

VICARDION®

Das 1x1 der E-Mail-Archivierung

Was Sie bei der Anschaffung und Einführung einer E-Mail-Archivierungslösung unbedingt beachten müssen

VICARDION GbR
Karl-Wirth-Str. 10
76694 Forst

+49 (0) 7251 32658 0
info@vicardion.de
www.vicardion.de

Autor(en):

Eduard Schwab

Stand:

Oktober 2022

Version:

2.0.0

Inhaltsverzeichnis

EINLEITUNG	2
VORTEILE EINER E-MAIL-ARCHIVIERUNG	2
GESETZLICHE GRUNDLAGEN	3
GESETZE UND GELTENDE REGELN	3
WELCHE DOKUMENTE UNTERLIEGEN DER ARCHIVIERUNGSPFLICHT?	4
WIE LANGE MÜSSEN DIE DATEN AUFBEWAHRT WERDEN?	6
ORGANISATORISCHE ASPEKTE	6
ORGANISATORISCHE HERAUSFORDERUNGEN	7
LÖSUNGSANSÄTZE	7
TECHNISCHE ASPEKTE	8
UNTERSTÜTZTE E-MAIL-SERVER	8
BEREITSTELLUNGSARTEN DER LÖSUNGEN	8
GRUNDSATZENTSCHEIDUNGEN	9
INTEGRATIONSVARIANTEN	9
HUB-MODUS	9
TRANSPARENTER MODUS	10
ARCHIVSPEICHER	10
RAID-UNTERSTÜTZUNG	10
SPEICHERKAPAZITÄT	11
WORAUF IST SONST NOCH ZU ACHTEN?	12

Einleitung

Die E-Mail-Archivierung ist sowohl aus technischer als auch aus organisatorischer Sicht sehr sinnvoll und hilfreich. Darüber hinaus machen gleich mehrere Gesetze und Verordnungen das Thema „E-Mail-Archivierung“ quasi zu einer Pflicht.

Doch bereits bei der Anschaffung einer Lösung gilt es einiges zu beachten. Das betrifft auch die Vorbereitung des Projekts sowie die finale Einführung der Lösung in das bestehende Unternehmensnetzwerk. Beachtet man jedoch einige wichtige Aspekte, so wird die Einführung einer professionellen und revisionssicheren E-Mail-Archivierungslösung garantiert zu einem Erfolg.

Dieses Dokument informiert über Punkte und Aspekte, die bei der Anschaffung, Einführung und beim Betrieb einer E-Mail-Archivierungslösung wichtig sind und daher Beachtung finden sollten.

Die in diesem Dokument enthaltenen Informationen ersetzen keine Rechtsberatung. Alle rechtlichen Angaben sind ohne Gewähr. Lassen Sie sich in rechtlichen Fragen von einem Juristen beraten.

Vorteile einer E-Mail-Archivierung

Heutzutage sind die Postfächer voll mit wichtigen und meistens auch sehr sensiblen Informationen. Die Praxis zeigt, dass die Postfächer oftmals gar keine Speicherplatzbegrenzung haben und somit E-Mails der letzten 5-10 Jahre beinhalten. Häufig haben Daten mit einem Alter von bis zu zwei Jahren auch noch Relevanz in der täglichen Arbeit des jeweiligen Postfachbesitzers. All diese Daten können gelöscht sowie manipuliert werden oder durch eine Störung bzw. einen Sicherheitsvorfall verloren gehen. Somit gehört die Sicherheit der Emails, die Entlastung des E-Mail-servers und die manipulationssichere Aufbewahrung sowie einfache Wiederherstellung der E-Mails inkl. aller Anhänge mit zu den bedeutendsten Vorteilen einer guten E-Mail-Archivierung.

Da die E-Mails und vor allem deren Anhänge vom Gesetzgeber als echte Dokumente angesehen werden, greift u.a. auch die Regelung für diverse Aufbewahrungsfristen. Die Pflichten lassen sich mit einer gesetzeskonformen E-Mail-Archivierung ebenfalls ganz einfach erfüllen.

Zusätzlich bieten gute Lösungen den Benutzern einen einfachen Zugriff inkl. einer guten Suchfunktion auf eigene historische Daten ohne dass diese bewusst oder versehentlich gelöscht oder manipuliert werden können.

Je nach Unternehmen und Organisation kommt es aber auch vor, dass E-Mails zu früh oder zu unüberlegt gelöscht und somit wichtige Daten vernichtet werden. Da die E-Mails bereits archiviert sind ist dieser Vorgang nicht mehr von Bedeutung. Darüber hinaus stehen die Daten im E-Mail-Archiv nicht nur unverfälscht, sondern zeitlich gesehen auch länger zur Verfügung als gewöhnliche Backupdaten.

Gesetzliche Grundlagen

Der Unterschied zwischen elektronischen Dokumenten wie z.B. E-Mails und Dokumenten in Papierform wird immer kleiner. Mittlerweile hat die elektronische Post vor Gericht die volle Beweiskraft erlangt. E-Mails und deren Anhänge, die elektronische Signaturen mit qualifizierten Zeitstempeln tragen, werden als rechtsverbindliche Originale angesehen.

Gesetze und geltende Regeln

Folgende Gesetze und Regeln sind rund um das Thema E-Mail und E-Mail-Archivierung erwähnenswert bzw. müssen unbedingt beachtet werden:

- HGB (Handelsgesetzbuch)
- AO (Abgabenordnung)
- Basel II
- TR 03125 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)

Die GoBD wurde zum 01.01.2017 verschärft und besagt, dass alle geschäftsrelevanten elektronischen Dokumente wie **Rechnungen, Verträge, Angebote und Korrespondenzen** nach den entsprechenden Grundsätzen eine bestimmte Zeit lang aufbewahrt werden müssen. Dabei hängt die Aufbewahrungsfrist maßgeblich von der Branche und dem Tätigkeitsumfeld ab.

Welche Dokumente unterliegen der Archivierungspflicht?

Sämtliche Kommunikation mit Kunden, Partnern und Lieferanten aber auch Buchführung, Unterlagen aus dem Personalwesen, medizinische Dokumente sowie Akten in Verwaltungsämtern unterliegen der Archivierungspflicht.

Anwendungsgebiete	Aufzubewahrende Dokumente	Rechtsgrundlage
Buchführung	▪ Elektronische Rechnungen	§ 238 ff. HGB
	▪ Handelsbücher	§ 140 AO
	▪ Handelsbriefe	§ 14b UStG
	▪ Inventarverzeichnisse	
	▪ Eröffnungsbilanzen	
	▪ Jahresabschluss	
	▪ Lagebericht	
	▪ Konzernabschluss	
	▪ Konzernlagebericht	
	▪ Arbeitsanweisungen	
	▪ Organisationsunterlagen	
	▪ Buchungsbelege	
Personalsachen	▪ Kündigung, Auflösungsvertrag	§ 623 BGB § 2 Abs. 1 Satz 3 NachwG
	▪ Befristungsvereinbarung	§ 16
	▪ Arbeitszeitnachweise	Abs. 2 ArbZG
	▪ Lohn und Berechnungsnachweis	§ 165 Abs. 4 Satz 2 SGB VII § 22 Abs. 3 LadenSchlussG
	▪ Beschäftigungsverzeichnis	§ 41 Abs. 1, 50 Abs.
	▪ Ärztliche Bescheinigung, Verzeichnis der Jugendlichen	2 JArbSchG § 80 SGB IX § 13 Abs.
	▪ Integrationsverzeichnis	4 Satz 1 und Satz 2
	▪ Beschäftigungsverzeichnis	BiostoffVO
	▪ IOS, EN-ISO-Normen, ASTM-Methoden	§ 7 der 3. BImSchV § 27 StrlSchVO
	▪ Zulassungsschein, Prüfbefunde	§ 19 WO § 14 Abs. 4 TzBfG
	▪ Wahlakten	
	▪ Befristungsvereinbarung	

Anwendungsgebiete	Aufzubewahrende Dokumente	Rechtsgrundlage
Medizinische Dokumentation	<ul style="list-style-type: none"> ▪ Ärztliche Dokumentation: z. B. Arztbrief, Patientenkartei, Medikamentenverschreibung ▪ Aufzeichnungen über Röntgenbehandlung: z. B. Röntgenaufzeichnungen, Röntgenbilder 	<p>Landesrechtliche Berufsordnungen Für Ärzte z.B. § 10 Abs. 3 BerufsO Ärzte Hessen § 28 Abs. 4 RöntgV</p>
Bankunterlagen	<ul style="list-style-type: none"> ▪ Vollständige Geschäftsdokumentation: vgl. HGB; z. B. Risikohandbücher ▪ Identifizierungsunterlagen ▪ Dokumente der Wertpapierdienstleistung: z. B. Aufträge 	<p>§ 25a Abs. 5 KWG § 9 GWG § 34 WpHG</p>
Akten der Verwaltung	<ul style="list-style-type: none"> ▪ Haushaltsplan ▪ Haushaltsrechnung ▪ Akten ▪ Öffentlich-rechtliche Verträge ▪ Unterlagen der öffentlich-rechtlichen Verwaltungstätigkeit 	<p>§ 33, 33a HGrG § 29 VwVfG § 57 VwVfG § 56 SGB X i.V.m § 3a Abs. 2 VwVfG § 110a SGB IV</p>
Gerichtsakten	<ul style="list-style-type: none"> ▪ Vollständige Prozessakten ▪ Schriftgut der Bundesgerichte und der Generalstaatsanwaltschaft: z. B. Aktenregister, Namensverzeichnis, Karteien (§ 1 Abs. 2 SchrAG) 	<p>§ 298a ZPO SchriftgutaufbewahrungsgG</p>

Tabelle 1: Archivierungspflichtige Dokumente

Wie lange müssen die Daten aufbewahrt werden?

Die Aufbewahrungspflicht reicht je nach Dokumentenart von zwei Jahren bis „uneingeschränkt“ wobei uneingeschränkt eine endlose Aufbewahrungspflicht nach sich zieht. Für die meisten Unternehmen sind ein 6-Jähriges Standard- und ein 10-jähriges Langzeitarchiv jedoch ausreichend.

Aufbewahrungsdauer	Dokumentenart
2 Jahre	Nahrungsmittelfertigung nach der Markteinführung
3 Jahre	Morphine und Medikamente nach Verkaufsende
4 Jahre	Finanzaudit bei AG nach der Prüfung
5 Jahre	Biologische Produkte nach der Fertigung
6 Jahre	Handelsbriefe, Schriftwechsel, Reklamationen, Verträge, Protokolle, Gutachten, Zollbelege, Angebote, Preislisten, Einfuhr-/ Exportunterlagen, Frachtbriefe, Geschäftsbriefe
10 Jahre	Behandlungsakten, Grundbuchauszüge, Lieferscheine, Journale, Jahresabschlüsse, Kassenbücher, Kontoauszüge, Gehaltslisten, Personaldaten, Rechnungen, Prozessakten
21 Jahre	Medizinische Aufzeichnungen bei Kindern
30 Jahre	Röntgenbehandlungen, Krankengeschichte, Haftungsfälle
100 Jahre	Lebensversicherungspolicen
dauerhaft	Gerichtsurteile, Baupläne

Tabelle 2: Übersicht Aufbewahrungsdauer

Organisatorische Aspekte

Sicherlich müssen nicht alle E-Mails archiviert werden. Doch der Aufwand die zu archivierenden von den nicht zu archivierenden E-Mails zu trennen ist einfach zu groß. Daher ist die Archivierung aller E-Mails gängige Praxis. Jedoch bringt dies wiederum Überschneidungen mit anderen Gesetzen sowie einige Herausforderungen mit sich.

Organisatorische Herausforderungen

- Häufig befinden sich auch unerwünschte E-Mails wie z.B. Spam-Mails in den jeweiligen Benutzerpostfächern. Die automatische Archivierung aller E-Mails übernimmt auch diese E-Mails ins Archiv. Dies verschwendet den Archivspeicher und verursacht dadurch zusätzliche Kosten.
- Es kommt sehr häufig vor, dass die geschäftlichen E-Mail-Postfächer von den Mitarbeitern auch für private Angelegenheiten genutzt werden. Archiviert ein Unternehmen die privaten E-Mails der Mitarbeiter, so tritt es gegenüber den Mitarbeitern ungewollt als Serviceprovider auf. Als Serviceprovider unterliegt das jeweilige Unternehmen plötzlich dem Bundes Datenschutzgesetz (BDSG) sowie dem Telekommunikationsgesetz (TKG) und muss die Datenschutzrechte der Mitarbeiter wahren. Mitarbeiter können z.B. beim Verlassen des Unternehmens auf die Löschung der privaten E-Mails vergangener Jahre bestehen.
- Darüber hinaus gibt es vereinzelt geschäftliche E-Mails die ebenfalls nicht archiviert werden dürfen. Dazu zählen per E-Mail eingegangene Bewerbungen die bei Ablehnung nicht archiviert werden dürfen sondern innerhalb einer bestimmten Zeit gelöscht werden müssen. Ähnliches gilt auch für Mails an den Betriebsrat oder den Betriebsarzt.
- Admin-Postfächer bekommen häufig viele Systemmeldungen. Diese zu archivieren ist nicht nur sinnlos, sondern auch eine Speicherplatzverschwendung.

Lösungsansätze

- Um die Spam-Mails nicht archivieren zu müssen, muss dafür gesorgt werden, dass diese erst gar nicht angenommen, sondern vor der Annahme vom Sicherheitssystem abgelehnt werden. Hierfür gibt es bereits sehr gute E-Mail-Sicherheitslösungen am Markt die sehr effektiv vor Spam-Mails schützen, indem sie diese vor der Annahme gleich ablehnen. Jedes Unternehmen das mehr als 2-10% Spam-Mail-Anteil hat, sollte seine Sicherheitslösung optimieren oder überdenken und ersetzen.
- Die wohl einfachste Lösung des Problems mit den privaten E-Mails ist, die private Nutzung der geschäftlichen Postfächer per Betriebsvereinbarung zu untersagen. Da die Mitarbeiter nach dem ausgesprochenen Verbot in der Regel aber keinen direkten Einfluss mehr auf den Empfang privater E-Mails haben, müssen diese zumindest über die Einführung einer E-Mail-Archivierungslösung und die Folgen informiert werden. Grundsätzlich sagt man, dass der Schutz des Gewerbebetriebes mit allen seinen Pflichten die Datenschutzrechte der Mitarbeiter im Zweifel überwiegt.
- Um dem Problem der Archivierung spezieller geschäftlicher E-Mails aus dem Weg zu gehen, müssen extra Sammelpostfächer eingerichtet und von der Archivierung

ausgeschlossen werden. Darüber hinaus muss eine Regelung geschaffen werden, die eine Nutzung dieser speziellen Postfächer für die speziellen Aufgaben vorschreibt. Somit dürfen z.B. die Bewerbungen nur über `bewerbungen@beispieldomain.de` angenommen werden. Kommen die Bewerbungen im Postfach `personal@beispieldomain.de` an, so müssen diese an das Bewerbungspostfach weitergeleitet und aus dem Personalpostfach umgehend gelöscht werden.

- Auch für die Status- und Systemmeldungen empfiehlt es sich ein extra Postfach anzulegen und von der Archivierung auszuschließen.

Technische Aspekte

Aus der technischen Sicht muss bei der Wahl der E-Mail-Archivierungslösung ebenfalls einiges beachtet werden.

Unterstützte E-Mail-Server

Auch wenn die meisten Unternehmen einen Microsoft Exchange Server im Einsatz haben, trifft man in der Praxis auch auf Lotus Notes, Open Xchange sowie Kerio E-Mail-Server. Somit ist der Einsatz des Microsoft Exchange Servers längst nicht mehr selbstverständlich. Hinzu kommt, dass die E-Mail-Archivierungslösung für eine Laufzeit von mindestens 5 bis 10 Jahren geplant wird. Um eine möglichst zukunftsichere Entscheidung treffen zu können, muss man darauf achten, dass die E-Mail-Archivierungslösung alle gängigen E-Mail-Server unterstützt. Darüber hinaus muss die Lösung die gängigen E-Mail-Protokolle unterstützen. Gerade wenn das Unternehmen cloudbasierte E-Mail-Dienste nutzt oder die Nutzung solcher für die Zukunft nicht ausschließt muss die Lösung neben SMTP auch POP3 bzw. IMAP unterstützen.

Bereitstellungsarten der Lösungen

Eine moderne sowie zukunftsichere E-Mail-Archivierungslösung muss in mehreren Varianten zur Verfügung stehen. In Form einer Hardwarelösung, als Software zum Betrieb auf einer beliebigen Hardware oder als eine virtuelle Maschine basierend auf den gängigsten Hypervisoren wie z.B. VM Ware ESXi oder Microsoft HyperV.

Grundsatzentscheidungen

Vor der Einführung der Lösung muss man sich überlegen, ob die Archivierung ab einem bestimmten Zeitpunkt, also kurz nach der Einführung der Lösung beginnt oder ob zuerst der bereits vorhandene Inhalt bestehender Postfächer ins Archiv übertragen werden soll. Dies hat wiederum direkte Auswirkungen auf die Planung des Archivspeicherplatzes sowie auf die Projektdauer. Die Übernahme alter E-Mails ist je nach Zustand der Daten nicht immer reibungslos möglich. Daher ist es vorteilhaft, wenn der Hersteller für den Transfer der Daten entsprechende Tools oder Funktionen zur Verfügung stellt.

Integrationsvarianten

Grundsätzlich lässt sich ein E-Mail-Archiv auf unterschiedliche Arten in ein bestehendes Netzwerk integrieren.

Hub-Modus

Bei dieser Variante wird das E-Mail-Archiv parallel zum E-Mail-Server installiert. Dabei wird auf dem E-Mail-Server ein Journal-Postfach angelegt. Eine Journalregel sorgt dafür, dass für alle eingehenden und ausgehenden E-Mails noch vor der Zustellung eine Kopie in dem Journal-Postfach abgelegt wird. Ein Agent des E-Mail-Archivs holt sich die E-Mail-Kopien dort ab, versieht diese mit einer Signatur, verschlüsselt diese und speichert sie revisionssicher in einem Archiv. Um den E-Mail-Server zu entlasten, werden nach einer erfolgreichen Archivierung die Kopien vom Journal-Postfach automatisch wieder gelöscht.

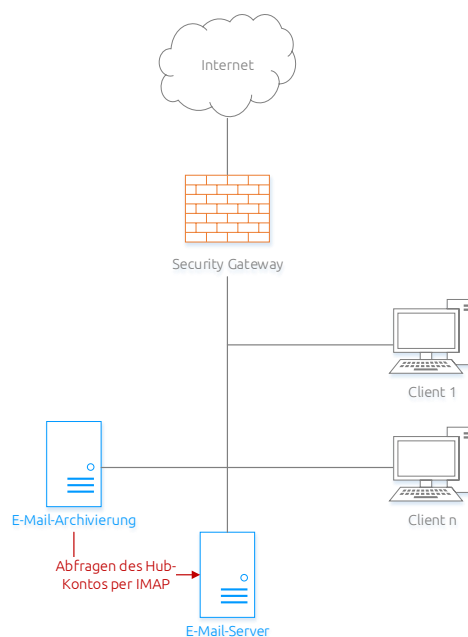


Abbildung 1: Darstellung des Hub-Modus

Transparenter Modus

Neben der Implementierung des E-Mail-Archivs im Hub Modus lässt sich dieses auch im sogenannten transparenten Modus installieren. Hierbei durchlaufen alle Mails zunächst die Archiv-Appliance, werden revisionssicher im Standard-/Langzeitarchiv gespeichert und danach an den E-Mail-Server weitergeleitet. Diese Implementierungsvariante ist aber äußerst selten und nur in besonderen Ausnahmefällen zu empfehlen.

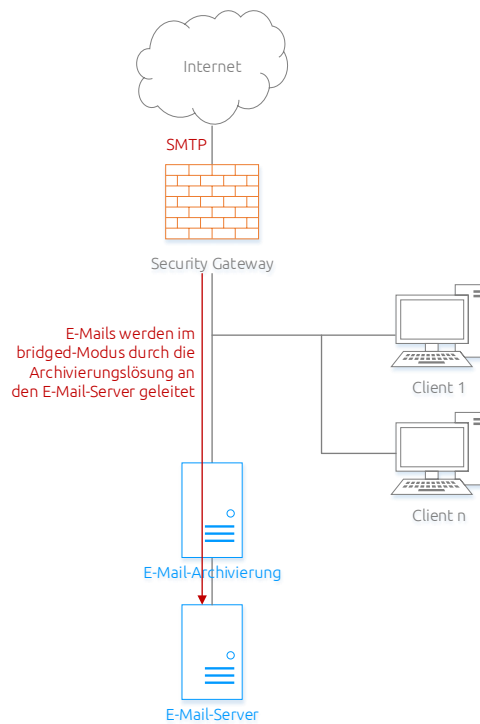


Abbildung 2: Darstellung des Transport-Modus

Archivspeicher

Auch bei der Gestaltung des Archivspeicherplatzes muss einiges bedacht werden.

RAID-Unterstützung

Unabhängig vom Hersteller und von der Bereitstellungsart (Hardware, Software, virtuell) muss es möglich sein das Archiv in einem RAID-Verbund zu betreiben. Gute E-Mail-Archivierungslösungen verfügen standradmäßig über Soft- oder Hardware RAID-Controller. Je nach Anzahl der Festplatten können unterschiedliche RAID-Level eingestellt werden:

Anzahl HDDs	Größe je HDD	RAID-Level	Speicherkapazität
2	1 TB	RAID 1	1 TB
3	1 TB	RAID 5	2 TB
4	1 TB	RAID 6	2 TB

Tabelle 3: Übersicht RAID-Level

Beim Betrieb der Lösung als virtuelle Maschine auf eigener Hardware und einem eigenen Hypervisor, muss die Bereitstellung und Einbindung des Speichers entsprechend bedacht und eingeplant werden.

Speicherkapazität

Im Allgemeinen geht man davon aus, dass der Archivspeicherplatz für 5 bis 10 Jahre ausreichen muss. Danach wird die Hardware getauscht oder es finden sonstige Modernisierungsmaßnahmen statt. Somit sollte der Speicherbedarf von vorne herein so kalkuliert werden, dass er auch tatsächlich für einen dauerhaften Betrieb ausreicht. Denn die Erweiterung der Speicherkapazität während der Lebenszeit des Archivs ist aufwändiger und teurer als die Einplanung einer Reserve. Hierbei muss auch beachtet werden, dass ein Teil der Speicherkapazität für das System, die Logfiles, die Verschlüsselung und ähnliche Systemressourcen benötigt wird. Somit bleiben von der Gesamtspeicherkapazität je nach Lösung ca. 85% für das eigentliche E-Mail-Archiv übrig.

Berechnung der Speicherkapazität

Zur Berechnung der Speicherkapazität sollte zunächst ein Faktencheck stattfinden, um folgende Punkte zu ermitteln:

- Sollen Bestandsdaten zu Beginn des Projekts in das neue Archiv importiert werden? Wenn ja, wie groß ist das Datenvolumen?
- Wie hoch ist der durchschnittliche Zuwachs an Daten pro Jahr?
- Wie lange soll die Lösung im Einsatz bleiben bevor diese erneuert wird (meistens 5 Jahre)?
- Welcher Puffer soll einkalkuliert werden (neue Mitarbeiter, erhöhtes E-Mail-Aufkommen, etc.)?

Daraus lässt sich ganz allgemein folgende Formel zur Berechnung der Speicherkapazität ableiten:

$$\text{Netto-Speicherbedarf} = \text{Importdaten} + \text{jährlicher Datenzuwachs} * 1,5 * \text{Laufzeit}$$

Der Faktor 1,5 stellt 50% Puffer für den jährlichen Zuwachs an Daten dar. Zusätzlich kommt noch der serverbezogene Speicherbedarf wie z.B. die Metadaten, Indexdatenbanken für die Suche und Speicherbedarf für Systemaktualisierungen hinzu.

Was technisch sonst noch wichtig ist

- Ausgereifte Benutzerverwaltung und AD-Integration.
- Einfacher Backup des gesamten Archivs. Wichtig bei Hardwareproblemen oder bei Erneuerung der Hardware.
- Das Archivierungssystem muss in der Lage sein systemintern automatisch die erforderlichen Benutzerpostfächer anzulegen in die die zu archivierenden E-Mails abgelegt werden können.
- Einfache, plattformunabhängige und manipulationssichere Suchfunktion für Mitarbeiter und Revisoren (Wirtschaftsprüfer).
- Performante Hardware, die nach Jahren selbst mit großen Datenmengen noch klarkommt.
- Mehrere Zugriffsmöglichkeiten Web GUI, Mail Clients, Outlook Plug-Ins, etc.
- Einfache Administration - die Lösung muss im Optimalfall ein „wartungsarmer Selbstläufer“ sein.

Worauf ist sonst noch zu achten?

Beachtet man möglichst viele der beschriebenen Anmerkungen, ist man mit der Wahl einer Lösung die solche Punkte erfüllt auf der sicheren Seite. Ist die Lösung darüber hinaus z.B. vom BSI zertifiziert und als revisionssicher anerkannt so erfüllt man auch noch alle aktuell geltenden Regeln und Gesetze. Ein inländischer Support mit kurzen Reaktionszeiten rundet das Anforderungsprofil einer guten Lösung ab und macht die Wahl perfekt.