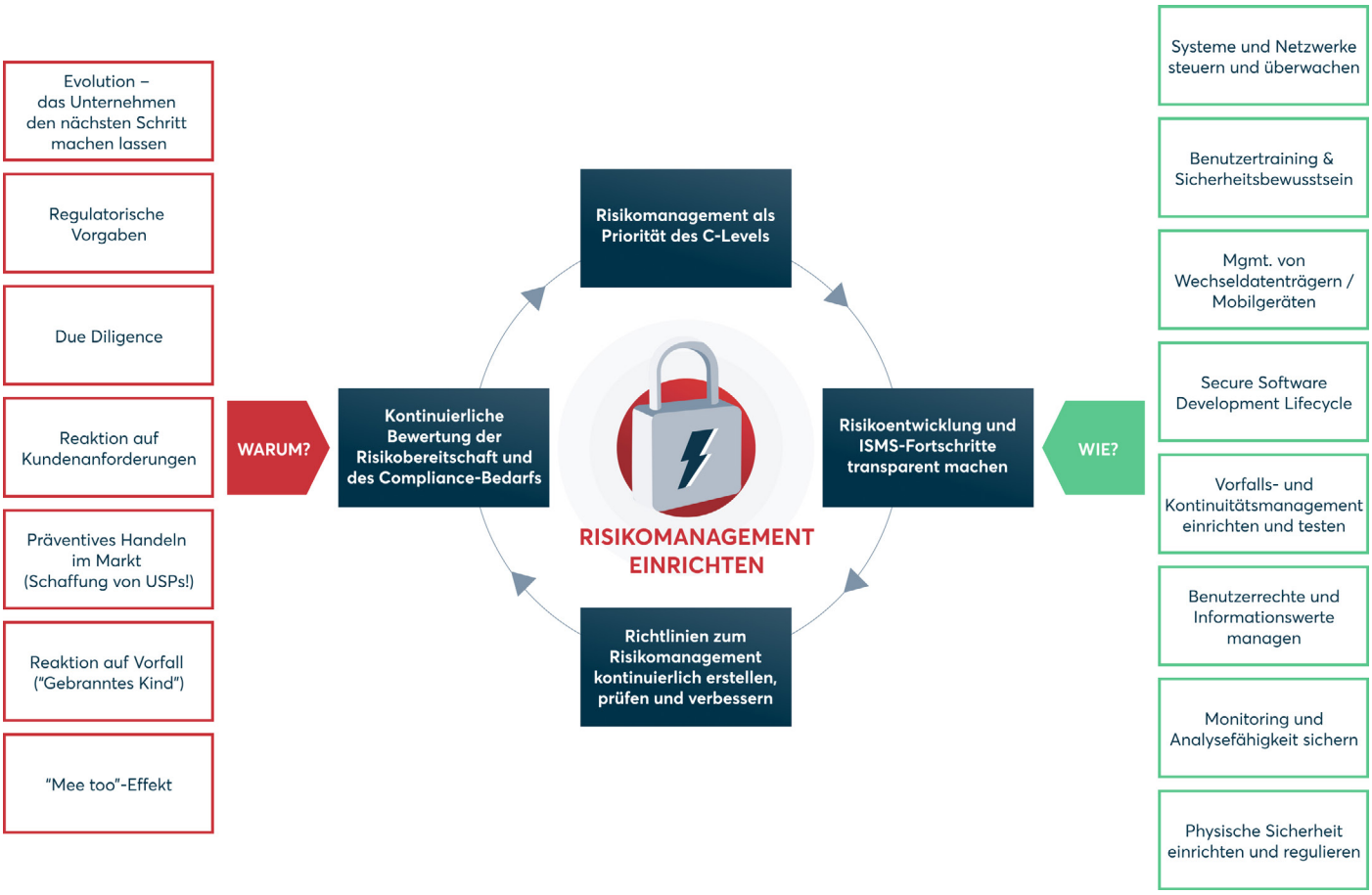
IN DIESEM KAPITEL

- Ein ISMS macht die Informationssicherheitsrisiken für Unternehmen kalkulierbar und beherrschbar.
- In Branchen mit komplexen regulierten Lieferketten wie z. B. Automotive und Gesundheit ist ein ISMS meist eine Schlüsselvoraussetzung zur Marktteilhabe.
- Darüber hinaus ist ein ISMS in der Regel zwar nicht vorgeschrieben, aber für alle Unternehmen höchst wert- und sinnvoll.
- Die Verantwortung für Einführung und Betrieb eines ISMS liegt immer beim Management (Top-Down-Ansatz).
- Über Umsetzung und Reichweite eines ISMS entscheidet der individuelle Risikoappetit einer Organisation.

Ziel eines Informationssicherheits-Managementsystems

Managementsysteme für die Informationssicherheit in Unternehmen sind prozessorientiert und – wie der Name schon sagt – immer Verantwortung des Managements. Sprich: Das ISMS verfolgt einen Top-Down-Ansatz. Das Management kann die Durchführung delegieren, nicht aber die Verantwortung selbst. Je nach Motivation entscheidet die Geschäftsführung, welche Maßnahmen und Mechanismen umgesetzt bzw. etabliert werden sollen, um das gewünschte Maß an Informationssicherheit in den Unternehmensprozessen sicherzustellen. Umfang, Intensität und Fortschritte der einzelnen Maßnahmen müssen dann fortlaufend vom Management überprüft und gesteuert werden.

Zum Verständnis: Bei einem ISMS geht es nicht darum, maximale Informationssicherheit zu erreichen. Ziel ist es vielmehr, das von der Organisation gewünschte Niveau an Informationssicherheit zu erreichen. Der Risikoappetit ist die entscheidende Kenngröße. Ein Unternehmen muss wissen, welche Informationen es hat, welchen Risiken diese ausgesetzt sind – und was es finanziell bedeuten würde, wenn sich diese Risiken realisierten. Auf dieser Wissensgrundlage hat das Management dann zu entscheiden, in welchem Umfang die Risiken durch ein ISMS reduziert werden sollen. Das ISMS ist also am Ende auch ein Instrument zur finanziellen Risikosteuerung.



Für die Einführung eines ISMS gibt es viele gute Gründe. Wer zum Beispiel in einem noch wenig regulierten Markt unterwegs ist, kann bei seinen Kunden mit hohen Standards in der Informationssicherheit punkten und seine Wettbewerbssituation verbessern. In jedem Fall steigert ein ISMS den Wert von Organisationen, denn erst ein ISMS verschafft einen genauen Überblick über die Prozesse und Informationswerte im eigenen Unternehmen. Bei der Suche nach möglichen Investoren zahlt sich ein ISMS daher unmittelbar aus: Fehlt es, ist eine **Due-Diligence-Prüfung** nur eingeschränkt möglich.

Hinzu kommen marktimmanente Gründe. Beispiel Automotive: Wenn ich als Unternehmen in diesen stark regulierten Markt eintreten und als Zulieferer eine Rolle in der Lieferkette spielen möchte, muss ich die Branchenvorgaben erfüllen und ein ISMS vorweisen. Am Ende ist auch ein bereits geschehener Informationssicherheitsvorfall immer ein Grund zum Handeln und für die Einführung eines ISMS. Doch so weit sollte es am besten gar nicht erst kommen.

Implementierung eines ISMS im Unternehmen

Spezifiziert sind die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS in der internationalen Norm ISO 27001. Aufbau und Betrieb eines ISMS folgen, vereinfacht gesagt, einem klassischen PDCA-Zyklus. PDCA steht für PLAN, DO, CHECK, ACT.

1. **ISMS-Richtlinie erstellen.** Warum wollen wir als Unternehmen ein ISMS aufbauen? Welche Ziele verbinden wir damit? Wie setzen wir ein solches System organisatorisch um? Wer übernimmt die Rolle des Informationssicherheitsbeauftragten (ISB), welche Ressourcen bekommt dieser, welche Maßnahmen sind zu ergreifen?

2. **Werte identifizieren und klassifizieren.** Welche Werte/Informationen wollen wir schützen? Wie schutzbedürftig sind diese Werte überhaupt? Beispiel Automotive: Bildmaterial von einem Fahrzeug, das noch gar nicht gebaut ist, wäre wesentlich schutzbedürftiger als Aufnahmen von einem Erlkönig im Straßentest, also einem Fahrzeug kurz vor der Markteinführung.

3. **ISMS-Organisation und Risikomanagement-Strukturen aufbauen.** Welche Tools wollen wir einsetzen? Welche finanziellen und personellen Ressourcen bekommt der ISB? Welche Strukturen soll dieser aufbauen?

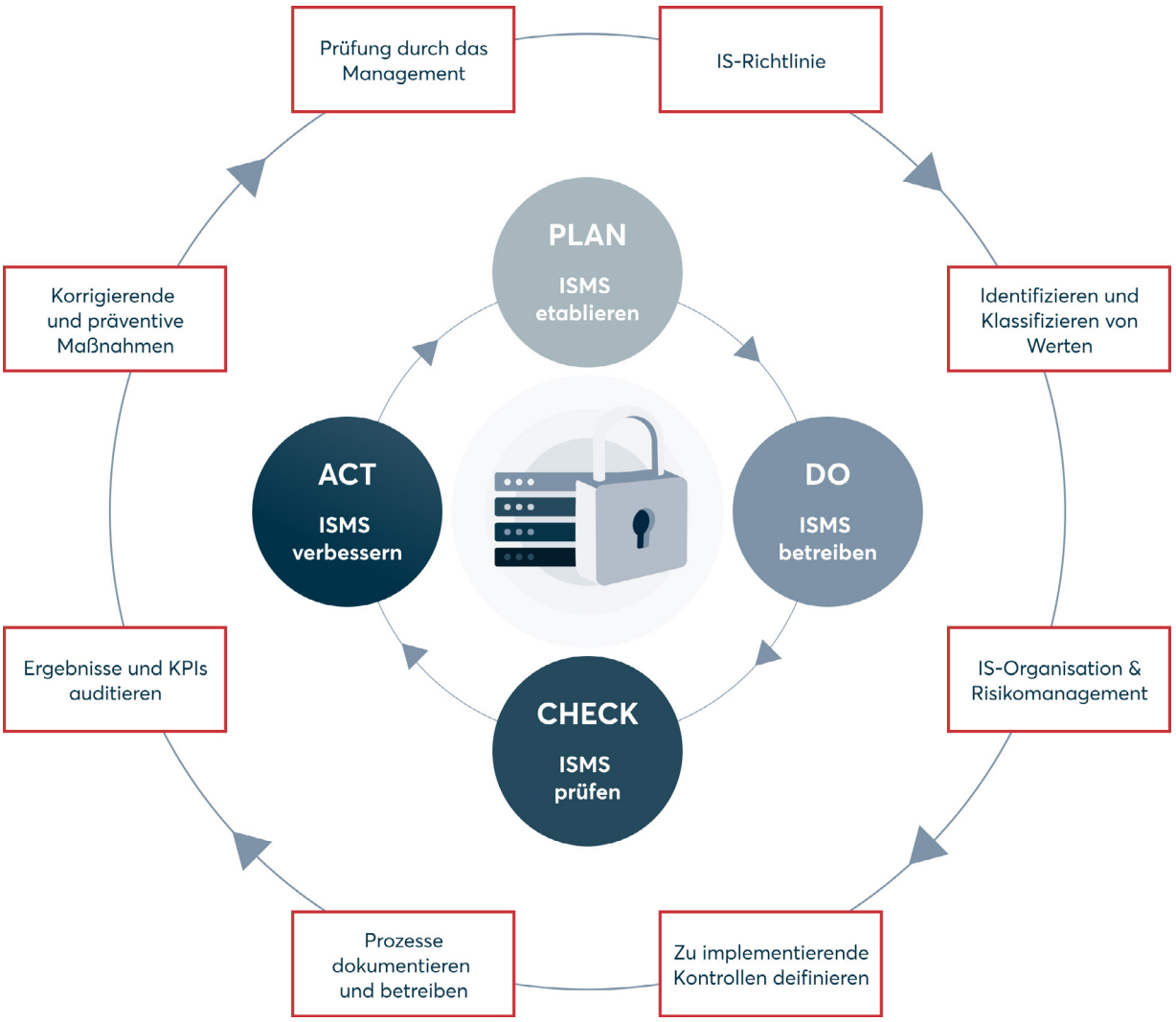
4. **Kontrollmechanismen entwickeln.** Wie überprüfen wir, ob das ISMS effektiv ist und unsere Unternehmenswerte in gewünschter Weise schützt?

5. **ISMS betreiben.** Welche Prozesse setzen wir wie im Alltag um, wie integrieren und dokumentieren wir sie?

6. **Ergebnisse und KPI überprüfen.** Es ist regelmäßig zu fragen: Welche Ergebnisse erzielt unser ISMS und welche Key Performance Indicators (KPIs) leiten wir daraus ab?

7. **Korrekturen vornehmen und vorsorgen.** An welchen Stellen müssen wir aufgrund der Ergebnisse nachbessern? Wie können wir Risiken präventiv begegnen?

8. **Überprüfung durch das Management.** Passen die ISMS-Ziele und die generelle Ausrichtung noch, oder sind Kurskorrekturen durch das Management erforderlich? Dies sollte wenigstens einmal jährlich hinterfragt werden.



KAPITEL 5

ZERTIFIZIERUNG EINES ISMS

Unternehmen, die über ein zertifiziertes Managementsystem für Informationssicherheit verfügen, profitieren vielfach. Allen voran durch systematisch erkannte und minimierte Risiken im Hinblick auf ihre IT, ihre Geschäftsaktivitäten und Prozesse sowie nicht zuletzt das Verhalten der Menschen im Unternehmen.

Sprich: Unternehmen mit zertifiziertem ISMS verfügen in puncto Informationssicherheit über ein nachweislich exzellentes Risikomanagement. Dies erhöht das Vertrauen der Kunden und potenziellen Partner oder Interessenten in die Leistungsfähigkeit eines Unternehmens und bringt somit wichtige Markt- und Wettbewerbsvorteile. Je nach Branche dient ein zertifiziertes ISMS auch als Nachweis über das Erfüllen von Compliance-Anforderungen und weiterer gesetzlicher Vorgaben, wie sie etwa für Betreiber von kritischen Infrastrukturen (KRITIS) gelten.

Sicher ist: Die Investitionen und der Aufwand für die Zertifizierung rechnen sich in jedem Fall – erst recht, wenn eine Due-Diligence-Prüfung bevorsteht. Denn diese lässt sich wesentlich schneller und einfacher durchführen, wenn das zu prüfende Unternehmen bereits nach ISO 27001 zertifiziert ist. Dies verkürzt das Verfahren und steigert den Wert eines Unternehmens oft erheblich.

IN DIESEM KAPITEL

- Die ISO 27001 ist der Goldstandard für Managementsysteme zur Informationssicherheit.
- Eine Zertifizierung des ISMS nach ISO 27001 ist für alle Unternehmen sinnvoll, die ihre Informationssicherheit gegenüber Dritten nachweisen müssen oder wollen.
- Eine Zertifizierung durch eine akkreditierte Stelle ist dabei zu empfehlen.
- Die Kosten für eine Zertifizierung hängen stark von der Unternehmensgröße, der Komplexität der Informationssicherheitsprozesse sowie den zu zertifizierenden Geschäftsbereichen ab. Für ein kleines Unternehmen mit einem Standort können erfahrungsgemäß Zertifizierungskosten von rund 10.000 € anfallen.

Gängige Zertifizierungen für Informationssicherheits-Managementsysteme

Die ISO 27001 ist so etwas wie der Goldstandard für Managementsysteme zur Informationssicherheit. Je nach Branche, Markt und nationaler Gesetzgebung können aber noch weitere Standards in Betracht kommen. In Deutschland sind dies etwa vom **Bundesamt für Informationssicherheit (BSI)** die Standards **BSI 200-1** und **BSI 200-2**. Speziell für Kommunen und KMU interessant ist **ISIS12**: Dieser Standard beschreibt ein Modell zur Einführung eines Informations-Sicherheitsmanagementsystems in 12 Schritten.

Wichtig für die Zusammenarbeit mit staatlichen US-Informationssystemen ist die **NIST-Norm** (National Institute of Standards and Technology) 800-53. Relevant im Hinblick auf die Finanzberichterstattung eines Unternehmens können darüber hinaus die internationalen **Service Organization Control Normen SOC 1 und SOC 2** sein.

Akkreditierte Zertifizierungen nach ISO 27001

Eine Zertifizierung des ISMS nach ISO 27001 ist für alle Unternehmen sinnvoll, die ihre Informationssicherheit gegenüber Dritten nachweisen müssen oder wollen. Aber eine solche Zertifizierung kostet Geld. Nicht nur das Audit an sich muss bezahlt werden, auch die Umsetzung der Anforderungen kann so einiges an Ressourcen fressen. Es wäre also ärgerlich, wenn am Ende der Anstrengungen ein Zertifikat stünde, das wenig bis nichts wert ist.

Für die ISO 27001 gibt es derzeit rund **50 akkreditierte Zertifizierungsstellen** in Deutschland. Das heißt, dass diese Stellen von der **„Deutschen Akkreditierungsstelle" (DAkkS)** geprüft und akkreditiert worden sind. Die DAkkS ist in Deutschland die Akkreditierungsstelle für alle Managementsysteme gemäß ISO-Standards und vom **Internationalen Accreditation Board B** benannt. Die durch die DAkkS akkreditierten Unternehmen auditieren gemäß der ISO 19011 – der Norm für Auditmanagementsysteme.

→ **Eine Liste aller aktuell akkreditierten Zertifizierungs-stellen finden Sie hier.**

Wird das Zertifikat nicht durch die internationale Akkreditierungsstelle bestätigt, wird es auch von Vertragspartnern oft nicht anerkannt. Enthält zum Beispiel ein Vertrag die Anforderung an eine ISO 27001-Zertifizierung, ist damit normalerweise die Zertifizierung durch eine akkreditierte Stelle gemeint. Daher ist in jedem Fall eine Zertifizierung durch eine akkreditierte Stelle zu empfehlen.

Kosten für eine Zertifizierung nach ISO 27001

Der größte Aufwand ist die eigentliche Umsetzung der Norm. Die Erfüllung aller Anforderungen kann Monate oder auch Jahre in Anspruch nehmen und erfordert häufig die Beratung durch externe Dienstleister, die nicht selten Tagessätze von 1.500 € und mehr berechnen.

Im Vergleich dazu fällt der Zertifizierungsprozess nicht mehr allzu sehr ins Gewicht. Allerdings entscheidet sich hier, inwiefern sich der Aufwand zur Umsetzung gelohnt hat. Findet die Zertifizierungsstelle erhebliche Mängel und besteht Ihr Unternehmen daher das Audit nicht, muss ein neuer Audittermin gefunden werden, der Prozess beginnt von vorne und die Kosten steigen.

Ganz grob können mittelständische Unternehmen mit 100 Mitarbeitern und relativ geringer Prozess-Komplexität pro 15 bis 20 Mitarbeiter mit einem Audit-Tag rechnen. Bei größeren Unternehmen ändert sich der Aufwand. Natürlich hängt der eigentliche Zeitaufwand stark von der Komplexität der Informationssicherheitsprozesse ab – und dem Geltungsbereich, den ein Unternehmen für sein ISMS definiert hat. Für ein kleines Unternehmen mit einem Standort können erfahrungsgemäß Zertifizierungskosten von rund 10.000 € anfallen. Die tatsächlichen Kosten teilen Zertifizierungsstellen auf Anfrage mit.

Ablauf und Häufigkeit von Re-Zertifizierungen

Weil die Umsetzung von Informationssicherheitsmaßnahmen kein einmaliges Projekt ist, sondern ein fortlaufender Prozess, müssen auch Zertifizierungen in gewissen Abständen aufgefrischt werden. Die ISO 27001 sieht alle drei Jahre eine Re-Zertifizierung mit einem komplett neuen Audit-Prozess vor. Weniger umfangreiche Kontrollen durch die Zertifizierungsstelle müssen sogar jährlich stattfinden. Werden hier gravierende Mängel festgestellt, kann Unternehmen die Zertifizierung frühzeitig entzogen werden. Zudem enthält die ISO 27001 Anforderungen, die interne Audits im Jahresrhythmus vorsehen.

KAPITEL 6

JOBS IN DER INFORMATIONSSICHERHEIT

Weltweit fehlen rund **3 Millionen Cyber-Security-Fachkräfte**. Das **Magazin IT-Sicherheit Online** ernannte den Fachkräftemangel in der Informationssicherheit zu einem der top vier Trends, auf den Unternehmen sich einstellen müssen. Überraschend ist das nicht – vereinen Berufe in der Informationssicherheit gleich mehrere Anforderungen, die rar sind auf dem Arbeitsmarkt: Neben fundierten IT-Kenntnissen müssen Bewerber sich mit gängigen Normen und Gesetzen der Informationssicherheit auskennen. Darüber hinaus erfordern die meisten Rollen Kommunikations- und Verhandlungsgeschick. Denn die Umsetzung von Informationssicherheitsprozessen klappt nur, wenn alle Abteilungen kooperieren.

IN DIESEM KAPITEL

- Informationssicherheitsexperten sind auf dem Arbeitsmarkt heiß begehrt.
- Für einen Job in der Informationssicherheit ist kein bestimmtes Studium erforderlich: Informatiker und BWLer sind gleichermaßen geeignet.
- Entscheidend sind vielmehr die bisherige Arbeitserfahrung und Kenntnisse zur ISO 27001 und Informationssicherheits-Managementsystemen.

Anforderungen an Angestellte in der Informationssicherheit

Wege in die Informationssicherheit gibt es viele. So können Informatiker Schulungen zur ISO 27001 sowie dem IT-Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik besuchen. Oder aber Betriebswirte bilden sich im Bereich der IT-Sicherheit fort und lassen sich als Informationssicherheitsbeauftragter zertifizieren. Viele Universitäten bilden mittlerweile Masterstudiengänge in der IT-Sicherheit an. Unbedingt erforderlich ist ein solches Studium aber nicht, um sich im Bereich der Informationssicherheit eine Karriere aufzubauen.

Vielmehr kommt es darauf an, dass Mitarbeiter Erfahrung in den folgenden Bereichen mitbringen:

- Implementierung der IT-Sicherheit, inkl. einem Verständnis kritischer Infrastrukturen
- Aufbau eines ISMS
- Zertifizierung des ISMS nach ISO 27001/TISAX®*
- Bearbeitung von und Umgang mit Informationssicherheitsvorfällen
- Mitarbeiterschulungen und Sensibilisierungsmaßnahmen
- Verhandlungen und Projektmanagement

Wer es in die Position eines Information Security Analysts, eines Informationssicherheitsbeauftragten oder einen ähnlichen Job geschafft kann, kann sich über hohes Ansehen im Unternehmen und schnell ein sechsstelliges Jahresgehalt freuen.

Der (Chief) Information Security Officer im Überblick

Der **Chief Information Security Officer (CISO) oder Informationssicherheitsbeauftragte (ISB)** kann sich auf die Interessen des Unternehmens konzentrieren. Dabei muss er einen wichtigen Balanceakt meistern: den zwischen dem Schutz von Informationen und einem reibungslosen Geschäftsablauf. Er ist normalerweise direkt dem Top-Management unterstellt, arbeitet aber besonders eng mit der IT-Abteilung sowie den Compliance- und Legal-Teams zusammen.

Zu seinen Aufgaben gehören:

- Schutz von Unternehmenswerten vor Angriffen und Datenverlusten (in Zusammenarbeit mit dem Datenschutzbeauftragen und der IT)
- Zertifizierungen nach ISO 27001/27002 bzw. TISAX®*
- Einführung eines Informationssicherheits-Managementsystems
- Auswahl geeigneter Methoden und Tools
- Risikomanagement und Beratung der Geschäftsführung
- Abteilungsübergreifende Kommunikation

Oft sind CISOs Informatiker oder Informatiker mit Weiterbildungen oder Spezialisierungen im Bereich Sicherheit und langjähriger Berufserfahrung. Der Aufgabenbereich eines CISO ist nicht gesetzlich vorgeschrieben und hängt sehr vom jeweiligen Unternehmen und den einzuhaltenden Regeln ab. Eine Ausnahme bieten hier z. B. Spezialfälle im öffentlichen Sektor.

Je nach Anforderungen des Unternehmens kann die Stelle des CISO durch einen internen Mitarbeiter oder einen externen Dienstleister besetzt werden.

* TISAX® ist eine eingetragene Marke der ENX Association

Informationssicherheit outsourcen

Nicht jedes Unternehmen kann oder will die Informationssicherheit mit internen Ressourcen umsetzen und managen. Oder aber das interne Team ist überlastet, kommt mit dem Dokumentationsaufwand nicht hinterher, besitzt nicht die nötige Expertise für ein bestimmtes Projekt, fällt durchs Audit …. Dann bietet sich ein externer Dienstleister an, der gezielt beraten kann.

Der Vorteil: Externe Services können schnell eingekauft werden und erfordern dank dem Erfahrungsschatz der Dienstleister kein langes Onboarding. Ein guter Anbieter teilt seinen Kunden einen persönlichen Ansprechpartner zu, der sich mit den aktuellen Herausforderungen des Kunden auskennt, und diese schon an anderer Stelle meistern konnte.

Auch die Kosten für einen externen Dienstleister liegen deutlich unter denen für eine Vollzeitstelle. Bei DataGuard zahlen Kunden zwischen 500 und 2.000 € pro Monat – je nach Komplexität.

DataGuard ist ein Compliance-Software-Unternehmen mit Fokus auf Datenschutz und Informationssicherheit. Als einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard Tausenden KMU und Großunternehmen die unkomplizierte Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance (kurz: „PIC"). Mit seiner Komplettlösung reduziert DataGuard für Unternehmen Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001. So können sich Kunden auf ihr Kerngeschäft konzentrieren, Mehrwert durch Vertrauen und Compliance schaffen und gleichzeitig Risiken minimieren. DataGuard hat Standorte in München, Berlin, London und Wien.

Weiterführende Ressourcen:

→ **ISO Roadmap**

→ **Vorbereitung auf Ihr Informationssicherheitsaudit - Webinar**

→ **ISO 27001 Assessment - Wie gut sind Sie auf Ihr Audit vorbereitet?**

dataguard.de kontakt@dataguard.de +49 89 452 459-900

DataGuard