



**HORNETSECURITY®**



# AETERNUM

Whitepaper

---

[www.hornetsecurity.com](http://www.hornetsecurity.com)

SIMPLY GOOD NEWS



---

<b>1 Problemstellung E-Mail Archiv .....</b>	<b>5</b>
1.1 Einleitung .....	5
1.2 Gründe für E-Mail Archivierung .....	5
1.2.2 Compliance – Erfüllung rechtlicher Anforderungen .....	6
1.2.3 Entlastung der Infrastruktur .....	6
1.3 Anforderungen an E-Mail Archivierung .....	7
1.3.1 Revisionssichere Speicherung .....	7
1.3.2 Datenschutz .....	8
1.3.3 Prüfzugang .....	9
1.3.4 Technische Anforderungen .....	10
1.4 Situation in Unternehmen .....	11
<b>2 Hornetsecurity Aeternum .....</b>	<b>12</b>
2.1 Cloud Architektur .....	12
2.2 Weg in das Archiv – Anbindung an Mailserver .....	14
2.3 Interner Aufbau / Architektur und Abläufe .....	15
2.4 Indizierung und Suche .....	16
2.5 Control Panel .....	17
2.6 Outlook Add-In .....	19
2.7 Aeternum App .....	20
2.8 Zugriff per Browser .....	21
2.9 Revisionszugang .....	21
2.10 Audit Log .....	23
2.11 Anpassung an eigenes Corporate Design .....	24
2.12 Import und Export von Daten .....	24
2.13 Leistungen im Überblick .....	25
<b>3 Optionale Leistungen und Services .....</b>	<b>25</b>
3.1 Spamfilter .....	25
3.2 Managed Archive Appliance .....	26
3.3 E-Mail Verschlüsselung .....	26
<b>4 Application Programming Interface (API) .....</b>	<b>27</b>



---

4.1 Frontend API .....	<b>27</b>
4.2 Backend API .....	<b>27</b>
4.3 Voraussetzungen für die Nutzung .....	<b>28</b>
<b>5 Hornetsecurity Aeternum aus Datenschutzsicht .....</b>	<b>28</b>
<b>6 Quellen .....</b>	<b>29</b>



## Hinweis

Im nachstehenden Dokument werden Rechtsvorschriften zitiert und es wird auf Rechtsvorschriften Bezug genommen. Die Empfehlungen und Hinweise im Dokument sind Ergebnis gründlicher Recherche und Prüfung. Für die Richtigkeit der Angaben, insbesondere der rechtlichen Hinweise wird aber ausdrücklich nicht garantiert. Dieses Dokument ersetzt keine rechtliche Beratung, vielmehr sollten vor der Einführung eines E-Mail Archivs die individuellen Anforderungen und geltenden rechtlichen Bestimmungen geprüft und dabei auch ein Rechtsexperte zu Rate gezogen werden.



# 1 Problemstellung E-Mail Archiv

## 1.1 Einleitung

E-Mail bildet heute einen, wenn nicht den zentralen Kommunikationskanal für Unternehmen – extern mit Kunden, Lieferanten und Dienstleistern genauso wie intern. Wesentliche Eigenschaften von E-Mail sind Schnelligkeit und Einfachheit der Übertragung zum Empfänger sowie die Schriftform. Letztere macht E-Mail zu einem nachhaltigen Medium. Per E-Mail ausgetauschte Informationen können noch nach langer Zeit wieder eingesehen werden, wenn die E-Mail denn noch gespeichert ist und man die entsprechende E-Mail auch findet.

Für klassische Kommunikation in Schriftform, Briefe, Fax oder dessen Vorgänger, das Fernschreiben, haben Unternehmen normalerweise klare Regeln, wie diese im Unternehmen geleitet, erfasst und abgelegt wird. Schriftstücke werden z. B. chronologisch oder vorgangsbasiert in Ordnern abgelegt und archiviert. Die Ablage als Papierdokument ermöglicht den Nachweis, dass es sich um ein unverändertes Original handelt, das auch als Beweis vor Gericht verwendet werden kann. Die von Rechtsnormen in den meisten Ländern geforderte reversionssichere Ablage über längere Zeiträume ist mit Papierdokumenten leicht erfüllbar. Die Suche nach Schriftstücken auf Papier ist allerdings meist aufwändig, zeitraubend und damit teuer.

## 1.2 Gründe für E-Mail Archivierung

### 1.2.1 Einfache Suche nach wichtigen Informationen

E-Mails sind als elektronische Dokumente für eine Online-Suche prinzipiell gut zugänglich. Solange die E-Mails im Mailserver gespeichert bleiben, könnten sie mit in den Mailserver oder Mailclient integrierten Suchwerkzeugen im Prinzip relativ gut gefunden werden. In der Praxis entstehen aber zwei Probleme:

1. Im Mailserver oder Mailclient eingebaute Suchwerkzeuge funktionieren nicht, nur langsam oder sind schlecht bedienbar. Das Suchergebnis entspricht deshalb oft nicht den Erwartungen, häufig werden gesuchte E-Mails nicht gefunden, obwohl sie tatsächlich vorhanden sind.
2. E-Mails verbleiben nicht im Mailserver, weil sie gelöscht oder in andere Datenspeicher verschoben wurden. Sie sind dann nicht mehr für die Suchwerkzeuge im Mailserver oder Mailclient zugänglich.

Demgegenüber speichern zentrale Mailarchive je nach Ausführung alle oder zumindest alle wichtigen E-Mails eines Unternehmens sicher für einen langen Zeitraum und stellen mit leistungsfähigen Suchwerkzeugen sicher, dass sich gesuchte E-Mails leicht auffinden lassen.



E-Mails, die nicht gefunden werden, verursachen Kosten: Einerseits für die (vergebliche) Suche an sich, gravierender aber dadurch, dass wichtige und wertvolle Informationen nicht vorliegen.

### 1.2.2 Compliance – Erfüllung rechtlicher Anforderungen

Verschiedene Rechtsnormen und Vorschriften erfordern die nachweislich unveränderte und unveränderbare Archivierung von Dokumenten, in Deutschland z.B. HGB, AO, GoBD, KonTraG, auf internationaler Ebene z.B. SOX und EuroSOX. Handelsbriefe müssen dabei sechs Jahre, übrige Dokumente zehn Jahre aufbewahrt werden.

Die meisten Vorschriften beziehen sich ursprünglich auf klassische Dokumente in Papierform. Es ist aber allgemein unstrittig, dass die Vorschriften auch auf elektronische Dokumente anwendbar sind. Ein Teil der Vorschriften, z.B. GoBD, beziehen sich zudem ausdrücklich auf originär elektronische Dokumente. Es ist insgesamt davon auszugehen, dass elektronische Dokumente wie E-Mails auch elektronisch zu archivieren sind.

Neben einer demnach bestehenden unmittelbaren Pflicht zur Archivierung kann es weitere Fälle geben, in denen die Archivierung von E-Mails aus rechtlicher Sicht zumindest vorteilhaft ist. Elektronische Dokumente werden generell immer wichtiger – unter bestimmten Voraussetzungen sind sie Papierdokumenten rechtlich gleichgestellt. So werden E-Mails in vielen Rechtsstreitigkeiten zur Beweisführung herangezogen, z.B. zur Frage des Zustandekommens von Verträgen oder in Arbeitsgerichtsverfahren. Tragen sie eine qualifizierte elektronische Signatur, sind sie unmittelbar als rechtsverbindliches Original anzusehen.

Ohne eine solche Signatur dienen E-Mails in Verfahren zwar in der Regel nicht als gerichtsfester Beweis, eine belegbare ordnungsgemäße Archivierung kann aber vor Gericht zu einer Verschiebung der Beweislast führen. Grundsätzlich können durch Erklärungen in E-Mails Verträge abgeschlossen, verändert und aufgehoben werden. Es wird der Gegenseite regelmäßig schwer fallen, mit Hilfe von ordnungsgemäß archivierten E-Mails dargelegte und untermauerte Tatsachen zu entkräften.

International kann es sogar zur Niederlage in einem Verfahren führen, wenn eine Seite nicht in der Lage ist, einen E-Mail Schriftverkehr beizubringen. In den USA z.B. ist es gängige Praxis, dass vor Beginn von Verfahren ein „Electronic Discovery“ Prozess durchgeführt wird. Ein solcher Ausforschungsantrag ist in Deutschland zwar prinzipiell unzulässig, von einem solchen Verfahren können dennoch alle in den USA tätigen Unternehmen getroffen werden. Die nicht lückenlose Beantwortung eines solchen Ausforschungsantrags führt in den USA dann zu gravierenden Nachteilen im Verfahren. Hinzu kommt, dass die Fristen zur Beantwortung solcher Anforderungen sehr kurz sind. Ohne systematisches E-Mail Archiv sind die Anforderungen von Electronic Discovery jedenfalls kaum zu erfüllen.

### 1.2.3 Entlastung der Infrastruktur

E-Mail Server sind dazu konzipiert, E-Mails vom Sender an den Empfänger zu übermitteln und Nachrichten ggf. zum Abruf durch den Empfänger vorzuhalten. Die langfristige Aufbewahrung von E-Mails war ursprünglich nicht vorgesehen. Aus diesem Grund haben viele Mailssysteme noch heute



Probleme mit der Verwaltung großer Mengen von E-Mail-Daten, unabhängig vom Hardware-Ausbau des Systems.

Sichtbar wird dies z.B. beim Backup von Mailservern. Auch wenn moderne Systeme die Sicherung von Daten parallel zum normalen E-Mail-Betrieb normalerweise problemlos ermöglichen, belastet der Sicherungslauf doch das System. Hinzu kommen Zugriffskonflikte von normalem E-Mail-Betrieb und Backup. Backups großer E-Mail-Datenbanken brauchen deshalb viel Zeit und können oftmals nicht vollständig in Zeiten niedriger Last durchgeführt werden. Als Folge muss die Hardware des Mailserver stärker ausgebaut werden, als es für den E-Mail Betrieb eigentlich nötig wäre. Dies verursacht erhebliche Mehrkosten.

Gänzlich unangenehm wird es, wenn Daten des Mailserver als Folge eines Ausfalls vollständig oder teilweise wiederhergestellt werden müssen. Die Wiederherstellung belastet den Server erheblich, ein normaler Mailbetrieb ist parallel kaum möglich. Dadurch wird der operative Betrieb nach einem Hardwareausfall deutlich länger gestört, als es eigentlich der Fall sein müsste.

Um diesen Problemen aus dem Weg zu gehen, schreiben viele Unternehmen maximale Mailboxgrößen vor. Anwender, die mehr als das zulässige Nachrichtenvolumen aufbewahren wollen, sind dadurch zur Anlage eigener E-Mail-Archive quasi gezwungen. Es entsteht ein Wildwuchs von E-Mail-Datenbanken und verstreut abgelegten Archiven, in denen gesuchte E-Mails nur sehr schwer wieder gefunden werden, die nicht systematisch gesichert werden und die Speicherkosten außerhalb des Mailserver verursachen.

## 1.3 Anforderungen an E-Mail Archivierung

### 1.3.1 Revisionssichere Speicherung

Im Zusammenhang mit Archivsystemen wird oft der Begriff „revisionssicher“ benutzt. Ein Archivsystem gilt als revisionssicher, wenn Informationen darin wieder auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher archiviert sind. Der Verband Organisations- und Informationssysteme e. V (VOI) hat folgende Merksätze zur revisionssicheren elektronischen Archivierung aufgestellt:

1. Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß aufbewahrt werden.
2. Die Archivierung hat vollständig zu erfolgen – kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
3. Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren.
4. Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden.



5. Jedes Dokument darf nur von entsprechend berechtigten Benutzern eingesehen werden.
6. Jedes Dokument muss in angemessener Zeit wiedergefunden und reproduziert werden können.
7. Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist vernichtet, d.h. aus dem Archiv gelöscht werden.
8. Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden.
9. Das gesamte organisatorische und technische Verfahren der Archivierung kann von einem sachverständigen Dritten jederzeit geprüft werden.
10. Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein.

Hinzu kommt, dass Mitarbeiter die Entscheidung, welche E-Mails später eventuell einmal wichtig sind und deshalb archiviert werden müssen, nicht mit hinreichender Sicherheit treffen können. Das Netzwerk Elektronischer Geschäftsverkehr empfiehlt daher den „Hundert-Prozent-Ansatz“: Wer auf Nummer Sicher gehen will, archiviert alle eingehenden und ausgehenden E-Mails.

### 1.3.2 Datenschutz

Der Revisionssicherheit entgegen stehen Anforderungen des Datenschutzes. E-Mails enthalten häufig personenbezogene Daten. Schon eine persönliche E-Mail-Adresse, etwa in der Form „nachname@domain“, wird allgemein als personenbezogene Information angesehen. Jede E-Mail, die eine solche Adressangabe enthält, kann damit dem Datenschutz unterliegen. Insbesondere das deutsche Datenschutzgesetz stellt hohe Anforderungen an den Schutz personenbezogener Daten.

Wenn Mitarbeitern zudem die Nutzung der dienstlichen E-Mail Adresse auch zu privaten Zwecken gestattet wird, so wird das Unternehmen zum Telekommunikationsdienstleister im Sinne des Telekommunikationsgesetzes, mit der Folge, dass eine automatische Archivierung der E-Mails zunächst nicht erlaubt ist. Der einfachste Weg, dieses Problem zu umgehen, führt über das Verbot der privaten Nutzung der betrieblichen E-Mail-Systeme. Ein solches Verbot muss allerdings auch überwacht und durchgesetzt werden.

Und selbst dann sind die Schwierigkeiten nicht vollständig behoben: Sollte nämlich eine private E-Mail trotz Verbots in das betriebliche E-Mail-System geraten sein, z.B. weil eine dritte Person eine private E-Mail an einen Mitarbeiter geschickt hat, so darf diese E-Mail prinzipiell nicht eingesehen werden. Mindestens nach Bekanntwerden der Existenz der privaten E-Mail kann der Betroffene (Absender oder Empfänger) grundsätzlich die Löschung verlangen, mindestens den Schutz vor unbefugtem Zugriff.



Auch für bestimmte Personengruppen, z.B. Adressen des Betriebsrats oder eines Obmanns, kann die Archivierung von E-Mails aus Datenschutzgründen insgesamt unzulässig sein. Für andere Daten, z.B. Bewerbungen, kann die Archivierung zunächst notwendig, nach Abschluss eines Bewerbungsverfahrens aber unzulässig sein.

Der Datenschutz steht damit der Anforderung nach lückenloser Speicherung des E-Mail-Verkehrs zunächst entgegen. Wie in Konfliktfällen zu verfahren ist, lässt sich deshalb oft nur im Einzelfall entscheiden. Archivsysteme sollten daher Ausnahmen von der Archivierung, unterschiedliche Archivierungsfristen und die Löschung oder Sperrung von Daten unter besonderen Voraussetzungen unterstützen. Solche Ausnahmen sollten aber im Sinne der Revisionssicherheit nachvollziehbar sein und protokolliert werden.

### 1.3.3 Prüfzugang

In den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GoBD, Schreiben des BMF vom 14. November 2014) sind drei Arten des Datenzugriffs im Rahmen steuerlicher Außenprüfungen vorgesehen:

#### 1. Unmittelbarer Zugriff (Z1)

Beim unmittelbaren Zugriff greift der Prüfer in lesender Form auf relevante Daten im System selbst zu. Das System muss diesen Zugriff ermöglichen und dabei das Lesen, Filtern und Sortieren der Daten erlauben.

#### 2. Mittelbarer Zugriff (Z2)

Beim mittelbaren Zugriff werden die relevanten Daten im System vom Steuerpflichtigen selber oder einem von ihm beauftragten Dritten maschinell ausgewertet und dem Prüfer zur Verfügung gestellt. Das System muss auch hier die notwendigen Auswertemöglichkeiten bereitstellen und den Lesezugriff durch den Prüfer auf die ausgewählten Daten erlauben.

#### 3. Überlassung eines Datenträgers (Z3)

Bei dieser Zugriffsart wird dem Prüfer ein maschinell lesbarer Datenträger mit den relevanten Daten zur Verfügung gestellt.

Prüfzugänge müssen so gestaltet sein, dass der Prüfer keinen Zugriff auf nicht relevante Daten erhält, z.B. auf Daten außerhalb des Prüfzeitraums oder auf Daten von nicht zu prüfenden Unternehmensbereichen.



### 1.3.4 Technische Anforderungen

Aus den vorhergehenden Betrachtungen ergeben sich folgende technische Anforderungen an ein E-Mail Archiv:

- Das Archiv muss eingehende und ausgehende E-Mails speichern. Eine 100% Archivierung des externen Mailverkehrs ist empfehlenswert, sofern nicht Datenschutzerfordernungen dem entgegen stehen.
- Zusätzlich kann die Archivierung des internen Mailverkehrs sinnvoll sein. Das Archiv sollte entsprechend in der Lage sein auch interne E-Mails zu archivieren.
- Die Speicherung der Daten im Archiv sollte automatisch, möglichst ohne aufwändige Eingriffe und idealerweise komplett ohne Interaktion von Benutzern und Administratoren erfolgen.
- E-Mails müssen das Archiv auf einem dokumentierten und nachprüfbar Weg erreichen, der Veränderungen der E-Mails vor der Ablage im Archiv ausschließt.
- Eine Veränderung von Daten im Archiv während der Archivierungsdauer muss grundsätzlich ausgeschlossen sein.
- Für private Daten im Archiv muss eine Möglichkeit zur Sperre gegen Einsicht der Daten oder zur Löschung vorhanden sein. Sofern eine Löschung durchgeführt wird, muss diese protokolliert werden.
- Daten im Archiv müssen über die gesamte geforderte Aufbewahrungszeit zugänglich und abrufbar sein. Die alternativ mögliche Umspeicherung von Daten auf ein neues System ist in der Regel aufwändig und teuer.
- Der Speicherplatz im Archiv muss ausreichend bemessen sein. Auf keinen Fall dürfen Größenbeschränkungen dazu führen, dass Daten nicht mehr archiviert werden.
- Archivierungsfristen und Ausnahmen von der Archivierung sollten durch Richtlinien (Policies) zentral festlegbar sein.
- Daten im Archiv müssen gegen Verlust gesichert sein, entweder durch entsprechende Maßnahmen im Archivsystem selbst (redundante Speicherung), oder durch ein separates Backup der Archivdaten.
- Das Archiv muss über ein Benutzermanagement verfügen, um Nutzern des Unternehmens den personalisierten Zugriff auf ihre Daten zu ermöglichen. Idealerweise ist das Benutzermanagement an ein vorhandenes Benutzermanagement im Unternehmen angebunden (z.B. per LDAP) und wird mit diesem synchronisiert.
- Der Zugriff auf archivierte Daten sollte für berechtigte Benutzer leicht vom Arbeitsplatz und ggf. mobil möglich sein.
- E-Mails müssen leicht und schnell gefunden werden, in der Regel wird dazu ein Volltextindex notwendig sein.
- Das Archiv muss verschiedene Berechtigungsstufen unterstützen, z.B. für normale Benutzer und Administratoren.
- Privilegierter Benutzer (Administratoren) sollten nicht oder nur eingeschränkt auf Inhalte von E-Mails zugreifen können.
- Das Archiv muss die Prüfzugänge für Abschlussprüfer und Betriebsprüfer bereitstellen. Prüfer müssen Daten selber recherchieren und abrufen können. Zusätzlich muss der Export der Daten auf einen Datenträger möglich sein.



- Prüfer sollten nur auf eingeschränkte Datenbestände zugreifen können, nicht auf das gesamte Archiv. Die Umsetzung des Vier-Augen-Prinzips zur Freischaltung des Prüfzugangs ist aus Datenschutzgründen geboten. Sinnvoll ist eine Protokollierung der Zugriffe und Abfragen, um Handlungen des Prüfers nachvollziehen zu können.

## 1.4 Situation in Unternehmen

Anders als bei klassischen Schriftstücken ist in vielen Unternehmen die Ablage von E-Mails nur unzureichend organisiert. Das hat eine Reihe von Folgen:

1. Alte E-Mails belasten unnötig die Mail-Infrastruktur sowie Arbeitsplatzrechner und verursachen zusätzliche Kosten für Speicherplatz, Mailserver und Backup.
2. E-Mails werden willkürlich gelöscht – z.B. weil ein Mitarbeiter sie als nicht wichtig eingestuft hat. Oft erzwingen Systemrichtlinien oder technische Anforderungen sogar das Löschen von E-Mails, weil z.B. die Größe der Mailbox begrenzt ist.
3. E-Mails werden systematisch gelöscht, z.B. die Mailbox eines Mitarbeiters, der das Unternehmen verlassen hat. Oft werden die Mailboxen ehemaliger Mitarbeiter zwar gesichert, sind aber in der Folge nur schwer zugänglich.
4. E-Mails sind trotz Speicherung nicht auffindbar, z.B. weil die Speicherung der E-Mails in die Verantwortung der Mitarbeiter gelegt wird und deshalb nicht systematisch erfolgt. E-Mail-Archive sind weit im Unternehmen verstreut, es ist unklar, welche E-Mail wo gelagert wird.
5. Von Mitarbeitern angelegte E-Mail Archive liegen auf schlecht geschützten und für die Bedeutung der Daten unzureichend gesicherten lokalen oder gar mobilen Datenspeichern – was im Falle des Datenverlustes unmittelbare und mittelbare Schäden verursachen kann. Diese Art der Speicherung kann außerdem auf Grund des mangelhaften Schutzes gegen unbefugte Einsicht gegen gesetzliche Bestimmungen des Datenschutzes verstoßen.
6. E-Mails werden zwar in einem zentralen Archiv abgelegt, der Weg dahin ist aber nicht hinreichend gesichert und dokumentiert. Unverschlüsselte E-Mails können sehr leicht inhaltlich verändert werden, ohne dass sich diese Veränderung später nachweisen ließe. Dies gilt für E-Mails, die sich bereits im Mailserver befinden (Abb. 1), aber grundsätzlich auch schon vorher, d.h. auf dem Transportweg zwischen Absender und Empfänger. Unabhängig davon, wie ein Unternehmen eine E-Mail langfristig archiviert, ist deshalb ein späterer Nachweis, dass diese E-Mail das Archiv unverändert erreicht hat, für das Unternehmen nicht oder nur sehr schwierig zu führen.
7. Zentrale Archivsysteme sind nicht hinreichend auf die geforderten langen Archivierungsfristen ausgelegt. 6, 10 oder sogar 30 Jahre sind für IT-Komponenten eine lange Zeit. Übliche Garantiezeiten für Hardware liegen bei bis zu zwei Jahren – ob nach Ablauf dieser Zeit noch kompatibler Ersatz zur Verfügung steht, ist oft nicht gesichert. Selbst wenn: die



Daten müssen oft vom alten auf das neue System übertragen werden, was weitere Kosten verursacht.

8. E-Mails werden zur Archivierung ausgedruckt und klassisch in Papierform archiviert. Dies erfüllt weder die gesetzlichen Anforderungen an die Archivierung elektronischer Daten, noch sind die E-Mails leicht wieder auffindbar. Je nach Umfang können für ausgedruckte E-Mails zudem erhebliche Kosten für Druck und Lagerung entstehen.

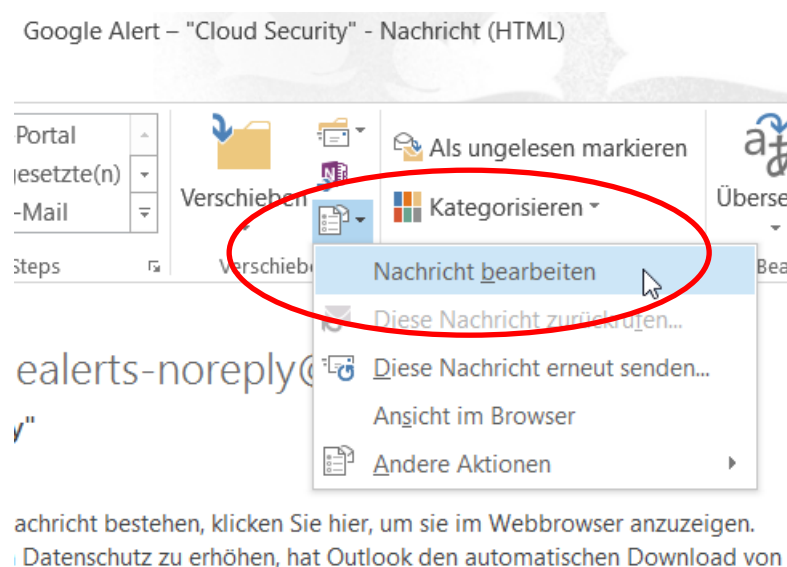


Abbildung 1: E-Mails können in vielen Mailssystemen nach dem Empfang leicht bearbeitet und dadurch verändert werden - hier: Outlook und Exchange

Ein vom Pestel-Institut im Auftrag von antispameurope im Jahr 2008 durchgeführte Studie kam zu dem Schluss, dass abhängig von der Unternehmensgröße nur zwischen 6% und 12% der Unternehmen in Deutschland E-Mails den geltenden Anforderungen entsprechend archivieren.

## 2 Hornetsecurity Aeternum

### 2.1 Cloud Architektur

Hornetsecurity nutzt das Prinzip der Public Cloud für seine Managed Security Services, u.a. den Hornetsecurity Aeternum. Cloud Computing wird von Forrester Research definiert als „ein Pool aus abstrakter, hochskalierbarer Infrastruktur mit Anwendungen, die nach Verbrauch abgerechnet werden“. Bildlich kann man sich eine Cloud als eine Wolke von Rechnern vorstellen, die aus der Distanz wie ein homogenes Gebilde wirkt und entsprechend als ein homogenes System behandelt und genutzt werden kann.



Wesentliche Vorteile von Cloud-Computing:

- Dynamische Bereitstellung von Ressourcen nach Bedarf
- Höhere Verfügbarkeit durch massive Redundanz
- Keine Installation dedizierter Hard- und Software
- Hardware- und Betriebssystem-unabhängig

Daraus resultiert: Cloud Computing ist erheblich flexibler, leistungsfähiger und kostengünstiger als entsprechende dedizierte Infrastrukturen.

Unterschieden wird zwischen verschiedenen Cloud-Typen:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Ferner gibt es Unterschiede in der Art der Bereitstellung

- Private Cloud: Einem für eine Organisation dedizierten Pool von Systemen, der für z. B. verschiedene Anwendungen gemeinsam genutzt wird.
- Public Cloud: Pool von Systemen, der von mehreren Organisationen gemeinsam genutzt wird.
- Hybrid Cloud: Eine Mischform von Private und Public Cloud; z. B. Nutzung einer Public Cloud als Ergänzung für eine Private Cloud.
- Community Cloud: Im Prinzip eine Private Cloud für eine Gemeinschaft von Nutzern (z. B. Mitglieder eines Verbandes).

Vor allem für Public Clouds gelten zusätzlich zu den allgemeinen Vorteilen von Cloud-Computing folgende Vorteile:

- Keine langfristige Kapitalbindung (OPEX statt CAPEX)
- Keine Installation von Hardware und Software
- Kein oder nur geringer interner Administrationsaufwand

Der von Hornetsecurity genutzte Ansatz der Archivierung in der Cloud hat folgende Vorteile gegenüber der klassischen On-Premise Archivierung:

- Speicherung der Daten außerhalb des physischen Zugriffsbereichs des Kunden, dadurch nachweislich unveränderte und unveränderbare Speicherung,
- Gemeinsame Nutzung von Hard- und Software durch alle Kunden, dadurch erheblich kostengünstiger als klassische Einzelinstallationen,
- Massiv redundante und verteilte Auslegung des Gesamtsystems, dadurch erheblich leistungsfähiger und robuster als Einzelinstallationen,
- Betrieb außerhalb der Infrastruktur der Unternehmen, dadurch Entlastung der Infrastruktur,
- Betrieb des Systems im Internet, damit grundsätzlich von allen Standorten, Heimarbeitsplätzen und mobilen Nutzern zugänglich (Zugangseinschränkungen sind konfigurierbar),



- 24/7 Überwachung der Systeme durch Security-Experten, dadurch Gewährleistung der Sicherheit und des kontinuierlichen Betriebs auch außerhalb der Arbeitszeiten des eigenen IT-Personals.

Eine Herausforderung für Public Clouds besteht in der Herstellung der Sicherheit und Abgrenzung der Daten verschiedener Nutzer untereinander. Die Lösungen von Hornetsecurity sind deshalb voll mandantenfähig und verfügen über abgestufte Benutzerberechtigungen und ein fein konfigurierbares Berechtigungssystem. Daten werden hierarchisch in separaten Datenbanken je Kunde abgelegt, so dass immer nur der Zugriff auf eigene Daten entsprechend der jeweiligen Nutzer-Hierarchieebene möglich ist.

Die Systeme von Hornetsecurity werden verteilt in mehreren gesicherten Rechenzentren betrieben. Generell ist der tatsächliche Ort der Verarbeitung oder Lagerung von Daten nicht auf ein bestimmtes System festgelegt. So steht z. B. für eine einzelne E-Mail vorab nicht fest, welches System sie durchläuft. Trotzdem können bei Hornetsecurity bestimmte Bereiche der Cloud an bestimmte Aufgaben gebunden werden. So kann gewährleistet werden, dass eine E-Mail z. B. in Deutschland archiviert wird. Für Unternehmen mit Sitz in Deutschland wird entsprechend, soweit gewünscht, die Archivierung der Daten gemäß Bundesdatenschutzgesetz in Deutschland vertraglich garantiert.

Da, wo es auf Grund großer Datenmengen sinnvoll ist, können Systeme auch in den Rechenzentren von Provider-Partnern und Firmenkunden aufgestellt und betrieben werden – als Hornetsecurity Managed Appliance. Hornetsecurity kombiniert dadurch die Vorteile der Cloud mit denen dedizierter Systeme.

## 2.2 Weg in das Archiv – Anbindung an Mailserver

Eingehender E-Mail-Verkehr erreicht das E-Mail Archiv durch Umleitung des SMTP-Verkehrs per Änderung der MX-Records der Kundendomains über die Hornetsecurity E-Mail Gateways (Abbildung 2). Ausgehender E-Mail-Verkehr erreicht das E-Mail Archiv durch Versenden ausgehender E-Mails über die Hornetsecurity E-Mail Relays. Dadurch ist sichergestellt, dass eingehende E-Mails vom Empfänger nicht vor der Speicherung im Archiv manipuliert werden können – sie werden exakt so im Archiv gespeichert, wie sie die Gateways von Hornetsecurity aus dem Internet erreichen. Entsprechendes gilt für ausgehende E-Mails: Sie werden exakt so in das Archiv gestellt, wie sie dem Empfänger über das Internet zugestellt werden – nach der Einstellung in das Archiv ist eine nachträgliche Manipulation durch den Absender unmöglich. Die Einbindung des Hornetsecurity Archivs in den externen SMTP-Datenverkehr des Unternehmens erfüllt damit eine wesentliche Voraussetzung für die Revisionssicherheit des Archivs: Es kann jederzeit zweifelsfrei nachvollzogen werden, welche E-Mails verschickt und empfangen wurden und welchen Inhalt diese hatten.

Sollen auch interne E-Mails archiviert werden (optionale Leistung) werden diese im Mailserver des Kunden in einem Journal-Postfach bereitgestellt und von dort durch Hornetsecurity abgerufen und in das Archiv gestellt. Die Unveränderlichkeit der archivierten E-Mails ist in diesem Fall ab dem Moment der Übertragung in das Archiv gesichert. Zusätzlich sind für Mailssysteme ohne Journalpostfach alternative Methoden zur Übermittlung interner E-Mails in das Archiv als Option verfügbar.



Im Mailverkehr werden folgende Verbindungen zwischen Systemen von Hornetsecurity und Systemen des Kunden hergestellt:

- SMTP-Verbindungen zur Übermittlung eingehender E-Mails an die Mailserver der Kunden
- SMTP-Verbindungen zur Übermittlung ausgehender E-Mails von den Mailservern der Kunden
- IMAP- oder POP3-Verbindungen zur Übermittlung interner E-Mails in das Archiv

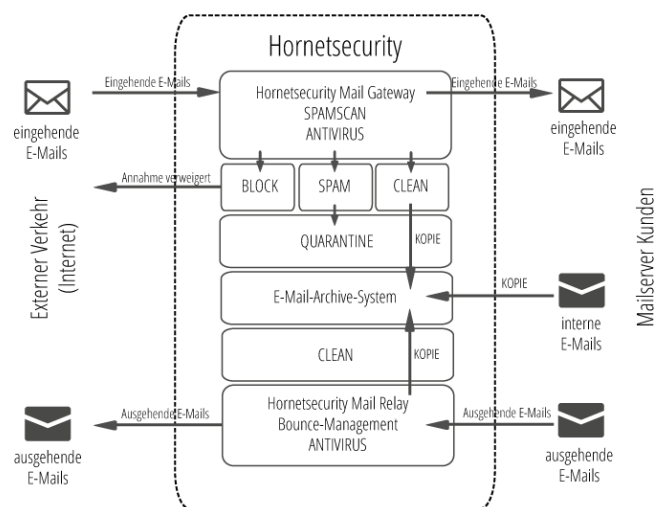


Abbildung 2: Weg der E-Mails in das Hornetsecurity E-Mail Archiv – Anbindung die Mail-Infrastruktur des Kunden

Die Herstellung dieser Verbindungen erfolgt in der Regel über das Internet. Zum Schutz der Verbindungen vor Einsichtnahme und Zugriffen Dritter werden Verbindungen zwischen Hornetsecurity und Systemen von Kunden durchgängig per TLS verschlüsselt (Transportverschlüsselung). Notwendig dazu sind die entsprechenden technischen Voraussetzungen in den Kundensystemen – bei jüngeren Release-Ständen ist diese Voraussetzung in der Regel erfüllt. Die Verschlüsselung von Nachrichten und Verbindungen nach außen (zwischen Systemen von Hornetsecurity und externen Absendern bzw. Empfängern) kann per Policy konfiguriert werden (optional zuschaltbarer Hornetsecurity Verschlüsselungsservice).

## 2.3 Interner Aufbau / Architektur und Abläufe

Zu archivierende externe E-Mails werden vom Hornetsecurity Gateway oder Hornetsecurity Relay per SMTP dem Storage Manager übergeben (Abbildung 3). Zu archivierende interne E-Mails werden vom Storage Manager durch einen Software-Agenten per POP3 oder IMAP im Mailserver des Kunden abgeholt.

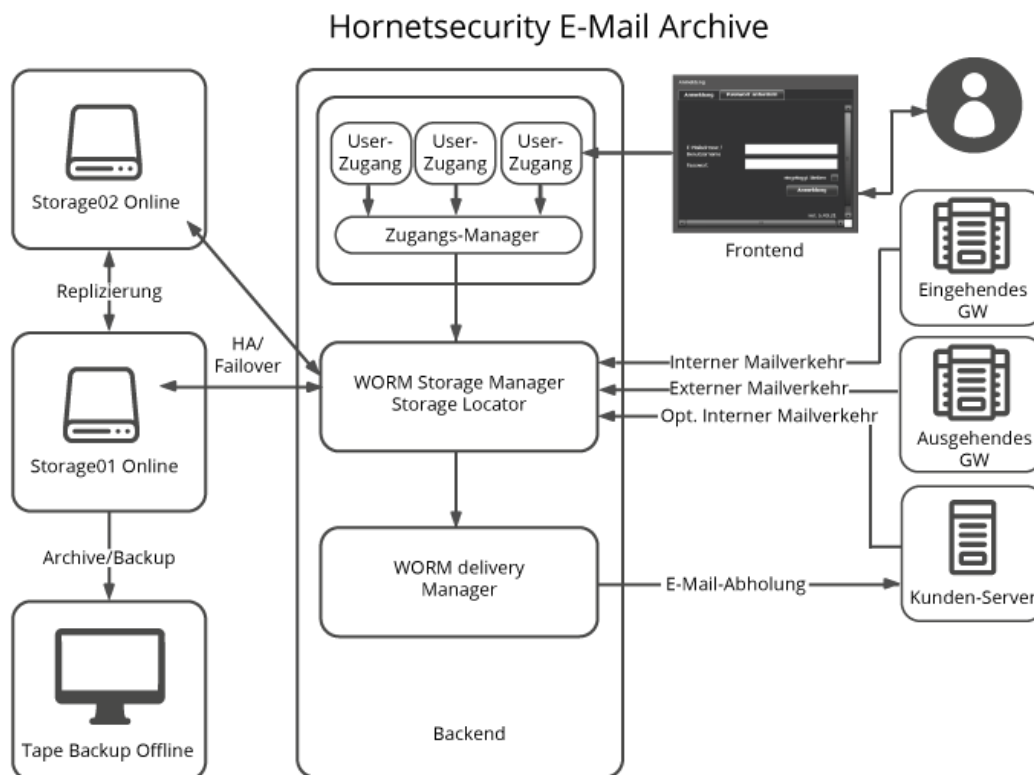


Abbildung 3: Technischer Aufbau des Hornetsecurity E-Mail Archivs und Datenfluss im Archiv

Der Storage Manager legt den Speicherort der Daten fest und sorgt für die Speicherung auf mehreren (mindestens zwei) verschlüsselten Storage-Systemen. Die Storage-Systeme sind jeweils als RAID Level 6 mit Hot Spare ausgelegt. Die Storage-Systeme sind außerdem zueinander redundant und werden stetig synchron gehalten. Zusätzlich wird eine Bandsicherung angefertigt.

Daten werden de-dupliziert, komprimiert und verschlüsselt abgelegt. Alle archivierten Daten werden stets online gehalten. Bei Ausfall einzelner Platten eines Storage-Systems werden nach Austausch defekter Platten die Daten durch das Storage-System selbsttätig wieder hergestellt. Bei Ausfall eines kompletten Storage-Systems werden die Daten nach Wiederherstellung der Hardware von einem redundanten Storage-System wiederhergestellt. Die Bandsicherung dient als zusätzlicher Schutz und wird nur für den unwahrscheinlichen Fall vorgehalten, dass Daten auf keinem der redundanten Storage-Systeme mehr vorhanden sind.

## 2.4 Indizierung und Suche

Im Archiv abgelegte E-Mails werden automatisch indiziert, das heißt für Inhalt der E-Mails und Anhänge wird eine Index-Datenbank mit Schlagworten gefüllt (Volltextindex). Als Schlagworte genutzt werden alle Wörter in als Text erkennbaren Daten – z.B. auch Word-Dateien, PDF, Excel, PowerPoint, HTML, XML, ODF, RTF etc. Nicht indiziert werden Texte, die z.B. in Bildern oder in verschlüsselter Form

gespeichert sind. Die Index-Datenbank wird für jeden Kunden getrennt angelegt, ein zusätzlicher Schutz gegen nicht autorisierte Zugriffe.

## 2.5 Control Panel

Der Zugriff auf das Archiv und die Suche im Archiv erfolgen über ein webbasiertes Frontend, das Hornetsecurity Control Panel. Das Control Panel (

Abbildung 4) ist der zentrale Zugangspunkt zu allen Informationen und Einstellungen zu Hornetsecurity Services. Es unterstützt Administratoren und Benutzer bei der Verwaltung von benutzerdefinierten Einstellungen, beim Umgang mit empfangenen E-Mails und bei der statistischen Auswertung des E-Mail-Verkehrs.

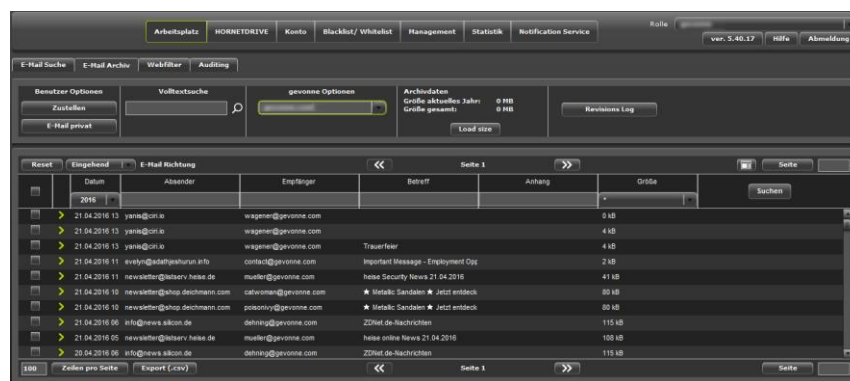


Abbildung 4: Aeternum im Hornetsecurity Control Panel

Das Control Panel stellt Benutzern eine einfach zu bedienende Oberfläche zur Verfügung, mit deren Hilfe jeder einzelne den Fluss seiner persönlichen Mails überwachen und steuern kann. Das Control Panel erlaubt die Suche nach archivierten E-Mails an Hand des Volltextindex sowie einer Vielzahl von Parametern wie Absender, Empfängeradresse, Datum etc. Archivierte E-Mails können durch Benutzer im Control Panel eingesehen und auf Knopfdruck erneut in ihre Mailbox zugestellt oder als privat markiert werden.

Administratoren erhalten weitergehende Werkzeuge an die Hand, mit deren Hilfe Maildomains, komplexe Konfigurationen und die Postfächer der Benutzer übersichtlich verwaltet werden können (Abbildung 5). Außerdem stehen globale und tiefgreifende Kontroll- und Konfigurationsmöglichkeiten zur Verfügung. Zudem kann detailliert eingestellt werden, welche Menüpunkte Endnutzern im Control Panel zur Verfügung stehen.

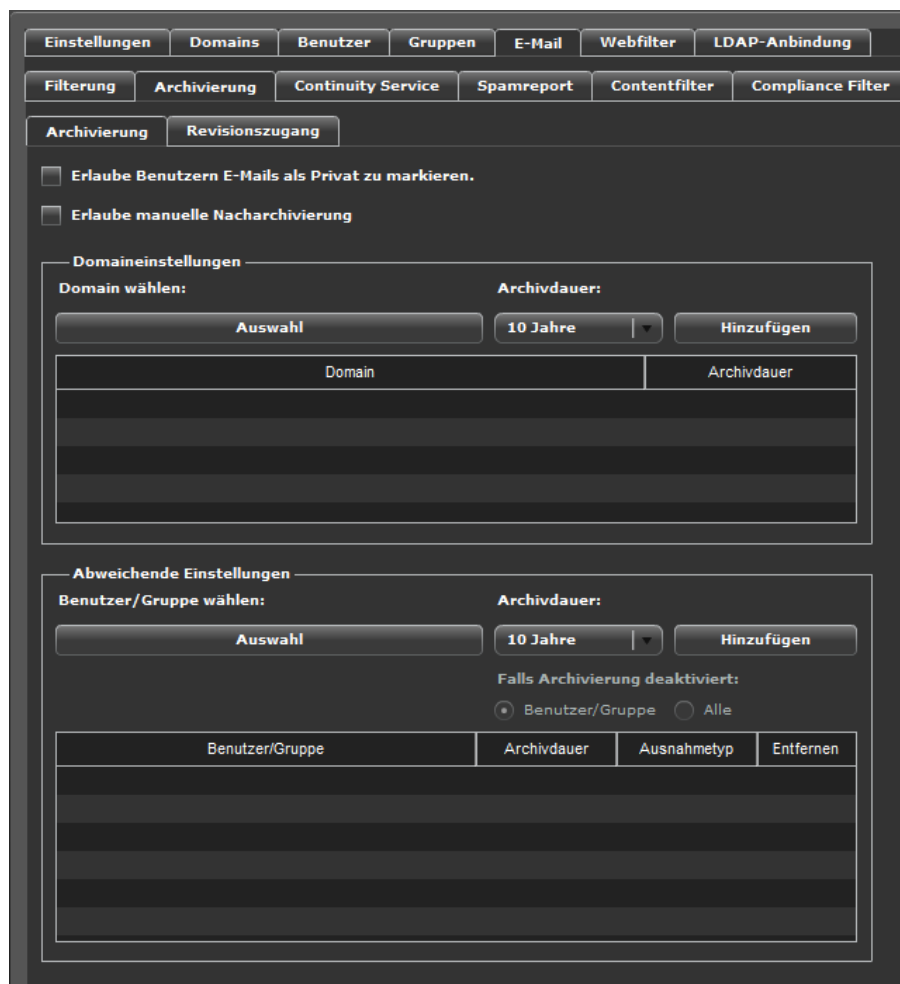


Abbildung 5: Umfangreiche Kontroll- und Konfigurationsmöglichkeiten für Administratoren im Control Panel

Im Control Panel vorgenommene Einstellungen werden automatisch in die Hornetsecurity Cloud übertragen und dort verteilt, typisch nach drei, in Ausnahmefällen spätestens zehn Minuten nach Speicherung arbeiten alle Systeme in der Cloud mit den neuen Einstellungen.

Die Einrichtung von Benutzern erfolgt standardmäßig automatisiert nach Maileingang ohne zusätzliche Interaktion, alternativ kann sie über das Control Panel entweder von Hand, durch Hochladen entsprechender Listen oder durch Abgleich mit einem LDAP-Server vorgenommen werden.

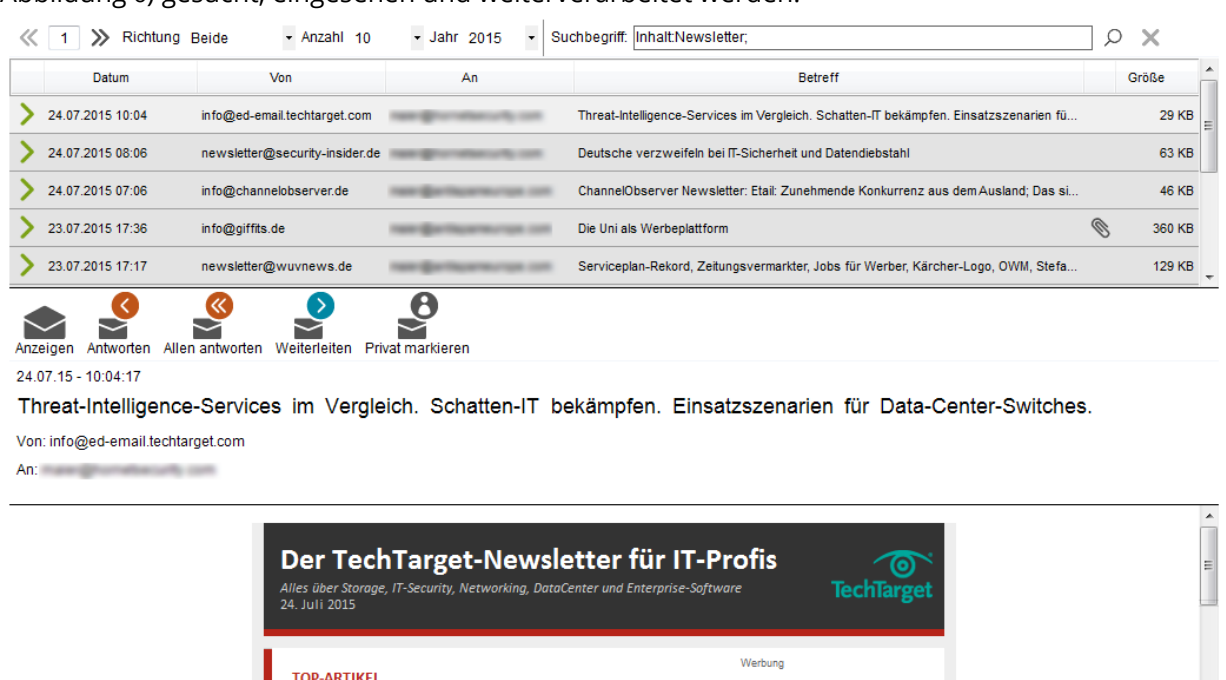
Die Nutzung des Control Panels ist mit jedem Browser mit aktuellem Flash-Add-In möglich. Als webbasierte Anwendung wird das Control Panel automatisch immer in der aktuellsten Version gestartet. So haben alle Nutzer stets Zugriff auf die aktuellsten Features.

Derzeit ist das Control Panel in 17 Sprachen verfügbar: Chinesisch, Deutsch, Dänisch, Englisch, Französisch, Italienisch, Japanisch, Katalanisch, Polnisch, Russisch, Schwedisch, Slowakisch, Spanisch,

Ukrainisch, Griechisch, Portugiesisch (PT und BR). Weitere Sprachen sind in kurzer Zeit implementierbar.

## 2.6 Outlook Add-In

E-Mails im Archiv können auch über das Hornetsecurity Outlook Add-In (Abbildung 6) gesucht, eingesehen und weiterverarbeitet werden.



The screenshot shows the Outlook interface with a search filter for 'Inhalt:Newsletter,'. A table lists five archived emails with columns for 'Datum', 'Von', 'An', 'Betreff', and 'Größe'. Below the table are navigation icons for 'Anzeigen', 'Antworten', 'Allen antworten', 'Weiterleiten', and 'Privat markieren'. The selected email is from 'info@ed-email.techtarget.com' with the subject 'Threat-Intelligence-Services im Vergleich. Schatten-IT bekämpfen. Einsatzszenarien für Data-Center-Switches.' Below the email header is a preview of a TechTarget newsletter titled 'Der TechTarget-Newsletter für IT-Profis' dated 24. Juli 2015, with a 'TOP-ARTIKEL' badge and 'Werbung' label.

Datum	Von	An	Betreff	Größe
24.07.2015 10:04	info@ed-email.techtarget.com	www@hornetsecurity.com	Threat-Intelligence-Services im Vergleich. Schatten-IT bekämpfen. Einsatzszenarien fü...	29 KB
24.07.2015 08:06	newsletter@security-insider.de	www@hornetsecurity.com	Deutsche verzweifeln bei IT-Sicherheit und Datendiebstahl	63 KB
24.07.2015 07:06	info@channelobserver.de	www@hornetsecurity.com	ChannelObserver Newsletter: Etail: Zunehmende Konkurrenz aus dem Ausland; Das si...	46 KB
23.07.2015 17:36	info@giffits.de	www@hornetsecurity.com	Die Uni als Werbeplattform	360 KB
23.07.2015 17:17	newsletter@wuvnews.de	www@hornetsecurity.com	Serviceplan-Rekord, Zeitungsvermarkter, Jobs für Werber, Kärcher-Logo, OWM, Stefa...	129 KB

Abbildung 6: Archivierte E-Mails im Hornetsecurity Outlook Add-In

Das Add-In unterstützt alle für Endnutzer wichtige Funktionen beim Zugriff auf das Archiv:

- Volltextsuche über indizierte Inhalte der archivierten E-Mails
- Suche an Hand von Eigenschaften der E-Mails: z. B. Absender, Empfänger, Betreff, Datum
- Direktes Weiterleiten von archivierten E-Mails bzw. Antworten auf archivierte E-Mails in Outlook

Zusätzlich unterstützt das Outlook-Add-In das Einstellen von E-Mails aus Outlook in das Archiv. Damit können E-Mails, die nicht schon auf andere Weise den Weg in das Archiv gefunden haben (z. B. aus einem anderen E-Mail Account), manuell archiviert werden.



## 2.7 Aeternum App

Um den mobilen Zugriff auf die archivierten E-Mails zu ermöglichen, bietet Aeternum eine App an. Diese zeigt alle im Archiv vorhandenen E-Mails an, wobei die E-Mails direkt im Speicher hinterlegt und nicht dauerhaft auf dem Gerät gespeichert sind.



Abbildung 7: Startbildschirm eines iPads mit der Aeternum App

Nach dem Start der App wird der Benutzer aufgefordert, sich einzuloggen. Anschließend kann er auf der linken Seite einzelne E-Mails auswählen und sich diese anzeigen lassen.

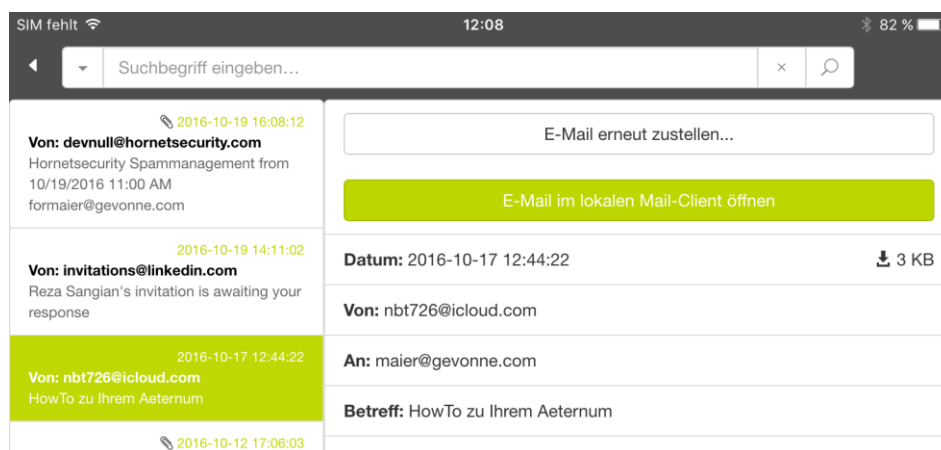


Abbildung 8: Anzeige einer E-Mail über die App



Ebenfalls in der App ist eine schnelle, umfassende Suchfunktion, über die sich archivierte Mails problemlos auffinden lassen.

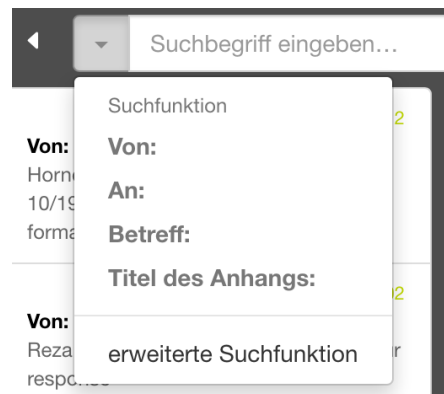


Abbildung 9: Eine einfach zu bedienende Suchfunktion liefert schnelle Ergebnisse

Befindet sich ein Mail-Client auf dem mobilen Gerät, können E-Mails auch erneut zugestellt, beantwortet oder weitergeleitet werden.

Die App ist in den gängigen App Stores zu finden.

## 2.8 Zugriff per Browser

Auch über einen Webbrowser erhält der Benutzer Zugriff auf sein persönliches E-Mail-Archiv. Unter <https://control.hornetsecurity.com/aeternum/> lassen sich wie bei der App gespeicherte E-Mails suchen, lesen und erneut zustellen.

## 2.9 Revisionszugang

Administratoren können im Control Panel einen Zugang für Revisoren einrichten (Abbildung ). Dieser Zugang muss jeweils durch einen zweiten Benutzer freigeschaltet werden (Vier-Augen-Prinzip). Der Revisionszugang ist für einen einstellbaren Zeitraum aktiv, danach ist ein Login nicht mehr möglich.



Archivierung Revisionszugang

Revisionszugang aktivieren

Benutzer für den Revisionszugang auswählen:

4augen@gevonne.com

Revisionszugang aktiv:

Von 15.05.1994 Bis 30.04.2016

Zugriff auf E-Mails:

Von 01.03.2015 Bis 20.10.2021

Benutzer zur Freischaltung (Vier-Augen-Prinzip)

contact@gevonne.com

Speichern

Abbildung 10: Einrichtung eines Revisionszugangs

Revisoren haben Zugriff auf alle E-Mails des vorab definierten Betrachtungszeitraums. Sie können E-Mails direkt im Control Panel einsehen oder diese E-Mails in ihr Postfach zustellen lassen (Abbildung 11).

Arbeitsplatz HORNETDRIVE Konto Blacklist/Whitelist Management Statistik Notification Service Rolle: gevonne ver. 5.40.18 Hilfe Abmeldung

E-Mail Suche E-Mail Archiv Webfilter Auditing

Benutzer Optionen Volltextsuche gevonne Optionen Archivdaten Größe aktuelles Jahr: 0 MB Größe gesamt: 0 MB Revisions Log

Reset Beide E-Mail Richtung Seite 1 Suchen

	Datum	Absender	Empfänger	Betreff	Anhang	Größe
<input type="checkbox"/>	24.05.2016 18:38	micropro@altma.net	contact@gevonne.com	Best watches. Pre-summer sale!		81 kB
<input type="checkbox"/>	24.05.2016 17:28	message@my.zalando.de	poisonivy@gevonne.com	Gekommen als Prinzessin, gegangen		70 kB
<input type="checkbox"/>	24.05.2016 14:06	crs@cirli.io	jahnke@gevonne.com	Conova02Test		1 kB
<input type="checkbox"/>	24.05.2016 13:58	jahnke@gevonne.com	conova02@gevonne.com	conova02 test		0 kB
<input type="checkbox"/>	24.05.2016 13:55	jahnke@gevonne.com	conova02@gevonne.com	Test GW400 Conova02		3 kB
<input type="checkbox"/>	24.05.2016 13:55	jahnke@gevonne.com	conova02@gevonne.com	Microsoft Outlook-Testnachricht		0 kB
<input type="checkbox"/>	24.05.2016 05:33	newsletter@listserv.heise.de	mueller@gevonne.com	heise online News 24.05.2016		64 kB
<input type="checkbox"/>	23.05.2016 11:13	newsletter@listserv.heise.de	mueller@gevonne.com	heise Security News 23.05.2016		39 kB
<input type="checkbox"/>	23.05.2016 10:28	subscribe@mota.ru	info@gevonne.com	Рассылка новых обоев от MOTA.RL		15 kB
<input type="checkbox"/>	23.05.2016 05:22	newsletter@listserv.heise.de	mueller@gevonne.com	heise online News 23.05.2016		28 kB
<input type="checkbox"/>	22.05.2016 11:36	newsletter@shop.deichmann.com	catwoman@gevonne.com	Neue Taschen & Accessoires online i		112 kB
<input type="checkbox"/>	22.05.2016 11:31	newsletter@shop.deichmann.com	poisonivy@gevonne.com	Neue Taschen & Accessoires online i		112 kB
<input type="checkbox"/>	22.05.2016 09:59	message@my.zalando.de	poisonivy@gevonne.com	Das könnte dich interessieren...		55 kB
<input type="checkbox"/>	22.05.2016 08:02	tiffany@tco.tiffany.com	poisonivy@gevonne.com	Sie sind uns Gold wert   Tiffany Gesc		24 kB
<input type="checkbox"/>	22.05.2016 05:31	newsletter@listserv.heise.de	mueller@gevonne.com	heise online News 22.05.2016		42 kB
<input type="checkbox"/>	21.05.2016 05:23	newsletter@listserv.heise.de	mueller@gevonne.com	heise online News 21.05.2016		58 kB
<input type="checkbox"/>	20.05.2016 13:31	alemndar@gevonne.com	alemndar@gevonne.com	SPF - Jetzt läuft aber		0 kB
<input type="checkbox"/>	20.05.2016 13:31	alemndar@gevonne.com	alemndar2@gevonne.com	SPF - Jetzt läuft aber		0 kB
<input type="checkbox"/>	20.05.2016 09:28	subscribe@mota.ru	info@gevonne.com	Рассылка новых обоев от MOTA.RL		15 kB
<input type="checkbox"/>	20.05.2016 06:30	noreply@updates.pm	contact@gevonne.com	Einloggen und Video abstauben, eizo!		87 kB

100 Zeilen pro Seite Export (.csv) Seite 1

Abbildung 11: Zugriff auf alle E-Mails des Revisionszeitraums im Revisionszugang



Alle Zugriffe von Revisoren werden im System protokolliert. Administratoren können diese Protokolle einsehen und sich detailliert Überblick über die Aktivitäten von Revisoren verschaffen – auch über eingesehene E-Mails (Abbildung 12).

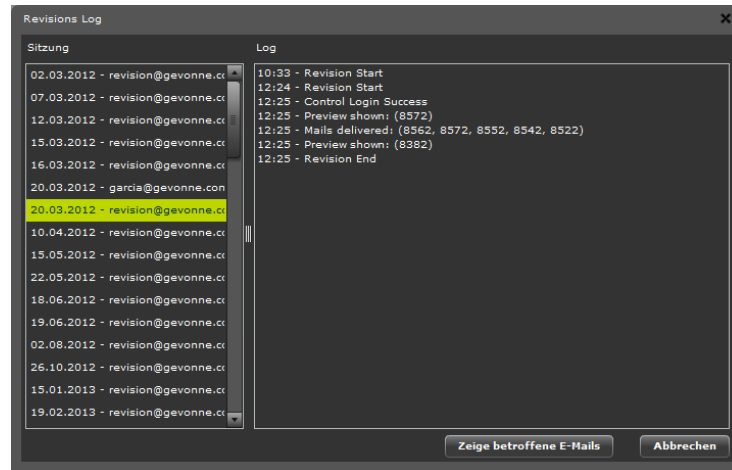


Abbildung 12: Revisionslog: Prüfung der Aktivitäten eines Revisors

## 2.10 Audit Log

Alle Logins von Administratoren und Benutzern sowie Konfigurationsänderungen im System werden bei Hornetsecurity automatisch protokolliert und können über das Control Panel eingesehen werden. Dadurch kann jederzeit lückenlos nachvollzogen werden, wer wann welche Konfigurationsänderungen vorgenommen hat – eine wichtige Information zur Fehlersuche im Falle von Fehlkonfigurationen (3).

Alle ...	Datum	Anmeldeame	Partner	Kunde	Wier	Aktion	Was	AB	Neu	P	URL
	21.04.16 13:59:10	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 13:31:19	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 13:09:57	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 11:00:47	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 11:00:36	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 10:57:25	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 10:44:13	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 10:42:31	f.lange@gevonne.com	gevonne	gevonne.com	f.lange@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 10:33:34	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	21.04.16 10:14:08	f.lange@gevonne.com	gevonne	gevonne.com	f.lange@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	20.04.16 10:27:56	hammer@hornetsecurity.com	gevonne	testdomäne.de	testdomäne.de	Hinzuftügen	MediaContentF-BerVO	status:0	size:20000Type:Station-Bevo	127.0.0.1	https://control.hornetsecurity.com
	20.04.16 10:27:56	hammer@hornetsecurity.com	gevonne	testdomäne.de	testdomäne.de	Hinzuftügen	MediaContentF-BerVO	status:0	size:20000Type:Station-Bevo	127.0.0.1	https://control.hornetsecurity.com
	20.04.16 10:27:56	hammer@hornetsecurity.com	gevonne	testdomäne.de	testdomäne.de	Hinzuftügen	Fähigung	type:User's-OrderType:10000	127.0.0.1	https://control.hornetsecurity.com	
	20.04.16 10:27:05	hammer@hornetsecurity.com	gevonne	testdomäne.de	testdomäne.de	Hinzuftügen	Produkt	masterPartner-assesmerpartner	127.0.0.1	https://control.hornetsecurity.com	
	20.04.16 10:27:05	hammer@hornetsecurity.com	gevonne	testdomäne.de	testdomäne.de	Hinzuftügen	Domain	domain-testdomäne.de&id=trackin	127.0.0.1	https://control.hornetsecurity.com	
	20.04.16 10:26:59	hammer@hornetsecurity.com	gevonne	testdomäne.de	testdomäne.de	Hinzuftügen	Benutzer	username=testdomäne.de&name=te	127.0.0.1	https://control.hornetsecurity.com	
	20.04.16 10:19:29	f.lange@gevonne.com	gevonne	gevonne.com	f.lange@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	20.04.16 09:56:06	gevonne.com	gevonne	gevonne.com	gevonne.com	Anmeldung erfolgreich				83.246.65.144	https://mail.archive.lensinet.com/
	20.04.16 09:47:52	wagner@hornetsecurity.com	gevonne	gevonne.com	gevonne.com	Hinzuftügen	MediaContentF-BerVO	status:1	status:0	127.0.0.1	https://control.hornetsecurity.com
	20.04.16 09:45:19	wagner@hornetsecurity.com	gevonne	gevonne.com	gevonne.com	Hinzuftügen	MediaContentF-BerVO	status:1	status:1	127.0.0.1	https://control.hornetsecurity.com
	20.04.16 09:45:11	wagner@hornetsecurity.com	gevonne	gevonne.com	gevonne.com	Hinzuftügen	Produkt	masterPartner-assesmerpartner	127.0.0.1	https://control.hornetsecurity.com	
	19.04.16 10:44:10	gevonne.com	gevonne	gevonne.com	gevonne.com	Anmeldung erfolgreich				83.246.65.147	https://mail.archive.lensinet.com/
	19.04.16 13:01:23	gevonne	gevonne	gevonne	gevonne	Anmeldung erfolgreich				83.246.65.147	https://mail.archive.lensinet.com/
	19.04.16 11:39:31	gevonne.com	gevonne	gevonne.com	gevonne.com	Anmeldung erfolgreich				83.246.65.147	https://mail.archive.lensinet.com/
	19.04.16 08:43:34	presales@test	presales@test	jahnke@test	jahnke@test	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	19.04.16 08:39:22	jahnke@hornetsecurity.com	gevonne	gevonne.com	gevonne.com	Hinzuftügen	Verchlussung Policy	direction:2	direction:jahnke@gevo	127.0.0.1	https://control.hornetsecurity.com
	19.04.16 08:39:21	jahnke@hornetsecurity.com	gevonne	gevonne.com	gevonne.com	Hinzuftügen	Produkt	userCount:117	userCount:119	127.0.0.1	https://control.hornetsecurity.com
	19.04.16 15:44:16	bob@gevonne.com	gevonne	gevonne.com	bob@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	19.04.16 15:37:06	gevonne	gevonne	gevonne.com	bob@gevonne.com	Hinzuftügen	Benutzer	username=bbb@gevonne.com	127.0.0.1	https://control.hornetsecurity.com	
	19.04.16 15:58:15	gevonne	gevonne	gevonne.com	gevonne.com	Gelöscht	Archivierung	name=rud@gevonne.com&urk	127.0.0.1	https://control.hornetsecurity.com	
	19.04.16 09:18:48	jahnke@gevonne.com	gevonne	gevonne.com	jahnke@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	19.04.16 09:18:45	gevonne	gevonne	gevonne.com	jahnke@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com
	19.04.16 08:18:00	gevonne	gevonne	gevonne.com	jahnke@gevonne.com	Anmeldung erfolgreich				127.0.0.1	https://control.hornetsecurity.com

Abbildung 13: Protokollierung von Logins und Konfigurationsänderungen sind im Audit Log jederzeit nachvollziehbar

## 2.11 Anpassung an eigenes Corporate Design

Das Hornetsecurity Control Panel kann vollständig an das Corporate Design des Kunden oder Hornetsecurity Partners angepasst werden (

Abbildung ). Die Anpassung umfasst:

- Im Control Panel genutzte Farben
- Logo
- Templates für Spamreport (Digest) und weitere Nachrichten
- URL für das Control Panel (Optional Zugriff über Webserver des Kunden bzw. Partners, z.B. <https://controlpanel.kundendomain.com/>)

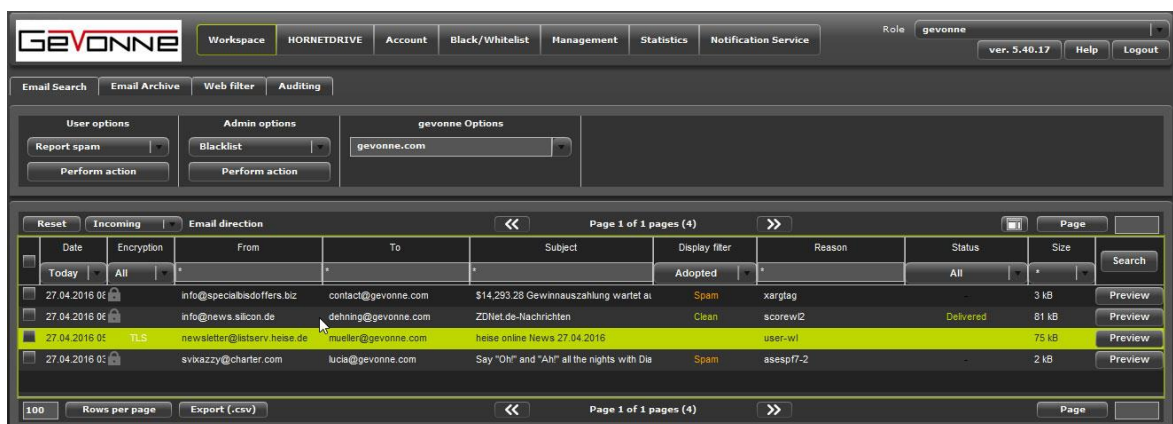


Abbildung 14: Hornetsecurity Control Panel mit Anpassung an das Corporate Design eines Kunden

## 2.12 Import und Export von Daten

Bestandsdaten können auf zwei Wegen in das Hornetsecurity Archiv importiert werden:

1. Durch Zustellung an das Archiv per SMTP
2. Durch Direktimport von PST-Dateien (Anlieferung auf Datenträger).

Zum Export von archivierten E-Mails stehen folgende Wege zur Verfügung:

1. Auslösen aus dem Archiv und erneute Zustellung in die Mailbox des Benutzers
2. Auslieferung im Rohdatenformat (.eml, bzw. RFC 5322) auf Datenträger
3. Auslieferung im Outlook-Format (.msg) auf Datenträger



## 2.13 Leistungen im Überblick

- Nachstehend sind wesentliche Eigenschaften des Hornetsecurity Aeternum zusammenfassend aufgeführt:
- 100% Archivierung aller ein- und ausgehenden Mails
  - Auf Wunsch ist auch die Archivierung interner Mails unter Exchange, Notes, GroupWise und Tobit möglich
- Revisionssichere Archivierung über 10 Jahre
  - Zugriffsmöglichkeiten für die Steuerbehörde: Unmittelbar (Z1), mittelbar (Z2), Datenträger (Z3)
  - Verschlüsselte Archivierung der Daten im Ursprungsformat
  - Einhaltung gesetzlicher Vorgaben
- Mandantenfähigkeit unter Berücksichtigung des Bundesdatenschutzgesetzes
  - Einsicht in Inhalte der E-Mail ist dem Besitzer des Empfängerkontos vorbehalten
  - Zentrale Suchmaske zum Rücksichern einzelner Mails für Helpdesk und Administration
  - Stellvertreterregelung
- Individuelle Einstellungen auf Domain, Gruppen und Benutzerebene möglich
  - Ausschluss der Daten einzelner Nutzer oder von Benutzergruppen (z.B. Betriebsräte möglich)
  - Unterschiedliche Aufbewahrungsfristen (6 Monate für Bewerbungen, 30 Jahre für Buchhaltung)
- Eigene Verwaltung von Revisions- und Audit- Zugängen
  - Zeitliche Einschränkung des Kontrollzugangs
  - Schutz vor Missbrauch durch Nutzung des Vier-Augen Prinzips

## 3 Optionale Leistungen und Services

### 3.1 Spamfilter

Der Hornetsecurity Archiv Service wird direkt im Mail-Datenstrom zwischen Internet und den Mailservern des Unternehmens betrieben. Ein wirksamer Spamschutz ist deshalb von besonderer Bedeutung – einmal zum Schutz des Mailverkehrs vor Denial-of-Service (DoS) Angriffen, aber auch, um keine unerwünschten Daten wie Spam und Viren im Archiv zu speichern. Hornetsecurity bietet den E-Mail Archive-Service deshalb nur in Verbindung mit dem marktführenden Hornetsecurity Spamfilterservice an.

Der Spamfilterservice filtert eingehende E-Mails automatisch auf Spam und Viren. Von Hornetsecurity wird eine Erkennungsrate von 99,9% bei Spam und 99,99% bei Viren vertraglich garantiert. Durch eine

---



zweistufige Architektur wird der überwiegende Teil unerwünschter Nachrichten bereits bei der Verbindungsaufnahme abgewiesen, der verbliebene Rest durch Filter in der zweiten Stufe ausgefiltert und für den Benutzer zugreifbar in der Quarantäne abgelegt oder optional markiert zugestellt.

Detaillierte Informationen über den Hornetsecurity Spamfilterservice entnehmen Sie bitte der Produktdokumentation oder dem Whitepaper „Hornetsecurity Spamfilterservice“.

## 3.2 Managed Archive Appliance

Alternativ zur E-Mail Archivierung in der Hornetsecurity Cloud kann für größere Installationen (ab ca. 500 Nutzer) auch eine Hornetsecurity Managed Archive Appliance zum Einsatz kommen. Mit Einsatz der Managed Archive Appliance wird die Cloud-Lösung zur Hybrid Cloud: Die Speicherung der Daten erfolgt lokal auf Managed Archive Appliances im Rechenzentrum des Kunden, Steuerung und Sicherstellung des Betriebs erfolgen über die Hornetsecurity Cloud.

Verschiedene Modelle der Hornetsecurity Managed Archive Appliance ermöglichen den Einsatz vom mittelgroßen Unternehmen mit einigen hundert Nutzern über große Unternehmen mit mehreren tausend Nutzern bis zum Einsatz bei Providern mit mehreren zehntausend Nutzern. Die Systeme sind intern mit RAID 5, 6 oder 60 (je nach Ausbaustufe) konfiguriert. Zur Herstellung zusätzlicher Sicherheit lassen sich zwei Appliances als Cluster konfigurieren, bei größeren Modellen auch Standort-übergreifend.

Weitere technische Informationen zu den Hornetsecurity Managed Archive Appliance entnehmen Sie bitte dem Datenblatt „Hornetsecurity Managed Archive Appliance“.

## 3.3 E-Mail Verschlüsselung

E-Mails werden in der Regel unverschlüsselt durch ein öffentliches Netz, das Internet, übertragen. Grundsätzlich ist die Verschlüsselung des Transportwegs per TLS (Transport Layer Security) möglich, d. h. nicht die E-Mails selber, sondern der Übertragungskanal wird verschlüsselt. Hornetsecurity nutzt grundsätzlich TLS zur Übermittlung von E-Mails durch das Internet, sofern die Gegenseite ebenfalls TLS unterstützt. Damit sind E-Mails während der Übertragung von einem Mailserver auf den nächsten Mailserver vor Einblick und Veränderung durch Dritte geschützt.

Obwohl viele Mailserver bereits TLS unterstützen, hat sich dessen Benutzung allerdings bisher nicht vollständig durchsetzen können. Ein anderer und auch sichererer Ansatz, die Verschlüsselung der E-Mails selber (nicht des Transportwegs) zwischen Sender und Empfänger, z. B. per S/MIME, wird zwar von vielen Mailprogrammen unterstützt, ist aber sehr aufwändig in der Umsetzung und Betreuung.

Die Alternative ist der Verschlüsselungsservice von Hornetsecurity. E-Mails werden damit im Gateway bei Hornetsecurity vor der Übertragung über das Internet automatisch signiert und verschlüsselt. Sie sind dadurch auf dem gesamten Weg bis zum Empfänger gegen unbefugte Einsicht und Veränderung durch Dritte geschützt. Eingehende E-Mails werden automatisch im Hornetsecurity Gateway entschlüsselt und über TLS geschützt auf den Mailserver des Kunden zugestellt. Die gesamte



Schlüsselverwaltung ist automatisiert. Welche E-Mails verschlüsselt werden, kann per Policy vom Kunden im Control Panel voreingestellt werden.

Weitere Details zum E-Mail Verschlüsselungsservice entnehmen Sie bitte der Produktdokumentation.

## 4 Application Programming Interface (API)

### 4.1 Frontend API

Alle Module des Hornetsecurity Control Panels, z. B. die E-Mail Suche oder die E-Mail Statistik, können als eingebettetes Element (über das HTML-Tag „`<embed>`“) in eigene Web-Applikationen oder Webseiten eingebunden werden. Zur Gewährleistung des Zugriffsschutzes wird dabei ein 256-bit Authentisierungsschlüssel genutzt, der zuvor unter Angabe von Benutzername und Kennwort abgefragt werden muss. Die im Modul genutzte Sprache ist per Parameter im Aufruf einstellbar.

### 4.2 Backend API

Zur engeren Einbindung in Systeme von Partnern und Kunden aber auch zum Aufruf von Funktionen aus anderen Programmen heraus (Abbildung ) wird von Hornetsecurity eine Back-End API bereitgestellt. Die Back-End API ermöglicht Aufrufe und Kommandos direkt in das Backend der Hornetsecurity Cloud. Damit können z. B. Benutzer angelegt und Konfigurationen abgerufen oder verändert werden.

	C	D	E	F	G	H	I	J	K	L
17										
18	status	code	attachment	direction	id	From	To	Date	Subject	Size
19	OK	200	WAHR	IN	4476592	test@web.de	test@web.de	21.07.2011 14:38	test aus web.de	6
20	OK	200	WAHR	IN	4475062	test@web.de	test@web.de	21.07.2011 12:32	Test verschlüsselt und signiert	14
21	OK	200	WAHR	IN	2874612	test@web.de	test@web.de	01.06.2011 11:25	Internet Security Suite	1
22	OK	200	WAHR	IN	1625692	test@web.de	test@web.de	09.04.2011 08:26	Test	1
23	OK	200	WAHR	IN	1254242	test@web.de	test@web.de	10.03.2011 15:46	Test	5
24	OK	200	WAHR	IN	395593	test@web.de	test@web.de	24.01.2011 09:03	Sales Process and CRM	8
25	OK	200	WAHR	IN	392163	test@web.de	test@web.de	23.01.2011 17:55	Test an .com	3
26	OK	200	WAHR	IN	286022	test@web.de	test@web.de	13.01.2011 20:07	Subject:	5
27										
28										
29										
30										
31										

Abbildung 15: Ergebnis einer Suchabfrage im Archiv über die Hornetsecurity Back-End API aus Excel heraus



## 4.3 Voraussetzungen für die Nutzung

Voraussetzung für die Nutzung der API ist die Nutzung eines Hornetsecurity Cloud Service. Wenn Sie die Hornetsecurity Frontend oder Backend API nutzen wollen, nehmen Sie bitte Kontakt mit Hornetsecurity auf.

## 5 Hornetsecurity Aeternum aus Datenschutzsicht

E-Mails sind in der Regel als personenbezogene Daten zu betrachten (siehe auch Kapitel 1.3.2 Datenschutz). Bei der Speicherung von E-Mails im E-Mail Archiv von Hornetsecurity handelt es sich demnach um Datenverarbeitung im Auftrag gemäß §11, BDSG. Hornetsecurity stellt eine Vorlage für eine Datenschutzvereinbarung bereit, die Verantwortlichkeiten und Aufgaben im Rahmen der Auftragsdatenvereinbarung regelt. Bestandteil der Vereinbarung sind die von Hornetsecurity zum Schutz von Kundendaten durchgeführten allgemeinen technischen und organisatorischen Maßnahmen gemäß §9, BDSG.

Weitere, besondere Eigenschaften des Hornetsecurity Archive Service zum Schutz von Kundendaten:

- Nach Mandanten getrennte Datenhaltung in separaten Datenbanken – auch für Indizes,
- Verschlüsselung des Übertragungswegs zwischen Archiv und Mailserver per TLS, sofern vom Mailserver des Kunden unterstützt,
- Ablage von Daten im Archiv in verschlüsselten Speichern,
- Mehrfach redundante Datenspeicher,
- Betrieb in gesicherten Rechenzentren in Deutschland,
  - Anderer Speicherort optional möglich (z.B. RZ des Kunden)
- Löschung und Veränderung von Daten vor Ablauf der Aufbewahrungsfrist ist systemseitig ausgeschlossen,
- Detailliert konfigurierbare Benutzerrechte,
- Kein Zugriff auf Inhalte von E-Mails durch Administratoren des Kunden möglich, sichtbar sind lediglich Header-Daten,
- Ausschluss der Archivierung von Daten einzelner Nutzer (z.B. Betriebsräte) möglich,
- Unterschiedliche Aufbewahrungsfristen einstellbar (z.B. 6 Monate für Bewerbungen),
- Revisor-Zugriff durch vier-Augen-Prinzip geschützt,
- Protokollierung von Revisor-Zugriffen,
- Markierung von Daten als "privat" durch Benutzer möglich, dadurch Zugriffssperre auch für Revisoren (konfigurierbar).



## 6 Quellen

- Dr. jur. Jens Bücking: Leitfaden E-Mail Archivierung; <http://www.voi.de/publikationen/category/3-publikationen?download=48:leitfaden-e-mail-archivierung>
- VOI: Merksätze des VOI zur reversionssicheren elektronischen Archivierung; <http://www.voi.de/publikationen/category/3-publikationen?download=4:merksaetze-des-voi-zur-revisionssicheren-elektronischen-archivierung>
- BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.: Leitfaden E-Mail Archivierung; <https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Leitfaden-E-Mail-Archivierung.html>
- Bundesfinanzministerium: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GoBD); BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01; [http://www.bundesfinanzministerium.de/DE/Wirtschaft\\_und\\_Verwaltung/Steuern/Veroeffentlichungen\\_zu\\_Steuerarten/Abgabenordnung/Datenzugriff\\_GoBD/002,templateId=raw,property=publicationFile.pdf](http://www.bundesfinanzministerium.de/DE/Wirtschaft_und_Verwaltung/Steuern/Veroeffentlichungen_zu_Steuerarten/Abgabenordnung/Datenzugriff_GoBD/002,templateId=raw,property=publicationFile.pdf)
- Christian Böttger: Auf immer mein; iX 6/2011
- Pestel Institut: E-Mail Archivierung – Stand der Aktivitäten und Kenntnisse zum Thema in deutschen Unternehmen; <https://www.hornetsecurity.com/de/services/e-mail-archivierung>
- Wikipedia: E-Mail-Archivierung; <http://de.wikipedia.org/wiki/E-Mail-Archivierung>
- Wikipedia: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen; <http://de.wikipedia.org/wiki/GoBD>

Hornetsecurity ist Mitglied bei:



Hornetsecurity GmbH · Am Listholze 78 · 30177 Hannover

Tel.: +49 511 260 905-0 · Fax: +49 511 260 905-99 · [info@hornetsecurity.com](mailto:info@hornetsecurity.com) · [www.hornetsecurity.com](http://www.hornetsecurity.com)

Umsatzsteuer-ID: DE256599255 · Geschäftsführer: Oliver Dehning, Daniel Hofmann, Daniel Blank · Amtsgericht Hannover · HRB 201937

Hannoversche Volksbank · IBAN: DE 7425 19000 105 735 742 00 · BIC: VOHADE2H