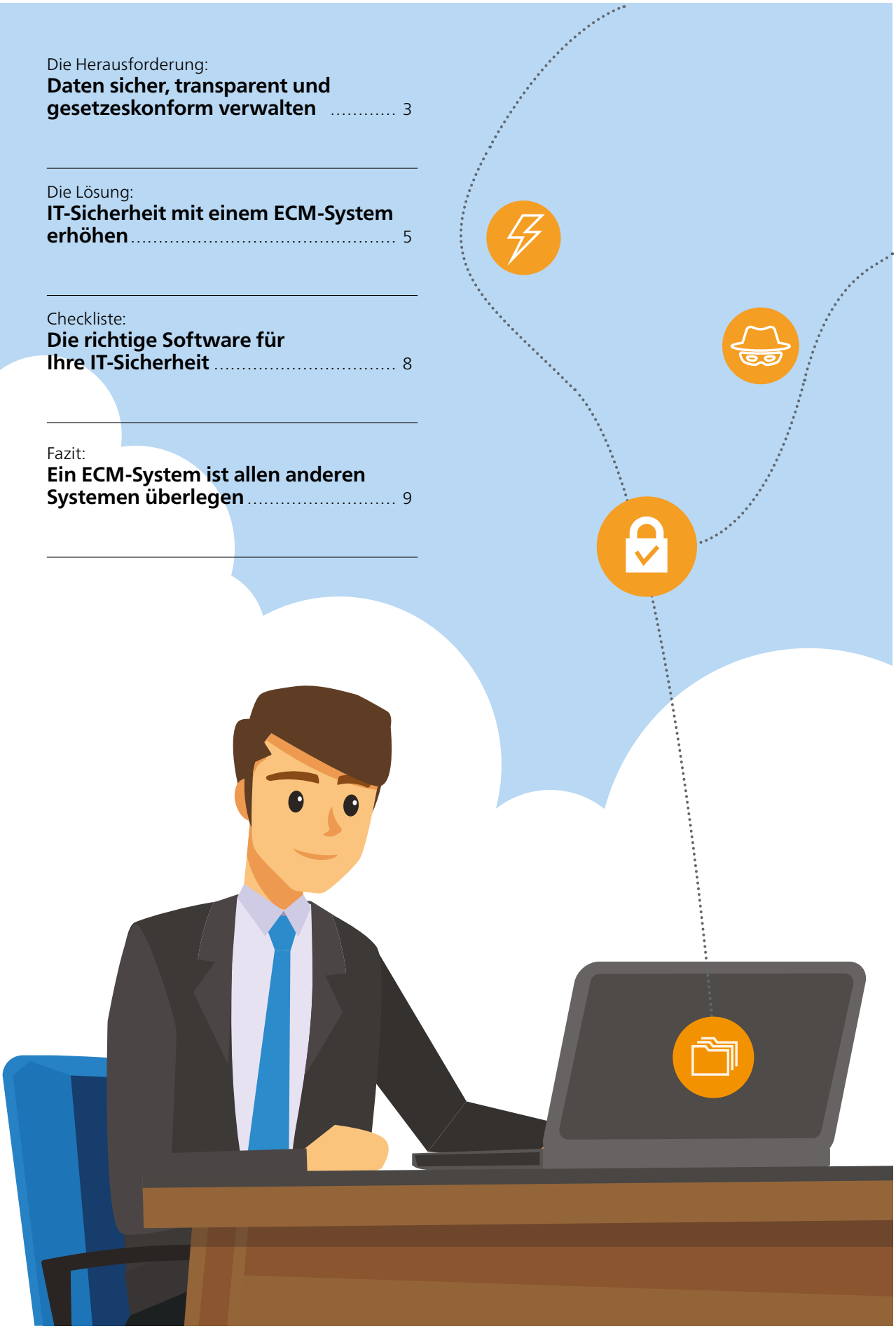
Whitepaper

Digital neu denken: IT-Sicherheit und modernes Informationsmanagement

Whitepaper über Sicherheit in der Informationstechnik und deren Unterstützung durch ein ECM-System



Die Herausforderung:

Daten sicher, transparent und gesetzeskonform verwalten

Digitalisierte Lebensbereiche und die steigende Zahl IT-bezogener Sicherheitsvorfälle

Das Thema IT-Sicherheit ist derzeit in aller Munde. Nicht ohne Grund, denn die Nachrichten sind voll von Meldungen wie „Sicherheitslücke in elektronischer Patientenakte", „Cyberangriffe: neues Jahr – neue Gefahren", „Sensible Daten ungeschützt im Netz" … An Computerviren, Trojaner etc. hatten sich die meisten gewöhnt und waren vorbereitet: „Ein guter Virenscanner und auf keinen Fall unbekannte Mailanhänge öffnen, sollten als Schutzmaßnahmen genügen. Und wenn nicht, dann setzt man eben den Rechner neu auf."

Neue Dimension der Cyberangriffe

Dieser naive Sicherheitsglaube war spätestens vorbei, als es Kriminellen gelang, mit Ransomware den Zugriff auf ein Betriebssystem oder potenziell wichtige Dateien zu verschlüsseln und die Betroffenen zu einer Lösegeldzahlung zu zwingen. Schlagartig wurde klar, dass die wahren Werte eines Unternehmens, ja jedes PCs, die gespeicherten Daten sind – geradezu unersetzlich, wenn man nicht mehr darauf zugreifen kann und im schlimmsten Fall keine aktuelle Datensicherung vorhanden ist.

Welche Dimensionen die durch Cyberattacken entstandenen Schäden 2020 allein im Homeoffice annahmen, zeigte ein Bericht des Instituts der deutschen Wirtschaft, der auf Zahlen einer repräsentativen Umfrage des Branchenverbandes Bitkom basierte:

Die 2021 von der Bitkom veröffentlichte Studie „Wirtschaftsschutz 2021" ergab, dass 88 Prozent der Unternehmen in den vergangenen 12 Monaten von Cyberattacken betroffen waren. Dadurch entstand der deutschen Wirtschaft durch Sabotage, Datendiebstahl oder Spionage ein Schaden von rund 223 Milliarden Euro, doppelt so viel wie noch 2019 und viermal so viel wie 2017. Verschärft wird das Problem, weil in Deutschland trotz aller Warnungen immer noch rund drei Millionen Computer mit alten Betriebssystemen laufen, vor allem mit Windows 7. Dabei hat Microsoft den Support und die Sicherheitsupdates für dieses Betriebssystem bereits 2020 eingestellt. Das Arbeiten mit solch alten Systemen ist daher grob fahrlässig.

IT-Sicherheit ist weit mehr als nur der Schutz vor Hackern

Im Zeitalter der digitalen Transformation sind vor allem (sensible) Daten (z. B. Kundendaten, Personaldaten oder Patientendaten) und Informationen (z. B. Unternehmensstrategien, Konstruktionspläne oder Forschungsergebnisse) die eigentlichen Unternehmenswerte. Gehen diese verloren oder sind nicht mehr verfügbar, kommt es zu erheblichen Störungen im Unternehmen, mitunter ist sogar die gesamte Existenz bedroht. Die Coronapandemie hat dies 2020 extrem verdeutlicht: Klare Wettbewerbsvorteile hatten jene Unternehmen, deren Mitarbeiter problemlos im Homeoffice weiterarbeiten konnten, weil sie flexibel und mobil auf die dazu erforderlichen, digital gespeicherten Daten und Informationen ihres Unternehmens zugreifen konnten – beispielsweise über ein ECM-System.

Da viele Daten und Informationen heute über Netzwerke und/oder mit dem Internet verbunden sind, ist die IT-Sicherheit aber nicht mehr isoliert zu betrachten. Sie schließt daher alle in einem Unternehmen eingesetzten technischen Systeme zur Informationsverarbeitung, -speicherung und -lagerung mit ein – und damit auch Infrastrukturen wie Stromversorgung oder Telekommunikation.

Datenschutz und Datensicherheit im Unternehmen

Datenschutz und Datensicherheit sind ein wichtiger Teil der IT-Sicherheit. Im täglichen Sprachgebrauch werden die Begriffe Datenschutz und Datensicherheit allerdings

oft missverständlich verwendet, durcheinandergebracht oder als Synonym benutzt, obwohl sie sich in ihren Zielen und Vorgängen deutlich unterscheiden.

Datenschutz

Beim Datenschutz geht es um den Schutz von personenbezogenen Daten, das heißt um die rechtlichen Fragen, unter welchen Voraussetzungen Daten von natürlichen Personen erhoben, verarbeitet, gespeichert oder genutzt werden dürfen. Personenbezogen sind Daten immer dann, wenn sich ein direkter Personenbezug herstellen lässt, beispielsweise durch Name, Adresse, Telefon- oder Sozialversicherungsnummer. Dazu gehören aber auch Meinungen, Religions- oder Verbandszugehörigkeiten etc.

Der Schwerpunkt des Datenschutzes liegt dabei aber nicht auf dem Inhalt der Daten, sondern auf dem Schutz des Persönlichkeitsrechts und der Privatsphäre sowie dem Recht auf informationelle Selbstbestimmung. Dies ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht, daher können Betroffene grundsätzlich selbst darüber entscheiden, wem sie welche persönlichen Informationen bekanntgeben (dieses Grundrecht wird im Grundgesetz allerdings nicht explizit erwähnt). Es geht also nicht nur darum, was Behörden oder Unternehmen dürfen, um personenbezogene Daten zu erheben, zu sammeln und zu verarbeiten, sondern vor allem darum, einen Missbrauch dieser Daten zu verhindern.

Grundlagen sind das Datenschutzrecht, das seit Mai 2018 in der Datenschutzgrundverordnung (DSGVO) geregelt ist, und das Bundesdatenschutzgesetz (BDSG). Ab 20 Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, besteht nach dem BDSG die Pflicht, einen Datenschutzbeauftragten zu benennen.

Die DSGVO verlangt technisch-organisatorische Maßnahmen (TOM), um die Sicherheit personenbezogener Daten zu gewährleisten. Diese sind vom Verantwortlichen zu dokumentieren. Einzelheiten der Maßnahmen sind im Bundesdatenschutzgesetz geregelt. Hierzu gehören beispielsweise Zutritts-, Zugangs- und Zugriffskontrolle, aber auch Eingabe-, Weitergabe-, und Verfügbarkeitskontrolle, sowie ein Trennungsgebot.

Ein wichtiger Hinweis: Auch wenn Ihr Unternehmen nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen, sollten Sie dies tun. Dadurch können Sie sicher sein, dass im Unternehmen die gesetzlichen Vorgaben umgesetzt und eingehalten werden – und Sie dies auch nachweisen können. Beachten Sie aber die rechtlichen Vorschriften, nicht jeder Mitarbeiter ist als Datenschutzbeauftragter geeignet.

Datensicherheit

Die Datensicherheit befasst sich mit dem generellen Schutz von Daten, unabhängig davon, ob ein Personenbezug besteht oder nicht. Somit fallen unter die Datensicherheit alle Maßnahmen zum Schutz von Daten, Speichermedien sowie einzelnen Programmen vor unbefugtem Zugriff, Fehlern, Fälschungen oder Verlust. Datensicherheit soll durch geeignete und effektive Maßnahmen erreicht werden. Dabei sind vor allem drei Gefahren angemessen zu berücksichtigen: höhere Gewalt, technische Störfälle und der Risikofaktor Mensch. Behörden und Unternehmen, die mit personenbezogenen Daten arbeiten, müssen entsprechende Datensicherungskonzepte erstellen, die auf dem neuesten Stand der Technik sind und den Datenschutz garantieren.

Datenschutz und Datensicherheit sind also unterschiedliche Vorgänge, aber untrennbar miteinander verbunden. Ein angemessener Datenschutz ist ohne eine ausreichende Datensicherheit nicht möglich. Allerdings kann sich die Datensicherheit negativ auf den Datenschutz auswirken: Beispielsweise ist ein Backup in der Cloud meist am besten vor Verlust geschützt, weil der Betreiber dafür zuständig ist und dies in aller Regel auch garantiert. Für den Datenschutz ist ein Backup in der Cloud aber aus zwei Gründen problematisch:

- Beim Rechenzentrum im eigenen Unternehmen oder in der nahen Umgebung können Sie jederzeit vorbeischauen und die Sicherheitsvorkehrungen gegen Serverschäden, Einbruch, Diebstahl etc. prüfen. In der Cloud können Sie in aller Regel nur darauf vertrauen. Falls aber die Cloud zudem in einem Land betrieben wird, dass es mit dem Datenschutz nicht so genau nimmt, könnte es beispielsweise schon möglich sein, dass Ihre vertraulichen oder gar geheimen Informationen auf dubiosen Wegen in die Hände Ihrer Konkurrenz gelangen.

- Die Datenspeicherung in der Cloud ist eine Datenübermittlung. Dafür müsste eine Rechtsgrundlage oder eine eindeutige Einwilligung für die personenbezogenen Daten vorliegen. Zudem wäre beispielsweise bei einem Zugriff durch IT-Mitarbeiter ein Auftragsdatenverarbeitungsvertrag erforderlich.

Es kann also tatsächlich vorkommen, dass Maßnahmen für die Datensicherheit ein Problem lösen, aber dafür ein neues Problem innerhalb des Datenschutzes erzeugen. Deshalb sind für den Erfolg beider Prozesse eine strukturierte Organisation und ein funktionierendes System unabdingbar. Beides lässt sich durch ein ECM-System erreichen.

Die Lösung:

IT-Sicherheit mit einem ECM-System erhöhen

ECM bietet alle wichtigen Werkzeuge zur Einhaltung gesetzlicher Anforderungen an Datenschutz und -sicherheit

Verfügt ein Unternehmen über ein ausgereiftes, am besten modular ausbaufähiges ECM-System, sind sehr gute Voraussetzungen geschaffen, um die unterschiedlichen Aufgaben und Erfordernisse eines Unternehmens in allen Abteilungen und Unternehmensbereichen erfolgreich umzusetzen. Denn Enterprise-Content-Management umfasst alle Technologien, Methoden und Werkzeuge, um sämtliche Informationen eines Unternehmens (Dokumente, Daten, Bilder, Videos etc.) zu erfassen, zu digitalisieren, zu speichern, zu verwalten und bereitzustellen. Dadurch lassen sich nahezu alle Unternehmensprozesse optimieren. Aber das Beste: Ein gutes ECM-System lässt sich nahtlos in Ihre IT-Infrastruktur integrieren.

Ein Enterprise-Content-Management (ECM)-System ist damit eines der Herzstücke der IT-Landschaft im Unternehmen. Es kommuniziert mit allen Systemen, bildet digitalisierte Arbeitsabläufe in unterschiedlichen Fachabteilungen ab und bietet vielfältige technische Erweiterungen für unterschiedliche Anforderungen. Die Hauptaufgaben eines ECM-Systems sind die digitale Archivierung, das Verwalten und das Managen von Dokumenten. Dabei werden alle unternehmensrelevanten Informationen zentral an einer Stelle abgelegt – zugänglich für jeden, der sie benötigt und dazu berechtigt ist, und bei Bedarf auch jederzeit bearbeitbar. Daher steht ECM für ein umfassendes intelligentes Informationsmanagement im Unternehmen. Die Vorteile sind offensichtlich:

- **Zeit einsparen durch automatisierte Abläufe**
- **Kosten reduzieren dank optimaler Ressourcennutzung**
- **Erhöhte Sicherheit Ihrer Prozesse**

Darüber hinaus bietet ein gutes ECM-System alle erforderlichen Werkzeuge, um die gesetzlichen Anforderungen an Datenschutz und -sicherheit einzuhalten. Die Unternehmensdaten sind dank einer hochentwickelten Verschlüsselungstechnologie jederzeit sicher aufbewahrt. Sind bestimmte Daten besonders zu schützen, sorgen Zugriffskontrollen, Protokollierung, ein ausgefeiltes Berechtigungssystem, unveränderbare Dokumentenhistorie sowie ein intelligentes System zur Einhaltung von Aufbewahrungspflichten für zusätzlichen Schutz. Es gibt aber nicht den einen richtigen Weg. Lassen Sie sich daher unbedingt beraten.

Beim Thema Datenschutz ist ein ECM-System unschlagbar

Ein ECM-System ist beim Thema Datenschutz allen anderen Systemen überlegen. Es bietet zahlreiche Möglichkeiten, die Anforderungen der DSGVO komfortabel umzusetzen, beispielsweise durch Berechtigungskonzepte für die Mitarbeiter (Wer darf was mit welchen Daten tun?). Damit ist man in diesem Bereich auf der sicheren Seite. Konkret unterstützt ein ECM-System bei folgenden Anforderungen der DSVGO:

Speicherung und Sicherung personenbezogener Daten

Ein ECM-System speichert alle Daten strukturiert und übersichtlich. Dabei spielt es keine Rolle, ob es sich um Abrechnungen, E-Mails, Verträge oder andere wichtige Dokumente handelt. Dies ermöglicht es, ganz einfach den Überblick zu behalten. Das aufwändige Suchen und Prüfen von Verträgen in der Rechtsabteilung, von Rechnungen in der Buchhaltung oder nach Unterlagen im Archiv gehört damit der Vergangenheit an. Und selbstverständlich lässt sich die Datensicherung aus einem zentralen Archiv einfacher und sicherer gestalten, als wenn jede Abteilung selbst dafür sorgen müsste. Zudem unterstützt eine gute ECM-Lösung unterschiedlichste Backup-Konzepte.

Recht auf Vergessenwerden

Ein ECM-System erleichtert auch das vollständige Löschen aller personenbezogenen Daten. Dadurch ist garantiert, dass keine Daten zurückbleiben oder übersehen werden. Denn das Recht auf Vergessenwerden räumt jeder betroffenen Person ein Recht auf Löschung ein, wenn die Gründe für die Speicherung nicht mehr bestehen. Daher hat die verarbeitende Person die Pflicht, die jeweiligen Daten zu löschen, sobald der Speicherungsgrund oder die Aufbewahrungsfrist entfällt (Kassation). Einer guten ECM-Lösung gelingt dies durch eine frei definierbare Kassationssteuerung und gemäß den gesetzlichen Anforderungen.

Berechtigungssystem

Ein gutes ECM-System ermöglicht es auch, digitale Akten für Kunden, Lieferanten, Projekte, Personal und andere Geschäftsvorfälle anzulegen. Bei sensiblen Daten, vor allem Personaldaten, lassen sich die Daten zusätzlich verschlüsselt ablegen. Eine empfehlenswerte ECM-Lösung nutzt hierfür eine 256-Bit-Verschlüsselung (mit AES-256 – Advanced Encryption Standard). Das im ECM-System vorhandene Berechtigungssystem bietet umfangreiche Berechtigungsfunktionen für Funktionalitäten, Dokumente und Archivbereiche. Somit sind alle Dokumente und Daten nur für die Mitarbeiter einseh- und ggf. veränderbar, die eine entsprechende Zugangsberechtigung haben. Selbst der Systemadministrator kann dann nicht ohne weiteres auf sensible personenbezogene Daten zugreifen.

Verfügbarkeit

Wichtig ist nach den Vorgaben der DSGVO auch die Verfügbarkeit der personenbezogenen Daten. Ein ECM-System unterstützt Sie daher auch bei der regelmäßigen Datensicherung, die selbstverständlich für alle Daten im Unternehmen extrem wichtig ist. Ziel dabei ist, die Daten vor Verlust, Diebstahl oder anderen Risiken zu schützen, also verfügbar zu halten, damit Sie jederzeit darauf zugreifen können. Wichtig ist, die passende Datensicherungsstrategie für Ihr Unternehmen und Ihre Daten zu entwickeln. Ob Sie Ihr Backup auf einem Magnetband, einem anderen Server oder in der Cloud machen, entscheiden Sie selbst. Wichtig ist vielmehr die richtige Aufbewahrung des Backups. Denken Sie an Feuer, Löschwasser, Diebstahl, mutwillige Zerstörung … Lagern Sie daher die Datensicherung generell gut geschützt oder besser räumlich getrennt an einem anderen Ort. Beachten Sie zudem bitte auch unsere obigen Hinweise zur richtigen Speicherlösung.

Auskunftsrecht

Das in der DSGVO vorgeschriebene Recht auf Auskunft bezieht sich auf die in einem Unternehmen gespeicherten, personenbezogenen Daten. Diese sind in aller Regel über alle Unternehmensbereiche verteilt, das Recht auf Auskunft ist daher oft schwierig oder nur zeitaufwändig umzusetzen. Eine ECM-Lösung speichert und verwaltet dagegen alle Daten zentral im Archiv. Durch eine spezielle und praktische Suchfunktion des ECM-Systems ist eine schnelle und gezielte Datensuche garantiert und eine Auskunft kein Problem. Ein gutes ECM-System hat hierzu beispielsweise eine feste Kennung „DSGVO-Bezug“ im Datenmodell eingefügt. Über diese Kennung lässt sich dann vorgangs- und bereichsübergreifend schnell und einfach suchen.

Recht auf Datenübertragbarkeit

Jeder hat das Recht, seine personenbezogenen Daten von einer verantwortlichen Stelle auf eine andere zu übertragen, sofern der Betroffene seine personenbezogenen Daten auf Grundlage einer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrages erforderlich ist. Dieses Recht wird in einem ECM-System durch den Export aller Daten ermöglicht. Die so exportierten Daten lassen sich ohne spezielle Programme jederzeit wieder anzeigen bzw. an anderer Stelle importieren.

Dokumentationspflicht

Unternehmen sind verpflichtet, exakt nachzuweisen, wie ein Dokument ins Unternehmen gekommen ist und wie es ggf. das Unternehmen wieder verlassen hat. Änderungen sind durch eine Versionierung vollständig zu belegen. Ein ECM-System verfügt hierzu über spezielle Nutzungsnachweise sowie Lösch- und Bearbeitungsprotokolle mit exakten Zeit- und Personenangaben. Somit ist sichergestellt, dass alle Arbeitsschritte zuverlässig und rechtssicher dokumentiert werden. Damit ist auch das gemeinsame Arbeiten an einem Dokument problemlos und rechtssicher möglich. Sämtliche Änderungen/Bearbeitungsschritte bleiben transparent und jederzeit nachvollziehbar. Über Workflows lässt sich zusätzlich der gesamte Arbeitsprozess dokumentieren.

Auf die Schnittstellen und Erweiterungen kommt es an

Einige ECM-Systeme lassen sich durch Module und Schnittstellen beliebig erweitern und an die Bedürfnisse eines Unternehmens anpassen. Warum ist das wichtig? Weil ein ECM-System als zentrales Daten- und Informations-Repository des Unternehmens fungiert – als zentrale Stelle des betrieblichen Informationsmanagements – und damit auch pflege- und kostenintensive Insellösungen sowie ausufernde Admin-Arbeit überflüssig macht. Zahlreiche Workflows und Automatismen eines ECM-Systems sorgen für die Zusammenarbeit zwischen den Abteilungen – schnell, vollautomatisiert und ohne Medienbrüche. Die erforderlichen Informationen werden aus den Schnittstellen des ECM-Systems zu kaufmännischen Fachanwendungssystemen, Groupware, Anwendungen der Finanzbuchhaltung, ERP-Systemen sowie zu den Fachapplikationen generiert, können aber auch manuell eingegeben werden.

Einige ECM-Systeme bieten zusätzlich standardisierte Softwarelösungen für Fachbereiche an, beispielsweise für das Bewerbermanagement, das E-Mail-Management oder das Vertragsmanagement. In aller Regel basieren diese Lösungen auf Standardvorgaben, die aus Erfahrungen entstanden sind. Sie eignen sich daher für rund 90 % aller Anwender, ohne jegliche Anpassungsnotwendigkeit. Dies garantiert eine schnelle Projektumsetzung. Zudem sind sie bei empfehlenswerten ECM-Systemen wie aus einem Guss. Sie sind identisch aufgebaut und haben dieselben Strukturen.

Das heißt, wer das E-Mail-Management seines ECM-Systems nutzt, findet sich sofort in anderen Lösungen zurecht, beispielsweise in einer digitalen Personalakte. Wer eine Lösung versteht, kann mit allen anderen umgehen – ohne teuren Schulungsaufwand – und ohne die gewohnte Arbeitsumgebung des ECM-Systems zu verlassen. Das ist Anwendernutzen und Usability in Perfektion.
Ein ECM-System ist daher für Ihr Unternehmen ein echtes Win-win-System, mit dem Sie Kosten reduzieren, Mitarbeiter motivieren, Zeit sparen und Ressourcen schonen. Von den Umwelt- und Kostenaspekten dank Papiervermeidung einmal ganz abgesehen.

Die richtige Speicherlösung zur Datensicherung ist wichtig

Natürlich ist IT-Sicherheit nicht die Standardaufgabe einer ECM-Software. Der Hauptschutz ist in aller Regel vorgelagert, das IT-System wird beispielsweise über eine Firewall abgesichert, damit man nicht von außen auf das ECM-Archiv zugreifen kann. Unbefugte kommen daher leichter an Dokumente in einem nicht abgeschlossenen oder nicht gesicherten Personalbüro als über einen passwortgeschützten Personalrechner, der sich noch zusätzlich absichern lässt. Doch einen absoluten Schutz vor Cyberangriffen gibt es nicht, man kann es einem Hacker nur möglichst schwer machen, so schwer, dass sich sein Aufwand gemessen an der „Beute" nicht lohnt.

Hierzu gehört beispielsweise, die gespeicherten Daten auf einem speziellen Storage zu sichern, das die Unveränderbarkeit der Daten garantiert, weil das Storage beispielsweise die Verschlüsselungsversuche eines Erpressungstrojaners (Ransomware) gar nicht erst zulässt. Ein gutes ECM-System bietet hierfür passende Schnittstellen zu solchen Speicherlösungen an. Das Storage speichert dann kontinuierlich jede Veränderung auf dem Volume automatisch in einem separaten, vom Filesystem nicht zugänglichen Bereich ab. Sollte es einem Angreifer gelingen, Backups im Netzwerk zu kompromittieren, Daten zu verändern oder zu löschen, können Sie somit jederzeit zu vorherigen Versionen zurückkehren. Der Hacker konnte zwar eindringen, aber der Schaden hielt sich in Grenzen.

Aber Achtung: Ihr System war kompromittiert, Daten könnten bereits manipuliert sein, das bedeutet die Integrität der gespeicherten Informationen ist nicht mehr gewährleistet. Ihr System ist nicht mehr vertrauenswürdig.

Achten Sie also darauf, dass Ihre Daten möglichst in solch einem sicheren Storage abgelegt werden und nicht in Ihrem Filesystem. Dort wären Ihre Daten beispielsweise nach einem Angriff mit Ransomware verschlüsselt und nur noch gegen Lösegeld wieder zugänglich. Lassen Sie sich deshalb beim Kauf und Einrichten eines ECM-Systems zu den unterschiedlichen Speicherlösungen beraten. Bei hochsensiblen Daten lohnt sich ein sicheres Storage auf jeden Fall.

Checkliste:

Die richtige Software für Ihre IT-Sicherheit

Es hängt von Ihren Anforderungen ab, welches Konzept hinter der Sicherheit Ihrer IT steht. Aber bedenken Sie: Ihr Unternehmen entwickelt sich weiter! Achten Sie daher auf folgende Punkte, wenn Sie die Aspekte Datensicherheit und Datenschutz hinsichtlich eines ECM-Systems betrachten:

Eine gute ECM-Lösung sollte ...

- ☑ modular aufgebaut, skalierbar und zukunftssicher sein.
- ☑ alle rechtlichen Anforderungen beim Einsatz erfüllen.
- ☑ anwenderfreundlich und einfach zu verstehen sein (Usability).
- ☑ die Zusammenarbeit untereinander und mit anderen Abteilungen verbessern.
- ☑ schnelle, auch visualisierte Auswertungen ermöglichen.
- ☑ eine nahtlose Anbindung von Drittsystemen bieten.
- ☑ eine Langzeitarchivierung ermöglichen, beispielsweise auch durch Anbindungsmöglichkeiten moderner S3-Storage-Lösungen und/oder WORM-Storage-Lösungen.
- ☑ die Serverprozesse auf mehreren Hardwareplattformen verteilen können.
- ☑ auf Serverclustern einsetzbar sein.
- ☑ performante Suchfunktionen besitzen.
- ☑ eine optimale Integration in Microsoft Office bieten.
- ☑ über mobile Softwarelösungen für Smartphone, Tablet und den Zugriff über einen Webbrowser verfügen.

Fazit:

Ein ECM-System ist allen anderen Systemen überlegen

Wir haben gezeigt, dass IT-Sicherheit nicht die Standardaufgabe einer ECM-Software ist. Aber mit einer guten ECM-Lösung schlagen Sie gleich „mehrere Fliegen mit einer Klappe". Daher ist ein ECM-System allen anderen Lösungen überlegen.

Die Gründe liegen auf der Hand: Das Automatisieren der Unternehmensprozesse ist ein großer Mehrwert und im Zeitalter der Digitalisierung ein entscheidender Wettbewerbsvorteil. Treiber dieser Prozessdigitalisierung sind vor allem die unbedingt notwendige, ständige Verfügbarkeit aller Daten sowie die daraus entstehenden Kosten- und Effizienzvorteile. Moderne ECM-Lösungen lassen sich exakt an individuelle Unternehmensprozesse anpassen und mit im Unternehmen vorhandenen Softwarelösungen verzahnen. Dies senkt die Kosten, sorgt für schlanke Prozesse, transparente Abläufe und reduziert erheblich den administrativen Aufwand. Gleichzeitig sind Ihre Unternehmensdaten dank einer hochentwickelten Verschlüsselungstechnologie jederzeit sicher aufbewahrt. Zugriffskontrollen, Protokollierung und ein ausgefeiltes Berechtigungssystem sorgen für einen zusätzlichen Schutz. Die enthaltenen Werkzeuge zur Einhaltung gesetzlicher Anforderungen erleichtern und vereinfachen darüber hinaus nicht nur die gesetzlichen Anforderungen an Datenschutz und -sicherheit, sondern auch der GoBD sowie allen anderen Rechtsvorschriften zur digitalen Datenverarbeitung und Aufbewahrung.

Angesichts des bestehenden Transformationsdrucks (durch Digitalisierung, KI, Globalisierung etc.) ist ECM daher ein wichtiger, notwendiger Schritt, um als Unternehmen zukunftsfähig zu bleiben.

Whitepaper

Digital neu denken: IT-Sicherheit und modernes Informationsmanagement

AT THE HEART OF YOUR BUSINESS

Deutschland (Hauptsitz)
ELO Digital Office GmbH
www.elo.com/de/contact

Österreich
ELO Digital Office AT GmbH
www.elo.com/at/contact

Schweiz
ELO Digital Office CH AG
www.elo.com/ch/contact

Weltweit
Weitere Standorte
www.elo.com/de/locations