Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

IT-Sicherheit und Recht

Themenheft Mittelstand-Digital

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Stand
März 2018

Text
LoeschHundLiepold Kommunikation GmbH, Berlin

Gestaltung
PRpetuum GmbH, München

Druck
MKL Druck GmbH & Co. KG, Ostbevern

Bildnachweis
Gina Sanders/stock.adobe.com (Titel)
enzozo/stock.adobe.com (S. 5)
Michaela Nestler, Foto-Steinke Wolmirstedt (S. 8)
REDPIXEL/stock.adobe.com (S. 11)
123erfasst.de (S. 12-13)
NSIDE ATTACK LOGIC GmbH (S. 15)
Gil C/shutterstock.com (S. 17)
Technische Universität Chemnitz (S. 22)
FZI (S. 25)
momius/stock.adobe.com (S. 26)
weerapat1003/stock.adobe.com (S. 29)

Zertifikat seit 2002
audit berufundfamilie

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C108626

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Editorial

Liebe Leserinnen und Leser,

Produkte können heute individuell und trotzdem kostengünstig produziert werden, Maschinen über verschiedene Standorte hinweg kommunizieren und Kunden aus aller Welt handgemachte Unikate mit wenigen Klicks über einen Onlineshop bestellen. Dank digitaler Technologien können kleine und mittlere Unternehmen mehr Kunden gewinnen, neue Geschäftsmodelle umsetzen und einfacher internationale Märkte erschließen.

Die Digitalisierung bietet jedoch nicht nur Chancen – sie stellt auch neue Anforderungen an Sicherheitslösungen und rechtskonforme Prozesse. Denn nur, wenn gewährleistet ist, dass digitale Prozesse zuverlässig funktionieren und Daten geschützt sind, können Betriebe erfolgreich sein. Viele dieser Anforderungen und Vorkehrungen sind heute bereits selbstverständlich in den Unternehmensalltag integriert – von der Firewall bis hin zu Datenschutzschulungen. Dennoch zeigen Untersuchungen immer wieder, dass viele Betriebe unsicher sind, welche Unternehmensbereiche angreifbar sind und wie sie diese effektiv gegen Cyber-Angriffe oder Hardware-Ausfälle schützen können. Gleichzeitig sorgen neue Gesetze und Vorgaben, wie etwa die Datenschutz-Grundverordnung, für Handlungsbedarf, damit Unternehmen auch künftig rechtlich sicher agieren.

Mit dem vorliegenden Themenheft zeigen wir, wie dies gelingen kann: So kann gute Softwaregestaltung dazu beitragen, dass Anwendungen sicher und effektiv benutzt werden – gleichzeitig können soziale Medien Hinweise geben, wo Hersteller ihre Produkte verbessern können, damit keine Sicherheitsrisiken drohen. Und auch Hacker können Gutes bringen: Durch fingierte Angriffe können Betriebe lernen, welche Schwachstellen sie haben, und diese systematisch abbauen.

Mittelstand-Digital unterstützt kleine und mittlere Betriebe als Förderschwerpunkt des Bundesministeriums für Wirtschaft und Energie dabei, effektive IT-Sicherheitskonzepte zu entwickeln. Die regionalen Mittelstand 4.0-Kompetenzzentren informieren und demonstrieren, wie technische Lösungen sie dabei unterstützen, gegen Angreifer gewappnet zu sein. Gleichzeitig helfen die Experten dabei, Mitarbeiter für das Thema zu sensibilisieren, und informieren, welche Gesetze beim Thema Datenschutz, Dateneigentum und mehr wichtig sind – und werden. Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung, wie z. B. Mitarbeiter/Innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

Wenden Sie sich bei Ihren Fragen jederzeit an die Anlaufstelle in Ihrer Nähe – nähere Informationen dazu finden Sie ab Seite 18.

Wir wünschen Ihnen eine spannende Lektüre.

Ihr Bundesministerium für Wirtschaft und Energie

Rechtssicher digitalisieren

Martin Lundborg, Leiter der Begleitforschung Mittelstand-Digital

Die Digitalisierung des deutschen Mittelstands schreitet weiter voran und bietet den Unternehmen neue Wachstumschancen. Ergreifen die kleinen und mittleren Unternehmen diese Möglichkeiten, stoßen sie jedoch häufig auf neue oder für sie bisher nicht relevante IT-Sicherheits- und Rechtsfragen. Für das Vertrauen von Kunden und Lieferanten ist es unbedingt erforderlich, dass die mittelständischen Unternehmen notwendige IT-Sicherheitsmaßnahmen schnell implementieren und geltende Rechtsvorschriften zum Umgang mit Daten frühzeitig und rechtskonform umsetzen. Für datengetriebene Geschäftsmodelle stellt das Vertrauen schließlich einen ganz wesentlichen Erfolgsfaktor dar.

Recht und IT-Sicherheit als Bestandteil der Digitalisierung

Die Frage nach der Rechtssicherheit ist beispielsweise für alle Unternehmen relevant, die Teil digitaler Wertschöpfungsnetzwerke sind, indem sie zum Beispiel freie Fertigungskapazitäten in ihren Produktionsanlagen über Internet-Plattformen anbieten und vermitteln. Neben zahlreichen Vorteilen in Form von Umsatz- und Produktivitätssteigerungen, höherer Transparenz und flexibleren und dynamischeren Unternehmensprozessen entstehen hierdurch zwangsläufig auch neue Abhängigkeiten zwischen den Kooperationspartnern, die vertraglich geregelt werden müssen. Die am Wertschöpfungsnetzwerk beteiligten Unternehmen müssen sich darauf verlassen können, dass die vereinbarten Leistungen gesetzeskonform, fehlerfrei und termingerecht erbracht werden und die geteilten Daten gut geschützt sind. Rechts- und Sicherheitsfragen werden hierdurch zwangsläufig integraler Bestandteil von Digitalisierungsprozessen: Wie müssen die verarbeiteten Daten geschützt werden? Wie kann das Recht auf Löschen von personenbezogenen Daten umgesetzt werden? Wie können alle beteiligten Parteien Betriebs- und Geschäftsgeheimnisse schützen? Wer haftet, wenn Daten verloren gehen? Nur wenn diese Fragen zwischen den beteiligten Partnern geklärt sind, kann das notwendige Vertrauen im Wertschöpfungsnetzwerk entstehen, das für den Erfolg von essentieller Bedeutung ist.

Digitale Innovationen werfen neue Fragen auf

Rechtliche Grundlagen wie das Bundesdatenschutzgesetz, die Datenschutz-Grundverordnung (DSGVO) oder die europäische Richtlinie für Netzwerk- und Informationssicherheit geben Betrieben zwar erste und wichtige Anhaltspunkte zur rechtskonformen Beantwortung dieser Fragen. Durch die fortschreitende Digitalisierung entstehen allerdings fortlaufend neue offene Rechtsfragen, die durch das jetzige gesetzliche Regelwerk nicht umfassend abgebildet sind. Darf zum Beispiel eine Maschine die Daten Dritter verarbeiten und sie auch löschen oder speichern? Wem gehören Daten, die eine Maschine im Rahmen einer Zusammenarbeit erzeugt?

Die Wirtschaft braucht neue rechtliche Regelungen, die technische, organisatorische und rechtliche Fragen der IT-Sicherheit klären. Um Vereinbarungen auch prüfen zu können, müssen Unternehmen zudem einheitliche IT-Dokumentationssysteme einführen. Diese erfassen Datenflüsse und -verarbeitungsprozesse und machen sie dadurch nachvollziehbar. Je konkreter und praxisnäher die Vorgaben sind, desto leichter können Betriebe auch ihre IT-Sicherheit danach ausrichten.

In künftigen Wertschöpfungsnetzwerken wird es außerdem darauf ankommen, dass Unternehmen, die sich mit ihren Leistungskapazitäten daran teilweise oder ganz beteiligen, nicht immer wieder neu mit ihren (teilweise oder überwiegend unbekannten) Partnern Verträge über den zeitlich begrenzten oder dauerhaften Leistungsaustausch schließen müssen. Die Transaktionskosten wären beträchtlich und würden einen großen Teil des Effizienzgewinns zunichtemachen. Folglich gibt es einen Bedarf an standardisierten Lösungen, die es allen Beteiligten ermöglichen, an solchen kooperativen Wertschöpfungsprozessen in vollem Vertrauen mitwirken zu können.

Angesichts zunehmend vernetzter und autonom agierender Produktionsanlagen wird deutlich, wie komplex die Diskussion zu den IT-rechtlichen Fragen der Industrie 4.0 ist. Einerseits benötigen Mittelständler genauso wie Großkonzerne zeitnah praktische Antworten rund um die Themen Datenschutz, Datenhoheit und Datenhaftung, um digitale Innovationen in ihren Betrieben vorantreiben zu können. Andererseits sind vorab möglichst viele konkret umgesetzte Anwendungsfälle nötig, um realitätsnahe rechtliche Regelungen ableiten zu können.

Rechtsdiskurs aktiv mitgestalten

Die gerade erst in der Tiefe anlaufende Debatte rund um das IT-Recht bietet Unternehmen die Möglichkeit, sich mit ihren Anliegen in die Diskussion einzubringen. Umfragen zeigen, dass sich Unternehmer zum Beispiel bei allen Rechtsfragen zur Digitalisierung mehrheitlich EU-einheitliche Lösungen wünschen, damit auch bei grenzüberschreitenden Geschäften die Regelungen klar sind. Die Unternehmer zeigen vielfältiges Interesse an Neuregelungen in Kernthemen wie bei Haftungsfragen für Produkte, den Einsatz künstlicher Intelligenz, das Outsourcing von IT-Lösungen oder auch Cloud-Computing. Mit diesem Interesse und vor allem ihren bereits existierenden oder geplanten Digitalprojekten sollten die Betriebe den Diskurs bereichern und aktiv mitgestalten. Auch kleine und mittlere Unternehmen besitzen wertvolle fachspezifische Praxiserfahrungen, welche in das künftige IT-Recht einfließen sollten.

Eine transparente IT-Rechtslage bietet zukünftig allen Unternehmen die Chance, digitale Projekte und Kooperationen in einem sicheren Rahmen durchzuführen und die Potenziale der Vernetzung voll auszuschöpfen. Auf dem spannenden Weg dorthin stehen die Mittelstand 4.0-Kompetenzzentren von Mittelstand-Digital kleinen und mittleren Betrieben auch in Fragen des IT-Rechts mit Unterstützung zur Seite.

Zahlen & Fakten

DEFINITION

Kleine Unternehmen: <50 Mitarbeiter
Größere Unternehmen: 50-499 Mitarbeiter

IT-Sicherheit – Bedeutung: ja, Analyse: nein

Für **83 Prozent** aller größeren Unternehmen und **64 Prozent** der kleinen Unternehmen hat IT-Sicherheit eine hohe Bedeutung.

Aber nur **48 Prozent** der größeren und **20 Prozent** der kleinen Unternehmen führen eine regelmäßige IT-Sicherheitsanalyse durch.

Die häufigsten Ursachen für IT-Sicherheitsprobleme

II Probleme durch Virenangriffe

I Ausfall der IT-Systeme

III Versehentlich veränderte/ verloren gegangene Daten

Quelle: WIK-Studie „Aktuelle Lage der IT-Sicherheit in KMU“ im Rahmen der BMWi-Initiative „IT-Sicherheit in der Wirtschaft“ Dezember 2017, www.it-sicherheit-in-der-wirtschaft.de

Welche technischen Maßnahmen werden am häufigsten umgesetzt?

Virenschutz
Kleine Unternehmen:
98 Prozent
Größere Unternehmen:
100 Prozent

Passwörter
Kleine Unternehmen:
96 Prozent
Größere Unternehmen:
98 Prozent

Firewall
Kleine Unternehmen:
94 Prozent
Größere Unternehmen:
99 Prozent

Sicherungskopien von Daten
Kleine Unternehmen:
89 Prozent
Größere Unternehmen:
99 Prozent

Software-Patches und -Updates
Kleine Unternehmen:
90 Prozent
Größere Unternehmen:
97 Prozent

Woran fehlt es noch?

Nur **47 Prozent** aller Unternehmen mit weniger als 50 Mitarbeitern schulen ihre Mitarbeiter für Sicherheitsrisiken.

Nur **55 Prozent** der kleinen und größeren Unternehmen in Deutschland verfügen über Personal mit IT-Sicherheitskenntnissen.

Datenschutz?

Nur **15 Prozent** aller kleinen und größeren Unternehmen in Deutschland haben einen externen Datenschutzbeauftragten engagiert.

IT-Sicherheit richtig angehen

IT-Sicherheit ist mehr als nur eine Firewall. Die Mittelstand 4.0-Agentur Prozesse unterstützt auf dem Weg zum sicheren Betrieb.

Jedes Unternehmen arbeitet heute mit elektronischen Daten – von der E-Mail bis hin zur vernetzten Produktion werden Informationen zu Aufträgen, Produkten und Herstellungsdetails digital ausgetauscht. Diese Kommunikation beschleunigt die Prozesse von Betrieben, vernetzt sie mit Auftraggebern und Partnern in der ganzen Welt und stärkt ihre Wettbewerbsfähigkeit. Gleichzeitig machen die Daten jedes Unternehmen angreifbar. Wenn sie nicht umfassend geschützt sind, können sie leicht gestohlen oder gelöscht werden. „Daten sind heute die Kronjuwelen der meisten Unternehmen. Sie umfassen wertvolles Fachwissen etwa zu Produktionsabläufen oder Konstruktionsskizzen, das nicht in die falschen Hände geraten sollte“, erklärt Roland Hallau von der Mittelstand 4.0-Agentur Prozesse. „Jeder Betrieb muss sich deshalb zunächst überlegen, welche Daten für seine Arbeit unerlässlich sind. Diese gilt es entsprechend gut zu sichern.“

Den Anfang machen

Gerade kleinen Unternehmen ohne spezielle IT-Abteilung fällt es oft schwer einzuschätzen, was im Bereich IT-Sicherheit alles zu beachten ist. Um sich einen ersten Überblick zur Sicherheitslage im eigenen Unternehmen zu verschaffen, können Online-Tests Unterstützung bieten: So führt das Sicherheitstool-Mittelstand (SiToM) der Agentur Prozesse Unternehmer durch einen Fragebogen zu allen relevanten Aspekten der IT-Sicherheit und deckt damit mögliche Lücken auf.

IT-Sicherheit beginnt grundsätzlich mit der Basissicherheit der Daten im Unternehmen. „Dazu zählen Backups, also Sicherungskopien der wichtigsten Daten. Betriebe sollten hier klare Prozesse festlegen: Wer ist in welchen zeitlichen Abständen für die Sicherung zuständig? Die sensibelsten Daten sollten auf allen Wegen nur verschlüsselt übertragen werden“, erläutert Roland Hallau.

Daneben sind etwa ein guter Virenschutz sowie regelmäßige Software-Updates auf allen betrieblich genutzten Endgeräten wichtig. „Wir sehen viele Unternehmen, die zwar ihre PCs im Büro oder der Produktionshalle angemessen schützen, doch Smartphones und Tablets ihrer Mitarbeiter vergessen“, gibt Hallau zu bedenken.

IT-Sicherheit ist Chefsache

Eine gut geschützte IT muss vor allem gut organisiert werden und sollte daher Chefsache sein. Nur wenn alle Mitarbeiter Bescheid wissen, wie sie die IT-Strukturen

nutzen sollen und welche Regeln gelten, funktionieren Schutzmechanismen. „Es ist Aufgabe eines Geschäftsführers, seine Mitarbeiter regelmäßig für IT-Themen zu sensibilisieren.“ Hallau rät, klare Richtlinien vorzugeben, wie beispielsweise, ob es erlaubt ist, das private Handy für Berufliches zu nutzen. Der Chef eines Betriebs sollte seine IT mitsamt ihren Gefahren kennen und für den Ernstfall vorbereitet sein. Ein vorher strukturierter Notfallplan hilft im Zweifelsfall, wertvolle Zeit zu sparen und Schäden möglichst gering zu halten.

Zuletzt sollten Betriebe auch die rechtlichen Aspekte der IT-Sicherheit berücksichtigen. „Unternehmen besitzen viele personenbezogene Daten von Kunden, wie deren Adresse oder Kontonummer. Sie sind gesetzlich dazu verpflichtet, diese Informationen angemessen zu schützen“, erklärt Roland Hallau. „Allein mit Blick auf die wachsende Regulierung der IT-Sicherheit sollten sich alle Unternehmen eingehend mit ihren Strukturen und Prozessen auseinandersetzen, um sich selbst und die Kunden auf der sicheren Seite zu wissen.“

CHECKLISTE

Welche Aspekte müssen beachtet werden?

Basissicherheit

- ☐ **Datensicherung:** Wertvolle Daten definieren und zuverlässig sichern
- ☐ **Virenschutz:** Alle Geräte berücksichtigen und Mitarbeiter einweisen
- ☐ **Updates:** Software immer auf dem neusten Stand halten
- ☐ **Netzwerk:** Zugriffsrechte klären und beschränken

Organisation

- ☐ **Mitarbeiter:** Schulungen für besseres IT-Sicherheits-Verständnis
- ☐ **Sicherheitsrichtlinien:** Prozesse und Verantwortlichkeiten klären
- ☐ **Benutzerkonzept:** Berechtigungen prüfen und zuweisen
- ☐ **Verschlüsselung:** Wichtige Daten zusätzlich schützen
- ☐ **Risikoanalyse:** Schwachstellen kennen
- ☐ **Notfallmanagement:** Wiederherstellung sichern

Recht

- ☐ **Datenschutz:** Relevante Vorgaben einhalten
- ☐ **Gesetze:** Aktualität regelmäßig prüfen

Sicherheit muss einfach sein

Schon wieder das Passwort aktualisieren? Viele Mitarbeiter verbinden IT-Sicherheit mit lästigen Anweisungen, die Zeit kosten und in denen sie keinen Sinn sehen. Das Mittelstand-Digital-Projekt „USecureD – Usable Security by Design“ unterstützt Unternehmen deshalb dabei, Sicherheitsmaßnahmen so benutzerfreundlich wie möglich zu gestalten.

IT-Sicherheit verbinden die meisten Menschen mit einer geschützten Internetverbindung, sicheren Netzwerken, Firewalls und guter Hardware. Doch in ihrer Arbeit als Berater für Informationssicherheit machten die Mitarbeiter der bee security GmbH die Erfahrung, dass es häufig gar keine Cyberkriminellen sind, die sich aufwändig in Systeme von Unternehmen hacken. Oftmals besteht der sicherheitsrelevante Fehler darin, dass ein Mitarbeiter Sicherheitsmaßnahmen nicht beachtet und Hackern bildlich gesprochen die Tür ins Unternehmen öffnet. Das geschieht in den seltensten Fällen mit böser Absicht, sondern eher aus Unwissenheit oder Bequemlichkeit. Das Passwort wird auf einen Haftzettel aufgeschrieben, um es sich nicht merken zu müssen, oder die Datenverschlüsselung wird deaktiviert, weil sie den PC so langsam macht. Die Unachtsamkeit eines Einzelnen kann jedoch das gesamte Sicherheitskonzept eines Unternehmens zu Fall bringen. Das zeigen auch immer wieder Untersuchungen, die belegen, dass das größte Sicherheitsrisiko in vielen Unternehmen von der Unachtsamkeit der Mitarbeiter ausgeht – und nicht durch Angriffe von außerhalb.

IT-Sicherheit funktioniert nur gemeinsam

Die Berater von bee security wissen aus Erfahrungen mit ihren Kunden, dass Mitarbeiter Sicherheitsanwendungen vor allem dann nutzen, wenn sie einfach und verständlich gestaltet waren. „IT-Sicherheit setzt immer ein Mitwirken der Nutzer und Administratoren voraus. In der Unternehmenswirklichkeit erweisen sich viele Maßnahmen als ineffektiv, weil sie aus Nutzersicht sehr anspruchsvoll oder umständlich sind“, erläutert Dr. Lars Fink von bee security. Um die Kunden mit Blick auf die Usability, also Nutzerfreundlichkeit und Gebrauchstauglichkeit von Sicherheitslösungen noch besser beraten zu können, belegte bee security im Rahmen des Mittelstand-Digital-Projekts USecureD einen Workshop bei der Projektgruppe der TH Köln. USecureD hat ein Modell für die Entwicklung nutzerfreundlicher und gleichzeitig sicherer IT-Systeme entwickelt und stellt dazu konkrete Methoden und Werkzeuge zur Verfügung.

„USecureD gibt Softwareentwicklern Designempfehlungen und Checklisten an die Hand, um ein gleiches oder höheres Sicherheitslevel bei besserer Usability zu erreichen. Viele Unternehmen setzen auf individuell erstellte Softwarelösungen, die häufig von sehr vielen Mitarbeitern genutzt werden und in denen hochsensible Daten verarbeitet werden. Berater können die Richtlinien von USecureD dazu nutzen, diese Lösungen so zu verbessern, dass das Sicherheitsniveau steigt“,

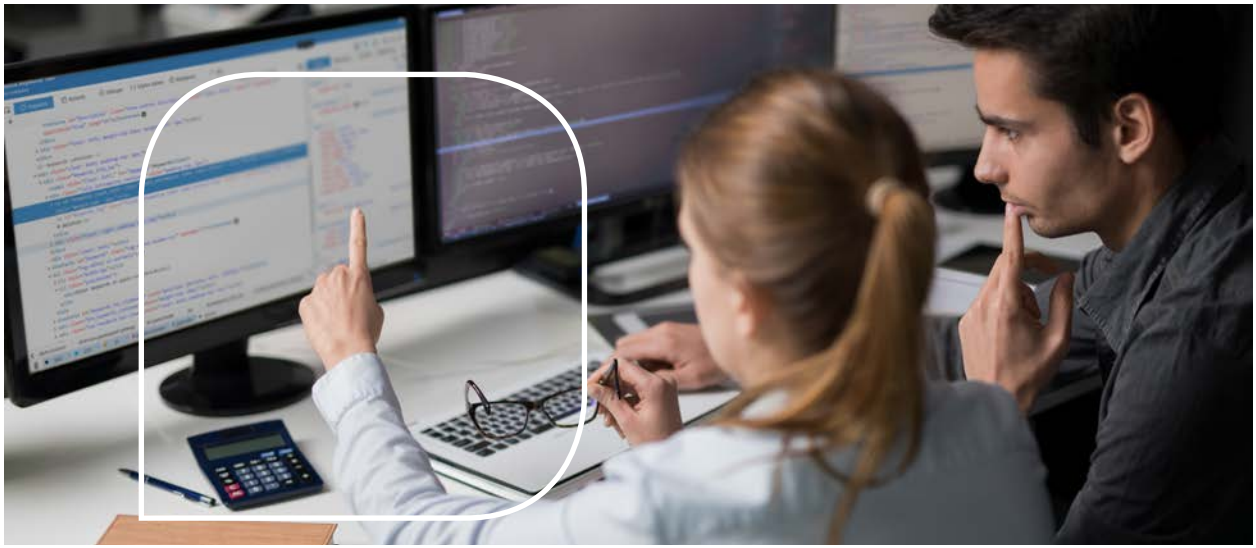
erklärt Hartmut Schmitt von der HK Business Solutions GmbH. Das Unternehmen entwickelt Software für kleine und mittlere Unternehmen und hat als Projektpartner von USecureD selbst viel Erfahrung in der Umsetzung von benutzerfreundlichen Sicherheitsfunktionen.

Der Laie als Ausgangspunkt

Bei der Entwicklung von nutzerfreundlichen IT-Sicherheitskonzepten müssen sich Betriebe in die eigenen Mitarbeiter hineinversetzen, die meist über keine Vorkenntnisse verfügen. Das System muss immer so intuitiv wie möglich zu bedienen sein, denn für die Lektüre von Handbüchern oder Anleitungen fehlt im Arbeitsalltag die Zeit. In die Entwicklung sollten Modelle aus der Psychologie, Erkenntnisse aus der Designforschung und der Mensch-Computer-Interaktion einfließen.

Bei einem guten Endprodukt, also einem bestimmten Anwendungsprogramm, sollen auch Laien und technikferne Anwender in der Lage sein, Sicherheitselemente zumindest grundlegend zu verstehen und sie wie vom Unternehmen vorgesehen zu verwenden.

Um IT-Sicherheitsfunktionen von vorherein nutzerfreundlich zu gestalten, bieten die Forschungsergebnisse von USecureD Werkzeuge für den gesamten Softwareentwicklungsprozess. „Für Unternehmen lohnt es sich, neue IT-Systeme strategisch anzugehen und etwas Zeit in die Entwicklung zu investieren: Denn wenn Mitarbeiter in den Entwicklungsprozess einbezogen werden und merken, dass auf ihre Bedürfnisse Rücksicht genommen wird, sind sie motivierter, Sicherheitstechnologien korrekt anzuwenden – was im Zweifelsfall vor großem Schaden bewahrt“, resümiert Hartmut Schmitt.



Sicheres Werkzeug aus der Hosentasche

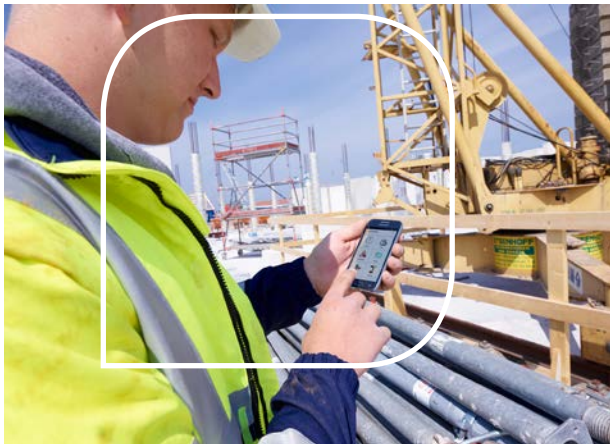
Bauunternehmer Jürgen Bruns entwickelte eine mobile Zeiterfassungslösung, mit der kleine und mittelständische Unternehmen der Baubranche sicher und unkompliziert ihre Daten verwalten können und gleichzeitig alle rechtlichen Anforderungen erfüllen.

Beim Hausbau für einen Softwareunternehmer kam Jürgen Bruns vor rund 10 Jahren die Idee: Gemeinsam mit seinem damaligen Auftraggeber konzipierte der Geschäftsführer eines mittelständischen Bauunternehmens eine Anwendung, die gleich mehrere Probleme für ihn lösen sollte. Zum damaligen Zeitpunkt erfassten die rund 20 Angestellten ihre Arbeitszeiten, Auftragsdaten oder Standortinformationen auf Papier. „Das hatte nicht nur den Nachteil, dass diese Informationen händisch in unsere Buchhaltungssoftware übertragen werden mussten: Gingen Dokumente verloren oder gab es Probleme mit gespeicherten Daten auf der lokalen Festplatte, war eine detaillierte Rekonstruktion der Arbeitszeiten oder Baustelleninformationen oft sehr schwierig, wenn nicht gar unmöglich“, erklärt Bruns. Also entschied er sich dafür, gemeinsam mit dem Softwareunternehmer seine Anwendung „123erfasst“ zu entwickeln, mit der seine Mitarbeiter nicht nur mobil ihre Stunden erfassen und übermitteln, sondern gleichzeitig auch wichtige andere Auftragsinformationen festhalten können. „Als Bauunternehmer sind wir zum Beispiel rechtlich dazu verpflichtet, ein Bautagebuch zu führen. Mit der entwickelten App können automatisch Wetterdaten, Materialverbrauch und Fotos erfasst werden. So kann dieser Pflicht viel leichter nachgekommen werden.“ Aber auch bei Zollkontrollen auf Baustellen, bei denen etwa die rechtlichen Vorgaben für die maximale Arbeitszeit überprüft werden, sorgt die App dafür, dass der Arbeitgeber seine Aufzeichnungspflicht nachweisen kann.

Datenschutz und Ausfallsicherheit

Die Zeiterfassungslösung sorgt jedoch nicht nur dafür, dass rechtliche Vorschriften zur Dokumentation auf der Baustelle erfüllt werden. Mit der cloudbasierten Lösung

wollte Bruns die erfassten Daten auch besser schützen. „Viele Unternehmer haben ja grundsätzlich eher Angst, dass ihre Daten durch die Erfassung in einer Cloud verloren gehen oder ‚gelöscht‘ werden.“ Tatsächlich überwiegen oftmals aber die Vorteile der Cloud-basierten Softwarelösungen: So werden die erfassten Daten auf einem externen Server in einem speziell gesicherten Rechenzentrum gespeichert, der mit einem Server in einem zweiten Rechenzentrum in einer anderen Stadt gespiegelt wird, so dass ein Datenverlust durch einen Brand oder Einbruch im eigenen Betrieb oder einem Rechenzentrum ausgeschlossen wird. Gleichzeitig sorgt die Software dafür, dass die erfassten Mitarbeiterdaten datenschutzkonform gespeichert werden – ein wichtiger Punkt beim Umgang mit den sensiblen Daten, der viele Unternehmer im Alltag herausfordert. Für den Bauunternehmer haben sich durch die Umsetzung seiner Idee nicht nur viele Prozesse erleichtert, er wurde gleichzeitig auch zum Unternehmer für seine eigene Softwarelösung. „Mit 123erfasst sind Unternehmen nicht nur deutlich sicherer, sondern auch effektiver unterwegs. Das erleichtert den Unternehmensalltag ungemein“, freut sich Bruns.



MOBILE IT-SICHERHEIT

Mobile Endgeräte wie Tablets oder Smartphones werden immer beliebter – auch im Handwerk setzen immer mehr Betriebe auf die intelligente Unterstützung im Geschäftsalltag. „Die Mitarbeiter müssen dafür sensibilisiert werden, dass hier die gleichen Sicherheitsvorschriften gelten wie an den anderen Geräten des Firmen-Netzwerks. Auch mobile Endgeräte können von Angriffen oder Viren befallen werden“, erklärt Rainer Holtz vom Kompetenzzentrum Digitales Handwerk. Das Kompetenzzentrum hat deshalb einen Kurzleitfaden zum Einsatz von Smartphones im Geschäftsalltag erstellt, der auch die wichtigsten Grundlagen zum sicheren Gebrauch auflistet:

- Keine privaten Smartphones im betrieblichen Einsatz
- Aktualität des Betriebssystems und von Apps sicherstellen
- Sichere Geräte- und Displaysperre einrichten
- Verschlüsselung von Zusatzspeicherkarten
- Möglichst wenige Apps installieren, um Datensammlung zu reduzieren
- Regelmäßige Backups durchführen
- Notfallplan für den Verlust oder Diebstahl des Smartphones

Hacken für den guten Zweck

Für Unternehmer ein Alptraumszenario: Der eben noch exakt arbeitende Industrieroboter kommt plötzlich aus dem Takt und seine Bewegungen lassen sich nicht mehr kontrollieren. Doch manchmal ist das sogar gewollt: Mithilfe von sogenannten Penetration Tests und Red Team Assessments können Unternehmen Sicherheitslücken aufdecken. Ein Blick von außen hilft Betrieben, sich besser zu schützen.

Die Zuschauer staunten beim Live-Hacking auf einer Veranstaltung des Mittelstand 4.0-Kompetenzzentrums Augsburgs nicht schlecht: Die vermeintlichen Angreifer brauchten nur wenige Minuten, um den mannshohen Produktionsroboter unter ihre Kontrolle zu bringen. Im echten Leben stünde die Produktion still und der Roboter könnte großen Schaden anrichten. In diesem Fall handelte es sich aber nur um eine Simulation: Ein Spezialist für die Aufdeckung von Schwachstellen in Firmennetzwerken hackt Betriebe auf deren Wunsch hin, um die IT-Sicherheit auf die Probe zu stellen. Ziel der Prüfverfahren wie Penetration Tests und Red Team Assessments ist es, Mittel und Wege aufzuspüren, die Angreifer anwenden würden, um unautorisiert in die Unternehmenssysteme einzudringen, und anschließend den Sicherheitsstatus des Unternehmens zu bewerten. Damit werden Betriebe für ihre eigenen IT-Gefahren sensibilisiert, denn wer seine Schwachpunkte und individuellen Risiken kennt, kann passgenaue Schutzmaßnahmen ergreifen.

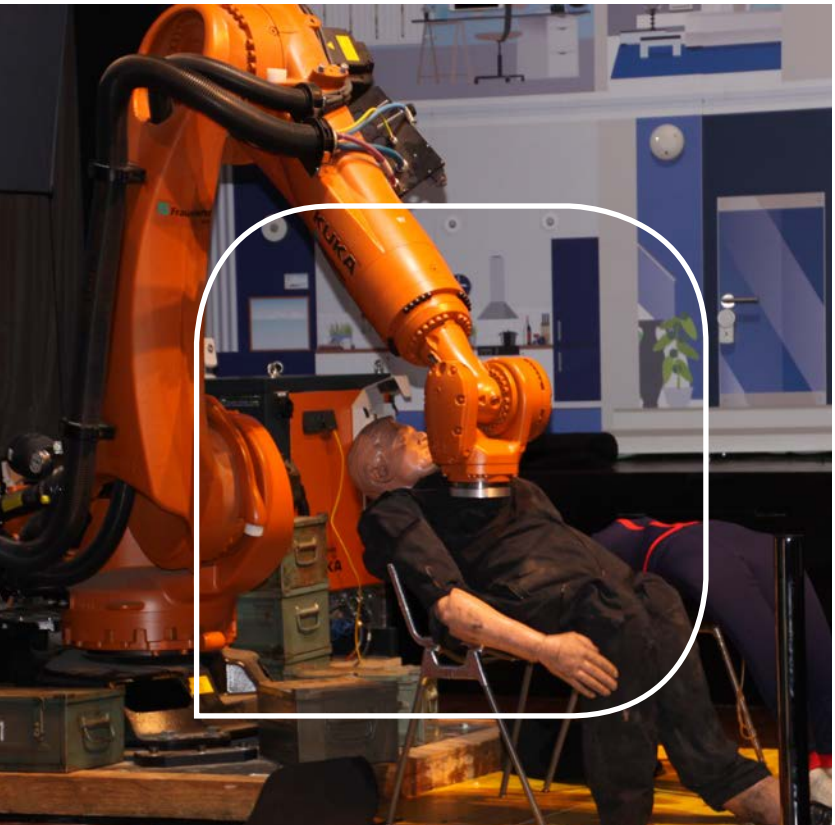
Blickwinkel der Cyberkriminellen

Während neue Maschinen getestet werden, bevor sie ans System angeschlossen werden, ist das bei neuen IT-Lösungen nicht immer der Fall. Dabei bietet jede neue Soft- oder Hardware-Komponente Cyberkriminellen neue Einfallstore in ein Unternehmen. Gerade der Mittelstand ist ein beliebtes Ziel für Hacker, da viele Betriebe über wertvolles Fachwissen verfügen. Trotzdem kaufen die meisten Unternehmen etwa eine neue Firewall, ohne genauer zu prüfen, was sie kann und was nicht. „Wir versetzen uns in die Lage des Angreifers: Wo kommen wir rein und welchen größtmöglichen Schaden können wir anrichten?“, berichtet Sascha Herzog, technischer Geschäftsführer der NSIDE ATTACK LOGIC GmbH, der täglich derartige Angriffe für Unternehmen durchführt und zusammen mit dem Mittelstand 4.0-Kompetenzzentrum Augsburg Live-Hacking-Veranstaltungen umsetzt, um Firmen zu sensibilisieren.

Neutraler System-Check

Externe Sachverständige können Betriebe dabei unterstützen, einen neutralen Blick auf das eigene IT-System zu erhalten. Sie wollen keine Soft- oder Hardware-Produkte verkaufen, sondern werden gezielt dafür beauftragt, deren Sicherheit zu testen. Sie prüfen zum einen bereits bestehende IT-Werkzeuge ihrer Kunden und beraten andererseits, wie der Schutz weiter verbessert werden kann. Sie spielen alle möglichen Angriffsszenarien durch, die ein Betrieb erleiden könnte: Als Hacker

greifen die IT-Berater im Rahmen von Penetration Tests einzelne IT-Systeme an. Schaffen sie es zum Beispiel, die Kesselsteuerung eines Chemieunternehmens unter ihre Kontrolle zu bekommen? Oder sie testen die Awareness von Mitarbeitern: Öffnet der Personaler die gefälschte Bewerbungs-E-Mail mit einem Computervirus im Anhang? IT-Sicherheit hängt zudem auch davon ab, wie sicher der Unternehmensstandort im Ganzen ist. Schaffen es die IT-Berater, sich nachts Zugang zum Gelände zu verschaffen und den Server zu stehlen, oder auch tagsüber Zutritt zu sensiblen Bereichen zu erhalten? All das können Betriebe gründlich prüfen lassen.



Zum Glück nur eine Demonstration: Ein missbräuchlich gesteuerter Roboterarm kann großen Schaden anrichten.

„Für viele kleine Betriebe sind Penetration Tests oder komplexe Angriffssimulationen zu aufwendig und teuer. Die Methodik können sie sich aber dennoch zunutze machen: Jeder Betrieb sollte sich kontinuierlich fragen, wo Angreifer bei ihnen die besten Einfallschancen haben, und diese direkt angehen. Zudem können Einrichtungen wie die Mittelstand 4.0-Kompetenzzentren dabei helfen, eine realistische Risikoanalyse durchzuführen“, erklärt Christoph Berger vom Mittelstand 4.0-Kompetenzzentrum Augsburg.

Vorsorge für den Ernstfall

Nach der Analyse der eigenen Schwachstellen können Unternehmen besser vorsorgen. „In ein Unternehmen reinzukommen schafft man fast immer“, so Sascha Herzog. „Die wichtigste Frage ist, wie weit beziehungsweise wohin kommt der Hacker, sobald er im System ist?“ Neben der externen Sicherheit eines Unternehmens ist auch die interne ausschlaggebend. „Einem Hacker soll der Weg zum Ziel maximal schwergemacht werden“, erläutert Herzog. Daher sind interne Schranken im IT-System sehr wichtig. Unternehmen müssen sich beispielsweise die Frage stellen, welche Mitarbeiter welche Zugriffsrechte haben. Braucht zum Beispiel die Empfangssekretärin Zugang zu Produktionsdaten? Je spezifischer Zugriffsberechtigungen gestaltet sind, desto komplexer wird es für Cyberkriminelle, sich etwa mit einem Virus an den „richtigen“ Mitarbeiter im Unternehmen zu wenden.

Mit Social Media auf der sicheren Seite

Vorsicht, heiß! Diesen Hinweis lesen Kaffee-Liebhaber heute auf fast jedem Becher. Warum? Hersteller müssen ihr Produkt und den Umgang damit so sicher und leicht verständlich wie möglich gestalten. Auf Social-Media-Kanälen finden Unternehmen wichtige Hinweise, wie Kunden die eigenen Produkte qualitativ bewerten und tatsächlich nutzen. Aus den Kundenkommentaren ergeben sich für Hersteller wertvolle Ableitungen, um die Vorgaben des Produktsicherheitsgesetzes zu erfüllen.

Wozu einen Heckenschneider kaufen, wenn man einen autonomen Rasenmäher hat? Der Mann im Internet berichtet schließlich, er würde den Rasenmäher einfach hochheben und damit seine Hecken stutzen. Und auch im Beautyforum gibt es gute Tipps: Eine Userin berichtet darüber, wie sie sich das Glätteisen spart, indem sie ihre Haare mit dem Bügeleisen bearbeitet. Herstellern stehen bei diesen „Tipps“ sicherlich selbige zu Berge.

Kundenfeedback richtig nutzen

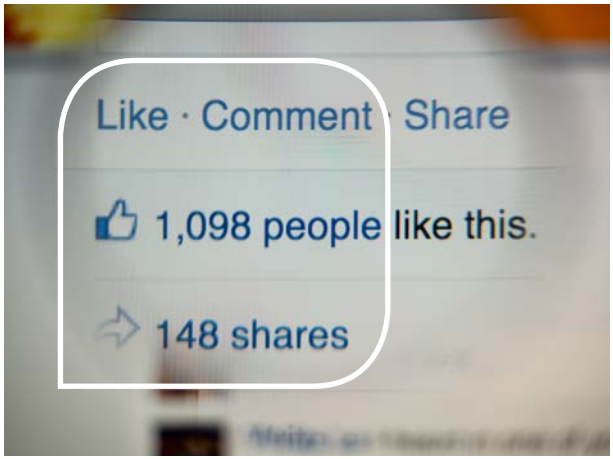
Dass online über die eigenen Produkte gesprochen wird, ist für Hersteller Fluch und Segen zugleich. Fünf- oder Vier-Sterne-Bewertungen und Ausführungen darüber, warum das Produkt überzeugt, locken weitere potenzielle Kunden an. Negative Bewertungen, Shitstorms und ominöse Ratschläge können aber auch schnell eine falsche Richtung nehmen. Für Unternehmen ist es daher beinahe unumgänglich, die Beiträge ihrer Kunden zu beobachten und aus den Daten Rückschlüsse für die Verbesserung der eigenen Produkte oder Services abzuleiten.

Produkte sicherer machen

Kundenfeedback bei Facebook oder Twitter dient nicht nur dazu, noch mehr Produkte zu verkaufen, sondern hilft auch, Sicherheitsaspekte zu beleuchten und zu verbessern. Im Rahmen des Produktsicherheitsgesetzes sind Hersteller nämlich dazu verpflichtet, nur solche Produkte auf den Markt zu bringen, die in der Verwendung die gesetzlichen Anforderungen an die Sicherheit und den Gesundheitsschutz erfüllen. Hersteller müssen dabei sowohl die bestimmungsgemäße Verwendung (Rasenmäher zum Mähen) eines Geräts als auch die vorhersehbare Verwendung (Rasenmäher zum Schneiden der Hecke) berücksichtigen. Und Informationen in Bezug auf die tatsächliche Produktverwendung, sei sie bestimmungsgemäß, vorhersehbar oder kreativ, lassen sich im Netz finden. Auf dieser Basis können Unternehmen also Gegenmaßnahmen zu gefährlichen Verwendungszwecken ergreifen und ihre Produkte überarbeiten. So erhält der Rasenmäher zum Beispiel einen automatischen Abschaltmechanismus, der greift, sobald der Bodenkontakt fehlt.

Analyse von Online-Diskussionen

Falls online sehr viel über ein Produkt gesprochen wird, oder ein Unternehmen noch nicht weiß, auf welchen Seiten sich die Kunden austauschen, können Betriebe Social-Media-Analyse-Tools nutzen, um sich einen Überblick zu verschaffen. Diese Programme können mittlerweile nicht nur Schlagworte erfassen, sondern auch den Tenor der Social-Media-Diskussionen erfassen. Hersteller müssen bei jeder Markteinführung vorhersehen, wie ihre Kunden das Produkt verwenden könnten. „Für jede denkbare Missbrauchsmöglichkeit muss der Hersteller konstruktive Gegenmaßnahmen ergreifen, mindestens jedoch Hinweise in die Bedienungsanleitung aufnehmen. So können Unternehmen mögliche Risiken aus dem Produkthaftungsgesetz minimieren. Auf Social-Media-Kanälen sehen Hersteller, wie Kunden sich in welchem Zusammenhang zu ihrem Produkt äußern, und können dann entscheiden, ob diese Nutzung einen möglichen Missbrauch impliziert oder alles im grünen Bereich ist“, erklärt Verena Heinrichs, Head of Social Media Intelligence bei der PRS Technologie Gesellschaft mbH. Laut des externen Partnerunternehmens des Mittelstand 4.0-Kompetenzzentrums Dortmund verfolgen Unternehmen über Social-Media-Analysen immer mit einem Ohr die laufende Diskussion der Kunden und können rechtzeitig gegensteuern, wenn beispielsweise neue, gefährliche Nutzungsfälle beschrieben werden. Das Produkt kann regelmäßig verbessert werden und der Hersteller engagiert sich nachweislich für die Produktsicherheit, was Haftungsrisiken unwahrscheinlicher macht.



Ob sich eine umfassende Analyse lohnt, hängt von der Betriebsgröße und den Social-Media-Aktivitäten der Kunden ab. In jedem Fall rentiert sich ein regelmäßiger Blick in thematisch passende Foren und Blogs, um auf dem Laufenden zu bleiben, welche Aspekte eines Produkts bei den Kunden aktuell für Gesprächsstoff sorgen.

So unterstützt Mittelstand-Digital

Mittelstand-Digital unterstützt kleine und mittlere Betriebe durch anbieterneutrale Angebote vor Ort. Die Mittelstand 4.0-Kompetenzzentren informieren deutschlandweit über Herausforderungen und Handlungsfelder bei den Themen IT-Sicherheit und Recht. Gleichzeitig bieten sie Unterstützung bei der Erarbeitung entsprechender Arbeitspläne und der Auswahl von passenden Anwendungen und Dienstleistern. Auch Workshops, Schulungen und Informationsveranstaltungen bieten sie an. Die Mittelstand 4.0-Agenturen setzen sich mit den übergreifenden Fragen der Digitalisierung auseinander: Ihre Schwerpunktthemen sind Cloud, Prozesse, Kommunikation und Handel. Ihr Expertenwissen geben sie an Multiplikatoren wie Kammern, Berufsverbände und die Mittelstand 4.0-Kompetenzzentren weiter. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung dieser Angebote.

Das BMWi bietet mit der Initiative „IT-Sicherheit in der Wirtschaft“ zudem konkrete Maßnahmen zur nachhaltigen Verbesserung des Bewusstseins für IT-Sicherheit speziell bei kleinen und mittleren Unternehmen. Informationen gibt es auf der Website: www.it-sicherheit-in-der-wirtschaft.de

Zu den Themenbereichen „Recht und IT-Sicherheit“ bieten die Mittelstand 4.0-Agenturen und -Kompetenzzentren Expertenwissen zu folgenden Spezialgebieten:

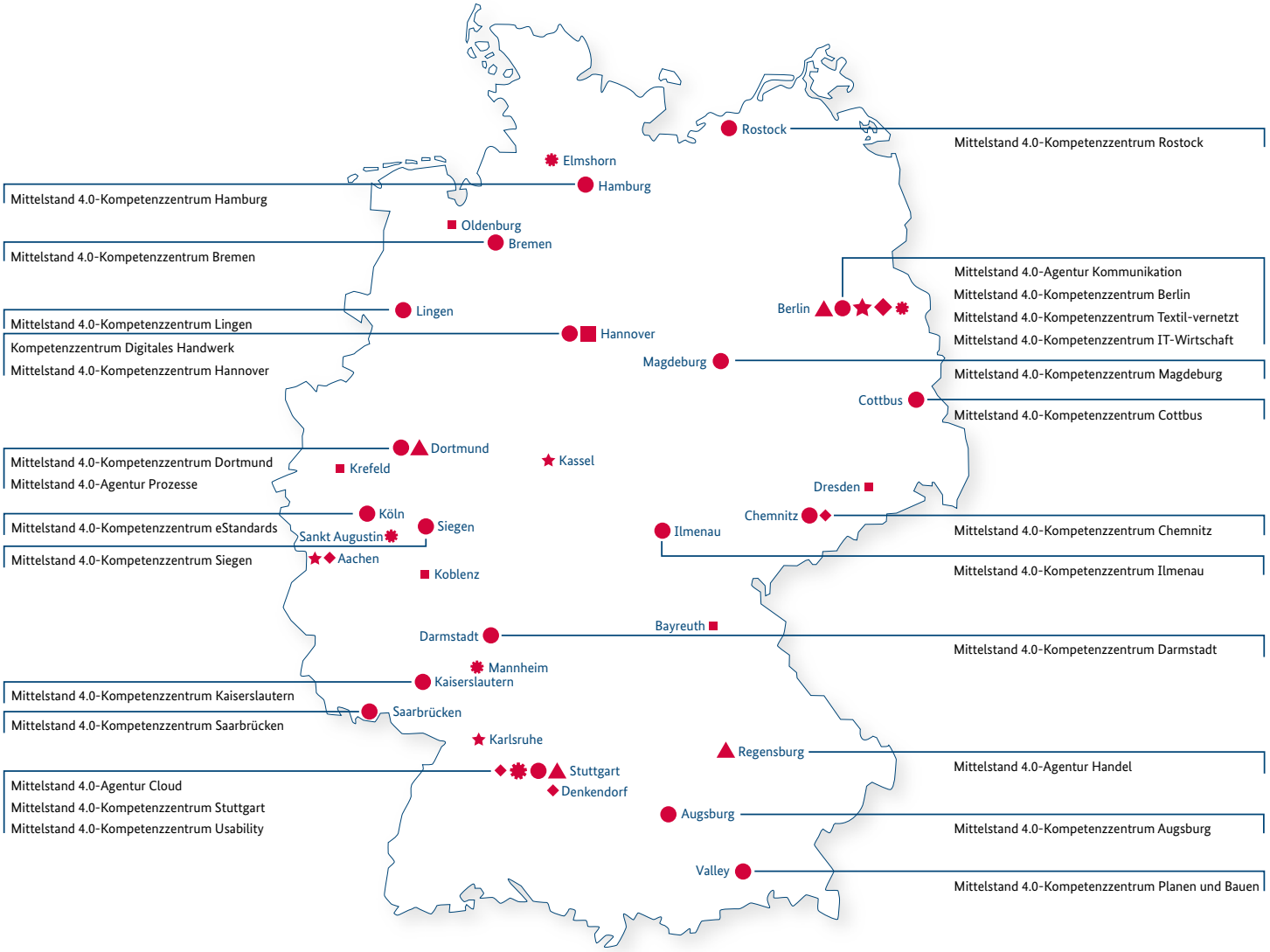
Mittelstand 4.0-Kompetenzzentrum Augsburg
- Spionageattacken auf Industriesysteme
- Sicherheit von Industrie-Robotern
- Sicherer Datenaustausch in der automatisierten Produktion

Mittelstand 4.0-Kompetenzzentrum Berlin
- Rechtssicheres WLAN
- Grundlagen Internetsicherheit
- Sicherheitsrisiko Mensch im Unternehmen

Mittelstand 4.0-Kompetenzzentrum Bremen
- Sichere Mensch-Technik-Interaktion in der Produktion
- Datensicherheit und Rechtemanagement für digitale Produktdaten
- IT-Sicherheit für Maritime (Verkehrs-) systeme/ Navigationssysteme

Mittelstand 4.0-Kompetenzzentrum Chemnitz

„Wissensbox Recht 4.0“:
- Wichtige Literatur und Rechtsvorschriften in der Übersicht
- Aktuelle Urteile
- Eigene Anfrage an die Rechtsexperten stellen



- 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
- Kompetenzzentrum Usability
- Regionale Anlaufstellen Usability
- Kompetenzzentrum IT-Wirtschaft
- Regionale Stützpunkte IT-Wirtschaft
- Kompetenzzentrum Textil-vernetzt
- Regionale Schaufenster Textil-vernetzt

Mittelstand 4.0-Kompetenzzentrum Cottbus
- IT-Sicherheit
- Datensicherheit
- BSI-Grundschutzkatalog

Mittelstand 4.0-Kompetenzzentrum Darmstadt
- Integrität-Prüfung & Anomalie-Erkennungen (Frühwarnungen) bei Produktionssystemen
- Verarbeitung sensibler Mitarbeiterdaten
- IT-Sicherheit in der Produktion

Mittelstand 4.0-Kompetenzzentrum Dortmund
- Cybersicherheit in der Produktion
- Rechtssicherheit bei CMS- und ERP-Systemen
- Datensicherheit und Datensouveränität in unternehmensübergreifenden Netzwerken (Industrial Data Space)

Mittelstand 4.0-Kompetenzzentrum eStandards
- Rechtssichere Archivierung elektronischer Rechnungen
- Umsetzen gesetzlicher Richtlinien (wie LMIV, UDI) mit Standards
- IT-Sicherheit und Datenschutz in der Produktion

Kompetenzzentrum Digitales Handwerk
- Cyber-Sicherheit und Datensicherung im Handwerk
- Sicherer Fernzugriff auf Unternehmensdaten
- IT-Sicherheitsbotschafter im Handwerk

Mittelstand 4.0-Kompetenzzentrum Hamburg
- IT-Sicherheit beim mobilen Arbeiten
- Prävention von Cyberkriminalität im Handwerk
- Rechtliche Herausforderungen der Digitalisierung

Mittelstand 4.0-Kompetenzzentrum Hannover
- IT-Sicherheit in der Produktion
- Datenschutzanforderungen und Arbeitnehmerrechte in der vernetzten Produktion
- Rechtssicher in die digitale Zukunft

Mittelstand 4.0-Kompetenzzentrum Ilmenau
- Recht & Sicherheit in Wertschöpfungsnetzwerken
- Sicherheit von Mess- und Sensordaten
- Sicherheit bei Open-Source-Software-Lösungen

Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft
- IT-Sicherheit und Datenschutz in der standardisierten Interoperabilität von IT-Systemen (Information Security Policy)
- Vorlagen für Dokumente und Instrumente des Datenschutzes (EU DSGVO/IT-Sicherheit) für die mittelständische IT-Branche
- Rechtliche Gestaltung von Unternehmens-Kooperationen und kooperativen Geschäftsmodellen

Mittelstand 4.0-Kompetenzzentrum Kaiserslautern
- Sicheres Datenmanagement in der Produktentwicklung
- IT-Sicherheit von Maschinendaten in der Produktion

Mittelstand 4.0-Kompetenzzentrum Lingen
- Sicherer digitaler Datenaustausch zwischen Unternehmen
- (Rechts)sicheres digitales Prozessmanagement und Geschäftsprozesse

Mittelstand 4.0-Kompetenzzentrum Magdeburg
- IT-Sicherheit von Unternehmens- und Kundendaten
- IT-Risiko- und Zuverlässigkeitsanalysen
- IT-Sicherheit und Blockchain

Mittelstand 4.0-Kompetenzzentrum Planen und Bauen
- Sichere digitale Kommunikation zwischen allen Akteuren beim Bau
- Rechtliche Besonderheiten und Datenschutz beim digital unterstützten Bauen
- Datensicherheit in cloudbasierten IT-Lösungen

Mittelstand 4.0-Kompetenzzentrum Rostock
- IT-Sicherheit im Bereich Medizintechnik und eHealth
- Datenschutz für IT-Lösungen im Bereich Tourismus

Mittelstand 4.0-Kompetenzzentrum Saarbrücken
- Industrial IT-Security bei Vernetzung in Zulieferketten
- Industrial IT-Security bei der Digitalisierung der Produktion
- Rechtskonforme Internetseiten und Online-Shops

Mittelstand 4.0-Kompetenzzentrum Siegen
- Mitarbeiterdatenschutz und Usable Privacy
- Rechtliche Aspekte der Mensch-Maschine-Kooperation
- Schutz von Know-how und Geschäftsgeheimnissen in der Industrie 4.0

Mittelstand 4.0-Kompetenzzentrum Stuttgart
- Demonstratoren, u. a. im Living Lab smartSecurity und IT-Sicherheitslabor
- Angewandte IT-Sicherheitsforschung mit Fokus auf anwendbare Sicherheitslösungen
- Sensibilisierung und Schulung

Mittelstand 4.0-Kompetenzzentrum Textil-vernetzt
- Durchgängige und effiziente IT- und Datensicherheit bei E-Textiles
- Durchgängige und effiziente IT- und Datensicherheit bei Sensorsystemen und Produktionsanlagen der Textilindustrie

Mittelstand 4.0-Kompetenzzentrum Usability
- Usability-Wissen und -Methoden für Sicherheit bei der Nutzung von Informationstechnik
- IT-Sicherheit durch Usability bei der Entwicklung von Software
- IT-Sicherheit durch Usability bei der Beschaffung von Software

Mittelstand 4.0-Agentur Cloud
- IT-Sicherheit bei Cloud-Anwendungen
- Rechtssichere Cloud-Lösungen
- Herausforderungen durch die EU-Datenschutz-Grundverordnung

Mittelstand 4.0-Agentur Handel
- Elektronische Rechnungen sicher abwickeln
- Rechtliche Vorgaben für B2B-Websites und Onlineshops praktikabel umsetzen
- Webbasierte Kundendaten rechtssicher erheben und nutzen

Mittelstand 4.0-Agentur Kommunikation
- Sensibilisierung zu Recht und IT-Sicherheit-Themen durch Informationsveranstaltungen und Workshops
- Führungskräfte und Mitarbeiter bei der Einführung neuer Anwendungen mitnehmen, beteiligen und qualifizieren
- Aufklärungsarbeit zu rechtssicherer Online-Kommunikation mit Kunden, Partnern und Mitarbeitern

Mittelstand 4.0-Agentur Prozesse
- Sensibilisierung zur IT-Sicherheit und zum Datenschutz
- Feststellung des IT-Sicherheitsniveaus in Unternehmen
- Management von IT-Sicherheit in Produktionsumgebungen

Im Gespräch

„Die Fragestellungen werden durch die Digitalisierung spezifischer“

Dr. Dagmar Gesmann-Nuissl ist Professorin für Privatrecht und Recht des geistigen Eigentums an der Technischen Universität Chemnitz. Am Mittelstand 4.0-Kompetenzzentrum Chemnitz ist sie Expertin für alle juristischen Fragen – gleichzeitig leitet sie auch die Arbeitsgruppe „Recht“, in der ein fachlicher Austausch und Wissenstransfer aller Kompetenzzentren des Mittelstand-Digital-Netzwerks stattfindet.

Frau Professorin Gesmann-Nuissl, welche Fragen werden am häufigsten von den Unternehmen gestellt, wenn es ums Thema Recht geht?

Das ist ganz unterschiedlich und abhängig davon, in welcher Branche die Unternehmen tätig sind: So haben wir es zum Beispiel bei uns in Chemnitz sehr häufig mit Betrieben aus dem produzierenden Mittelstand zu tun. Und da die Digitalisierung der Produktionsprozesse naturgemäß auch die Umstrukturierung und Veränderung von Produktionsabläufen anbetrifft, werden auch die Arbeitsprozesse tangiert. Tätigkeiten können zum Beispiel digital unterstützt oder deutlich flexibler gestaltet werden als bislang. Dies wiederum bedingt, dass derzeit die Fragen zum Arbeitsrecht und zur Arbeitssicherheit bei uns im Vordergrund stehen.

Was bedeutet das konkret?

Durch die Digitalisierung und das Nutzen von Tablets und Smartphones kann sich z. B. die Arbeit von der Arbeitsstätte entkoppeln, was klassische arbeitsrechtliche Fragestellungen aufwirft, etwa zum Arbeiten von zuhause, von unterwegs, während der Urlaubszeit oder im Krankheitsfall. Die Fragen werden dann aber auch spezifischer. Wenn Unternehmen ihren Mitarbeitern z. B. die digitalen Anwendungen auf Tablets oder Smartphones ermöglichen möchten, stellen sie weitergehende Fragen, wie zum Beispiel: Müssen die Unternehmen hierfür den Betriebsrat einbeziehen? Wie müssen Mitarbeiter im Umgang mit diesen Geräten und den darauf befindlichen Daten geschult werden, damit sie die Geräte rechtssicher nutzen und keine Daten des Unternehmens verloren gehen? Besteht zur Schulung und Unterweisung eine unternehmerische Verpflichtung? Bestehen arbeitssicherheitsrechtliche Anforderungen, die zu beachten sind?

Nicht nur arbeitsrechtliche Fragen beschäftigen viele Betriebe: Viele Unternehmen fragen sich auch, wie sie dafür sorgen können, dass Unternehmensdaten trotz immer stärkerer Vernetzung geschützt bleiben.

Das betrifft die Themenbereiche der Datenhoheit und -sicherheit. Der Begriff der Datenhoheit zielt auf die Rolle der Daten als Wirtschaftsgut ab: Viele kleine und mittlere Unternehmen sind inhabergeführt oder besitzen eine sehr spezielle Marktführerschaft, so dass die Unternehmensdaten der „zu hütende

Viele kleine und mittlere Unternehmen sind inhabergeführt oder besitzen eine sehr spezielle Marktführerschaft, so dass die Unternehmensdaten der „zu hütende Schatz“ sind – und diese „Schatztruhe soll für Dritte geschlossen bleiben“.

Schatz“ sind – und diese „Schatztruhe soll für Dritte geschlossen bleiben“. Um dieses Ziel zu erreichen müssen sie einerseits technische und organisatorische Schutzmaßnahmen nutzen, um Angriffen und einer missbräuchlichen Nutzung ihrer Daten vorzubeugen. Es ist aber ebenso wichtig, dass sich die Betriebe über Verträge die „Rechte an ihren eigenen Daten“ sichern, gegebenenfalls auch im Rahmen bestehender Allgemeiner Geschäftsbedingungen (AGBs); besonders wenn Informationen an Dritte weitergegeben oder ihnen der Zugang zu den Daten gewährt wird. Auf der anderen Seite ist natürlich auch immer das Datenschutzrecht relevant, welches die personenbezogenen Daten des Einzelnen schützt. Auch hier müssen Unternehmen sicherstellen, dass sie zum Beispiel durch den Einsatz von Sensoren oder die automatisierte Weitergabe von Daten keine rechtlichen Vorgaben verletzen, und die Anforderungen berücksichtigen, welche die Datenschutz-Grundverordnung von den Unternehmen ab Mai abfordert.

Welche Fragen ergeben sich zudem durch die immer stärkere Digitalisierung?

Die Unternehmen beschäftigen sich auch mit der Haftung und Verantwortung. Sie wollen wissen, in welcher Weise sie in Anspruch genommen werden können, wenn Schäden durch Maschine-Maschine-Interaktionen in vernetzten Systemen entstehen oder durch die neuen Zusammenarbeitsformen von Menschen und Maschinen, z. B. unter Nutzung von Sensortechnik, Scannern, Datenbrillen und sonstigen Wearables. Daran schließt sich dann häufig auch die Frage nach der Versicherbarkeit solcher neueren Szenarien an. Es geht aber auch um neue Geschäftsmodelle oder effizientere Produktionsverfahren, wie etwa das der additiven Fertigung: Bei der Fertigung in „Losgröße 1“ tauchen mitunter Urheberrechtsfragen auf, die gelöst werden müssen, etwa wenn die Kunden eigene Ideen einreichen, die ihrerseits Schutz genießen, oder die Unternehmen einfach wissen wollen, ob sie einzelne schwer zu bekommende Ersatzteile ohne weiteres einscannen und nachbauen dürfen.

Wo finde ich als Unternehmen Unterstützung zum komplexen Themenfeld Recht?

Zum einen sind natürlich die Mittelstand 4.0-Kompetenzzentren Anlaufstellen, die bei der Klärung von Rechtsfragen Unterstützung leisten können. Zudem haben wir am Mittelstand 4.0-Kompetenzzentrum in Chemnitz eine „Wissensbox Recht 4.0“ entwickelt, die sich vor allem den angesprochenen Rechtsthemen widmet, also denen, die im Zusammenhang mit der Digitalisierung von Unternehmensprozessen relevant werden. In unserer „Wissensbox“ werden die vorgenannten Themenbereiche aufgenommen und allgemeinverständlich erläutert. Außerdem werden einschlägige Urteile vorgestellt und ihre Relevanz für die Unternehmen aufgezeigt, mitunter auch mit Handlungsempfehlungen verknüpft: Das leistet in vielen Fällen eine erste wertvolle Orientierung.

Im Gespräch

„Ein ganzheitliches IT-Sicherheitskonzept ist das A und O“

Frauke Goll ist die stellvertretende Leiterin des Mittelstand 4.0–Kompetenzzentrums Stuttgart und leitet zusammen mit Dr. Thomas Usländer die Arbeitsgruppe IT-Sicherheit. Die Arbeitsgruppe bietet den Teilnehmern die Möglichkeit, aktuelle IT-Sicherheitsfragen zu erörtern und Erfahrungen auszutauschen. Im Interview erklärt sie, worauf Betriebe achten müssen, um die Digitalisierung sicher anzugehen.

Frau Goll, was würden Sie als momentan drängendste Herausforderung im Bereich IT-Sicherheit ansehen? Und was als künftige?

Das A und O für jedes Unternehmen ist ein ganzheitliches IT-Sicherheitsmanagement. Das ist bei vielen Betrieben leider noch nicht ausgeprägt. Es ist wichtig, einen IT-Sicherheitsbeauftragten zu ernennen und die bestehende Sicherheitssoftware aktuell zu halten. Ein ganzheitliches Management setzt aber eben nicht nur auf solche Teilmaßnahmen, sondern integriert sämtliche Unternehmensebenen. Dabei geht es vor allem darum, das Personal in regelmäßigen Schulungen für den Umgang mit Daten und Software zu sensibilisieren und dadurch ein IT-Sicherheitsbewusstsein fest in der Unternehmenskultur zu verankern. Nur so ist es für kleine und mittlere Betriebe möglich, sich effektiv gegen Angriffe und Datenmissbrauch abzusichern.

Was die künftigen Herausforderungen angeht, wird die IT-Sicherheit im Internet der Dinge immer wichtiger werden. Die Vernetzung von internetfähigen Geräten, Maschinen und Fahrzeugen sorgt für größtmöglichen Komfort für die Nutzer. Gleichzeitig macht die Vernetzung Menschen und Unternehmen angreifbar für Hackerangriffe von außen, und es wird für eine ausreichende Sicherung der digitalen Infrastrukturen gesorgt werden müssen, um sich vor unerlaubten Zugriffen zu schützen.

Welche Sicherheitsfragen werden am häufigsten an die Experten in Ihrer Fachgruppe herangetragen?

In unseren Gruppensitzungen behandeln wir vorrangig Fragen, wie sich Firmen nachhaltig gegen Schadsoftware, Spionage und Datenmissbrauch schützen können. Vor allem durch zunehmende Datenerfassung und deren Zusammenführung über Cloud-Computing ist das Thema IT-Sicherheit in den letzten Jahren in den Vordergrund gerückt. Die immer größer werdenden und schneller anfallenden Datenmengen (Big Data) und deren Auslagerung an externe Dienstleister bereiten Betrieben, die mit personenbezogenen Daten arbeiten oder hochsensibles Spezialwissen nutzen, immer größere Sorgen. Deshalb beschäftigen wir uns etwa damit, was Betriebe im Ernstfall, also wenn es zu einem Sicherheitsvorfall kommt, tun können. Wenn Sicherheitsrisiken bestehen oder Datenschäden erfolgt sind, stellt sich für viele Unternehmen prinzipiell die

Frage, ob sie künftig noch mehr in IT-Sicherheit und Personal investieren sollen oder ob es vielleicht nicht sogar sinnvoller ist, auf Angebote wie Cloud-Computing generell zu verzichten. Das müssen die Betriebe dann gründlich erörtern.

Wird dem Thema IT-Sicherheit ausreichend Stellenwert eingeräumt?

Viele Firmen sind mit der Sicherung ihrer IT-Strukturen zeitlich und finanziell überfordert oder sie messen dem Thema nicht die entsprechende Bedeutung bei. Ein gutes IT-Sicherheitskonzept ist komplex und kostspielig und besonders kleinere Mittelständler neigen dazu, derartige Aufgaben an einen IT-Beauftragten zu übertragen, der IT-Sicherheit oftmals nur als weitere Zusatzaufgabe übernimmt. In erster Linie sollte sich in jedem Unternehmen die Chefetage dem Thema widmen, ihm oberste Priorität einräumen und Schutzziele definieren, damit die entsprechenden Weichen gestellt und Strukturen aufgebaut werden können. Erst dann sollten die Zuständigkeitsbereiche weiter delegiert werden. Darüber hinaus sind regelmäßige IT-Schulungen von allergrößter Bedeutung, denn ungeschulte Mitarbeiter bieten Einfallstore für Cyberangriffe. Leider fehlen vor allem kleineren Firmen dazu oftmals die Zeit und die finanziellen Mittel. Gerade deshalb ist das Angebot der Mittelstand 4.0-Kompetenzzentren hier so wichtig.

„Ein ganzheitliches IT-Sicherheitsmanagement integriert die Mitarbeiter sämtlicher Unternehmensebenen.“

Welche Fehler sollten Betriebe bei der Umsetzung von Sicherheitslösungen unbedingt vermeiden?

Wichtig ist vor allem das Einmaleins der IT-Security: Unverzichtbar sind ein ausreichender Passwortschutz, Kenntnis und Analyse der Verwundbarkeiten, eine ausführliche IT-Dokumentation sowie ein Schutz für den E-Mail-Verkehr. Ebenso sollten Mitarbeiter auf einen vertraulichen Umgang mit den Daten achten, alle Programme immer auf dem neuesten Stand halten und regelmäßige Backups aller Daten durchführen. Werden diese grundlegenden Maßnahmen nicht getroffen, kann es schnell zu einem Ausfall der digitalen Infrastruktur kommen und Daten können sehr leicht verloren gehen. Eine nachträgliche Rekonstruktion der Daten ist – falls überhaupt noch möglich – meist sehr aufwendig und kostspielig. Wichtig ist beim Thema IT-Sicherheit, dass Unternehmen nicht nur einzelne Teilbereiche sichern, sondern das große Ganze im Blick behalten: ein einheitliches IT-Sicherheits- und Risikomanagement minimiert die Wahrscheinlichkeit eines Angriffes enorm. Auch wenn die Kosten für IT-Sicherheit auf den ersten Blick hoch erscheinen, so sind diese letzten Endes immer noch niedriger als die Kosten eines Datenverlustes.

Endspurt zur Datenschutz-Grundverordnung

Mit der Datenschutz-Grundverordnung kommen umfangreiche Informations- und Dokumentationspflichten auf Unternehmen zu. Was Betriebe vom Klempner bis zum Autozulieferer mit Blick auf die neue Datenschutz-Regelung beachten müssen:

Es dauert nicht mehr lange, bis die EU-Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 zur Anwendung kommt. Die Verordnung betrifft alle Unternehmen, die personenbezogene Daten verarbeiten und eine Niederlassung in der EU haben, bzw. alle Unternehmen ohne EU-Sitz, die ihre Produkte und Dienstleistungen EU-Bürgern anbieten – also so gut wie jeden kleinen oder mittleren Betrieb in Deutschland. Denn egal ob Kundendaten wie Kontonummer und Adresse oder Informationen aus einer Personalakte: Personenbezogene Daten fallen fast überall an. Im Rahmen der Regelung ergeben sich neue Pflichten im Umgang mit diesen personenbezogenen Daten. Mit der vollständigen Umsetzung der Vorschriften profitieren Unternehmen jedoch von umfassender Rechtssicherheit und können ihren Kunden guten Gewissens eine sichere Datenverarbeitung versprechen.

Viele Betriebe sind unsicher, was die DSGVO für ihre betrieblichen Prozesse bedeutet. „Da die Umsetzung der Vorgaben erfahrungsgemäß Zeit in Anspruch nimmt, sollten sich Unternehmer sehr zeitnah mit der DSGVO auseinandersetzen“, erklärt Dr. Hans Markus Wulf, der als Fachanwalt für IT-Recht und Partner der Sozietät SKW Schwarz das Mittelstand 4.0-Kompetenzzentrum Hamburg bei rechtlichen Aspekten der Digitalisierung berät. Insbesondere müssen Unternehmen vier Bereiche betrachten: die Datenverarbeitung, die Auftragsdatenverarbeitung, organisatorische Maßnahmen mit Blick auf Dokumentations- und Informationsprozesse sowie technische Maßnahmen. Alle Neuregelungen dienen dazu, dass personenbezogene Daten im EU-Raum einheitlich geschützt und sicher verarbeitet werden.

Transparente Interessenabwägung

Im Bereich der Datenverarbeitung gilt weiterhin die Grundregel, dass personenbezogene Daten nur mit Erlaubnis des Betreffenden verarbeitet werden dürfen. „Bereits vorhandene, heute rechtskonforme Einwilligungen bleiben zwar zunächst gültig. Doch in Zukunft müssen Unternehmen ihre Kunden ausführlicher über die geplante Verwendung der Daten informieren. Daher sollten alle Einwilligungsvorlagen überarbeitet werden“, rät Rechtsanwalt Wulf. Wenn keine Einwilligung vorliegt, können personenbezogene Daten nur ausnahmsweise verarbeitet werden, etwa wenn sie für die Vertragserfüllung erforderlich sind oder überwiegende, „berechtigte Interessen“ des Unternehmens vorliegen. Diese Interessenabwägung müssen Betriebe künftig genau dokumentieren.

Dienstleister unter die Lupe nehmen

Hinsichtlich der Auftragsverarbeitung müssen Betriebe genau hinschauen, wenn sie beispielsweise Cloud-Dienste nutzen oder externe IT-Dienstleister in Anspruch nehmen, die auf interne personenbezogene Daten zugreifen können. „Dieser Punkt gehört ganz oben auf die Prioritätenliste. Auftragsdatenverarbeitung bedeutet nicht mehr nur, dass Daten nach außen gesendet werden. Auch der passive Datenzugriff von außen (z. B. der Wartungszugriff von IT-Dienstleistern) muss richtig geregelt werden“, so der Fachanwalt. Die Unternehmen sind verpflichtet, jeden Auftragsverarbeiter zu prüfen, ob dieser – insbesondere aus technischer Sicht – ausreichenden Datenschutz sicherstellen kann.

Prozesse und Technik prüfen

Organisatorisch kommen auf Unternehmen durch die DSGVO umfangreiche Dokumentations- und Informationspflichten zu. Alle Geschäftsprozesse rund um die Datenverarbeitung müssen dokumentiert werden und Dateninhaber detailliert und verständlich über die Verwendung ihrer Angaben aufgeklärt werden. Zudem gilt mit der neuen Regelung auch bei einfachen Datenpannen grundsätzlich eine Meldepflicht: Soweit nicht Risiken für die Betroffenen ausgeschlossen werden können, muss das betroffene Unternehmen die zuständige Aufsichtsbehörde innerhalb von 72 Stunden informieren. „Damit im Ernstfall jeder Mitarbeiter weiß, was bei einer Datenpanne zu tun ist, ist eine Richtlinie oder Arbeitsanweisung dazu sehr sinnvoll“, erläutert Wulf.

Auch bei Mittelstand-Digital spielt die DSGVO eine gewichtige Rolle: Auf der Mittelstand 4.0-Regionalkonferenz in Chemnitz im März 2018 macht auch die gemeinsam vom Bundesministerium für Wirtschaft und Energie und dem Deutschen Industrie- und Handelskammertag organisierte „Road Show“ zum Thema DSGVO Halt. Die Roadshow wird auch bei weiteren Mittelstand 4.0-Kompetenzzentren zu Gast sein. Unternehmer können sich dort praxisnah über die Verordnung informieren.

Ausführliche Informationen zur DSGVO finden sich auch in einer Publikation der Bundesbeauftragten für den Datenschutz und die Informationssicherheit.

Ungebetene Gäste

Die Sage des Trojanischen Pferdes, mit dem sich griechische Soldaten unentdeckt Zugang nach Troja verschafften und anschließend großen Schaden anrichteten, ist Namensgeber für tückische Schadprogramme, die sich in Unternehmen schleusen. Christopher Tebbe vom Mittelstand 4.0-Kompetenzzentrum Hannover erklärt, wie sich Betriebe vor Angriffen schützen können.

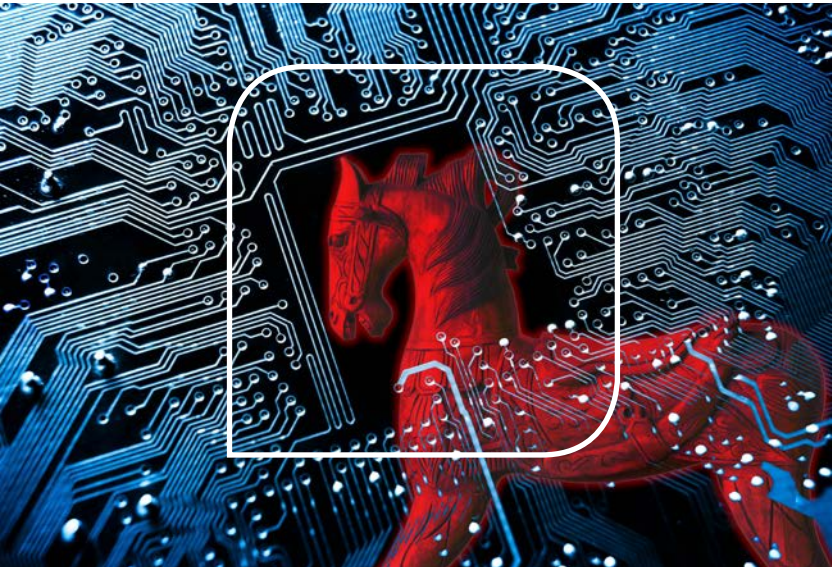
Eben noch die vermeintlich freundliche Bewerbungsmail eines kompetenten Universitäts-Absolventen angeklickt und den angehängten vermeintlichen Lebenslauf geöffnet – Minuten später wird der Computerbildschirm schwarz und ein Text klärt darüber auf, dass der Computer mit Schadsoftware infiziert und alle Dateien verschlüsselt wurden. Wenn nicht schnell ein bestimmter Geldbetrag in Bitcoins bezahlt wird, bleibt der Zugriff auf alle Daten verwehrt. Wie in diesem Beispiel einer gefälschten Bewerbung an eine Rechtsanwaltskanzlei ergeht es vielen Unternehmen, die von einem Trojaner attackiert werden und mit der Verschlüsselung ihrer Daten erpresst werden. Dass nur große Unternehmen im Fokus von Kriminellen stehen, ist ein Irrglaube: Auch kleine und mittlere Unternehmen, vor allem sogenannte „Hidden Champions“, also potenziell wenig bekannte Weltmarktführer, sind vielversprechende Ziele für Angreifer.

Unbemerkt einschleusen

Als Trojaner werden Programme bezeichnet, die gezielt auf Hardware wie Computer oder mobile Endgeräte eingeschleust werden, um dort (teilweise) ferngesteuert schädliche Funktionen auszuführen. Sie sind dabei als regulärer Inhalt, zum Beispiel als PDF-Anhang oder Software-Update, getarnt. Seit einigen Jahren sind vor allem Verschlüsselungstrojaner auf dem Vormarsch: Sind sie erfolgreich eingeschleust worden, übernehmen sie die Kontrolle und verschlüsseln alle oder gezielt besonders wertvolle Datensätze. Gefälschte E-Mails, etwa als Bewerbung oder Rechnung getarnt, sind beliebte Einfallstore. Aber auch manipulierte Websites oder Datenträger wie USB-Sticks, die Kriminelle auf einem Firmenparkplatz vermeintlich verlieren, können Schadsoftware enthalten, die sich ausbreitet, sobald das Trägermedium an einen Rechner angeschlossen ist. Aber auch private USB-Sticks von Mitarbeitern können Schadsoftware übertragen.

Sind die Computer über Netzwerke mit weiteren Rechnern verbunden, breitet sich die Schadsoftware mitunter minutenschnell im ganzen Betrieb aus. Je nachdem, wie schnell der Schädling erkannt wird, entsteht für kleine und mittlere Betriebe dadurch leicht ein Schaden in fünfstelliger Höhe[1]. Maßgeblich ist vor allem, auf welche Informationen der Trojaner zugreifen und sie verschlüsseln kann. Das betrifft nicht nur Dokumente oder Datenbanken, auch ganze Produktionsnetzwerke können durch eine Verschlüsselung der Steuerungsrechner lahmgelegt werden: Das Schadprogramm WannaCry,

1 Kaspersky Lab 2017



das im Frühjahr 2017 Rechner mit Windows-Betriebssystemen mit einer bestimmten Schwachstelle attackierte und Benutzerdateien verschlüsselte, sorgte zum Beispiel dafür, dass beim Automobilhersteller Honda ein Werk einen ganzen Tag geschlossen blieb.[2]

Wachsamkeit und Datensicherung

Viele Betriebe erhalten täglich zig Mails mit gefälschten Links und Dateianhängen. Eine Sensibilisierung aller Mitarbeiter für die Gefahren durch Trojaner ist daher unabdingbar. Auch wenn viele schädliche Mails relativ leicht zu erkennen sind, ist dies bei gezielten Angriffen ungleich schwerer. Neben der Schulung der Mitarbeiter sollte auch kritisch geprüft werden, ob alle Rechner eines Betriebs ungehindert miteinander kommunizieren müssen, so dass sich im Ernstfall eine Schadsoftware relativ ungebremst auf allen Rechnern ausbreiten kann. Updates müssen regelmäßig möglichst zeitnah durchgeführt werden, damit bekannt gewordene Sicherheitslücken, wie bei WannaCry, sofort geschlossen werden. Bei industriellen Anlagen kann dies für viele Komponenten eine Freigabe durch den Hersteller voraussetzen.

Besonders wichtig ist die zuverlässige und manipulationssichere Datensicherung. Eine Datensicherung über das Netzwerk sollte nicht im laufenden Betrieb erfolgen bzw. Benutzer keine Schreibrechte auf die Netzwerkdatensicherung haben – manche Trojaner sind nämlich genau dafür ausgerichtet und schlagen dann bei der Erstellung des Backups im Netzwerk zu. Eine Alternative ist die Datensicherung auf einem externen Datenträger, so dass im Falle eines Angriffs auf diese Kopie zurückgegriffen werden kann. Doch auch hier können Trojaner versuchen, genau diese USB-Festplatte zu verschlüsseln. Deshalb sollten zwei oder mehr Speichermedien im Wechsel genutzt werden.

Wenn Unternehmen angegriffen werden, sollten sie sofort den eigenen IT-Experten oder einen externen Sachverständigen zu Rate ziehen und den infizierten Rechner vom Netzwerk trennen. Ist die Gefahr eingedämmt, muss das gesamte Betriebssystem neu eingespielt werden und der Vorfall der Polizei gemeldet werden – auch wenn es für den eigenen Betrieb dank Datensicherung glimpflich ausgeht.

2 Reuters Staff 2017

Notizen

Notizen

www.bmwi.de