Mittelstand 4.0
Agentur Prozesse

LEITFADEN

IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen

Grundvoraussetzungen, organisatorische und rechtliche Anforderungen für die Digitalisierung und Industrie 4.0

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Analysieren Sie das IT-Sicherheitsniveau in Ihrem Unternehmen unter **www.sitom.de**

Inhalt

Impressum

Herausgeber und Redaktion
Mittelstand 4.0-Agentur Prozesse
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9, 39108 Magdeburg
Tel.: +49 391 74435-20 • Fax: +49 391 74435-11
E-Mail: rhallau@tti-md.de
Geschäftsführer: Dr. Michael Klaeger, Marko Wunderlich
Amtsgericht Stendal, HRB 104429
Umsatzsteuer-Identifikationsnummer: DE 139 310 185

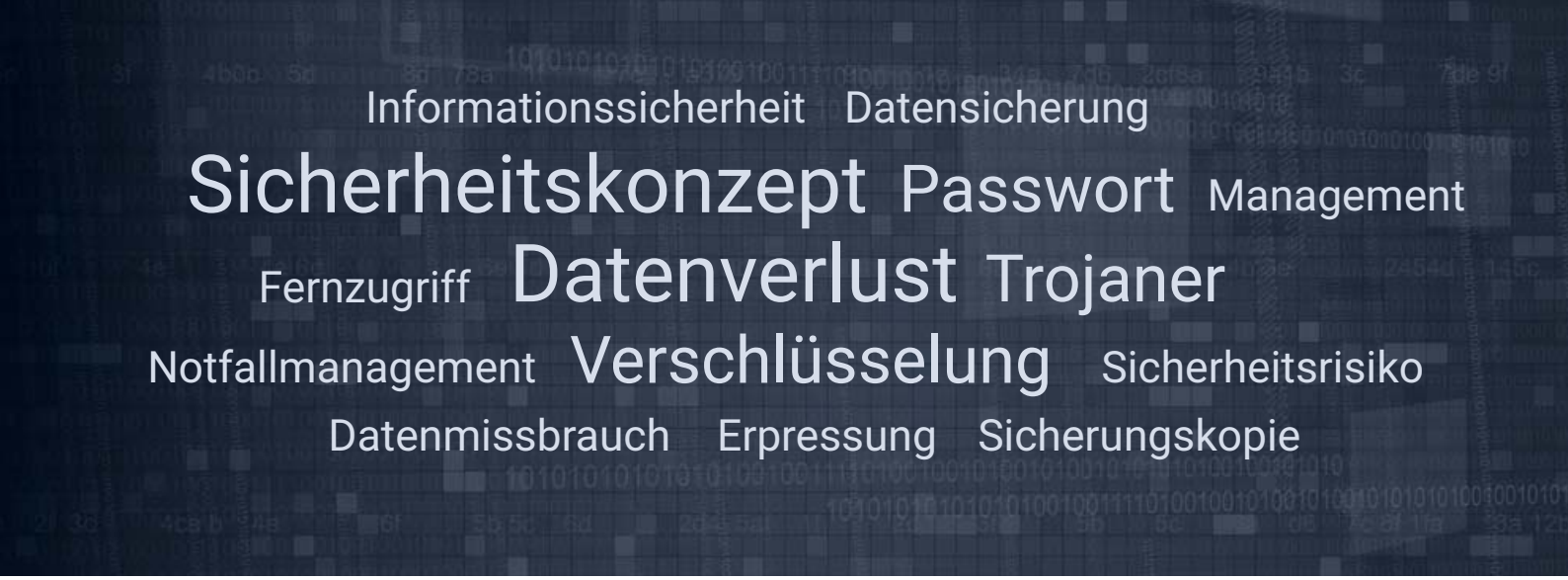
Redaktionelle Unterstützung:
Mittelstand 4.0-Agentur Handel
c/o IFH Institut für Handelsforschung GmbH
Dürener Str. 401 b, 50858 Köln
www.ifhkoeln.de

Grafische Konzeption und Gestaltung
toolboxx-media UG (haftungsbeschränkt), www.toolboxx.de

Bildnachweis
sdecoret, Jakub Jirsák, ekostsov, rvlsoft, hywards, markus dehlzeit, adam121, WavebreakMediaMicro, designer491, Olivier Le Moal – Fotolia.com
tti Magdeburg GmbH, Bundesministerium für Wirtschaft und Energie

Auflage: 1.000 Stk.

Magdeburg, Oktober 2017



Editorial

Liebe Leserinnen und Leser,

Die zunehmende Digitalisierung führt zu weitreichenden Veränderungen in Produktions- und Arbeitsprozessen. Um die langfristige Wettbewerbsfähigkeit sicherzustellen, sind in allen Bereichen informationstechnische Unterstützungen erforderlich. Dies geht über etablierte Prozesse wie das Anbieten von Waren und Dienstleistungen oder die Vorstellung der eigenen Firma im Internet weit hinaus.

Ein Großteil der Kommunikation mit Kunden, anderen Unternehmen und internen Abteilungen findet zunehmend digital statt. Die Einrichtung und Nutzung derartiger Systeme erfordert oft spezielles Fachwissen über Informationstechniken (IT), wodurch die Anforderungen an die Mitarbeiter steigen.

In den meisten Fällen sind in kleinen und mittleren Unternehmen (KMU) jedoch keine Mitarbeiter mit fachspezifischen IT-Kenntnissen oder gar IT-Fachleute angestellt. Das birgt die Gefahr, dass Unternehmen bei der alltäglichen Nutzung der IT-Systeme manche Sicherheitsgefahren nicht oder nur unzureichend erkennen. Dieser Leitfaden gibt Auskunft über Grundanforderungen an die Basissicherheit in Unternehmen und welche organisatorischen sowie rechtlichen Anforderungen Unternehmen bewältigen müssen.

Die unternehmensspezifische Ausgestaltung der firmeneigenen Informationssicherheit ist von zahlreichen individuellen Gegebenheiten des Unternehmens abhängig und kann an dieser Stelle nicht pauschal beantwortet werden. In Abhängigkeit von der Branche, Größe und Ausrichtung Ihres Unternehmens müssen Sie gegebenenfalls weiterführende Schutzmaßnahmen etablieren. Die Aspekte der Basissicherheit müssen in jedem Fall Berücksichtigung finden, um ein Mindestmaß an Sicherheit zu gewährleisten.

Die in diesem Leitfaden zusammengestellten Informationen und Handlungsempfehlungen sollen für KMU eine Hilfestellung zur Verbesserung ihrer IT-Sicherheit darstellen. Die enthaltenen Checklisten unterstützen Sie dabei, herauszufinden, ob Sie die organisatorischen und rechtlichen Anforderungen bereits erfüllen oder ob noch Handlungspotenziale offen sind.

Mit den besten Grüßen

Mittelstand 4.0-Agentur Prozesse
c/o tti Technologietransfer und
Innovationsförderung Magdeburg GmbH

1. Aspekte der Basissicherheit

Ein entscheidender Faktor bei der Digitalisierung ist das Auseinandersetzen mit der IT. Zwar erleichtert der IT-Einsatz viele Prozesse und ist wichtig, um wettbewerbsfähig zu bleiben, jedoch darf die Verwendung nicht allzu sorglos erfolgen. Sie müssen sicherstellen, dass Sie alle Ihre Daten regelmäßig sichern, sich um Virenschutzsoftware kümmern, Updates regelmäßig einspielen und Ihr Netzwerk ausreichend absichern. Auf was Sie dabei im Einzelnen achten müssen, wird in den nächsten Kapiteln erläutert.

DATENSICHERUNG

Daten, wie etwa Kunden- oder Lieferantendaten sowie mit Sicht auf die zunehmende Digitalisierung von Produktionsprozessen insbesondere auch Auftrags-, Prozess- und Maschinendaten, zählen heute zu den wichtigsten Gütern im Unternehmen. Sie ausreichend zu schützen, ist für Unternehmen eine Überlebensfrage.

Wertvolle Daten schützen

Nicht nur Viren, Würmer und andere Schadsoftware können unternehmenskritische Daten vernichten. Mindestens genauso hoch ist das Risiko des Datenverlustes durch Ausfälle von Hard- und Software oder durch Fehlbedienung, wie etwa versehentliches Löschen. Wenn beispielsweise ein so genannter Festplatten-Crash die Daten zu Kunden, Aufträgen, Buchhaltung und Personal vernichtet, können kleine Unternehmen praktisch schon vor dem Aus stehen.

Daten sind wichtige Unternehmenswerte

Das versehentliche Löschen eines elektronischen Dokuments kann die Arbeit von Tagen oder Wochen zerstören.

Beispiele für empfindliche Datenverluste durch

- unabsichtliches Löschen einer zentralen Adressdatenbank,
- Vernichtung oder Verschlüsselung von bestimmten Dateien durch Schadsoftware,
- Verlust aller Daten durch einen Festplattenausfall oder
- den Diebstahl eines Notebooks gibt es viele.

Was sollten Sie sichern?

Sie sollten auf jeden Fall die Daten sichern, die Sie selbst erzeugt haben. Dazu zählen die Daten, die Sie durch Anwendungsprogramme (z.B. Textverarbeitung, Tabellenkalkulation, Präsentation, E-Mail, Rechnungswesen, Konstruktion, Lager und Finanzen) erstellt haben oder die Sie im Rahmen Ihrer Geschäftsbeziehungen mit Ihren Kunden (z.B. Artikeldaten, Preisangaben, Informationen zu den Angeboten und zum Auftrag) erhalten haben.

Weiterhin ist es wichtig, dass Sie auch produktionsspezifische Daten (Auftrags- und Prozessdaten, Maschinenprogramme wie z.B. für die Steuerung von CNC-Maschinen) sichern.

DATENBESTAND STRUKTURIEREN
Organisieren Sie die zu sichernden Daten auf Ihren Rechnern in möglichst wenigen Ordnern in einer klaren Struktur. Sichern Sie diese Ordner komplett und definieren Sie die Zugriffsrechte. Schaffen Sie auch für die relevanten Daten aus dem Produktionsbereich eine transparente Struktur für eine effektive Datensicherung.

Wann sollten Sie sichern?

Wie oft Sie Ihre Daten sichern, hängt davon ab, welche Risiken Sie in Kauf nehmen wollen. Generell ist jedoch eine tägliche Sicherung empfehlenswert.

SICHERUNGSINTERVALL FESTLEGEN
Bestimmen Sie in Ihrem Unternehmen einen Verantwortlichen für die Datensicherung. Wenn Sie täglich sichern wollen, legen Sie möglichst einen Zeitpunkt nach Feierabend fest.

Wie sollten Sie sichern?

Da eine manuelle Sicherung immer mit einem gewissen Risiko (Sicherung wird vergessen, Sicherung mit fehlerhaften oder wechselnden Einstellungen und andere) verbunden ist, sollten KMU den Sicherungsvorgang idealerweise automatisieren. Für die Datensicherung gibt es professionelle Programme, die teilweise auch als freie Software zur Verfügung stehen.

SICHERUNG AUTOMATISIEREN
Schon die vom Betriebssystem bereitgestellten Systemprogramme zur Datensicherung (Backup) genügen den Grundanforderungen in Bezug auf eine automatisierte Sicherung der Daten in KMU.

Wohin sollten Sie die Daten sichern?

Grundsätzlich sind alle Medien geeignet, auf die sich Daten speichern lassen (z.B. CD/DVD, Magnetband, externe Festplatte, USB-Stick). Die Praxis hat jedoch gezeigt, dass CD/DVD aufgrund der Fehleranfälligkeit nur eingeschränkt zu empfehlen sind. Da Datenträger nur eine begrenzte Haltbarkeit haben, sollten Sie darauf achten, diese regelmäßig zu testen und vor Ablauf der zugesicherten Haltbarkeit auszutauschen. Bei einer täglichen Sicherung empfehlen wir zudem, mehrere Medien (z.B. eine externe Festplatte für jeden Tag der Woche) zu verwenden.

DAS RICHTIGE MEDIUM AUSWÄHLEN
Da Datenträger nur eine begrenzte Haltbarkeit haben, sollten Sie darauf achten, ein Medium zu verwenden, auf das die komplette Datensicherung passt.

ANGEBOTE VON ONLINEDIENSTEN PRÜFEN
Die Datensicherung kann auch über verschiedene Anbieter im Internet online durchgeführt werden. Lassen Sie sich hierbei ausführlich von Experten beraten.

Wo sollten Sie die Sicherungsmedien aufbewahren?

Je nach Vertraulichkeit (z.B. personenbezogene Daten) und Wichtigkeit (z.B. für Betriebsprüfungen, PPS-Programme) der Daten sollten Sie die Medien in einem verschließbaren Schrank oder Safe aufbewahren. Für einen zusätzlichen Schutz vor Feuer- oder Wasserschäden achten Sie bei der Auswahl auf eine entsprechende Schutzklasse.

DEN AUFBEWAHRUNGSORT RICHTIG WÄHLEN
Bewahren Sie zusätzlich eine Sicherheitskopie (z.B. die vorletzte Sicherung) an einem anderen sicheren Ort auf (z.B. Bankschließfach).

Worauf sollten Sie besonders achten?

Bei automatisierter Sicherung sollten Sie prüfen, ob die Datensicherung auch tatsächlich erfolgt ist und ob sie vollständig war. Ihre IT-Infrastruktur kann sich im Lauf der Zeit verändern (neue Software, neue Hardware), daher sollten Sie die Datensicherung entsprechend anpassen.

SICHERUNGSPROTOKOLLE EINSEHEN
Sicherungsprogramme erstellen in der Regel ein Protokoll, aus dem Sie ersehen können, was und wann gesichert wurde. Achten Sie hier insbesondere auf Fehlerhinweise.

PRÜFEN UND WIEDERHERSTELLUNG VON DATEN
Prüfen Sie gelegentlich, ob sich Ihre Daten auch zurücksichern lassen. Schulen Sie hier entsprechend das Personal.

KONZEPT DER DATENSICHERUNG FORTSCHREIBEN
Prüfen Sie bei Neuanschaffungen oder Änderungen in der IT-Infrastruktur, ob die Datensicherung angepasst werden muss. Beziehen Sie die im Produktionsbereich vorhandenen Daten immer mit ein.

Was ist keine Datensicherung?

Die Daten sind nicht ausreichend gesichert, wenn Sie sie einfach nur auf dieselbe Festplatte in ein anderes Verzeichnis kopieren oder auf eine andere interne Festplatte. Ebenso wenig reicht das Speichern von Daten auf einem Server oder der Einsatz von gespiegelten Festplatten (z.B. RAID-Systeme).

SPEICHERMEDIUM NACH SICHERUNG VOM IT-SYSTEM TRENNEN
Das Medium, auf das die Daten gesichert werden, sollte nach einer erfolgten Datensicherung physikalisch von der vorhandenen IT-Infrastruktur getrennt werden (z.B. Speicherband herausnehmen, USB-Stick abziehen, Verbindung zur externen Festplatte trennen).

CHECKLISTE DATENSICHERUNG

- Einen verantwortlichen Mitarbeiter für die Durchführung der Sicherung bestimmen.
- Eine Vertreterregelung etablieren, um sicher zu stellen, dass dieser Prozess unterbrechungsfrei durchgeführt wird.
- Eine Liste der wichtigsten Daten erstellen sowie deren Speicherort ermitteln.
- Die Liste in regelmäßigen Abständen auf Aktualität überprüfen.
- Die wichtigsten Daten regelmäßig sichern.
- Die geheimen und/oder sensiblen Daten unbedingt verschlüsseln.
- Die Datensicherungen regelmäßig auf Funktion und Rückspielbarkeit überprüfen.
- Datenrücksicherung stichprobenartig testen.
- Den Prozess der Datensicherung dokumentieren.
- Beim Arbeiten mit mobilen Datenträgern (Laptops) eine Regelung treffen, wie diese Daten gesichert werden.
- Eine sichere Aufbewahrung der Speichermedien gewährleisten (insbesondere als Schutz vor Diebstahl, unberechtigtem Zugriff und Schäden durch Feuer und Wasser).
- Im Störfall eine automatisierte Warnmeldung an den verantwortlichen Mitarbeiter versenden.

VIRENSCHUTZ

Ein weiterer grundlegender Aspekt bei der Gewährleistung einer umfassenden Basissicherheit ist der Schutz vor Schadsoftware (Viren, Trojaner usw.). Dazu ist die Anschaffung, Installation und der Betrieb eines Antivirenprogrammes auf ausnahmslos jeder IT-Komponente zwingend notwendig. Des Weiteren müssen Unternehmen ihre Mitarbeiter über das Thema aufklären und sensibilisieren.

Um ein Unternehmen ausreichend vor den Bedrohungen durch Schadsoftware zu schützen, müssen alle Systeme, wie z.B. PC, Server, (Produktions-)Anlagen entsprechend geschützt werden. Dazu gehört die Installation von Virenschutzprogrammen auf allen lokalen Rechnern und – soweit vorhanden – auf allen Servern sowie auch auf evtl. vorhandenen mobilen Endgeräten (Tablets, Smartphones). Denken Sie auch daran, dass bei einer entsprechenden Ausstattung auch Ihre Produktionsanlagen von

Viren befallen werden können. Bei der Auswahl geeigneter Virenschutzmaßnahmen ist die nebenstehende Checkliste zu beachten.

Der ständigen Aufklärung und Sensibilisierung der Mitarbeiter über die Gefahren kommt eine besonders große Bedeutung zu. Mit einem bewussten Handeln auf der Basis von nur wenigen Grundsätzen können KMU die größten Gefahrenquellen ausschalten.

- Niemals unbekannte E-Mail-Anhänge herunterladen oder öffnen sowie enthaltene Links anklicken,

- Keine Daten von Internetseiten unbekannten Ursprungs herunterladen,

- Datenträger (wie USB-Sticks und CD/DVD) von externen Personen vor der Verwendung immer erst auf Schadsoftware überprüfen,

- Sperren diverser Funktionen, wie aktive Inhalte, Autostart-Funktion bei Einlegen eines Datenträgers, automatisches Herunterladen bei Downloads usw.

CHECKLISTE VIRENSCHUTZ

- Analyse und Dokumentation aller relevanten Schnittstellen, über die das Eindringen von Schadsoftware möglich ist (Systeme mit Internetanbindung, physische Anschlüsse, Verwendung externer Datenträger).
- Überprüfung, ob auf allen Geräten ein Schutzprogramm installiert ist.
- Schutzsoftware so konfigurieren, dass eine automatische Aktualisierung stattfindet.
- Stichpunktartig und wiederholt prüfen, ob die Schutzsoftware auf einem aktuellen Stand ist.
- Systeme, auf denen keine Schutzprogramme installiert werden können, sollten keine Internet verbindung haben und durch separate Firewalls geschützt werden. Optimal ist in diesen Fällen eine komplette Trennung dieser Systeme, auch von den internen Netzwerken (z.B. Office-Bereich).
- Mobile Endgeräte wie Tablets und Smartphones benötigen ebenso ein Schutzprogramm.
- Beachten Sie bei der Softwareauswahl eventuell vorhandene heterogene Systeme (Windows, Apple, oder Linux).
- Das Virenschutzprogramm sollte Schadprogramme in aktiven Inhalten erkennen.
- Im Zusammenhang mit einer sicheren E-Mail-Kommunikation bei der Nutzung eines eigenen E-Mail-Servers einen Mail-Proxy aufsetzen.
- Hinsichtlich der Bedrohungen durch das Surfen im Internet empfiehlt sich das Einrichten eines Web-Proxys.
- Bei den eingesetzten Internet-Browsern sollte die Installation von sogenannten Add-ons geprüft werden, die das Ausführen von Scripten verhindern (z.B. NoScript bei Firefox).

Sollten Sie sich bei der Auswahl eines geeigneten Schutzprogrammes mit den genannten Aspekten überfordert fühlen, nehmen Sie die Hilfe externer IT-Dienstleister in Anspruch. Zusätzlich gibt es zahlreiche Testberichte zu vorhandenen Schutzprogrammen.

Weitere Informationen zum Thema “Virenschutz“ liefern die Mittelstand 4.0-Kompetenzzentren bzw. Agenturen und das Internetportal des Bundesamtes für Sicherheit in der Informationstechnik (http://www.bsi.de).

UPDATES

Der Aktualität von Software auf allen eingesetzten IT-Komponenten kommt unter dem Aspekt der IT-Sicherheit eine sehr große Bedeutung zu. Die von den Herstellern angebotenen Aktualisierungen bringen nicht nur Verbesserungen an der Software, sondern schließen bekannt gewordene Sicherheits-

lücken. Deshalb ist es sehr wichtig, dass nicht nur bei den im vorangegangenen Abschnitt beschriebenen Schutzprogrammen auf Aktualität geachtet wird. Das bezieht sich neben den Betriebssystemen und der Anwendungssoftware auch auf die sogenannte Firmware von Geräten und Anlagen (z.B. das BIOS eines Rechners).

Zwecks Prüfung, ob alle Geräte immer auf dem aktuellen Stand sind, müssen Sie sich erst einen Überblick verschaffen, welche Programme Sie einsetzen. Hierfür empfiehlt sich eine entsprechende Dokumentation. Notieren Sie sich, welche Programme und Systeme sich automatisch aktualisieren und welche Sie selbst aktuell halten müssen. Zahlreiche Softwareprodukte ermöglichen die Einstellung einer automatischen Aktualisierung. Informieren Sie sich über die Updatemöglichkeit Ihrer Softwareprodukte und achten Sie darauf, ob es noch einen Support (Unterstützung, unter anderem auch das Herausbringen von Updates) zu ihrer Software gibt. Falls der Support für Ihr Softwareprodukt schon ausgelaufen ist und somit die Gefahr besteht, dass Sicherheitslücken nicht geschlossen werden, informieren Sie sich über Upgrade-Möglichkeiten (Update der Software auf eine neue Version) oder ein alternatives Produkt.

ACHTUNG:

Das Einspielen von Updates für Betriebssysteme und Firmware kann unter Umständen zu Störungen bei weiteren Anwendungsprogrammen und Ihrer Produktion führen. Um zu vermeiden, dass branchenspezifische Programme nach der Durchführung des Updates nicht mehr oder nur eingeschränkt zur Verfügung stehen, sollten Sie:

- entweder einen Testlauf auf lediglich einem Rechner Ihres Unternehmens durchführen oder
- eine gewisse Zeit warten, bevor Sie das Update durchführen, um dieses Problem zu vermeiden.

Im Endeffekt kommt es hier zu einer Abwägung zwischen einer tagesaktuellen Sicherheit durch das sofortige Einspielen der neuen Programmbausteine oder aber einer gewissen Verzögerung zu Testzwecken, um auf diesem Weg zu erreichen, dass alle Programme störungsfrei betrieben werden können.

CHECKLISTE UPDATES

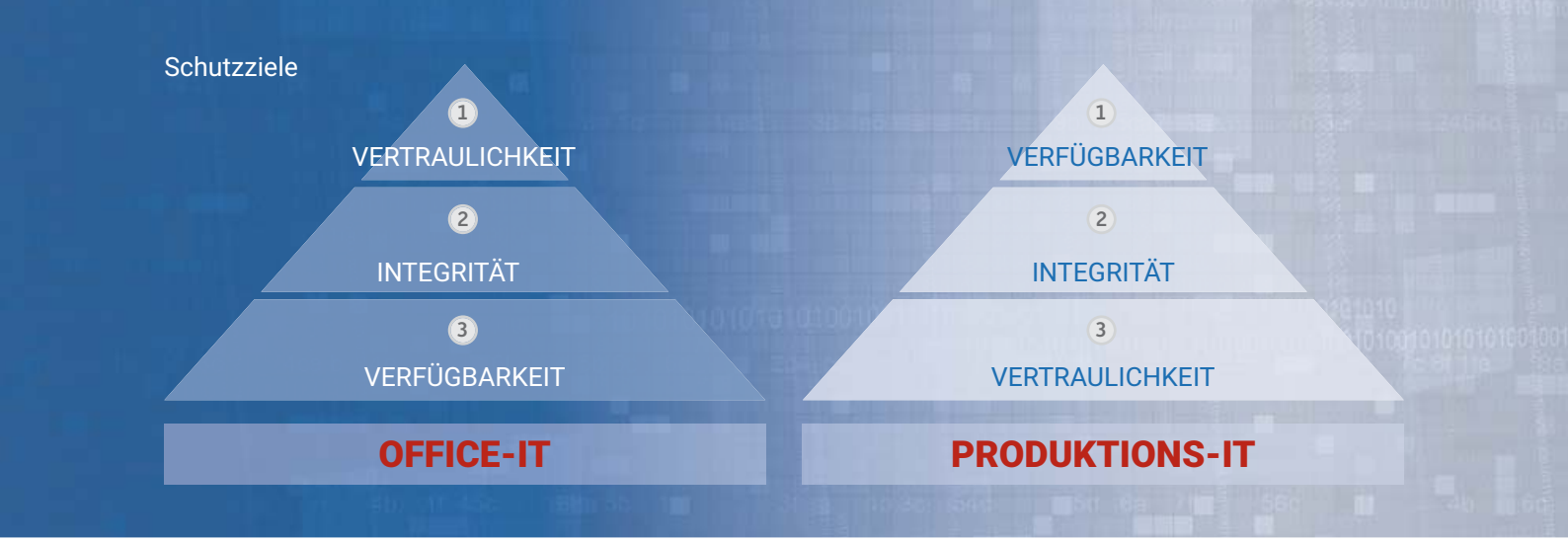
- Liste aller genutzten Programme und Systeme erstellen.
- Jedes gelistete Programm und System auf die Möglichkeit von Updates prüfen.
- Bei Software: Die Anwendung starten und dort in der Hilfefunktion das Suchwort „Update“ eingeben.
- Bei Hardware: Die aktuelle Firmware-Version aus lesen und beim Hersteller nach neueren Versionen suchen (Achtung: nicht in jedem Fall ist der Einsatz einer aktuellen Firmware ratsam, da unter Umständen die Systeme bzw. Software nicht kompatibel sind).

Liste der genutzten Programme und Systeme neu strukturieren:

- Automatisches Update des Programms/Systems ist eingestellt,
- Automatisches Updaten ist nicht eingestellt, aber möglich,
- Das Einspielen von Updates ist nur manuell möglich.
- Regelmäßiges Updaten aller Programme und Systeme, die nur manuell aktualisierbar sind (spätestens jeden Monat). Hierfür sollten Sie sich entsprechende Termine eintragen, damit diese Maßnahmen im Arbeitsalltag integriert werden können.
- Regelmäßige Überprüfung aller Programme und Systeme auf Aktualität, die sich automatisch updaten (mindestens einmal im Quartal).
- Upgrade auf neuere Versionen oder Ersatzbeschaffung für alle Programme, für die es keine Updates und/oder Support mehr gibt.

NETZWERK

Unabhängig davon, ob es in Ihrem Unternehmen ein Firmennetzwerk gibt oder nur einzelne Rechner, die an das Internet angebunden werden, sind technische Schutzmaßnahmen zu ergreifen. Diese dienen dazu, den Datenverkehr zu überwachen und nicht erlaubte Zugriffe zu unterbinden. So ist der Betrieb einer Firewall wichtig, um im Falle einzelner – an das Internet angebundener – Clients vor unberechtigten Zugriffen zu schützen.



Es existieren Hard- und Software-Firewalls am Markt, in der Regel reicht jedoch eine Softwarelösung aus.

Falls ein Firmennetzwerk existiert, sollte – neben einer Software-Firewall – auf jedem Rechner zusätzlich eine Netzwerk- bzw. Hardware-Firewall betrieben werden. Eine Netzwerk- bzw. Hardware-Firewall ist ein Schutzsystem, das auf einem zusätzlichen Gerät betrieben wird. Die meisten Switch- und Router-Hersteller (siehe Glossar, Seite 19) bieten solche Geräte in Kombination mit einer Firewall an. Lassen Sie sich bei der Auswahl bzw. einem Kauf von einem Fachmann beraten.

In der Produktion ist es aufgrund der Echtzeitanforderungen oft notwendig, das Ziel der Verfügbarkeit deutlich über alle anderen zu stellen. So kann ein Verlust der Datenverfügbarkeit zum Stillstand der Produktion führen (siehe Grafik). Daher sind oftmals Maßnahmen wie Netzwerksegmentierung notwendig, um trotzdem eine Datensicherheit zu gewährleisten.

Betreiben Sie ein WLAN-Funknetz in Ihrem Unternehmen, so müssen Sie auch dieses absichern. Die Übertragung muss unbedingt verschlüsselt werden. Achten Sie bei der Einstellung Ihrer Geräte (in der Regel Router) auf die Aktivierung der WPA2-Verschlüsselung. Steht Ihnen diese Verschlüsselungsart nicht zur Verfügung, dann kann in der Regel die WPA oder WEP-Verschlüsselung aktiviert werden. Beherrscht Ihr Gerät nur noch eine WEP-Verschlüsselung, so sollte mittelfristig ein neues Gerät mit der Möglichkeit einer WPA2-Verschlüsselung angeschafft werden. Die WEP-Verschlüsselung bietet aus heutiger Sicht keine ausreichende Sicherheit mehr. Alle Geräte, die Sie über WLAN einbinden, sollten eine eigene Software-Firewall besitzen.

Der Betrieb des WLANs sollte sich auf die Arbeitszeiten im Unternehmen beschränken, um sich vor Missbrauch durch Dritte zu schützen. Ist Ihr Unternehmen in verschiedene Abteilungen bzw. Bereiche wie Verwaltung (Office) und Produktion gegliedert, ist es sinnvoll, entsprechende Teilnetze für die verwendeten IT-Komponenten einzurichten. Zum einen kann die IT-Sicherheit dadurch wesentlich erhöht und zum anderen können Zugriffsberechtigungen und die Schutzziele (siehe Grafik) differenzierter gestaltet werden.

Insbesondere zwischen dem Produktionsbereich und der Office-IT kehren sich die Schutzziele um (Vertraulichkeit vs. Verfügbarkeit).

CHECKLISTE NETZWERK

- Dokumentieren Sie das Netzwerk mit seinen Komponenten.
- Achten Sie auf die Aktualität der Firmware (siehe Abschnitt Updates).
- Installieren Sie zwischen Ihrem Netzwerk bzw. auch Netzwerkbereichen und dem Internet eine Firewall.
- Ändern Sie die Standardpasswörter und verwenden Sie für die einzelnen Komponenten sichere Passwörter.
- Achten Sie auf eine sichere Konfiguration, insbesondere darauf, dass von außen keine Manipulation stattfinden kann.
- Datenfreigaben und Zugriffsberechtigungen sind auf ein Mindestmaß zu beschränken.

2.

Organisatorische Anforderungen

Im unternehmerischen Alltag gibt es zahlreiche organisatorische Herausforderungen. Aus Sicht der IT-Sicherheit sind das insbesondere

- der richtige Umgang mit Mitarbeitern,
- deren Unterweisung in Ihre Aufgaben am Arbeitsplatz und in die Anforderungen im Unternehmen,
- die Etablierung einer rechtssicheren und bindenden Sicherheitsrichtlinie und den dazugehörigen Sicherheitskonzepten,
- der Entwurf eines Berechtigungskonzeptes,
- die Pflicht zur Datenverschlüsselung und
- die Analyse potenzieller Risiken im Unternehmen.

Unterstützen können Sie dabei verschiedene Normen und Richtlinien.

MITARBEITERUNTERWEISUNG

Entscheidender Faktor für den sicheren Betrieb von Rechnern, Servern, Produktionsanlagen und der Telekommunikationsinfrastruktur ist die regelmäßige Unterweisung der Mitarbeiter in die IT sowie die Hinführung zum Thema „Sicherheit". Die Unterweisung der Mitarbeiter ist wichtig, um ihnen einen Einblick in die Prozesse und Abläufe und die damit verbundenen Bedrohungen zu geben. Die Einweisung eines neuen Mitarbeiters in die Handhabung einer Maschine (wie z.B. einer Drehbank) ist selbstverständlich. Genauso selbstverständlich sollte auch eine Unterweisung in den Umgang mit der IT des Unternehmens sein. Werden dort elementare Fehler begangen, kann dies den kompletten Geschäftsbetrieb unterbrechen. Grundsätze für die Unterweisung der Mitarbeiter:

- Unterrichten Sie die Mitarbeiter über ihre IT-Nutzungsrechte und -pflichten.
- Zeigen Sie neuen Mitarbeitern, wo sich relevante Programme auf dem Rechner befinden und erläutern Sie die maßgeblichen Funktionen.
- Unterrichten Sie über zentrale Vorgaben, wie z.B. Speicherung von Daten, Benennung von Dateien oder Klassifikation von Informationen (welche Inhalte dürfen nach außen weitergegeben werden und welche nicht).

Viele Weiterbildungs- und Schulungsangebote werden nur wahrgenommen, wenn diese verpflichtend sind. Daher empfiehlt es sich, die Mitarbeiter zur Schulung in einem Mindestportfolio an Themengebieten zu verpflichten. Dazu gehört auch eine Schulung zum Thema „IT-Sicherheit". Sind Sie selbst nicht in der Lage, Schulungen zu diesem Thema durchzuführen, dann nehmen Sie die kostenfreien Schulungen der Mittelstand 4.0-Kompetenzzentren oder die der weiteren Fremdanbietern (HWK, IHK usw.) bzw. externen Trainer in Anspruch, die für Ihr Unternehmen maßgeschneiderte Lösungen anbieten. Der Inhalt einer Schulung zur IT-Sicherheit sollte alle genannten Aspekte dieses Ratgebers enthalten und die IT-Landschaft Ihres Unternehmens abdecken. Erfahrungen zeigen, dass bei der Fortbildung von Einzelpersonen eines Unternehmens Schulungen

von Kammern oder vergleichbaren Anbietern sinnvoll sind, bei Gruppen ab ca. fünf Personen (aus einem Unternehmen) sich eine maßgeschneiderte Schulung empfiehlt. Das liegt zum einem an dem angepassten Schwierigkeitsgrad an die Personengruppe sowie dem Behandeln der für das Unternehmen bzw. die Branche relevanten Themengebiete. Weiterhin haben sich in der Praxis auch aufeinander aufbauende Workshops oder Seminare als sinnvoll erwiesen.

CHECKLISTE MITARBEITERUNTERWEISUNG

- Neue Mitarbeiter am ersten Tag begleiten und unterstützen.
- Alle Mitarbeiter über Spezifika bei der Nutzung der IT aufklären.
- Schulungen für alle Mitarbeiter regelmäßig und verpflichtend anbieten.
- Durch das Aufzeigen von potenziellen Schadensszenarien wird den neuen Mitarbeitern ein grundsätzliches Verständnis dafür vermittelt, warum die vorgestellten Vorgaben existieren.

SICHERHEITSRICHTLINIE UND -KONZEPT

Das vorangegangene Kapitel macht deutlich, dass Mitarbeiter eindeutige, schriftlich fixierte Regeln benötigen. In diesem Zusammenhang ist die Erstellung einer Sicherheitsrichtlinie sowie eines Sicherheitskonzeptes notwendig. Die Sicherheitsrichtlinie beinhaltet mehrheitlich Sachverhalte, die sich mittelfristig nicht ändern und beinhaltet folgende Punkte:

- Benennung der Sicherheitsziele und Beschreibung der Sicherheitsstrategie,
- Beschreibung der Sanktionierung von Verstößen gegen die Richtlinie,
- Darstellung der regelmäßigen Überprüfung von Sicherheitsmaßnahmen,
- Umgang mit verpflichtenden Schulungs- und Weiterbildungsmaßnahmen,
- Benennung des Verantwortlichen für die IT-Sicherheit und dessen genaue Funktion.

Wichtig ist zudem, dass die Sicherheitsrichtlinie durch den Geschäftsführer bzw. die Geschäftsleitung unterstützt wird, von diesen Personen offiziell verabschiedet wurde und dadurch nachweislich eine hohe Bedeutung für das Unternehmen hat.
Neben der Richtlinie müssen KMU noch ein Sicherheitskonzept erstellen, welches die für die IT relevanten Themen behandelt, die sich kurzfristig ändern können. Dazu gehören Hinweise beim Umgang mit der IT (z.B. Umgang mit Handys in Maschinenhallen) sowie allgemeine Handlungsanweisungen (z.B. Der Schrank mit den Datensicherungen muss immer verschlossen sein). Weitere Punkte, die in einem Sicherheitskonzept festgehalten werden, sind:

- Fixierung eindeutiger Regeln für den Umgang mit der betriebseigenen Hardware (PC und Telefon),
- Passwortwahl und -umgang,
- Datensicherungskonzept,
- Virenschutzkonzept,
- betriebliche Nutzung von privaten mobilen Geräten wie Tablets und Smartphones (BYOD – Bring your own Device).

Zentraler Punkt ist, dass die Inhalte der Sicherheitsrichtlinie und des -konzeptes den Mitarbeitern bekannt sind, alle Beteiligten den Inhalt verstehen und die Einhaltung der Vorgaben schriftlich bestätigen. Daher sind regelmäßige Informationsveranstaltungen Pflicht, um neue Mitarbeiter einzuweisen und den bestehenden Mitarbeitern Veränderungen und Neuerungen mitzuteilen. Darüber hinaus müssen die Verantwortlichen in regelmäßigen Abständen prüfen, ob die Regelungen auch befolgt werden. Denn nur dann kommen die Mitglieder der Geschäftsleitung ihrem Kontrollanspruch nach.

CHECKLISTE IT-SICHERHEITSKONZEPT

- IT-Sicherheitskonzept erstellen und aktuell halten.
- Wirkung von Sicherheitsmaßnahmen regelmäßig prüfen.
- Verantwortlichkeiten festlegen
- Regeln zur Nutzung von geschäftlicher und privater Hardware aufstellen.
- Regeln zum Umgang mit Passwörtern aufstellen.
- Datensicherungskonzept
- Konzept für den Schutz nach außen

BENUTZERKONZEPT

In einem Benutzerkonzept wird der Zugang und die Berechtigung zu einzelnen Informationen und Netzwerkkomponenten des Unternehmens geregelt. Hierzu können neben Ihren Office-Computern auch Server, Leitstände und industrielle Steuerungen gehören. Im schlimmsten Fall hat jeder Benutzer des Firmennetzwerkes uneingeschränkten Zugriff auf diese Komponenten. Im Idealfall sind die Zugriffsrechte innerhalb des Unternehmens für jeden Angestellten entsprechend seiner Position und Funktion klar geregelt. Wichtig ist, dass die Verantwortlichen für die Freigabe eindeutig benannt werden und es ein Freigabeverfahren gibt, das allen Mitarbeitern bekannt ist.

Folgende Punkte sind bei der Erstellung eines Benutzerkonzeptes zu beachten:

- Entwerfen Sie ein Benutzerkonzept, in dem fest gelegt wird, welche Daten für alle Mitarbeiter zugänglich sein dürfen/müssen.
- Benennen Sie einen Verantwortlichen für die Zuweisung der Nutzerrechte und informieren Sie die Mitarbeiter über diese Zuständigkeit.
- Legen Sie einen klaren Ablauf fest, wie die Erteilung/Veränderung und Löschung der Nutzerrechte zu erfolgen hat.

HINWEIS
Die eindeutige Definition von Benutzerrechten wird auch vom Bundesdatenschutzgesetz (BDSG) gefordert.

CHECKLISTE BENUTZERKONZEPT

- Regelung des Zugangs zur Hard- und Software
- Regelung des Zugangs zu Informationen und Datenbeständen
- Festlegen der Verantwortlichkeiten und der IT-Administration
- Verwaltung der Nutzerrechte bei Mitarbeiterwechsel bzw. Verlassen des Unternehmens

VERSCHLÜSSELUNG

Mit einer Verschlüsselung der eingesetzten Datenträger sowie der E-Mail-Kommunikation schützen Sie Ihr Unternehmen davor, dass sich unberechtigte Personen Zugang zu Ihren Daten bzw. Know-how (wie z.B. Kundendaten, Konstruktionszeichnungen von Produkten) verschaffen. Geht z.B. ein Notebook auf Reisen verloren und die Daten auf dem Rechner sind unverschlüsselt, kann jeder die Daten kopieren und lukrativ an die Konkurrenz verkaufen oder anderweitig missbrauchen. Dies verdeutlicht den Aufwand einer Datenträgerverschlüsselung im Vergleich zum Verlust von Informationen.

Benutzen Sie die Datenträger nur im eigenen Büro, so scheint eine Verschlüsslung nicht notwendig zu sein. Bei der Risikoanalyse bietet sich bei einem möglichen Einbruch und Diebstahl sowie entsprechenden Datenbeständen in jedem Fall eine generelle Datenverschlüsselung an. Haben Sie Daten mit sensiblen Informationen auch auf Außeneinsätzen, Dienstreisen oder im Urlaub dabei, so sollten Sie die Daten ebenfalls verschlüsseln. Auf dem Softwaremarkt gibt es eine große Auswahl an kommerziellen und Open-Source-Verschlüsselungsprogrammen.

HINWEIS
Bei der Auswahl einer Software zur Verschlüsselung müssen Sie darauf achten, dass die Software einfach zu bedienen ist und eine Verschlüsselungsrate von 128 Bit oder besser mehr hat.

Alternativ zur Verschlüsselung mit einer Software gibt es die Möglichkeit, Daten hardwareseitig zu verschlüsseln. Neuere Systeme verfügen bereits über diese Möglichkeit einer kompletten Festplattenverschlüsselung und es entstehen auch keine zusätzlichen Kosten. Gleich nach einem Systemstart erfolgt hier die Eingabe eines zusätzlichen Kennwortes, erst danach startet das Betriebssystem. Bei Fragen ist es ratsam, den IT-Dienstleister einzubeziehen.

HINWEIS

Achten Sie darauf, dass der Prozess der Ver- und Entschlüsselung die Arbeitsabläufe auf keinen Fall beeinträchtigen darf. Die Umsetzung einer Verschlüsselungslösung sollte vom Anwender im Idealfall nicht bemerkt werden, da lediglich das zusätzliche Passwort einzugeben ist. Nur wenn dieser Prozess als problemlos eingestuft wird, findet er vollumfassend bei allen Geschäftsprozessen Anwendung.

Prüfen Sie mit Ihrem IT-Dienstleister die Möglichkeit sowie auch Sinnfälligkeit einer Verschlüsselung der E-Mail-Kommunikation. Hier gibt es eine breite Diskussion über den Aufwand und Nutzen. In der Anwendung mangelt es oft an einer hinreichenden Akzeptanz durch die Nutzer, da sowohl beim Absender als auch beim Empfänger bestimmte Installationen bzw. jeweils vorbereitende Arbeiten durchzuführen sind. Die Entscheidung hängt natürlich im Wesentlichen von den Inhalten ab. Unter Umständen ist es effektiver, dass sensible Daten selbst in einer Datei verschlüsselt werden und Sie mit Ihrem Partner den Schlüssel austauschen.

CHECKLISTE VERSCHLÜSSELUNG

- Identifizieren von relevanten Datenbeständen
- Einzelne Datenbestände per Software verschlüsseln
- Verschlüsselung kompletter Festplatten
- Verschlüsselung der E-Mail-Kommunikation und/oder der Anhänge

RISIKOANALYSE

Ein Aspekt, der oftmals erst in großen Unternehmen zum Tragen kommt, ist die Risikoanalyse. Um IT-Risiken zu identifizieren und diesen anschließend entgegenzuwirken, müssen Unternehmen sie im Vorfeld zunächst analysieren. Ein unentdecktes Risiko kann insbesondere in komplexen Geschäftsprozessen oder einem aufwändigen Aufbau der IT sowie aktuellen Angriffsarten, wie z.B. einem neuen Computerschädling, liegen.

An die Erkennung von Risiken müssen sich insbesondere KMU systematisch heranarbeiten. Eine Risikoanalyse setzt sich aus den folgenden Teilschritten zusammen:

- Identifikation der möglichen Risiken
- Bewertung aller identifizierten Risiken hinsichtlich Relevanz und Schadenspotential

Ein Risiko besteht in der Regel immer dann, wenn das Unternehmen mit einer externen oder internen Bedrohung konfrontiert wird. Diese entwickelt sich zu einer Gefahr, wenn das Unternehmen durch eine offene Schwachstelle eine entsprechende Angriffsfläche bietet. Nur durch angemessene Schutzmaßnahmen können KMU solche Schwachstellen schließen, um somit zu vermeiden, dass eine Bedrohung zur Realität wird.

Viele Risiken sind mit einem Gespür für das eigene Unternehmen bzw. für die vorhandenen Prozesse erkennbar und bereits mit einem geringen Mitteleinsatz reduzierbar. Andere Risiken sind akzeptabel, falls sie weder eine hohe Eintrittswahrscheinlichkeit noch eine empfindliche Schadenshöhe besitzen. Mit einer Risikoanalyse sollen gerade die häufig auf-

tretenden und besonders kostspieligen Schadensfälle schon im Vorfeld entdeckt und im Idealfall ausgeschlossen werden. Jedoch besteht gerade bei der Identifikation der möglichen Risiken die Gefahr des Übersehens. Die besten Erfahrungen haben Unternehmen gemacht, die in enger Zusammenarbeit zwischen Mitarbeitern und externen Beratern erfolgreich ihre unternehmensspezifischen Risiken identifiziert haben.

CHECKLISTE RISIKOANALYSE

- Risikoanalyse durchführen
- Schutzmaßnahmen festlegen und umsetzen
- Risikoanalyse bei Veränderungen im Unternehmen wiederholen

NOTFALLMANAGEMENT

Kommt es in einem Unternehmen trotz aller vorbeugenden Maßnahmen zu einem Schadensfall, ist es notwendig, dass der gesamte IT-Betrieb mit seinen Systemen (inkl. Komponenten, Anwendungen und Prozessen) schnellstmöglich wiederhergestellt wird. Je nach Digitalisierungsgrad des Unternehmens ist eine funktionierende Informationstechnik von entscheidender Bedeutung für die Geschäftsprozesse und damit für das ganze Unternehmen.

Aus diesem Grund sollte jedes Unternehmen ein entsprechendes Notfallkonzept bzw. Notfallhandbuch besitzen. In einem Notfallhandbuch werden für mögliche Schadensfälle Kontaktdaten von Ansprechpartnern und Maßnahmen zur Wiederherstellung der ausgefallenen Funktionen dokumentiert. Dabei spielt die Wichtigkeit der Systeme für die Geschäftstätigkeit des Unternehmens eine besondere Bedeutung und ist bei der Reihenfolge einer Wiederherstellung entsprechend zu beachten. So stehen produktionsspezifische Prozesse in der Relevanz fast immer vor den Prozessen in einer Verwaltung. Daraus wird deutlich, dass es für ein Unternehmen sehr wichtig ist, seine Prozesse genau zu kennen und zu priorisieren.

Im Zusammenhang mit einem Notfallmanagement müssen alle Mitarbeiter kontinuierlich informiert und geschult werden. Analog dem Erste-Hilfe-Szenario muss jeder Mitarbeiter Kenntnis über den Standort des Notfallhandbuches haben.

CHECKLISTE NOTFALLMANAGEMENT

- Einen Verantwortlichen für das Notfallhandbuch festlegen.
- Notfallhandbuch erstellen
- Information und Schulung aller Mitarbeiter
- Notfallhandbuch aktuell halten

3. Rechtliche Anforderungen

Viele wichtige Rechtsvorschriften im Bereich der IT-Sicherheit sind nicht in einem einzelnen Gesetz zusammengeführt, sodass Unternehmen ihre Zusammenhänge oftmals unterschätzen. Eine Zuwiderhandlung kann nicht nur haftungsbedingt einen zivilrechtlichen Schadensersatz zur Folge haben, sondern auch eine Ordnungswidrigkeit oder gar Strafe bedeuten.

Daher sind die Geschäftsführer bzw. Vorstände sowie alle Mitarbeiter gut beraten, wenn sie die rechtlichen Anforderungen zur IT-Sicherheit beachten. Klassische Herausforderungen im Rahmen der IT-Sicherheit sind:

- Datenschutz
- unterschiedliche unternehmensspezifische Gesetze
- Gestaltung eines Vertrages im Falle des Outsourcings von IT-Dienstleistungen.

Diese werden nachfolgend analysiert und zudem wird ein Ausblick auf aktuelle Entwicklungen hinsichtlich der fortschreitenden Digitalisierung und Industrie 4.0 gegeben.

UMSETZUNG DER VORGABEN DES DATENSCHUTZES

Beim Umgang mit personenbezogenen Daten (z.B. Geburtsdatum, Familienstand usw.) müssen die gesetzlichen Bestimmungen eingehalten werden. Die Vorschriften zum Datenschutz für Unternehmen sind im Bundesdatenschutzgesetz (BDSG) niedergeschrieben. Die Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Hinzu kommen bereichsspezifische Regelungen, die Vorrang vor dem BDSG haben, wie z.B. das Sozialgesetzbuch oder die Polizeigesetze.

HINWEIS

Im Sinne des BDSG sind personenbezogene Daten insbesondere Informationen über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diesen Informationen müssen die Verantwortlichen ein besonders hohes Augenmerk zukommen lassen, da ein zu sorgloser Umgang mit diesen Daten schnell zu juristischen Folgen führen kann.

Zwecks Einhaltung der Anforderungen des Datenschutzes empfiehlt es sich, einen eigenen, entsprechend qualifizierten Datenschutzbeauftragten (DSB) im Unternehmen zu berufen oder die Dienste eines externen DSB in Anspruch zu nehmen. Die Notwendigkeit zur Bestellung eines DSB ist im BDSG geregelt und abhängig von der Anzahl der Mitarbeiter, die sich mit der Verarbeitung personenbezogener Daten, wie z.B. von Angestellten, Kunden oder Lieferanten, beschäftigen. Auch wenn laut Gesetz kein Datenschutzbeauftragter bestellt werden muss, ist es empfehlenswert, eine fachkundige Person im Unternehmen zu haben.

Hierfür stehen KMU zwei Varianten zur Auswahl:

- **Ausbildung zum Datenschutzbeauftragten**

Diese wird von unterschiedlichen Bildungsträgern angeboten. Ein selbständiges Einarbeiten in das Thema ist meistens mühsam und weniger erfolgreich. Um sich in dem Themenfeld zügig und erfolgreich weiterbilden zu können, ist fachliches Vorwissen im IT-Bereich nahezu unerlässlich.

- **Bestellung eines externen Datenschutzbeauftragten**

Je nach Unternehmenssituation kann der Aufbau eines eigenen Datenschutzbeauftragten sinnvoll sein oder das Abschließen eines (evtl. kostengünstigeren) Vertrages mit einem externen Dienstleister.

HINWEIS

Beachten Sie aktuelle Änderungen des Bundesdatenschutzgesetzes sowie die entsprechenden Umsetzungen in den einzelnen Bundesländern.

CHECKLISTE DATENSCHUTZ

- Prüfen Sie in Ihrem Unternehmen, ob per Gesetz ein Datenschutzbeauftragter bestellt werden muss.
- Ist gesetzlich kein DSB zu bestellen, benennen Sie trotzdem eine für den Datenschutz verantwortliche Person.
- Kontrollieren Sie die Unternehmensprozesse auf Einhaltung des Datenschutzes.
- Schulen Sie Ihre Mitarbeiter.

GESETZE

Gesetze und Vorschriften betreffen jedes Unternehmen. Da sich manche Gesetze und Vorschriften hin und wieder ändern, müssen Sie sich über gesetzliche Änderungen informieren. Die jeweiligen Kammern (IHK oder HWK) bieten gute Informationen, können aber – allein schon aus Zeitgründen – nicht immer alle für ihre Unternehmen relevanten Gesetzesänderungen sofort erfassen und kommunizieren.

HINWEIS

Nehmen Sie neben dem Service der Kammern die Beratung durch externe Dienstleister in Anspruch. Wägen Sie jedoch ab, ob diese für die Beratung in Ihrer Branche das notwendige Wissen über Ihr Unternehmen und die dazugehörige Gesetzeslage mitbringen. Gute Ansprechpartner sind hier auch Branchenverbände u.ä.

In jedem Fall ist es wichtig, dass sie sich mit Gesetzesänderungen zeitnah und proaktiv auseinandersetzen. Denn nur so können Sie sicherstellen, dass Sie alle Geschäftsprozesse vollumfänglich gesetzeskonform abwickeln.

CHECKLISTE GESETZE

- Erstellen Sie mit Unterstützung Externer eine Liste der für Sie zutreffenden Gesetze.
- Prüfen Sie die Einhaltung der Gesetze.
- Kontrollieren Sie regelmäßig die Aktualität.

VERTRÄGE MIT DIENSTLEISTERN

In vielen Unternehmen werden IT-Leistungen ausgelagert und an andere Firmen weitergegeben. Haben Sie beispielsweise den Internetauftritt oder die Wartung Ihrer IT-Systeme an ein anderes Unternehmen übertragen, so müssen Sie zahlreiche Aspekte berücksichtigen. Die größten Fehler werden bei der

Vertragsgestaltung gemacht. Im schlimmsten Fall werden nur mündliche Vereinbarungen getroffen, im Idealfall erfolgt eine vollumfängliche vertragliche Fixierung. Gerade wenn der Leistungsanspruch des Unternehmens und die Leistungserbringung des Anbieters stark auseinandergehen, ist ein ordentlich erstellter, rechtssicherer Vertrag von Vorteil. Um einer – im schlimmsten Fall – gerichtlichen Auseinandersetzung standzuhalten, muss im Vertrag geregelt sein, welche organisatorischen und technischen Maßnahmen in welchen Zeitabständen durch den Partner zu realisieren sind. Des Weiteren sollten größere Verträge von einem Juristen erstellt bzw. kleinere Verträge vom Juristen zumindest qualitätsgesichert werden.

Die folgenden Punkte sollten Berücksichtigung finden:

- Der Leistungsumfang des Dienstleistungsvertrages sollte detailliert geregelt werden.
- Es ist eindeutig zu fixieren, welche Aufgaben und Pflichten der Dienstleister zu erbringen hat. Hierfür müssen Termine verankert werden.
- Die Eigentumsverhältnisse sind juristisch einwandfrei zu regeln (z. B. Besitz der Internetadresse bei der Vergabe des Betriebes der eigenen Homepage).
- Wenn zeitkritische Aspekte zu berücksichtigen sind, müssen Themen wie „Verfügbarkeit“ und „Reaktion bei Störfällen“ eindeutig festgeschrieben sein, da ein Ausfall des Dienstleistungsgegenstandes (z.B. ein Online-Shop) schnell zu einem erheblichen Verdienstausfall führen kann. In einem solchen Fall müssen Haftungsfragen juristisch geregelt werden.

CHECKLISTE VERTRÄGE MIT IT-DIENSTLEISTERN

- Stellen Sie fest, ob für alle ausgelagerten IT-Dienstleistungen Verträge existieren.
- Prüfen Sie vereinbarte inhaltliche Leistungen auf Vollständigkeit und Umsetzung.
- Terminmanagement für Vertragsverlängerungen

Folgende Gesetze sind aus IT-Sicherheitsgesichtpunkten relevant und unterliegen auch einer dynamischen Anpassung:

§

ÜBERSICHT ZU GESETZEN MIT BEZUG ZUR IT-SICHERHEIT

IT-Sicherheit
- IT-Sicherheitsgesetz (KRITIS)
- Telekommunikationsgesetz (TKG)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Vertragsrechtliche Regelungen
- Bürgerliches Gesetzbuch (BGB, z.B. § 307)
- Rom I-VO

Haftungsrecht
- Handelsgesetzbuch (HGB)
- Rom I. und II-VO
- BGB (§§ 280ff. & §§ 823ff.)

Datenschutz und Auftragsdatenverarbeitung
- Bundesdatenschutzgesetz (BDSG)
- EU Verordnung 2016/679

Finanzen
- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff durch die Finanzverwaltungen (GoBD)
- Basel II

Grenzüberschreitender Fernhandel und -wartung
- General Agreement on Trade in Services (GATS)
- Trade Related Aspects of Intellectual Property Rights (TRIPS)

Geheimnisschutz
- Gesetz gegen den unlauteren Wettbewerb (UWG)

4. Fazit

Der Aufbau und die Aufrechterhaltung eines hohen Maßes an IT-Sicherheit stellen KMU vor eine große Herausforderung, bieten jedoch auch zahlreiche Chancen.

Neben dem umfassenden Schutz der IT verbessern viele Sicherheitsmaßnahmen die Abläufe im Geschäftsverkehr. Zum Beispiel gibt eine Sicherheitsrichtlinie Mitarbeitern eine klare Regelung an die Hand, wie sie mit unterschiedlichen Vorkommnissen umzugehen haben. Anstatt der Suche nach den für diesen Bereich Verantwortlichen und der – im schlimmsten Fall – Nennung unterschiedlichster Herangehensweisen, kann in der Sicherheitsrichtlinie der betreffende Punkt nachgeschlagen werden.

In Zukunft wird der Einsatz von IT-Komponenten und Systemen immer stärker zunehmen. Dabei darf die Sicherheit nicht vernachlässigt werden. Je nachdem in welcher Branche Ihr Unternehmen tätig ist, kann IT-Sicherheit in Zukunft eine zentrale Rolle einnehmen. Viele große Unternehmen fordern schon jetzt von den Zulieferunternehmen eine Zertifizierung nach dem Qualitätsmanagement (ISO 9001). Mit der steigenden Vernetzung von Unternehmen wird in Zukunft neben der ISO 9001 auch immer öfter ein Managementsystem für die Informationssicherheit (ISMS), wie z.B. eine Zertifizierung nach der ISO 27001 oder ein Management entsprechend dem IT-Grundschutz des BSI, nachgefragt werden.

Setzt Ihr Unternehmen die hier im Leitfaden angesprochenen Themen gut um, so profitieren Sie von verbesserten Abläufen, klaren Regeln für Mitarbeiter sowie der Möglichkeit sich verändernden Anforderungen – wie beispielsweise der Forderung eines Auftraggebers, zwecks Zusammenarbeit die eigene IT-Sicherheit zertifizieren zu lassen – schneller stellen zu können.

Die in diesem Leitfaden zusammengestellten Informationen und Handlungsempfehlungen sollen für KMU eine Hilfestellung zur Verbesserung ihrer IT-Sicherheit darstellen. Die enthaltenen Checklisten unterstützen Sie dabei, herauszufinden, ob Sie die organisatorischen und rechtlichen Anforderungen bereits erfüllen oder ob noch Handlungspotenziale offen sind.

Glossar

Add-On – Erweitert vorhandene Hard- oder Software um bestimmte Funktionen.

Bit – Steht für „binary digit" und ist die kleinste elektronische Speichereinheit. Mögliche Werte sind 1 und 0 (an und aus).

Byte – 1 Byte = 8 Bit

BIOS – Steht für "basic input/output system", welches die Firmware eines PCs ist. Sie wird in der Regel in einem Chip auf der Hauptplatine des Rechners gespeichert.

Client – Ein Endgerät in einem Netzwerk, das mit einem Server kommuniziert.

CNC-(Maschinen) – Sind „Computerized Numerical Control" Maschinen, die durch Rechentechnik automatisch gesteuert werden.

Digitalisierung – Steht zum einen als Synonym für die digitale Transformation / Revolution und zum anderen für die Überführung von analogen in digitale Inhalte.

Firewall – Elementares Sicherungssystem von (IT-)Netzwerksystem, dass das Netzwerk vor unerwünschten Zugriffen schützen soll bzw. nur bestimmte Kommunikationswege zulässt.

Firmware – Elementare (engl. firm, „feste") Software, die in elektronischen Systemen die grundlegende Kommunikation zwischen Hardware und Anwendungssoftware regelt.

IT-Infrastruktur – Umfasst alle Dienste, Hard- und Software, die für die Informationsverarbeitung einzelner Organisationen zur Verfügung stehen.

Mail-Proxy – Ist ein spezieller Viren- und Spamfilter für E-Mails, um schädliche Inhalte zu erkennen und ggf. Aktionen wie Markierungen oder Löschungen zu initiieren.

PPS (-Programme) – Steht für Produktionsplanungs- und Steuerungssysteme, welche die Anwender bei typischen Analysen und Steuerungen zu produktionslogistischen Kennzahlen (Durchlaufzeiten, Termineinhaltung, Kapazitäten etc.) unterstützen.

RAID-System – Steht für „Redundant Array of Independent Disks" und ist eine Organisationsform mehrerer physischer Massenspeicher (wie Festplatten), um eine höhere Ausfallsicherheit zu erreichen und ggf. höhere Datendurchsätze zu ermöglichen.

Router – Sind typische Netzwerkgeräte zum aktiven Verteilen bzw. Weiterleiten von Daten zwischen mehreren Teilnehmern und Netzwerken. Typische Anwendung ist die Nutzung zur Internetanbindung.

Skripte – Sind kleine Programme, die verschiedene Rechnerbefehle und -anweisungen kombinieren, um diese auszuführen. Oftmals sind diese nur in Quelltextdateien angefertigt.

Server – Ist ein Computer bzw. Computerprogramm, der spezielle Dienste, Programme oder Ressourcen für Clients zur Verfügung stellt.

Switch – Verbindung- und Vermittlungsgerät zwischen mehreren Geräten in einem Netzwerk.

Trojaner – Schadsoftware, die sich als eine andere ausgibt oder andere nützliche Funktionen aufweist, im Hintergrund aber ungewünschte Funktionen ausführt (z.B. Manipulation von Werbeinhalten im Browser).

Verschlüsselungsrate – Wert, der die Stärke der Verschlüsselung z.B. von Daten, Kommunikationswegen oder Zertifikaten widerspiegelt. Dieser wird in Bit gemessen.

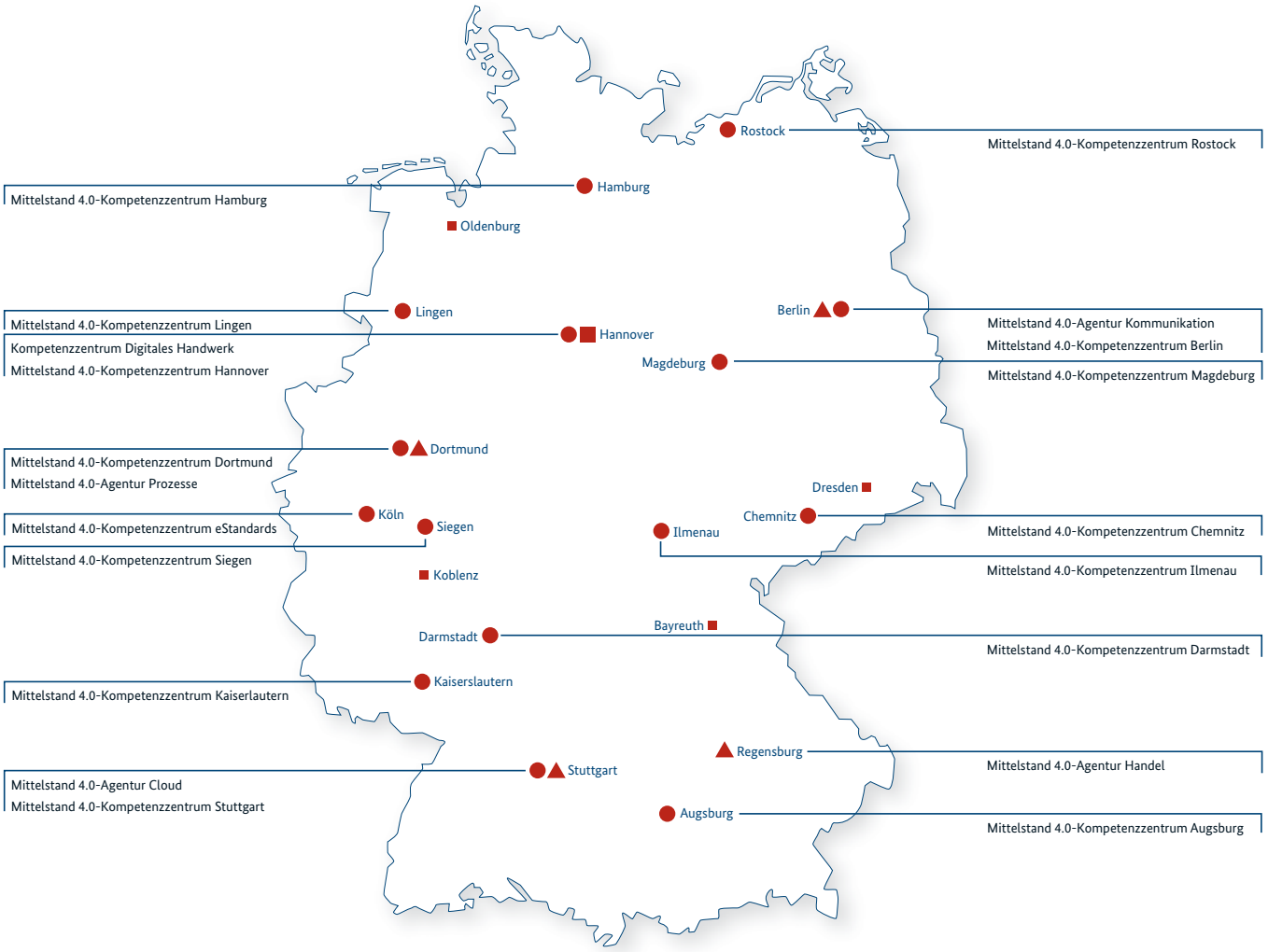
Virus/Viren – Selbstverbreitende und -reproduzierende Schadsoftware.

WEP – Steht für „Wired Equivalent Privacy" und ist ein Verfahren zur Datenverschlüsselung und Authentifizierung für WLAN-Verbindungen. Dieses Verfahren gilt mittlerweile als unsicher.

WLAN – Steht für „Wireless Local Area Network", also dem drahtlosen lokalen Netzwerk, welcher auf Funkstandards basiert.

WPA – Steht für „Wi-Fi Protected Access" und ist ein Verfahren zur Verschlüsselung. Diese ist eine Weiterentwicklung von WEP und gilt mittlerweile als unsicher.

WPA2 – Ist eine Erweiterung von WPA und heutiger Sicherheitsstandard.



- Kompetenzzentren der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“
- Agenturen der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“
- Kompetenzzentrum Digitales Handwerk
- Regionale Schaufenster Digitales Handwerk

STANDORTÜBERSICHT

Partner der Mittelstand 4.0-Agentur Prozesse

FTK Forschungsinstitut für Telekommunikation und Kooperation

- FTK – Forschungsinstitut für Telekommunikation und Kooperation e.V., Holger Schneider, E-Mail: hschneider@ftk.de, **www.ftk.de**

tti Technologietransfer und Innovationsförderung Magdeburg GmbH

- tti Technologietransfer und Innovationsförderung Magdeburg GmbH, Roland Hallau, E-Mail: rhallau@tti-md.de, **www.tti-magdeburg.de**

IHK Industrie- und Handelskammer Chemnitz

- Industrie- und Handelskammer Chemnitz, Janek Götze, E-Mail: janek.goetze@chemnitz.ihk.de **www.chemnitz.ihk24.de**

TECHNISCHE UNIVERSITÄT CHEMNITZ

- Technische Universität Chemnitz Professur Fabrikplanung und Fabrikbetrieb, Anne Götze, E-Mail: anne.goetze@mb.tu-chemnitz.de **www.tu-chemnitz.de/mb/FabrPlan**