Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

Sicherer Datenaustausch

Themenheft Mittelstand-Digital

bmwi.de

Impressum

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

Stand
April 2021

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG, 60386 Frankfurt

Gestaltung
PRpetuum GmbH, 80801 München

Bildnachweis
AdobeStock
NicoElNino / Titel
pressmaster / S. 13

DsiN / S. 29
Mittelstand 4.0-Kompetenzzentrum Siegen / S. 15
SICP | Universität Paderborn / S. 36

Zentraler Bestellservice für Publikationen der Bundesregierung:
E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Editorial

Liebe Leserinnen und Leser,

seit Monaten kommunizieren Menschen weltweit mehr denn je digital, teilen Geschäftsunterlagen über E-Mail oder Video-Calls und arbeiten online gemeinsam an Projekten. Der Austausch vertraulicher Daten in Unternehmen und mit anderen Firmen stellt eine nicht zu unterschätzende Herausforderung dar. Dabei ist es besonders wichtig, neben dem in der Krise oftmals nötigen Pragmatismus die Datensicherheit nicht aus den Augen zu verlieren. Denn der Dauerzustand Homeoffice wirft auch für Unternehmen mit guter digitaler Infrastruktur neue Fragen der Datensicherheit auf. Damit die digitale Transformation des deutschen Mittelstands auf sicheren Beinen steht, müssen sich Unternehmerinnen und Unternehmer mit der Datensicherheit im eigenen Betrieb befassen. Denn das Thema ist wichtiger denn je:

Mehr digitale Prozesse bedeuten leider auch Sicherheitsrisiken. Umso wichtiger ist es, durch einen sicheren Austausch von sensiblen Geschäftsdaten die Einfallstore etwa für Hacking-Angriffe zu verringern. Schon kleine Maßnahmen, wie die konsequente Verschlüsselung von E-Mails oder die Datenübertragung mit einer Datenschleuse, können hier den Unterschied machen. Gestaltet sich der Datenaustausch aufgrund einer Vielzahl an beteiligten Parteien komplexer, eignet sich etwa die Blockchain-Technologie.

Neben der Einführung technischer Sicherheitsmaßnahmen ist die Sensibilisierung der eigenen Mitarbeiterinnen und Mitarbeiter elementar, um den sicheren Datenaustausch zu gewährleisten. Dazu gehört auch die Frage nach den Verantwortlichkeiten, die sich alle Unternehmen – egal welcher Größe – stellen sollten.

In diesem Heft finden Sie Anregungen, Informationen und ermutigende Beispiele, wie kleine und mittlere Unternehmen oft schon mit wenigen Maßnahmen für mehr Datensicherheit sorgen können.

Mit Mittelstand-Digital stärkt das Bundesministerium für Wirtschaft und Energie kleine und mittlere Unternehmen dabei, die digitale Zukunft in Angriff zu nehmen, nachhaltige Konzepte und sichere Lösungen zu entwickeln und die damit einhergehenden Chancen für sich zu nutzen.
Die regionalen und thematischen Mittelstand 4.0-Kompetenzzentren unterstützen mittelständische Unternehmen dabei, die richtigen Maßnahmen zu identifizieren, damit der Datenaustausch sicher gelingt.

Wo es welche Angebote gibt, finden Sie ab Seite 24.
Wir wünschen Ihnen eine spannende Lektüre!

Bleiben Sie gesund,
Ihr Bundesministerium für Wirtschaft und Energie

Ohne sicheren Datenaustausch keine erfolgreiche Digitalisierung

Erhebliche Datenmengen werden durch die Digitalisierung bei Unternehmen generiert, gespeichert und zur Analyse sowie Optimierung bestehender Prozesse genutzt. Das volle wirtschaftliche Potenzial der Daten wird aber erst dann ausgeschöpft, wenn diese zwischen verschiedenen Endgeräten, Mitarbeitenden, Firmen und Behörden sicher ausgetauscht werden können. Heute ist eine Welt ohne E-Mails, Cloud-Speicher, Videokonferenzen oder den Transfer elektronischer Dokumente und Rechnungen nur schwer vorstellbar. Die Menge an ausgetauschten, häufig hochsensiblen Daten steigt exponentiell.[1] Die Gewährleistung eines sicheren Datenaustauschs intern, zwischen Standorten und mit anderen Unternehmen ist demnach eine Voraussetzung für die erfolgreiche Digitalisierung.

Sicherheitslücken frühzeitig erkennen und schließen

In dieser vernetzten Welt stellt die Sicherheit beim Datenaustausch eine der größten Herausforderungen für Unternehmen dar. Jedoch trifft etwa die Hälfte der deutschen Unternehmen keine Sicherheitsvorkehrungen für den Versand von Nachrichten (48 Prozent) und nur 22 Prozent der Unternehmen achten auf verschlüsselte E-Mails. Nur 19 Prozent verwenden einen Passwortschutz für die Übertragung von Daten.[2]

Mit dem Beginn der Corona-Pandemie und der damit verbundenen Verlagerung der Arbeit ins Homeoffice rückt auch für viele kleine und mittlere Unternehmen das Thema sicherer Datenaustausch in den Fokus. IT-Sicherheit ist nun nicht nur im Büro, sondern auch im privaten Arbeitszimmer und am Küchentisch der Mitarbeiterinnen und Mitarbeiter erforderlich. Dabei können die veränderten Arbeitsmethoden und Prozesse zu Unklarheiten im sicheren Umgang mit Unternehmensdaten,

1 Siehe u. a. Bundesnetzagentur, Jahresbericht 2019, S. 52 und S. 59

2 DsiN-Praxisreport Mittelstand 2020, S. 27

mangelnden Abstimmungen und Intransparenz führen. Zudem haben Cyberkriminelle die Corona-Pandemie als Chance für sich entdeckt: Laut einer Umfrage des Antiviren-Spezialisten Bitdefender bestätigen 80 Prozent der über 500 befragten IT-Sicherheitsfachleuten aus Deutschland, dass in der Krise die Attacken durch Trojaner oder Phishing zugenommen haben.[3]

Obwohl die Gefahr mit zunehmender Digitalisierung der Geschäftsprozesse steigt, reagiert noch immer über ein Drittel der Unternehmen (35 Prozent) erst im Falle eines Angriffs mit der Definition und Umsetzung geeigneter Schutzmaßnahmen. Immerhin geben 43 Prozent der befragten Unternehmen ihren Mitarbeiterinnen und Mitarbeitern präventiv konkrete Handlungsanweisungen, zehn Prozent trainieren ihre Angestellten regelmäßig für den Ernstfall und zwölf Prozent der Unternehmen verfügen über spezielle Notfallpläne, die sie kontinuierlich überprüfen.[4]

Ein sicherer Datenaustausch ist für jedes Unternehmen möglich

Mit den richtigen Maßnahmen können Unternehmen jeder Größe einen sicheren Datenaustausch gewährleisten. Wichtig ist dabei, dass Verantwortliche nicht nur die technischen, sondern auch die organisatorischen Maßnahmen im Blick haben.

Durch die Verlagerung der nahezu gesamten privaten und geschäftlichen Kommunikation in den digitalen Raum gewinnen zahlreiche Fragen rund um die IT-Sicherheit in Unternehmen an Gewicht: Wie können IT-Sicherheitsanalysen durchgeführt werden und was muss dabei beachtet werden? Wie können Daten zwischen Unternehmen sicher ausgetauscht werden? Können dabei neue Technologien wie Blockchain helfen? Wie werden Mails sicher verschlüsselt?

Kleine und mittlere Unternehmen in Deutschland stehen bei diesen Fragestellungen nicht allein da: Die vom Bundesministerium für Wirtschaft und Energie geförderten Mittelstand 4.0-Kompetenzzentren und die Transferstelle IT-Sicherheit im Mittelstand unterstützen bei allen Fragen rund um die Digitalisierung und das Thema IT-Sicherheit. So gelingt auch in mitunter turbulenten Zeiten eine sichere Kommunikation.

3 https://veranstaltungen.handelsblatt.com/cybersecurity/angriff-auf-das-homeoffice-kmu-im-fokus, abgerufen am 04.02.2021

4 DsiN-Praxisreport Mittelstand 2020, S. 29

ZAHLEN UND FAKTEN

64 PROZENT der kleinen KMU finden **IT-Sicherheit** sehr wichtig.

83 PROZENT der großen KMU finden **IT-Sicherheit** sehr wichtig.

56 PROZENT der mittelständischen Unternehmen schätzen Bedeutung von **Cybersicherheit** aktuell als (sehr) hoch ein.

54 PROZENT der deutschen Entscheiderinnen und Entscheider sehen im **Datenschutz** eine große Herausforderung.

DATENSICHERHEIT: zentrale Herausforderung für KMU

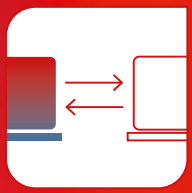
61 PROZENT der mittelständischen Unternehmen sehen fehlendes **Sicherheitsbewusstsein** der Mitarbeitenden als größte Herausforderung bei der Abwehr von Cyberrisiken.

FAKTOR MENSCH: Sensibilisierung ist elementar

16 PROZENT der KMU bieten ein verpflichtendes **Sicherheitsschulungsprogramm** an.

In **50** PROZENT der Betriebe unter 10 Mitarbeitenden kümmert sich die Geschäftsleitung selbst um **IT-Fragen**.

Quellen: WIK (2017) – „Aktuelle Lage der IT-Sicherheit in KMU“/Deloitte Private (2020) – „Cyber Security im Mittelstand“/Cisco (2020) – „Future of Secure Remote Work“/ DsiN-Praxisreport 2020 „Mittelstand@IT-Sicherheit“



DATENAUSTAUSCH:
sichere
Übertragungswege

64 PROZENT

der deutschen Entscheiderinnen und Entscheider sehen den sicheren **Fernzugriff** auf Unternehmensdaten als größte Herausforderung an.

11 PROZENT

der KMU versenden ihre Daten ausschließlich über **Austauschplattformen**.

19 PROZENT

der KMU schützen übertragene Daten mit einem **Passwort**.

48 PROZENT

der KMU sichern übertragene **Daten in Anhängen** nicht ab.

56 PROZENT

der Arbeitnehmenden verzichten auf eine **Verschlüsselung** ihrer **E-Mails**.

82 PROZENT

der Unternehmen sehen ein (sehr) großes Potenzial in **Blockchain** zum Datenaustausch.

22 PROZENT

der KMU verschlüsseln **E-Mails** mit **Anhängen** oder nutzen eine **elektronische Signatur**.

Quellen: Cisco (2020) – „Future of Secure Remote Work“/DsiN-Praxisreport 2020 „Mittelstand@IT-Sicherheit“/REDDOXX „Studie E-Mail 2020. Status der E-Mail in Deutschland“/bitkom (2019) „Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen“

Sichere Kommunikation dank umfassender Verschlüsselung

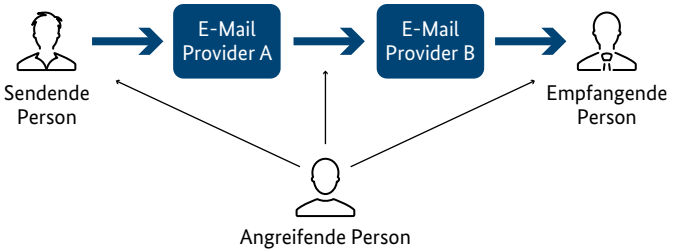
E-Mails sind oft das Mittel der Wahl, wenn es um Geschäftskommunikation geht. Sind die Nachrichten nicht umfassend geschützt, entstehen Sicherheitsrisiken. Das Mittelstand 4.0-Kompetenzzentrum Magdeburg gibt Tipps, wie E-Mail-Kommunikation sicher gelingt.

Neben dem Telefon sind E-Mails der am häufigsten genutzte Kommunikationskanal zwischen Unternehmen, ihren Geschäftspartnern und Kunden. Aus einer Studie des Bitkom geht hervor, dass drei von zehn Berufstätigen bereits 2018 mehr als 30 dienstliche E-Mails pro Tag erhielten.

Vor allem geschäftliche E-Mails enthalten oft eine Vielzahl sensibler und schützenswerter Informationen. Dabei müssen gesetzliche Datenschutzvorgaben erfüllt werden. Damit E-Mails nicht zum Einfallstor für Viren oder andere Malware und damit zum Sicherheitsrisiko werden, muss die Kommunikation via E-Mail geschützt werden. Mit einfachen Mitteln kann festgestellt werden, welche Verschlüsselungsmöglichkeiten bereits genutzt werden und wo noch Nachholbedarf besteht.

Der Weg einer E-Mail

„Um E-Mails zu schützen, gibt es vor allem zwei Wege der Verschlüsselung: Die Transportverschlüsselung und die Inhaltsverschlüsselung“, erklärt Sebastian Nielebock, Experte für den Bereich Safety & Security beim Mittelstand 4.0-Kompetenzzentrum Magdeburg. Um zu verstehen, wo beide Verschlüsselungsvarianten ansetzen, ist es wichtig, den Weg einer E-Mail vom Sender zum Empfänger nachzuvollziehen.



Der Weg einer unverschlüsselten E-Mail

Nach dem Klick auf den „Senden“-Button prüft das Mailprogramm (E-Mail-Client) des Absenders im Hintergrund verschiedene Parameter und leitet sie an den Mailserver des eigenen E-Mail-Providers weiter. Dieser Mailserver ist ein Programm für Empfang, Speicherung, Verarbeitung und Weiterleitung von E-Mails. Der Mailserver überprüft im nächsten Schritt, ob die Zieladresse korrekt ist, die Größe der Mail den Richtlinien entspricht und ob Spam, Viren oder sonstige Malware enthalten sind. Ist dies nicht der Fall, speichert der eigene Mailserver die Mail und sucht den Mailserver des Empfangenden. Ist dieser gefunden, wird die Mail in mehrere kleine Datenpakete unterteilt und Stück für Stück an den Mailserver der Zieladresse weitergeleitet. Dieser Mailserver prüft nun seinerseits die Mail auf Größe, Spam und Viren. Zeigt die Nachricht keine besonderen Auffälligkeiten, speichert der Mailserver des Empfangenden die Mail. Ist die Mail nun verfügbar, wird die Empfängerin oder der Empfänger benachrichtigt und die Mail in das Mailprogramm heruntergeladen.

Das Problem: Wenn die E-Mail nicht verschlüsselt ist, haben potenzielle Angreiferinnen oder Angreifer an unterschiedlichen Punkten die Möglichkeit, auf die Daten der E-Mail zuzugreifen, sie zu lesen, zu verändern oder ganz zu löschen. Deshalb wird in der Regel auf zwei Arten der Verschlüsselung von E-Mail-Kommunikation zurückgegriffen.

Unterwegs geschützt: Die Transportverschlüsselung

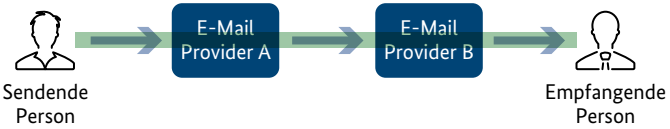
Bei der Transportverschlüsselung werden die in der E-Mail übertragenen Daten auf den einzelnen Übermittlungsabschnitten, also der Kommunikation des E-Mail-Clients mit dem Server oder beim Austausch zwischen den verschiedenen Servern, verschlüsselt. Damit sind sie für Dritte nicht einsehbar.

Die Transportverschlüsselung

„Die meisten E-Mail-Provider bieten die Transportverschlüsselung kostenlos an, meist ist sie sogar automatisch integriert“, sagt Nielebock. Ob E-Mail-Programme diese Verschlüsselung bereits nutzen, erkennt man daran, dass als Verbindungssicherheit TLS (für Transport Layer Security) oder SSL (für Secure Sockets Layer) eingestellt ist.

Alle Inhalte, immer geschützt: Die Inhaltsverschlüsselung

Die Transportverschlüsselung ist bereits ein erster, wichtiger Schritt beim sicheren Datenaustausch. Da die Daten bei dieser Art der Verschlüsselung allerdings auf den jeweiligen Servern von Sendenden und Empfangenden weiterhin unverschlüsselt vorliegen, sollte zusätzlich ein weiteres Verschlüsselungsverfahren eingesetzt werden: die Inhaltsverschlüsselung.



Die Inhaltsverschlüsselung

Bei der Inhaltsverschlüsselung, oft auch als Ende-zu-Ende-Verschlüsselung bezeichnet, werden die Inhalte der Nachricht bereits beim Sendenden umfassend verschlüsselt und erst durch das Programm des Empfangenden wieder in Klartext übersetzt. Damit ist der Zugriff von unbefugten Dritten nahezu unmöglich. Gängige Verfahren der Inhaltsverschlüsselung sind PGP (Pretty Good Privacy) und S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME wird, im Gegensatz zu PGP, von nahezu allen E-Mail-Programmen und auch auf Smartphones standardmäßig unterstützt.

Echtheit bestätigen durch digitale Signatur

Eine weitere Möglichkeit, sowohl den Inhalt einer Mail vor Manipulation zu schützen als auch ihrer Absenderin oder ihren Absender zu verifizieren, ist das Verfahren der digitalen Signatur. Dadurch können beispielsweise digital nicht-signierte Phishingmails, bei denen Betrügende im Namen von Unternehmen E-Mails versenden, um an Zahlungsinformationen oder andere sensible Daten der Empfängerinnen und Empfänger zu gelangen, von Userinnen und Usern besser als Betrug identifiziert werden.

Aus technischer Sicht basiert die elektronische Signatur von E-Mails auf dem Prinzip der asymmetrischen Verschlüsselung. Der digitale Absendende besitzt dabei sowohl einen privaten als auch einen öffentlichen Schlüssel. Beim Versand einer Mail erzeugt das Mailprogramm des Absendenden automatisch eine so genannte Prüfsumme des Mailinhaltes. Diese Prüfsumme wird mit dem privaten Schlüssel verschlüsselt und automatisch an die Mail angehängt.

Der oder die digitale Empfangende ist im Besitz eines öffentlichen Schlüssels (entweder weil dieser vom Absendenden mitgesandt wurde oder weil er oder sie den Schlüssel aus einem öffentlichen Verzeichnis bezieht). Mithilfe dieses Schlüssels wird die Prüfsumme der erhaltenen Mail entschlüsselt und anschließend erneut berechnet. Stimmen die Ergebnisse überein, ist sicher, dass die Mail echt ist und nicht manipuliert wurde.

Umfassender Schutz braucht verschiedene Werkzeuge

Um sensible Daten umfassend zu schützen, gibt es viele unterschiedliche Werkzeuge. Hier lohnt sich eine Prüfung, welche Tools bereits eingesetzt werden und wo noch Nachholbedarf besteht. Klar ist aber, dass zum optimalen Schutz auch der eigene Umgang mit E-Mails hinterfragt werden sollte.

Bereits vermeintlich einfache Handgriffe wie die Wahl eines starken und komplexen Passwortes für den Zugriff auf das E-Mail-Konto oder die Wahrung des Datenschutzes bei ausgedruckten Mails machen einen bedeutsamen Unterschied.

Ob und welche dieser Verschlüsselungsarten bereits vom beauftragten E-Mail-Provider eingesetzt werden, können KMU durch einen Blick in die Einstellungen ihres E-Mail-Kontos herausfinden. Bei Unsicherheiten kann auch eine direkte Nachfrage beim gewählten IT-Dienstleister weiterhelfen.

Das Mittelstand 4.0-Kompetenzzentrum Magdeburg unterstützt gerne bei weiteren Fragen zum Thema E-Mail-Verschlüsselung.

Kontaktinformationen zum Zentrum
Magdeburg

Mittelstand 4.0
Kompetenzzentrum
Magdeburg

Kooperation ohne Schwachstellen

Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft entwickelt Werkzeuge zur Selbstbefähigung und zur Erhöhung der Security Awareness.

Für eine sichere und vertrauensvolle Zusammenarbeit zwischen IT-Unternehmen braucht es klare Regeln und passende Werkzeuge. Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft zeigt, welche Schwachstellen es gibt, und hilft bei Lösungen.

IT-Sicherheit im Allgemeinen und der sichere Austausch von Daten im Besonderen sollten als ein wichtiger Grundpfeiler für eine erfolgreiche Unternehmensführung verstanden werden, um Unternehmenswerte zu schützen. Werden keine umfassenden Sicherheitsmaßnahmen ergriffen, geraten Unternehmen schnell in Schwierigkeiten. Deshalb lohnt es sich, genau hinzuschauen und gegebenenfalls Fachleute zur Unterstützung hinzuzuziehen – so wie das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft. Für das Kompetenzzentrum sind der sichere Austausch und die Arbeit mit Daten über Unternehmensgrenzen hinweg eines der Kernthemen seiner Arbeit: Es unterstützt kleine und mittlere IT-Unternehmen bei der Bildung von Projektkonsortien, die übergreifende IT-Lösungen für andere mittelständische Unternehmen entwickeln.

Klare Konzepte von Anfang an

„Sicherer Datenaustausch fängt mit rechtlichen und organisatorischen Regelungen und einer Einigung auf einheitliche Sicherheitsstandards aller beteiligten Akteure an. Das ist für die gute Zusammenarbeit unverzichtbar“, sagt Prof. Dr. Andreas Johannsen vom Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft, der Experte für das Thema IT-Schnittstellen und Datensicherheit ist.

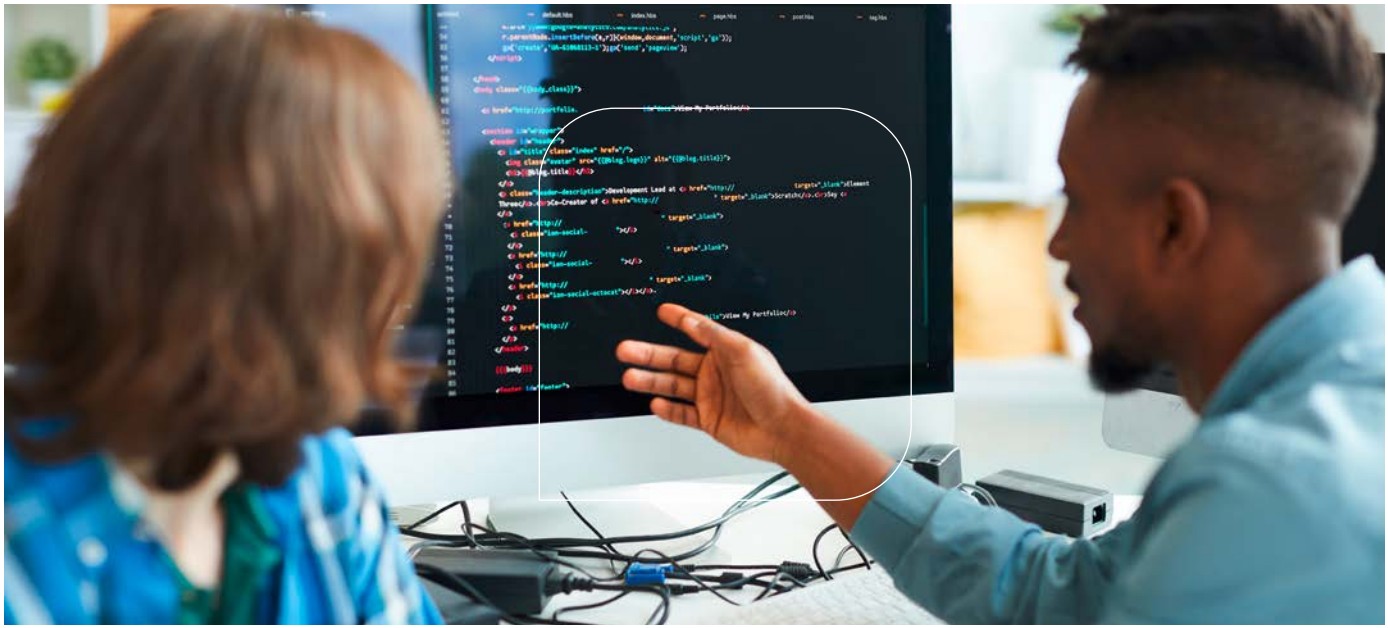
Bei der Bildung der Konsortien zwischen den mittelständischen Unternehmen kennen sich die Akteure untereinander oft noch nicht – sie müssen aber direkt viele Daten miteinander teilen. Deshalb sollte zu Beginn einer solchen Kooperation eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement) sowie eine Informationssicherheitsrichtlinie geschlossen werden. Sie sichert den Partnerinnen und Partnern zu, dass alle Informationen, die im

weiteren Verlauf der Zusammenarbeit ausgetauscht werden, vertraulich behandelt und damit nicht offengelegt werden. Ist die Basis der Zusammenarbeit geklärt, geht es darum, den gegenseitigen Austausch von Daten im gemeinsamen Projekt voranzubringen.

API, E-Mail, USB-Sticks: Schwachstellen beim Thema Datenaustausch

Das Teilen der Daten innerhalb von Projektkonsortien erfolgt oft auf unterschiedlichen Wegen, die jeweils zur Schwachstelle werden können. Dazu gehören E-Mails, externe Speichermedien wie USB-Sticks oder Festplatten. Bei Mails sind mehrere Verschlüsselungsmöglichkeiten zum Schutz der Datenübertragung (wie auf Seite 8/9) möglich, und auch das Problem extern eingeschleppter Malware lässt sich vergleichsweise leicht über so genannte Datenschleusen lösen. Nähere Informationen zur Datenschleuse finden Sie ab Seite 21.

Eine der gängigsten Varianten des Datenaustausches, vor allem bei Unternehmen der IT-Wirtschaft,



Zur vertrauensvollen Zusammenarbeit zwischen IT-Unternehmen gehört auch der sichere Datenaustausch über Unternehmensgrenzen hinweg.

ist die Datenübertragung via Programmierschnittstellen (application programming interface, kurz: API). Über diese Schnittstellen können Daten abgerufen und Prozesse automatisiert initiiert werden. Die Systeme tauschen sich also selbstständig miteinander aus und benötigen nicht für jeden Austausch eine Person, die den Befehl zum Austausch gibt.

Ein alltäglicher Bestellprozess in einem Onlineshop kann hier als Beispiel dienen: Eine Nutzerin oder ein Nutzer bestellt über die Weboberfläche eines Onlineshops ein Produkt. Das System des Onlineshops kann via Schnittstellen automatisiert bei anderen Systemen notwendige Informationen einholen oder Aktionen initiieren. Das kann beispielsweise die Bonitätsprüfung der bestellenden Person sein oder die Zahlungsabwicklung über einen Drittanbieter. Auch die Beauftragung einer Spedition ist darüber möglich. All diese Prozesse laufen dank API automatisiert und in Sekunden ab.

Damit erleichtern sie den Arbeitsalltag enorm, können aber schnell zum Einfallstor für Hacker werden. Um bei dieser Art der Datenübertragung optimalen Schutz zu gewährleisten, hat das Kompetenzzentrum IT-Wirtschaft einen offenen Schnittstellenkatalog entwickelt.

Bereit zur Kooperation? Tools und Checklisten

Um zu prüfen, wie es um das eigene IT-Sicherheitskonzept bestellt ist, wie die Zusammenarbeit aussehen könnte und auf welchem Wege Daten am sichersten untereinander ausgetauscht werden können, hat das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft zahlreiche digitale Tools wie den Schnittstellenkatalog und Vorlagen aus dem Bereich Recht und Datenschutz für die Zusammenarbeit von Konsortien entwickelt und stellt sie auf seiner Website itwirtschaft.de bereit. Zudem steht Interessierten die App IT2match als Basistool des Kooperationsaufbaus zur Verfügung.

Kontaktinformationen zum Zentrum
IT-Wirtschaft

Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

Kleine Schritte für mehr Sicherheit

Viele Unternehmen realisieren zu spät, dass ihre Daten schlecht geschützt sind. Dabei sorgen oft bereits kleine Maßnahmen für bedeutend mehr Sicherheit. Das Mittelstand 4.0-Kompetenzzentrum Siegen hat der Theodor Stephan KG gezeigt, wie es geht.

Ein Klick auf den Dateianhang einer verdächtigen E-Mail kann bereits ausreichen, um in eine Cyber-Falle zu tappen, die ein Firmennetzwerk lahmlegt – und damit manchmal sogar den gesamten Betrieb. Eine ganze Reihe deutscher Unternehmerinnen und Unternehmer musste diese Erfahrung bereits machen, wie der DsiN-Praxisreport Mittelstand 2020 zeigt: Fast die Hälfte aller Unternehmen in Deutschland hat bereits einen Hackerangriff erlebt. In drei von vier Fällen führten die Angriffe zu schädlichen Auswirkungen und in vier Prozent der Fälle sogar zu schweren Belastungen innerhalb der Betriebe, etwa hohem finanziellen Mehraufwand, über mehrere Wochen lahmgelegten Systemen oder Imageschädigungen. Solche Gefahrenszenarien haben auch Arndt Nikolaus Loh zum Handeln bewegt. Der Geschäftsführer der Theodor Stephan KG GmbH & Co. KG Ton- und Kaolinbergbau in Burbach kennt Fälle von zwei Betrieben, die durch Cyberattacken 14 Tage arbeitsunfähig gemacht wurden. Um seinem Betrieb ein ähnliches Schicksal zu ersparen und die Sicherheit der Betriebsdaten generell zu verbessern, hat er sich an das Mittelstand 4.0-Kompetenzzentrum Siegen gewandt.

Mit der Unterstützung von Nico Vitt, dem IT-Sicherheitsbeauftragten des Kompetenzzentrums, hat die Theodor Stephan KG eine IT-Analyse durchgeführt. „Wir haben uns genau angesehen, wie hier gearbeitet wird und wie die IT-Infrastruktur aussieht“, erklärt Vitt. Im Rahmen der IT-Sicherheitsanalyse wurde besprochen, wie groß der Schaden wäre, wenn etwas nicht mehr funktionieren würde. „Alle Teile, wo ein Ausfall besonders schwer wiegt,

IT-Sicherheitsanalyse bei der Theodor Stephan KG in Burbach

sollten zuerst angegangen werden“, rät der IT-Sicherheitsbeauftragte. Auf Basis des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik konnte er dem Unternehmen konkrete Empfehlungen geben. Dazu gehören auch wichtige Hinweise für einen sicheren Datenaustausch.

E-Mail-Postfächer stellen das größte Sicherheitsrisiko dar

E-Mails und andere digitale Kommunikationstools sind nach wie vor die größte Schwachstelle in den IT-Systemen vieler Firmen. Nur etwas mehr als die Hälfte der im Rahmen der DsiN-Studie[5] befragten Unternehmen treffen Sicherheitsvorkehrungen für den Versand von Nachrichten. Nur jedes fünfte Unternehmen achtet auf verschlüsselte E-Mails. Ein gefundenes Fressen für Cyber-Kriminelle, die so sensible Daten ausspähen oder Schadsoftware in die IT-Systeme einschleusen können. Dabei genügen schon einige Klicks im E-Mail-Programm, um eine handelsübliche Transportverschlüsselung zu erreichen. Auch hochwertigere Lösungen kosten in aller Regel wenig Aufwand. Um etwa die Verschlüsselungstechnologie S/MIME zu nutzen und damit Ende-zu-Ende-Verschlüsselung zu erzielen, benötigt man lediglich ein digitales Zertifikat, das wenige Euro im Jahr kostet. Auch den Versand von Dateien über E-Mail ganz zu vermeiden und stattdessen dezidierte Datenplattformen oder den hauseigenen Server zum Datenaustausch zu nutzen, kann sich sicherheitstechnisch lohnen. *(Lesen Sie hierzu auch den Artikel „Sichere Kommunikation dank umfassender Verschlüsselung“ zum Thema E-Mail-Kommunikation auf Seite 8/9.)*

Doch alle technischen Sicherheitsmaßnahmen nutzen wenig, wenn nicht auch die Mitarbeiterinnen und Mitarbeiter bzgl. eines sicheren Datenaustauschs geschult werden. Das weiß auch Nico Vitt, der mit dem Theodor-Stephan-Personal über den Umgang mit E-Mails, etwaige Sicherheitslücken und das richtige Vorgehen im Risikofall diskutierte. Ebenso ist zu beachten, dass Cyberkriminalität nicht die einzige Gefahr für Unternehmensdaten darstellt. IT-Systeme müssen auch gegen potenzielle Unfallszenarien geschützt werden. Vitt stellte etwa fest, dass der Serverraum der Firma in einem leicht zugänglichen Bereich auch äußeren Gefahren wie Wasser und Feuer ausgesetzt war. Alle Daten wären so im schlechtesten Fall auf einen Schlag vernichtet. Der Server sollte stattdessen an einem Ort frei von Gefahrenquellen platziert werden, zum Beispiel in einem höhergelegenen Raum, der zudem gut

5 DsiN-Praxisreport Mittelstand 2020, S. 27

gegen unbefugten Besuch gesichert ist – ein einfacher Ratschlag, der von Arndt Nikolaus Loh gleich umgesetzt wurde.

Im Notfall hilft ein Backup

Sollte es dennoch einmal zu schwerwiegenden technischen Problemen kommen, verfügt die Firma nun auf Anraten des Kompetenzzentrums über ein Back-up der Daten. Im Rahmen der Zusammenarbeit ist ein neues Konzept für die externe Datensicherung entstanden. Der Server wird nun jeden Tag ausgelesen. Die dabei befüllten externen Festplatten bleiben nicht im Firmengebäude. Eventuell verlorene Daten können so problemlos wiederhergestellt werden. „Selbst wenn uns jetzt nachts die Firma abbrennen würde – die Daten wären noch da. Das beruhigt uns sehr“, resümiert Loh. Vor allem hat er während der Zusammenarbeit mit dem Mittelstand 4.0-Kompetenzzentrum eines gelernt: Der Schutz der betriebsinternen Daten lässt sich auch Schritt für Schritt durch kleine Maßnahmen bedeutend verbessern.

Kontaktinformationen zum Zentrum

Siegen

Mittelstand 4.0
Kompetenzzentrum
Siegen

Geteilte Kapazitäten mit doppeltem Nutzen – aber sicher!

Digitale Zwillinge sind Grundlage für Gemeinschaftsproduktionen, bei denen Daten sicher in der Blockchain geteilt werden.

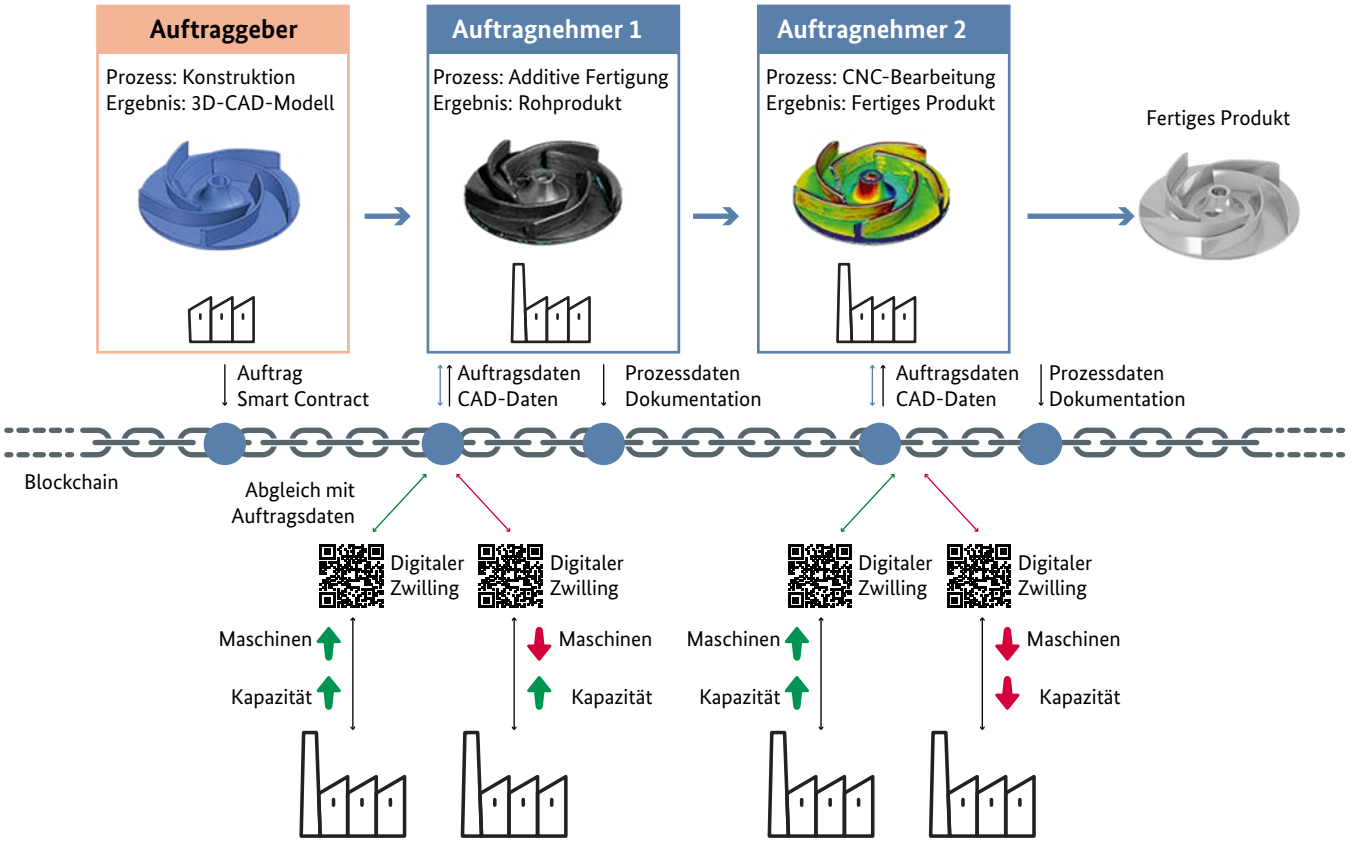
Nach dem Motto „Gemeinsam sind wir stark“ können sich Unternehmen zusammentun, um im Wettbewerb zu bestehen. Dafür müssen sie aber wissen, wer passende Maschinen mit freien Kapazitäten hat – und Daten sicher teilen können. Eine digitale Plattform kann vermitteln. Die Blockchain sorgt für die notwendige Datensicherheit. Wie das System funktioniert, hat das Mittelstand 4.0-Kompetenzzentrum Ilmenau durchgespielt.

„Sharing Economy“ ist das Stichwort, das vor allem für kleine und mittlere Unternehmen interessant sein kann. Sich mit der Konkurrenz zusammenzuschließen, ist aber mit Risiken verbunden. Denn wer gibt schon gern Betriebsgeheimnisse aus der Hand? Aber ohne Datenaustausch geht es nicht, und der soll noch dazu möglichst sicher sein. Hier kann die Integration einer Blockchain für Sicherheit sorgen. Das Mittelstand 4.0-Kompetenzzentrum in Ilmenau hat als Beispiel die additive Fertigung von Kleinserien mithilfe des so genannten Lichtbogendraht-Auftragschweißens durchgespielt: Auftragnehmer A fertigt ein Teil, bei dem ein Metalldraht mit einem Lichtbogen in einem 3D-Druck-Verfahren aufgeschmolzen wird – Schicht für Schicht. Dieser Rohling muss bearbeitet werden. Für Gewinde oder Bohrungen sind Maschinen notwendig, die Unternehmen A aber nicht besitzt. An dieser Stelle kommt Unternehmen B ins Spiel, das die Weiterverarbeitung übernehmen kann, weil es die passende Maschine hat und noch dazu die Kapazitäten.

„Ziel unseres Projektes war es, eine Art Marktplatz zu schaffen, auf dem Unternehmen und deren Maschinen als ‚Digitale Zwillinge‘ agieren“, erläutert Mathias Eiber vom Ilmenauer Kompetenzzentrum dieses Konzept der kooperativen Wertschöpfung. Jedes Unternehmen kann Teil dieses Netzwerks werden. Es muss sich nur eine „Digitale Identität“ zulegen. In diese digitale Visitenkarte stellt es seine Maschinen ein, die als so genannter „Digitaler Zwilling“ fungieren. Dieser Zwilling verfügt über Metadaten, die beschreiben, was die Maschine kann und wann sie freie Kapazitäten hat.

Blockchain als neutraler, sicherer und verlässlicher Vermittler

Nun möchten die Unternehmen ihre Daten aber nicht allen am Fertigungsprozess Beteiligten zur Verfügung stellen. Sie brauchen außerdem die Sicherheit, dass der Auftrag möglichst reibungslos abgewickelt wird. Deshalb hat das Mittelstand 4.0-Kompetenzzentrum Ilmenau die digitalen Abbilder in eine Blockchain integriert.



Das Prinzip Blockchain, verbunden mit Digitalen Zwillingen, am Beispiel des Kompetenzzentrums Ilmenau

In der Blockchain werden z. B. CAD-Modelle des Produkts, das gefertigt werden soll, hinterlegt. Verknüpft werden außerdem Materiallisten, Prüfprotokolle und vertragliche Unterlagen. Die eigentlichen Daten sind dezentral auf den jeweiligen Rechnern der Blockchain-Teilnehmer abgelegt. Jede Information bildet einen Block. Für jeden neu angefügten Block wird ein Hash, einem digitalen Fingerabdruck gleich, berechnet. Zusätzlich enthält er den Hash des vorherigen Blocks. Über die Hashs werden die Blöcke zu einer Kette verbunden: der Blockchain. Auf jedem Rechner ist dieselbe Kette mit denselben Links zu den eigentlichen Daten abgespeichert. Die Teilnehmenden sehen nicht alle Daten, wohl aber jede Transaktion. Jede veränderte Kette muss von allen bestätigt werden. Da die Blockchain dokumentiert, wer wann was gemacht hat, lässt sich auch feststellen, wo Fehler passiert sind.

Unternehmen, davon ist Mathias Eiber überzeugt, profitieren im Ilmenauer Modell gleich doppelt: „Sie können eigene freie Kapazität auf einem unabhängigen Marktplatz anbieten und so ihre Maschinen besser auslasten. Sie können aber auch Aufträge, die ihre eigenen zeitlichen und technischen Kapazitäten übersteigen, unkompliziert und sicher über das Netzwerk abwickeln, größere Aufträge annehmen oder von einer Teilfertigung profitieren.“ Transparent, smart und sicher.

Kontaktinformationen zum Zentrum

Ilmenau

Mittelstand 4.0
Kompetenzzentrum
Ilmenau

Digitale Einlasskontrolle sorgt für Sicherheit

Mit einer Datenschleuse können Daten sicher in Unternehmen übertragen werden.

Daten gelangen auf unterschiedlichen Wegen ins Unternehmen: unter anderem auf USB-Sticks und Speicherkarten oder per E-Mail. Damit Schadprogramme, die oft über Speichermedien unbemerkt eingeschleust werden, nicht das ganze Unternehmen lahmlegen, gibt es die so genannte Datenschleuse.

Software-Updates, Präsentationen oder Vertriebs- und Marketingunterlagen – die Liste von extern ins System eingespeisten Dateien ist oft lang. Ebenso wie die Wege, auf denen die Daten ins Unternehmen gelangen: Mitarbeitende, Dienstleistende oder die Kundinnen und Kunden bringen oft USB-Sticks, Festplatten oder andere Speichermedien mit, um ihre eigenen Dateien auf fremden Rechnern zu nutzen. Software-Updates werden, vor allem bei Unternehmen mit mehreren Standorten, zum Teil per Fernwartung eingespielt. Neben den gewünschten Dateien kommt dann allzu häufig auch Malware mit in das Unternehmenssystem und richtet dort zum Teil erhebliche Schäden an.

Viele Unternehmen greifen daher zu rigorosen Maßnahmen und verbieten den Einsatz von mitgebrachten Speichermedien grundsätzlich. In der Praxis zeigt sich aber, dass sich dieses Verbot oftmals nicht aufrechterhalten lässt, ohne einen praktikablen Ersatzweg anzubieten.

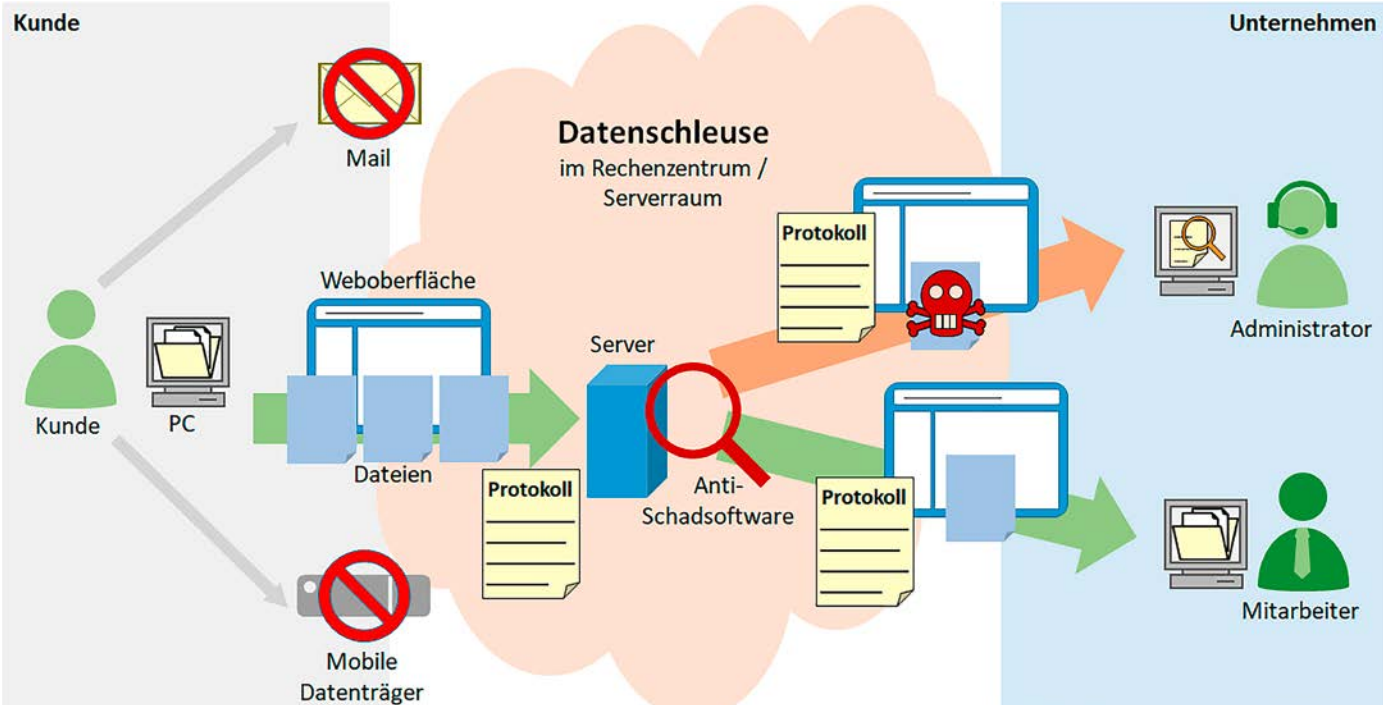
„Eine Datenschleuse zur Sicherheitsprüfung von Dateien ist eine Möglichkeit, unternehmensfremde Speichermedien durch eine zentrale Dateiablage oder freigegebene Speichermedien zu ersetzen, ohne dass die eigene Infrastruktur in Gefahr gerät“, erläutert Christopher Tebbe vom Mittelstand 4.0-Kompetenzzentrum Hannover.

Kleines Mittel, große Wirkung

Bei einer Datenschleuse handelt es sich um einen Dateiablage-Server mit einem oder mehreren Anti-Schadsoftware-Lösungen. Eingehende Dateien werden auf diesem Server geprüft und, wenn keine Schadsoftware gefunden wurde, zur weiteren

Nutzung freigegeben. So kann durch dieses einfache, aber effektive System verhindert werden, dass Malware Schäden in Systemen anrichtet und dadurch Worst-case-Szenarien wie Produktionsausfälle oder Dateiverschlüsselungen die Folge sind.

Beispielhaft lässt sich der Funktionsablauf der Datenschleuse so beschreiben: Ein Kunde möchte mit einem Unternehmen Daten teilen, beispielsweise um in einer Druckerei den Druck seines Firmenlogos in Auftrag zu geben. Dazu lädt er Dateien in die Datenschleuse hoch. Die auf der Datenschleuse laufenden Programme nehmen eine Prüfung auf Schadsoftware vor. Geht von der hochgeladenen Datei keine Bedrohung aus, kann die Mitarbeiterin des Unternehmens die Daten nach Prüfung abholen und sie guten Gewissens verwenden. Wurde Schadsoftware gefunden, gibt es mehrere Möglichkeiten: Die Datei wird entweder in Quarantäne verschoben oder direkt gelöscht. In beiden Fällen steht



Über eine Datenschleuse wird sichergestellt, dass beim Datenaustausch keine Schadprogramme ins Unternehmen gelangen.

sie aber zur Nutzung nicht zur Verfügung. Je nach Konfiguration der Datenschleuse kann ein Administrator benachrichtigt werden und das Ergebnis der Analyse prüfen. Wurde die betreffende Datei fälschlicherweise als Schadsoftware identifiziert, kann sie wieder freigeben und somit auch genutzt werden.

Datenschleusen gibt es in verschiedenen Varianten: Sie sind für Daten, die via Download oder Mail ins System kommen, und für Dateien verfügbar, die auf USB-Sticks, Festplatten oder sogar noch Disketten gespeichert mitgebracht werden.

Sicherheit zum Selbermachen

Eine Datenschleuse kann sowohl vom Unternehmen selbst als auch durch Dienstleistende betrieben werden. Soll die Datenschleuse im eigenen Unternehmen eingerichtet werden, ist dazu lediglich ein eigener Server mit der Datenschleusensoftware vor Ort oder im Rechenzentrum notwendig. Hat das Unternehmen keine eigene IT-Abteilung, bieten zahlreiche Dienstleistende unterschiedliche Modelle einer Datenschleuse an. Diese reichen von einer digitalen Schleuse, auf die über eine Weboberfläche zugegriffen werden kann, bis hin zu physischen Terminals, an die Speichermedien direkt angedockt werden können.

Kontaktinformationen zum Zentrum

Hannover

Mittelstand 4.0
Kompetenzzentrum
Hannover

Mittelstand-Digital unterstützt regional und thematisch

26 Mittelstand 4.0-Kompetenzzentren unterstützen kleine und mittlere Unternehmen in ganz Deutschland bei der Digitalisierung. Kompetent und anbieterneutral informieren sie nicht nur theoretisch über Chancen und Herausforderungen der digitalen Transformation, sondern bieten in ihren Lern- und Demonstrationsfabriken auch die Möglichkeit, digitale Technologien in der betrieblichen Praxis zu testen. In der aktuellen Situation haben sie zudem ihr Onlineangebot weiter ausgebaut.

Die 18 regionalen Mittelstand 4.0-Kompetenzzentren haben unterschiedliche Schwerpunktthemen, angefangen bei additiver Fertigung und digitalen Geschäftsmodellen über IT-Sicherheit bis hin zu Wissensmanagement und digitalem Zahlungsverkehr.

Die acht thematischen Zentren leisten jeweils an mehreren Standorten deutschlandweit gezielte Unterstützung für einzelne Branchen (Handel, Handwerk, Baugewerbe, IT- und Textilwirtschaft) bzw. Themen (eStandards, Kommunikation und Usability).

Wie können kleine und mittlere Unternehmen den sicheren internen und externen Austausch von Daten gewährleisten und so die Digitalisierung vorantreiben? Die Mittelstand 4.0-Kompetenzzentren unterstützen mit ihrer umfassenden Expertise bei der Konzeption und Umsetzung passender Maßnahmen.

Mittelstand 4.0-Kompetenzzentrum Augsburg

- Grundlagen IT-Sicherheit beim Datenverkehr im Netz
- Gesicherte Datenübertragung im EU-konformen Datenraum (GAIA-X)

Mittelstand 4.0-Kompetenzzentrum Berlin

- Praxisnahe Workshops zu IT-Sicherheitsmaßnahmen in KMU
- Identifikation von und Handlungsempfehlungen zur Schließung von IT-Sicherheitslücken

Mittelstand 4.0-Kompetenzzentrum Bremen

- Sichere Cloud-Anwendungen, -Konzepte und Methoden für geschützte Datenübertragungen
- Data Governance im Wertschöpfungsnetzwerk

Mittelstand 4.0-Kompetenzzentrum Chemnitz

- Datenschutz und IT-Sicherheit in der Produktion, Organisation und Kommunikation
- Sicherer Datenaustausch durch Verschlüsselung

Mittelstand 4.0-Kompetenzzentrum Cottbus

- BSI IT-Grundschutz, insbesondere Schulung und Informationen zu relevanter technischer Infrastruktur, organisationaler und prozessualer Einbettung, Sensibilisierung und Befähigung der Mitarbeitenden

Mittelstand 4.0-Kompetenzzentrum Darmstadt

- Identifikation der zu schützenden Werte sowie Bewertung der Unternehmensinfrastruktur hinsichtlich möglicher Risiken
- Entwicklung ganzheitlicher Sicherheitsmaßnahmen gegen unbefugte Zugriffe auf Unternehmenssysteme

Mittelstand 4.0-Kompetenzzentrum Dortmund

- Unterstützung bei Auswahl, Identifikation und Implementierung von Blockchain-Technologien im Unternehmen
- Datensicherheit und Datensouveränität im Kontext des International Data Space und GAIA-X

Mittelstand 4.0-Kompetenzzentrum Hamburg

- Technologieradar zur durchgängigen Datennutzung: Vorstellung aktueller Technologien zum sicheren Datenaustausch
- Einsatz von Blockchain-Anwendungen, u. a. für adaptive Supply Chain und Smart Contracts

Mittelstand 4.0-Kompetenzzentrum Hannover

- Bedrohungslage, Awareness, Schutzkonzepte (Schulung, Webinar, Firmengespräch, Projekt)
- Einschätzung IT-Sicherheitsstatus, Konzeptionierung von Schutzmaßnahmen (Firmengespräch, Projekt)

Mittelstand 4.0-Kompetenzzentrum Ilmenau

- Prozessdatenweitergabe und kooperative Wertschöpfung mit Blockchain
- Ortsunabhängiger und sicherer Zugriff auf Produktionsdaten und -technik durch Cloud-Lösungen

Mittelstand 4.0-Kompetenzzentrum Kaiserslautern

- Unterstützung bei der Einführung von Systemen zum Datenmanagement, z. B. ERP- und DMS-Systeme
- Unterstützung bei der Entwicklung von Apps zum sicheren unternehmensinternen Datenaustausch

Mittelstand 4.0-Kompetenzzentrum Kiel

- Identifikation möglicher Angriffspunkte, Analyse und Aufzeigen passender Schutzmechanismen
- Vernetzung kritischer Systeme, bspw. von Medizingeräten

Mittelstand 4.0-Kompetenzzentrum Lingen

- Datensicherheit und der Faktor Mensch als Grundlage für die Resilienz von Wertschöpfungsketten im Bereich des Datenaustauschs
- Datensouveränität beim/und Cloud Computing

Mittelstand 4.0-Kompetenzzentrum Magdeburg

- Sichere Datenübertragung: Effiziente Erfassung, Übertragung und Analyse von Prozessinformationen
- Informationssicherheit: Informationen rund um E-Mail-Verschlüsselung und Signierung zur Informationssicherheit

Mittelstand 4.0-Kompetenzzentrum Rostock

- „Der elektronische Arztbrief“ (eArztbrief – schnelle und sichere Übermittlung medizinischer Informationen)
- „Die elektronische Patientenakte“ (ePA – jederzeit verfügbare persönliche Gesundheits- und Krankheitsinformationen)

Mittelstand 4.0-Kompetenzzentrum Saarbrücken

- Industrial IT-Security: Grundlagen, Organisation und Prozesse, Faktor Mensch, notwendige technische Maßnahmen
- Sicherheit im Homeoffice: Situations- und Risikoanalyse, Maßnahmen für sicheres Arbeiten

Mittelstand 4.0-Kompetenzzentrum Siegen

- IT-Sicherheitsstrategie
- Begleitung bei der Einführung von Sicherheits-Frameworks im Unternehmen

Mittelstand 4.0-Kompetenzzentrum Stuttgart

- Einstieg in das Thema „Informationssicherheitsmanagement“ (Basis: ISO 27001/2, IT-Grundschutz)
- Bündelung von Angeboten zu Informationssicherheit und Infos zum sicherheitsrelevanten Lagebild für KMU

Kompetenzzentrum Digitales Handwerk

- „Routenplaner – Cybersicherheit im Handwerk“ – Handbuch für den sicheren Datenaustausch und eine geeignete Infrastruktur
- Digitalisierungsprojekt „Zertifizierte IT-Sicherheit“ mit dem E-CHECK IT

Mittelstand 4.0-Kompetenzzentrum eStandards

- Sichere Datenübertragung mit Distributed-Ledger-Technologien (z. B. Blockchain), Vertrauensumgebungen und digitalem Identitätsmanagement
- Einsatz im Rahmen von Plattformökonomie, Datenökonomie und Maschinendatenaustausch

Mittelstand 4.0-Kompetenzzentrum Handel

- Finanz- und Paymentprozesse im Online-Handel
- Schnittstellen zwischen gängigen IT-Systemen im Handel

Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft

- Vorlagen, Leitfäden, Tools und Online-Angebote zu Datenschutz und IT-Sicherheit für die Kooperationsbildung von IT-KMU
- Aufzeigen von Risiken und Lösungen in Live-Demos im Security-Lab

Mittelstand 4.0-Kompetenzzentrum Kommunikation

- Sichere Übermittlung von Daten mithilfe der Blockchain-Technologie, z. B. durch Smart Contracts
- Vertrauen in digitale Technologien durch IT-Sicherheit

Mittelstand 4.0-Kompetenzzentrum Planen und Bauen

- Hinweise und Informationen zu Datensicherheit und Datenübergabe in BIM-Projekten, insbesondere in Auftraggeberinformationsanforderungen (AIA)

Mittelstand 4.0-Kompetenzzentrum Textil vernetzt

- Valider Datenaustausch zwischen Industrie und Handel
- Sicherer Datenaustausch mithilfe smarter Sensorsysteme

Mittelstand 4.0-Kompetenzzentrum Usability

- Analyse und Optimierung von Usability und User Experience bei Mensch-Maschine-Schnittstellen für sicheren Datenaustausch
- Wissenstransfer zur Gestaltung und Testung von sicheren digitalen Systemen und agilen Arbeitsprozessen

„Wir wollen ermuntern, den ersten Schritt zu tun“

Das letzte Jahr hat viele Unternehmen zur Digitalisierung ihrer Arbeitsprozesse gezwungen. Lösungen, die auf sichere Dateninfrastrukturen setzen, standen bei den großen Herausforderungen nicht immer oben auf der Prioritätenliste. Auch Unternehmen, die bereits vor der Pandemie über eine gute digitale Infrastruktur und einen sicheren Datentransfer im Betrieb verfügten, sehen sich durch den Dauerzustand Homeoffice nun vor neue Fragen hinsichtlich der Datensicherheit gestellt. Denn auch im Homeoffice tauschen Mitarbeiterinnen und Mitarbeiter vertrauliche Nachrichten untereinander in E-Mails, digitalen Transfer-Lösungen und Kollaborationstools aus. Auch sensible Daten werden so mit der Kundschaft oder zwischen Mitarbeitenden geteilt.

Unternehmen, die in Sachen IT-Sicherheit nachrüsten möchten, bietet die Transferstelle für IT-Sicherheit im Mittelstand (TISiM) Unterstützung an. Anfang des letzten Jahres wurde diese vom Bundesministerium für Wirtschaft und Energie als ein Angebot von Mittelstand-Digital ins Leben gerufen. Bundesweit hilft die TISiM Selbstständigen, freiberuflich tätigen Personen, kleineren Unternehmen sowie Handwerksbetrieben dabei, passgenaue IT-Schutzmaßnahmen zu finden und umzusetzen.

Transferstelle IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.

TISiM-Leiterin Sandra Balz spricht im Interview darüber, was die größten Schwachstellen der Betriebe im Bereich des sicheren Datenaustauschs sind und wie die Transferstelle bei der Bekämpfung hilft.

Welche Sicherheitslücken begegnen Ihnen am häufigsten bei kleinen und mittleren Unternehmen, wenn es um das Thema Datenaustausch geht?

SANDRA BALZ: Der Praxisreport Mittelstand 2020 von Deutschland sicher im Netz e.V. (DsiN) zeigt, dass jeder vierte Betrieb über keinerlei Datensicherungen verfügt und nur jedes fünfte Unternehmen auf verschlüsselte E-Mails achtet. Besonders in kleinen und mittleren Unternehmen haben wir häufig das Problem, dass die IT-Sicherheit in den Händen von nicht gesondert qualifizierten Mitarbeitenden liegt. Bei 45 Prozent der Unternehmen unter zehn Mitarbeitenden kümmert sich die Chefin oder der Chef selbst um die IT-Sicherheit. Hier braucht es einfache und verständliche Unterstützungsangebote.

Wie unterstützt die TISiM die Unternehmen?

SANDRA BALZ: Die Sensibilität von Unternehmen für das Thema IT-Sicherheit hat deutlich zugenommen. Auch stehen bereits viele Angebote für IT-Sicherheit und Datenschutz bereit. Die Betriebe wissen jedoch oft nicht, welche davon die richtigen für ihren konkreten Bedarf sind. Die Transferstelle IT-Sicherheit im Mittelstand bündelt und sortiert diese Angebote, um sie anschließend zielgerichtet an kleine und mittlere Unternehmen sowie Handwerksbetriebe und Selbstständige zu vermitteln.

Wie sieht diese Vermittlung konkret aus?

SANDRA BALZ: Bei TISiM bauen wir sowohl auf digitale als auch analoge Informationskanäle. TISiM ist eine bundesweite Anlaufstelle, die regional agieren kann. Um Unternehmen regionale Ansprechpersonen zur Seite zu stellen, gibt es die TISiM-Regional-Standorte, die in den IHK angesiedelt sind – weitere TISiM-Regional-Standorte sind unter anderem bei den Mittelstand 4.0-Kompetenzzentren und Handwerkskammern geplant. Dort informieren die TISiM-Trainerinnen und -Trainer über die Angebote der Transferstelle. TISiM-Trainer werden in der TISiM-Workshopreihe dazu befähigt, die TISiM-Leistungen zu vermitteln und anwenden zu können – so stehen Unternehmen Ansprechpersonen direkt vor Ort zur Verfügung.

Sandra Balz ist Leiterin der Transferstelle IT-Sicherheit im Mittelstand.

Denn: die Unternehmens-individuellen Voraussetzungen sind ausschlaggebend für die Ausgestaltung der IT-Sicherheit. Hier geht es beispielsweise um die Frage, ob ein Unternehmen bereits über eine eigene IT-Abteilung verfügt oder bei null anfängt.

Das Herzstück der Transferstelle ist der so genannte Sec-O-Mat. Als Suchmaschine für IT-Sicherheit hält er zahlreiche Angebote und Handlungsempfehlungen bereit und stellt sie in passgenauen TISiM-Aktionsplänen zur Verfügung. Die Unternehmen werden damit Schritt für Schritt bei der Umsetzung begleitet und anbieterneutrale Hilfs- und Weiterbildungsangebote werden angezeigt. Eine Beta-Fassung des Sec-O-Mat steht bereits online zur Verfügung.

Sicher haben viele Unternehmen die Sorge, dass Maßnahmen zum sicheren Datenaustausch zeitaufwendig werden können – sind sie das?

SANDRA BALZ: Schon mit wenig Aufwand kann viel erreicht werden. Wir wollen dazu ermuntern, den ersten Schritt zu tun, konkrete Maßnahmen zu ergreifen und die IT-Sicherheit schrittweise zu verbessern. Wie bei allen anderen Entwicklungsprozessen in Unternehmen sind hier die Vorteile für das Unternehmen ausschlaggebend, die sich daraus ergeben. Wir zeigen, dass es sich lohnt, Zeit in den sicheren Datenaustausch zu investieren.

Wie gehen Unternehmen am besten vor, um sich dem Thema zu nähern?

SANDRA BALZ: Am besten beginnen Unternehmerinnen und Unternehmer mit unserem Sec-O-Mat. Er startet mit einer Unternehmensbefragung, in der angegeben werden kann, in welchen Bereichen eines Unternehmens Daten ausgetauscht werden – zum Beispiel im Personalmanagement oder in der Ausgangslogistik. Im Anschluss folgt ein TISiM-Aktionsplan, der konkrete Handlungsempfehlungen zu Maßnahmen für einen sicheren Datenaustausch gibt – aber auch zu weiteren Bereichen, in denen die IT-Sicherheit des Betriebes gestärkt werden kann. So gelangt das Wissen von Fachleuten dorthin, wo es benötigt wird: in die Betriebe.

Kontaktinformationen zur Transferstelle IT-Sicherheit im Mittelstand:

Transferstelle
IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.

Datenaustausch auf Augenhöhe

Das Beispiel von Cookies- und Nutzungsvereinbarungen auf Websites zeigt die Bedeutung transparenter, verständlicher Kommunikation bei digitalen Produkten.

Bevor Unternehmen Besucherinnen und Besucher auf ihre Website lassen, sind sie seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) im Jahr 2018 verpflichtet, eine Einwilligung in die Cookies- und Nutzungsvereinbarungen einzuholen. Das Instrument wurde geschaffen, um Nutzende darüber zu unterrichten, welche Daten sie durch den Besuch der Seite mit einem Serviceprovider austauschen. Viele Unternehmen nutzen es, um damit mehr Daten zu erfassen als früher – verschleiern das jedoch mit überlangen Texten und unübersichtlichen Designs. Stefan Brandenburg und Veronica Hoth vom Mittelstand 4.0-Kompetenzzentrum Usability raten Unternehmen in ihren Workshops von solchen Methoden ab. Da ein sicherer Datenaustausch immer auch Vertrauen erfordert, plädieren sie für Transparenz und Kommunikation auf Augenhöhe.

Durch Design Kunden in die gewünschte Richtung „schubsen“

Ein wichtiges Ziel von Unternehmens-Websites ist es, ihre Zielgruppen zu erreichen. Ob das gelingt, kann mithilfe der Nutzungsdaten der Besuchenden erfasst und anschließend ausgewertet werden. Die Versuchung ist groß, die Cookies- und Nutzungsvereinbarung so zu gestalten, dass die Nutzerinnen und Nutzer ihre Einwilligung zum Datenaustausch auch dann geben, wenn sie nicht wirklich verstanden haben, welche Daten sie von sich preisgeben. Oft gestalten Entwickelnde die Website beispielsweise mit Designelementen wie einem farblich hervorgehobenen Button so, dass die Nutzenden in die gewünschte Richtung gelenkt werden.

Diese Designmethode wird in ihrer positiven Anwendung Nudging (Englisch für „anstoßen“, „schubsen“) genannt. Sie dient dazu, die Nutzendenführung zu optimieren und es Nutzenden zu ermöglichen, sich intuitiv auf der Website zu bewegen. In der negativen Variante wird Nudging zu einem so genannten Dark Pattern (einer „verdunkelnden Musterung“). Auch dabei werden die Nutzenden an die Hand genommen, sodass sie intuitiv den Aufbau der Seite oder des geöffneten Fensters verstehen. Die Nutzendenführung verleitet Besucherinnen und Besucher

dann aber beispielsweise dazu, einem Datenaustausch zuzustimmen, über dessen Umfang und Inhalt sie nicht hinreichend informiert sind.

Beispiele für Nudging und Dark Pattern

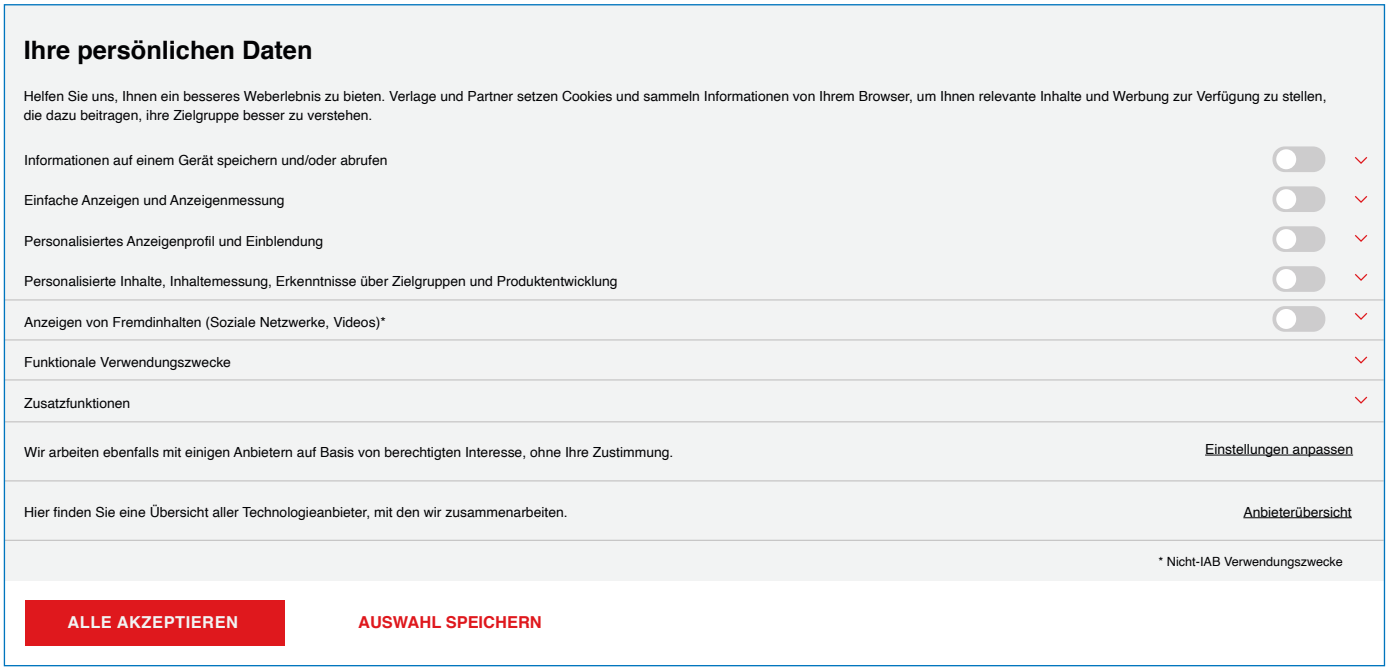
Das Beispiel A zeigt ein positives Nudging. Die Website-Betreibenden möchten die Daten ihrer Nutzenden mit einer so genannten Opt-in-Variante, also einer informierten Einwilligung, schützen. Nutzende müssen ihre Daten aktiv freigeben, was wiederum Datenschutz und -sicherheit fördert.

Im Beispiel B (Seite 33) versuchen die Website-Betreibenden dagegen, ihren Nutzerinnen und Nutzern über die Gestaltung des Abfragefensters nahezulegen, das Datentracking anzunehmen. Das widerspricht zwar der Absicht der DSGVO, mehr Transparenz herzustellen, ist aber nicht verboten. Unternehmen, denen es wichtig ist, mit ihrer Kundschaft und Geschäftspartnern auf Augenhöhe zu kommunizieren und das auch zu zeigen, folgen besser der Absicht der DSGVO und kennzeichnen entsprechend deutlich, wann sie von Nutzenden welche Daten abfragen.

Tipp: Mit Design-Mitteln einen vertrauensvollen Datenaustausch ermöglichen

Zur nutzendenfreundlichen Gestaltung von Cookies- und Nutzungsvereinbarungen gibt es bereits zahlreiche Gestaltungsempfehlungen. So empfehlen beispielsweise Mozilla.org und Netzpolitik.org. Datenschutzrichtlinien und Nutzungsvereinbarungen durch die Verwendung von Icons zu vereinfachen. Beide gemeinnützige Organisationen setzen sich seit Jahren für Transparenz und Fairness im Netz ein. Der Vorteil der empfohlenen Icons besteht darin, dass die Nutzerinnen und Nutzer sie bereits aus anderen Anwendungen kennen, und sie daher leichter zu verstehen sind. Im Infokasten sind Beispiele solcher frei verfügbarer Icons sowie weitere Designtipps zu finden.

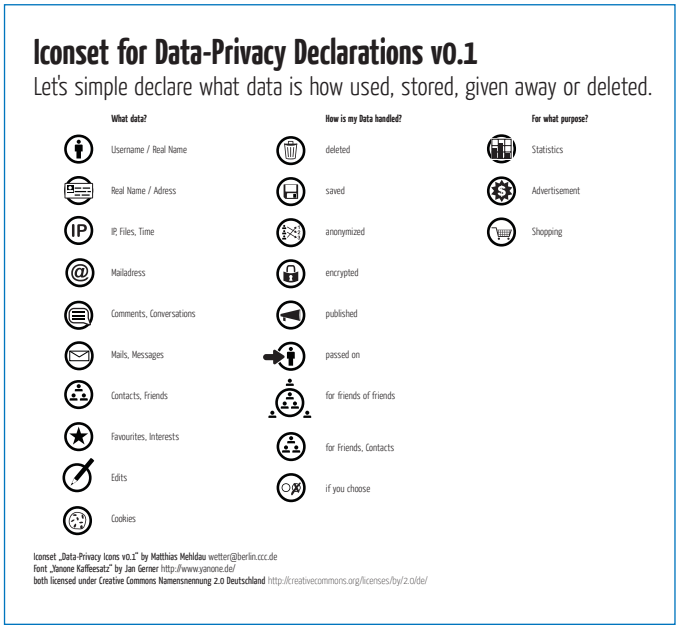
Beispiel A: Nudging zur Unterstützung von Datenschutz und -sicherheit



Beispiel B: Dark Pattern zur Verringerung von Datenschutz und -sicherheit

Datenaustausch auf Augenhöhe schafft Vertrauen in innovative, digitale Produkte

Transparenz und Kommunikation auf Augenhöhe beim Datenaustausch sind jedoch nicht nur bei Cookies- und Nutzungsvereinbarungen auf Websites von Bedeutung. Sie sind auch wichtig für die Akzeptanz innovativer, digitaler Angebote. Das zeigte sich beispielsweise in der Kooperation des Kompetenzzentrums Usability mit der Von Wegen GmbH. Das Unternehmen betreibt unter anderem die Plattform millionways.net. Die Plattform will Netzwerke zwischen Menschen schaffen, die gleiche oder ähnliche Ziele vorfolgen. Dafür werden Interviews angeboten, mit denen Nutzende zunächst selbst herausfinden können, welche Talente und Leidenschaften sie haben. Mithilfe Künstlicher Intelligenz und Spracherkennung werden die Ergebnisse ausgewertet und Menschen mit zueinanderpassenden Neigungen und Zielen vernetzt.



Beispiel C: Frei verfügbare Icons zur Gestaltung von Cookies- und Nutzungsvereinbarungen

Eine Befragung unter den Nutzenden der Plattform ergab, dass sie großen Wert auf eine transparente Kommunikation und Einhaltung des Datenschutzes legen. Die Bedienoberfläche sollte daher so gestaltet sein, dass sie effizient genutzt werden kann und zugleich Vertrauen und Sicherheit vermittelt. Unternehmen, die erfolgreich innovative, digitale Produkte anbieten wollen, sollten daher immer berücksichtigen, dass eine verständliche und transparente Kommunikation bei Nutzenden hoch im Kurs steht.

Kontaktinformationen zum Zentrum

Usability

Mittelstand 4.0
Kompetenzzentrum
Usability

Der Faktor Mensch

Die Weiterbildungsplattform „KMU. Einfach Sicher.“ rückt den Menschen in den Mittelpunkt der IT-Sicherheit.

Ist dem Anhang in der Mail zu trauen? Was muss ich beachten, wenn ich für den Austausch von Daten eine Cloudlösung nutze? Gerade in kleinen und mittleren Unternehmen stehen die Mitarbeitenden häufig vor Fragen wie diesen. Da es an Zeit, Geld und Expertise mangelt, handeln viele Beschäftigte dabei oft unbewusst fahrlässig. Das Projekt „KMU. Einfach Sicher.“ will das ändern. Wie das mit der dafür geplanten interaktiven Weiterbildungsplattform gelingen kann, erläutert Projektleiter Dr. Simon Oberthür im Gespräch.

Der Mensch gilt als Risiko, wenn es um sicheren Datenaustausch und andere Sicherheitsaspekte geht. Würde es nicht reichen, zu sagen, „passt einfach alle besser auf“? Wozu braucht es dafür eine Weiterbildungsplattform?

SIMON OBERTHÜR: Um Aufmerksamkeit für den sicheren Umgang mit Daten und IT-Systemen zu schaffen, wird bislang gern die Keule geschwungen. Man malt aus, welche rechtlichen Folgen durch DSGVO-Verstöße, beispielsweise beim unsicheren Austausch von Daten, drohen und welche Gefahren davon ausgehen, wenn etwa durch Phishing-Mails Cyberangriffe auf das Unternehmen gestartet werden. So richtig es ist, diese Gefahren im Blick zu haben, gilt auch: IT-Sicherheit wird dadurch von den meisten Menschen als etwas empfunden, das negativ besetzt ist. Im Ergebnis möchte man sich daher so wenig wie möglich damit beschäftigen. Durch das ständige Betonen der Gefahren und Risiken erreicht man so letztlich das Gegenteil dessen, was man eigentlich anstrebt: Die Menschen wenden sich innerlich von dem Thema ab.

Was schlagen Sie stattdessen vor?

SIMON OBERTHÜR: Wenn man die Menschen für Themen wie einen sicheren Datenaustausch gewinnen will, muss man ihnen aufzeigen, welche Mehrwerte sich für sie dadurch bieten – nicht nur im beruflichen, sondern auch im privaten Bereich. Bislang ist es umgekehrt: IT-Sicherheit wird von den Beschäftigten als etwas erlebt, das für sie mit Mehraufwand verbunden ist. Recht gut verdeutlichen lässt sich das beim Umgang mit Passwörtern. Da sich die Mitarbeitenden oft zu viele Passwörter

merken müssen, wählen sie gern sehr einfache Zahlenfolgen oder andere leicht zu entschlüsselnde Passwörter. Wir alle gehen eben immer gern den einfachsten Weg. Wir empfehlen daher unter anderem, einen Passwortmanager im Unternehmen einzuführen. Dieser füllt dann automatisch alle erforderlichen Passwörter ein. Die Beschäftigten erleben so im Alltag, dass sie nicht nur etwas für die Sicherheit im Unternehmen tun, sondern auch selbst effektiver arbeiten, weil das mühselige Eintippen von Passwörtern entfällt. Das Thema wird auf diese Weise positiv aufgeladen. Die Menschen erhalten als Feedback, dass IT-Sicherheit ihren Arbeitsalltag sogar erleichtern kann.

Mit der IT zurechtzukommen, ist für viele Beschäftigte oft schon Herausforderung genug. Wie wollen Sie erreichen, dass sich diese Menschen auch noch mit dem viel komplexeren Thema IT-Sicherheit auseinandersetzen?

SIMON OBERTHÜR: Hinter der Ablehnung des Themas steckt in der Regel das, was man „erlernte Hilflosigkeit“ nennt. Wer sich beispielsweise schon in der Schule mit Mathematik schwer tat, neigt auch später dazu zu betonen, nicht gut rechnen zu können. So ähnlich hört man das dann oft auch

Dr. Simon Oberthür, Manager im SICP – Software Innovation Campus Paderborn der Universität Paderborn

im Umgang mit Computern. Will man dagegen angehen, kommt es darauf an, die Kompetenz im Umgang mit der Technik zu erhöhen. Entscheidend dabei ist, die Lerninhalte nicht zu überfrachten. Es sollte immer nur das an technischem Know-how vermittelt werden, was die Anwendenden auch wirklich benötigen. Die Vermittlung von IT-Wissen sollte praxisnah sein und darf auch Spaß machen. Wir arbeiten auf unserer Weiterbildungsplattform mit Videos und nutzen narrative Elemente, sodass unser Protagonist vor ähnlichen Herausforderungen steht wie unsere Nutzerinnen und Nutzer. Insgesamt arbeiten wir interdisziplinär an den Feldern IT-Sicherheit, Didaktik und Medienpädagogik.

An wen richtet sich das Angebot der Weiterbildungsplattform – an IT-Beauftragte, an die Unternehmensleitung oder alle Mitarbeitenden?

SIMON OBERTHÜR: Ganz klar an alle. Daher bieten wir auch immer eine individuelle Risikoanalyse an, indem wir den Nutzenden Fragen hinsichtlich der IT-Sicherheitsrisiken stellen, denen sie in ihrem Arbeitsalltag begegnen. Wir fragen zum Beispiel, ob und wenn ja welche Cloud-Dienste sie nutzen, oder auch, ob sie besonders viel per E-Mail oder anderen Diensten kommunizieren. Je nach gegebener Antwort weisen wir auf individuell relevante Angebote hin. Wie wir diese Angebote didaktisch ausgestalten, erforschen wir derzeit noch. Unter anderem testen wir dafür Gamification-Angebote, sodass innerhalb von Unternehmen motivierende Wettbewerbe zur IT-Sicherheit durchführbar sind. In jedem Fall werden wir die Angebote auch bündeln, um sie so auch als geschlossene Fortbildungsmaßnahmen anbieten zu können.

Kann die Weiterbildungsplattform bereits genutzt werden?

SIMON OBERTHÜR: Derzeit befindet sich die Plattform noch im Aufbau. Wir haben allerdings auch schon erste Module im Testlauf. Wer schon jetzt teilnehmen möchte, kann sich auf unserer Projektwebsite in unserem Anwendendennetzwerk anmelden. Das bietet allen die Möglichkeit, die Plattform durch eigene Fragen und Wünsche mitzugestalten.

Wenn Sie im Jahr 2040 auf das Projekt zurückblicken, was haben Sie dann erreicht?

SIMON OBERTHÜR: Wir haben bei der IT-Sicherheit den Menschen mit seinen Stärken und Schwächen ins Zentrum gerückt. IT-Sicherheit wird dann nicht allein mit technischen Hilfsmitteln und Direktiven „von oben“ hergestellt, sondern im Arbeitsalltag als etwas erlebt, das allen bei der täglichen Arbeit hilft.

Kontaktinformationen zu KMU. Einfach Sicher. :

KMU. Einfach Sicher.

XING