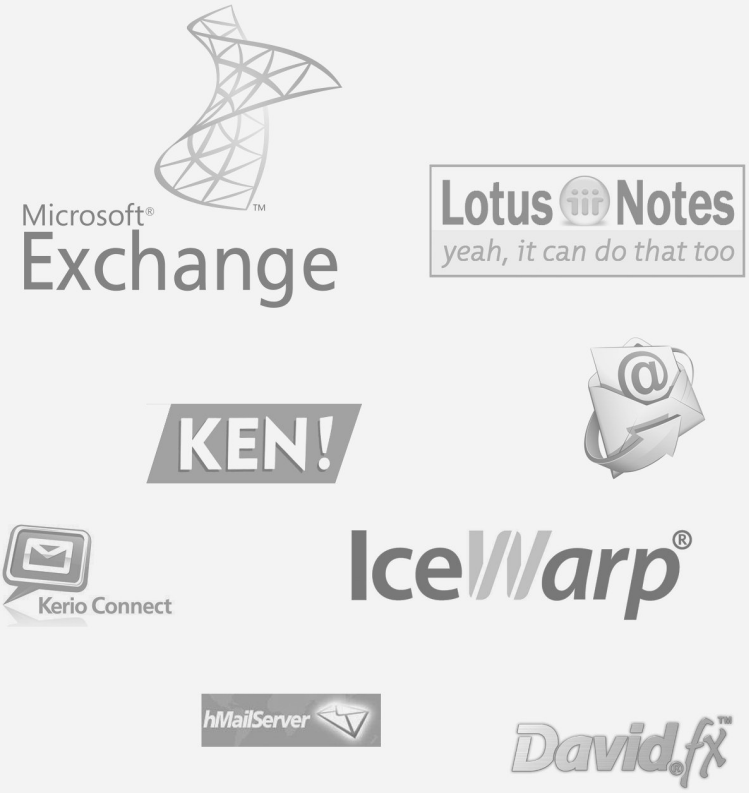
Stand: 14. November 2013

Leitfaden zur revisionssicheren und rechtskonformen E-Mail-Archivierung in Deutschland



In Unternehmen und Organisationen gewinnt E-Mail-Archivierung zunehmend an Bedeutung, denn sie bietet nicht nur eine Vielzahl an technischen und wirtschaftlichen Vorteilen, sie ist auch aus rechtlicher Sicht notwendig geworden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu aktuelle Richtlinen bereitgestellt, die ebenfalls berücksichtigt werden.

Sie erhalten damit einen übersichtlichen, aktuellen Leitfaden für den Einsatz von E-Mail-Archivierungsprodukten, der Ihnen technische, wirtschaftliche und gesetzliche Fragestellungen umfassend beantwortet.

SecurITy made in Germany

SECUREPOINT SECURITY SOLUTIONS

Einführung

In Unternehmen und Organisationen gewinnt die E-Mail-Archivierung zunehmend an Bedeutung, denn sie bietet nicht nur eine Vielzahl an technischen und wirtschaftlichen Vorteilen, sie ist auch aus rechtlicher Sicht eine Notwendigkeit geworden.

Welche Fragestellungen wichtig sind

Aber welche grundsätzlichen Fragen und Antworten ergeben sich für den Einsatz einer Archivierungslösung? Hier eine Einführung zu den wichtigsten und wesentlichen Bereichen:

1. Warum ist es sinnvoll zu archivieren?
2. Was muss archiviert werden?
3. Wie lange müssen Daten aufbewahrt werden?
4. Wer trägt die Verantwortung und was kann passieren, wenn nicht archiviert wird?
5. Welche Richtlinien gibt es dafür?
6. Gesetzliche Konflikte: Datenschutz versus E-Mail-Archivierung

1. Warum ist es sinnvoll zu archivieren?

E-Mails und die darin enthaltenen Dokumente und Kommunikation sind sehr wichtig für Unternehmen geworden, da sich mit der Zeit automatisch ein großer Wissens- und Datenpool in den Mailservern und in den Mitarbeitern-Accounts bildet.

Diese Daten dürfen einerseits nicht verloren gehen und sollte ein Verlust doch vorkommen, müssen sie schnell wieder herzustellen sein. Im Gegensatz zu einem Backup, muss eine Archivierungslösung nachweislich dafür sorgen, dass eine Manipulation der archivierten Daten nicht stattgefunden hat. Dies wird mit qualifizierten Zeitstempeln erreicht. Eine laufende Signierung des Zustandes der archivierten E-Mails mit qualifizierten Zeitstempeln sorgt für die Beweiswerterhaltung und garantiert selbst vor Gericht, dass keine Manipulation von archivierten Datenbeständen stattgefunden hat. Notwendig ist das aus rechtlicher Sicht, da sonst eine Beweisbarkeit – z. B. vor Gericht oder dem Finanzamt – nicht gegeben ist.

Des Weiteren ist auch ein schnelles Wiederfinden von Informationen wichtig, denn auch das kann ein normaler Mailserver/Mail-Client nur schlecht oder gar nicht leisten. Zudem sorgen die wachsenden Datenmengen für große Probleme auf Mailservern. Speicherkosten und Lizenzkosten steigen, da Accounts, die nicht mehr benötigt werden, trotzdem weiter gehalten werden müssen und der E-Mail-Verkehr stets zunimmt. Die Server und Clients werden immer langsamer und Informationen in riesigen E-Mail-Beständen zu finden, wird ebenfalls immer schwerer. Die Praxis zeigt: Anwender fangen in ihren Accounts dann oft an, Daten zu löschen und vernichten damit wichtige E-Mails und Dokumente, weil sie die Übersicht verloren haben. Aber auch ein kriminelles, absichtliches Löschen von E-Mails ist schon oft vorgekommen.

Rechtkonforme E-Mail-Archivierung? Warum?

Rechtskonforme E-Mail-Archivierung erfordert gesetzlich unveränderte und unveränderbare Speicherung über sehr lange Zeiten – zwei, sechs, zehn, 30 Jahre oder sogar ewig.

Eine Manipulation der Daten muss dabei ausgeschlossen sein. Viele Archivierungsprodukte erfüllen leider diese Anforderungen nicht und entsprechen damit nicht den Richtlinien (TR 03125) des Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die Rechtssicherheit im Sinne der Beweiswerterhaltung im Fall der Fälle vor Gericht, Finanzamt etc. geht damit verloren.
Die geltenden gesetzlichen Anforderungen schreiben jedoch den Einsatz einer revisionssicheren E-Mail-Archivierung zwingend und umfassend vor.

Prüfen Sie das in jedem Falle!

Bundesamt
für Sicherheit in der
Informationstechnik

2. Was muss archiviert werden?

Mailen ist eine rechtsrelevante Kommunikationsform geworden. E-Mails zu schreiben ist leicht, schnell und billig. So können z. B. Rechnungen, Angebote, Geschäftsbriefe und sonstige Dokumente sehr viel besser, schneller und kostengünstiger verschickt werden als per konventioneller Post. Die Ablösung des klassischen, schriftlichen Postversands ist durch den E-Mail-Verkehr inzwischen zu fast 75% ersetzt worden. Die Kommunikation mit Kunden oder Lieferanten, Buchführung, Personalsachen, medizinische Dokumentation, Akten der Verwaltung etc. all das unterliegt der Archivierungspflicht, denn inzwischen verlangen diverse Gesetze wie HGB, BGB, UStG etc. eine gesetzeskonforme Archivierung.

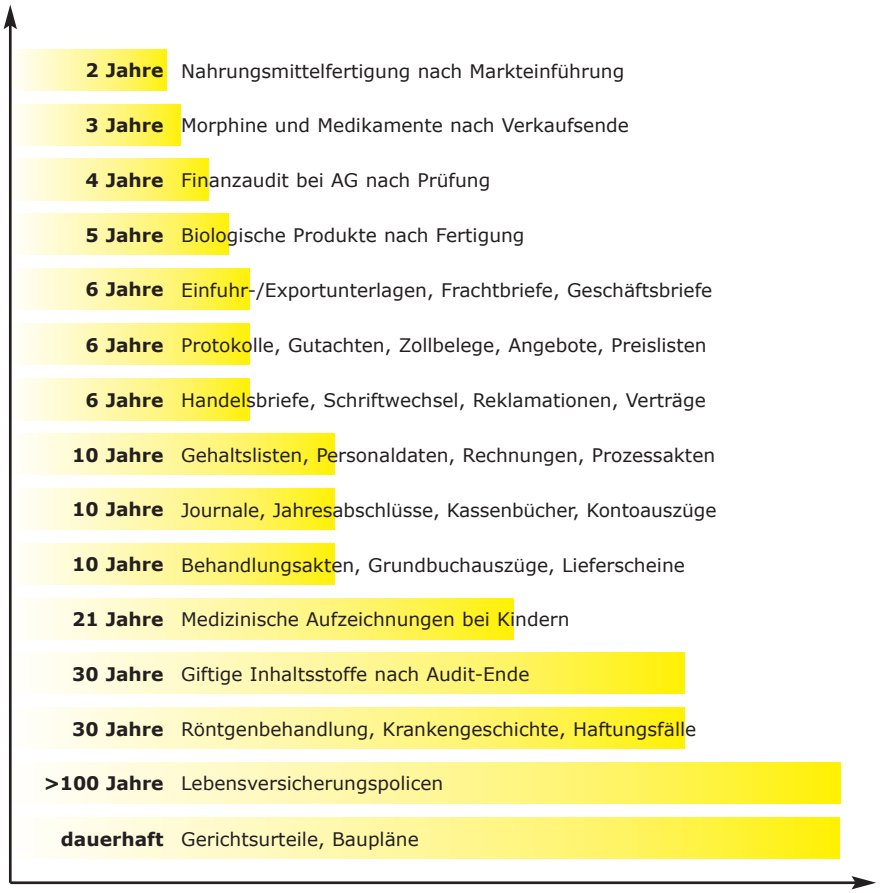
Konflikte mit Datenschutz

Nicht alle E-Mails müssen archiviert werden. Der Aufwand, zu Ermitteln was archivierungspflichtig ist oder was nicht, ist jedoch meist zu hoch.
Also wird in der Regel alles archiviert und das kann zu Konflikten mit anderen Gesetzen führen, siehe Seite 9

Anwendungsgebiete	Aufzubewahrende Dokumente	Rechtsgrundlage
Buchführung	– elektronische Rechungen – Handelsbücher – Handelsbriefe – Inventarverzeichnisse – Eröffnungsbilanzen – Jahresabschluss – Lagebericht – Konzernabschluss – Konzernlagebericht – Arbeitsanweisungen – Organisationsunterlagen – Buchungsbelege	§ 238 ff. HGB, § 140 AO, § 14b UStG
Personalsachen	– Kündigung, Auflösungsvertrag – Befristungsvereinbarung – Arbeitszeitnachweise – Lohn– und Berechnungsnachweis – Beschäftigungsverzeichnis – ärztliche Bescheinigung, Verzeichnis der Jugendlichen – Integrationsverzeichnis – Beschäftigungsverzeichnis – IOS-, EN-ISO-Normen, ASTM–Methoden – Zulassungsschein, Prüfbefunde – Wahlakten – Befristungsvereinbarung	§ 623 BGB § 2 Abs. 1 Satz 3 NachwG § 16 Abs. 2 ArbZG § 165 Abs. 4 Satz 2 SGB VII § 22 Abs. 3 LadenSchlussG, § 41 Abs. 1, 50 Abs. 2 JArbSchG, § 80 SGB IX, § 13 Abs. 4 Satz 1 und Satz 2 BiostoffVO, § 7 der 3. BImSchV, § 27 StrlSchVO, § 19 WO § 14 Abs. 4 TzBfG
Medizinische Dokumentation	– Arztliche Dokumentation: z. B. Arztbrief, Patientenkartei; Medikamentenverschreibung – Aufzeichnungen über Röntgenbehandlung: z. B. Röntgenaufzeichnungen, Röntgenbilder	Landesrechtliche Berufsordnungen für Arzte, z. B. § 10 Abs. 3 BerufsO Arzte Hessen § 28 Abs. 4 RöntgV
Bankunterlagen	– Vollständige Geschäftsdokumentation: vgl. HGB; z. B. Risikohandbücher – Identifizierungsunterlagen – Dokumente der Wertpapierdienstleistung: z. B. Aufträge	§ 25a Abs. 5 KWG § 9 GWG § 34 WpHG
Akten der Verwaltung	– Haushaltsplan – Haushaltsrechnung – Akten – Öffentlich-rechtliche Verträge – Unterlagen der öffentlich-rechtlichen Verwaltungstätigkeit	§ 33, 33a HGrG § 29 VwVfG § 57 VwVfG § 56 SGB X i.V.m § 3a Abs. 2 VwVfG § 110a SGB IV
Gerichtsakten	– vollständige Prozessakten – Schriftgut der Bundesgerichte und der Generalstaatsanwaltschaft: z. B. Aktenregister, Namensverzeichnis, Karteien (§ 1 Abs. 2 SchrAG)	§ 298a ZPO SchriftgutaufbewahrungsG

3. Wie lange müssen Daten aufbewahrt werden?

Gängige gesetzliche Aufbewahrungspflichten und -zeiten reichen je nach Dokumentenart von 2 Jahren bis ewig. Die Kommunikation mit Geschäftspartnern – dazu gehört jegliche Korrespondenz, durch die ein Geschäft vorbereitet, abgewickelt, abgeschlossen oder rückgängig gemacht wird – verlangt beispielsweise eine sechsjährige Archivierung. Rechnungen oder Personalakten dagegen müssen 10 Jahre archiviert werden. Gerichtsurteile und Baupläne müssen sogar dauerhaft aufbewahrt werden. Hier einige Beispiele für die Archivierung von unterschiedlichen Daten.



Wie sieht die Praxis aus?

In der Regel sollten E-Mails so archiviert werden, dass das Mindestaufbewahrungsdatum 10 Jahre beträgt. Im normalen Geschäftsbetrieb reicht das meist aus. Das Archivierungssystem sollte es aber zulassen, dass unterschiedliche Archivierungszeiträume gleichzeitig festgelegt werden können und E-Mails automatisch, durch von Ihnen festgelegte Regeln abgelegt bzw. kategorisiert werden können.

Achtung:
Sie sollen jedoch in bestimmten Berufsgruppen darauf achten, dass andere Aufbewahrungspflichten in der Regel vorkommen und Ihr Archvierungssystem eventuell entsprechend konfiguriert werden muss. Insbesondere Ärzte und Anwälte sind hiervon vermehrt betroffen.

4. Wer trägt die Verantwortung und was kann passieren, wenn nicht archiviert wird?

Der Verlust von Daten, durch Soft- oder Hardwarefehler oder auch durch absichtliche Löschung, kann geschäftskritisch, zu mindestens aber teuer oder kompliziert werden, sollten die Daten wiederhergestellt werden müssen. Manchmal ist ein Wiederherstellen aber auch nicht mehr möglich. Dabei reicht eine für IT-Systeme übliche Datensicherung/Backup nicht aus. Das Wiederherstellen von absichtlich oder aus Versehen gelöschten Emails ist hier nicht oder nur mit erhöhtem Aufwand möglich. Außerdem ist der Zeitraum auf den Sie zurückgreifen können meist viel zu gering. Wenn Sie beispielsweise am Ende eines zwei Jahre dauernden Projektes sich mit dem Kunden über den Projektumfang streiten, wird es keine passende Datensicherung mehr geben. Eine E-Mail-Archivierung hat dieses Problem nicht – E-Mails können direkt ohne Umwege gesucht, darauf sofort zugegriffen und diese wiederhergestellt werden. Es kommt oft vor, dass etwas nachvollzogen, verstanden, bearbeitet oder bewiesen werden muss. Im einfachsten Fall sollen versehentlich gelöschte E-Mails und Dokumente aus dem Archiv wiederhergestellt werden. Oder aber: Ein Mitarbeiter verlässt das Unternehmen und man muss sich in Projekte einarbeiten oder Aufträge nachvollziehen, Fehler oder Tätigkeiten Verantwortlichen zuordnen, dem Finanzamt oder dem Gericht Sachverhalten beweisen. Wichtig ist auch, dass Betriebe den unmittelbaren bzw. mittelbaren Zugriff seitens der Steuerbehörden langfristig sicherstellen müssen. Dies ist zwingend vorgeschrieben. Die Verantwortung liegt deshalb in jedem Fall bei einem EDV-Leiter, der das wissen sollte, und schlussendlich immer beim Geschäftsführer.

Geschäftsführerhaftung

Kommen Geschäftsführer den gesetzlichen Pflichten nicht nach, drohen in schweren Fällen und bei Schäden Geldbußen oder sogar Freiheitsstrafen.

5. Welche Richtlinien gibt es dafür?

Elektronische Dokumente wie E-Mails werden zunehmend papiergebundenen Dokumenten gleichgestellt. Eine Reihe von Gesetzen und Verordnungen stellen E-Mails bereits Briefen gleich. Verträge können per E-Mail geschlossen werden und die elektronische Post hat vor Gericht volle Beweiskraft erlangt. In Deutschland gibt es eine Reihe von Compliance-Anforderungen:

- HGB (Handelsgesetzbuch),
- AO (Abgabenordnung),
- GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
- Basel II
- sowie die TR 03125 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

All diese Gesetze und Verordnungen beeinflussen die Verwaltung von E-Mails. Wenn eine E-Mail eine elektronische Signatur mit qualifiziertem Zeitstempeln entsprechend dem Signaturgesetz trägt, wird sie als ein rechtsverbindliches Original betrachtet. Dementsprechend muss der Anwender sie zentral verwalten und langfristig sichern. Ebenso müssen steuerlich relevante, per E-Mail verschickte Informationen laut GDPdU in digitaler Form aufbewahrt werden. Qualifizierte Zeitstempel von einem Trustcenter sind deshalb für die Beweiswerterhaltung von archivierten Dokumenten unabdingbar. Da Verschlüsselungen mit der Zeit jedoch unsicher werden gehackt werden können und damit eine Manipulation von Daten in Zukunft möglich würde, ist es wichtig schon signierte Dokumente von Zeit zu Zeit wieder mit anderen, besseren kryptografischen Algorithmen neu zu signieren. Idealerweise und zur Sicherheit sollte dies in einer Archivierungslösung täglich und automatisch geschehen.

Wie sieht die Praxis aus?

Grundsätzlich müssen alle relevanten E-Mails und die Anhänge vollständig, manipulationssicher und jederzeit verfügbar archiviert werden. Die Daten müssen in dem Format vorliegen, in dem sie ursprünglich waren, d. h. ein Formatwechsel darf nicht stattgefunden haben. Gleichzeitig müssen sie maschinell auswertbar sein.

Anforderungen an eine revisionssichere E-Mail-Archivierung

Einen Leitfaden* stellen die Informationen des Verbandes Organisations- und Informationssysteme e.V. zur revisionssicheren elektronischen Archivierung dar:

- Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß aufbewahrt werden
- Die Archivierung hat vollständig zu erfolgen – kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren
- Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden
- Jedes Dokument darf nur von entsprechend berechtigten Benutzern eingesehen werden
- Jedes Dokument muss in angemessener Zeit wiedergefunden und reproduziert werden können
- Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist vernichtet, d. h. aus dem Archiv gelöscht werden
- Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden
- Das gesamte organisatorische und technische Verfahren der Archivierung muss von einem Sachverständigen Dritten jederzeit überprüftbar sein
- Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein

BSI-Richtlinie TR 03125

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu die technische BSI-Richtlinie TR 03125 zur Beweiswerterhaltung kryptographisch signierter Dokumente bereitgestellt. Diese beschreibt genau, wie E-Mails und andere elektronische Dokumente archiviert werden müssen, um den jetzigen und zukünftigen Erfordernissen des Gesetzgebers und der Beweiswerterhaltung zu genügen. Weiterführende Informationen zur Aufbewahrung elektronisch signierter Dokumente sind im Handlungsleitfaden des Bundesministeriums für Wirtschaft und Technologie beschrieben.

BSI-Richtlinie TR 03125

Siehe auch:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

Bundesamt für Sicherheit in der Informationstechnik

Handlungsleitfaden zur Aufbewahrung elektronisch signierter Dokumente

Im Verwaltungs- und Unternehmensbereich wird das Aufkommen elektronischer und elektronisch signierter Dokumente in den kommenden Jahren drastisch zunehmen. Die rechtsichere Behandlung dieser Dokumente wird hier näher erläutert:
http://www.securepoint.de/dokumente/BMWI_Leitfaden_zur_Aufbewahrung_elektronischer_und_elektronisch_signierter_Dokumente.pdf

Bundesministerium für Wirtschaft und Technologie

* Quelle: Verband Organisations- und Informationssysteme e.V. (VOI)

6. Gesetzliche Konflikte: Datenschutz versus E-Mail-Archivierung

Die Einführung einer Compliance in Verwaltungen, Organisationen und Unternehmen, mit deren Hilfe die gesetzlichen Anforderungen zur Aufbewahrung von E-Mails umgesetzt werden soll, kommt sehr oft in Konflikt mit anderen Gesetzen oder Richtlinien.

Fallstrick Betriebsvereinbarung zur privaten E-Mail-Nutzung

Es wird teilweise die Auffassung vertreten, dass eine private Nutzung des beruflichen E-Mail-Kontos nicht mit der Archivierung in einem Konflikt steht, wenn Mitarbeiter mittels einer Betriebsvereinbarung zugestimmt haben. Theoretisch ist das auch zutreffend. In der Praxis tauchen dann jedoch weitere Fallstricke auf, da Mitarbeiter zwar ihre eigenen durch das Fernmeldegeheimis geschützten Rechte abtreten können, jedoch nicht das Recht von externen Kommunikationspartnern, deren Kommunikation ja auch archiviert werden würde.

Private Inhalte in berufliche E-Mails

Auch berufliche E-Mails können datenschutzrechtlich relevante, personenbezogene Inhalte besitzen, denn eine berufliche E-Mail ist beispielsweise auch die Kommunikation eines Mitarbeiter mit einem Betriebsarzt.
Einige deutsche IT-Rechtler vertreten jedoch die Auffassung, dass bei einer Interessenabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem „Schutz des eingerichteten und ausgeübten Gewerbebetriebes des Arbeitgebers" (Art. 14 I GG) letzterer obsiegt. Der Begriff der „Erforderlichkeit" (§ 32 BDSG) spielt hierbei eine wichtige Rolle. Denn aufgrund der zahlreichen Gesetze und Vorschriften besteht eben nicht nur ein Interesse, sondern geradezu die Pflicht zur Archivierung. Allerdings muss der Arbeitgeber unbedingt seiner Informationspflicht über die E-Mail-Archivierung gemäß § 4 III BDSG nachkommen und alle Mitarbeiter vor der Implementation einer Archivierungslösung informieren.

Automatische Archivierung aller E-Mails und private Nutzung

Es wäre praxisfremd alle ein- und ausgehenden E-Mails dahingehend zu überprüfen, ob sie archivierungspflichtig oder nicht archivierungspflichtige sind. Da die Archivierung jedoch vollständig sein muss, ist die sofortige und automatische Archivierung bei Ein- und Ausgang zu gewährleisten, um mögliche Manipulationen zu unterbinden. Diese Archivierungsstrategie kann aber in Konflikt mit den Datenschutzrichtlinien sein. Ist Mitarbeitern z. B. die private E-Mail-Nutzung gestattet, unterliegt der Arbeitgeber als Telekommunikationsanbieter dem Bundesdatenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG).

Untersagung der privaten E-Mail-Nutzung

Aus vorgenannten Gründen und den Konflikten mit anderen Gesetzen sowie dem Datenschutz sollte die Nutzung des beruflichen E-Mail-Kontos für private Zwecke explizit untersagt werden. Dies muss mit dem Mitarbeiter besprochen und schriftlich fixiert werden. Die Kontrolle ist ebenfalls notwendig, um rechtlichen Bestand zu haben.

Best Practice/Lösung:

Nach Abwägung aller Möglichkeiten und den rechtlichen Problembereichen ist das Verbot der privaten Nutzung von beruflichen E-Mail-Konten der einzig gangbare Weg, um Konflikte zwischen Datenschutz und der gesetzlich vorgeschriebenen Archivierung von E-Mails zu vermeiden. Dies ist in der Praxis auch immer leichter für Ihre Mitarbeiter umzusetzen, da sich Smartphones und Tablets im Privatbereich durchgesetzt haben, diese auch in der Firma verwendet werden und so Mitarbeiter sowieso jederzeit privat kommunizieren können.

Leitfaden zum Thema E-Mail-Archivierung

Securepoint Unified Mail Archive: Rechtssicher. Revisionssicher. Vertrauenswürdig.

Rechtskonforme E-Mail-Archivierung erfordert gesetzlich unveränderte und unveränderbare Speicherung über sehr lange Zeiten – zwei, sechs, zehn, 30 Jahre oder sogar ewig. Die Bedeutung der E-Mail-Archivierung geht damit schon lange über die Entlastung Ihres Mailservers hinaus. Das Securepoint Unified Mail Archive (UMA) bietet eine effiziente Möglichkeit zur permanenten Archivierung der E-Mails. Es werden die komplexen Anforderungen des Gesetzgebers erfüllt. Die Archivierung erfolgt gesetzeskonform, revisionssicher und automatisch nach GDPdU und nach der Technischen Richtlinie 03125 des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Übersicht:

- 100-prozentige Archivierung aller ein-/ausgehenden und internen E-Mails für beliebig lange Zeiträume und nach einfach festzulegenden Regeln
- Indizierung von E-Mails
- Indizierung von an E-Mails angehängte Dokumente (diese können getrennt durchsucht werden).
- OCR von Bildern und Scanns
- Gesetzeskonforme, revisionssichere und automatische Archivierung des E-Mail-Verkehrs nach GDPdU und der aktuellen Technischen Richtlinie 03125 des BSI. UMA enthält Governikus LZA, einen Archivierungsstandard in vielen deutschen Behörden
- Performante Aufbewahrung und Prüfung elektronischer und elektronisch signierter Dokumente
- Sicherer Schutz vor Rechtsnachteilen wie z. B. steuerlichen Schätzungen, Beweisverlusten, Gutachten, Prozessen etc.
- zur Beweiswerterhaltung mit Qualifizierten Zeitstempeln; automatisches tägliches Signieren von E-Mails nach den neustens kryptografischen Methoden zu Beweiswerterhaltung
- Einfaches Wiederfinden und Wiederherstellung von versehentlich oder absichtlich gelöschten E-Mails
- Entlastung Ihres bestehenden E-Mailservers
- Kostengünstiger, vollautomatischer und einfacher Betrieb
- Verfügbar als Cloud-, VM- und Appliance-Version

Governikus LZA

SecurITy made in Germany

Securepoint GmbH, Salzstraße 1, 21335 Lüneburg
Tel.: 0 41 31 / 24 01-0, Fax: 0 41 31 / 24 01-50
Email: info@securepoint.de
Internet: www.securepoint.de

SECUREPOINT SECURITY SOLUTIONS