Cobion

Content-Security-Richtlinien in Unternehmen

Ein Leitfaden zur Entwicklung von Content-Security-Richtlinien für die Internet- und E-Mail-Nutzung am Arbeitsplatz

---

Am vorliegenden Leitfaden können sich Unternehmen bei der Konzeption einer Richtlinie orientieren. Trotz sorgfältiger Recherche übernimmt diese Publikation keine Garantie für Vollständigkeit, allgemeine Übertragbarkeit und Rechtsverbindlichkeit. Jedes Unternehmen sollte im Einzelfall vor der Implementierung individueller Richtlinien individuellen Rat suchen.

Diese Informationen sollen unterstützen, aber keinesfalls einseitig in der Gestaltung einer Internet-Zugangspolitik beeinflussen. Sie selbst kennen Ihr Unternehmen und dessen Kultur am besten. Es liegt bei Ihnen, ob Sie sich für einen liberalen oder konservativen Umgang mit dem Internet entscheiden. Doch wie Sie bei der Lektüre feststellen werden, ist es grundsätzlich wichtig, eine konsensfähige Regelung für den Umgang mit E-Mail und Internet am Arbeitsplatz zu finden, zu etablieren, bekannt zu geben und konsequent zu leben.

Wir unterstützen Sie...

Begleitend kann es sinnvoll sein, ein E-Mail- und/oder Internet-Filter-Programm zu implementieren, das höchstmögliche Sicherheit bei der Umsetzung Ihrer Vereinbarung bietet. Als führender Anbieter professioneller Internet- und E-Mail- Management-Software helfen wir Ihnen gerne weiter.

Detaillierte Informationen finden Sie im Internet unter www.cobion.com. Dort können Sie sich auch unsere kostenfreie 30–Tage-Testversion herunterladen.

Cobion AG
Miramstraße 87
34123 Kassel
Tel. +49(0)561 57087-0
Fax +49(0)561 57087-18
info@cobion.de

Cobion

Index

1 Hinführung

Das Internet ist heute als Kommunikationsmedium Nr. 1 etabliert und gehört zu den selbstverständlichsten Werkzeugen der modernen Arbeitswelt. Mitarbeiter arbeiten an Computern und verbringen einen wachsenden Anteil ihrer Arbeitszeit im Netz. Durch die Anbindung der betriebsinternen Netzwerke an das Internet stehen Dienste zur Beschaffung, Verarbeitung und Übermittlung von Informationen für die Mitarbeiter zur Verfügung. Durch diese Dienste beschleunigen sich die Geschäftsprozesse untereinander und gegenüber Interessenvertretungen des Unternehmens.

Was bedeutet Content-Security für Unternehmen?

Content Security dient dazu, den unkontrollierten Datenfluss in ein Unternehmen, innerhalb des Unternehmens und aus einem Unternehmen heraus zu überprüfen und zu managen – gleich einer Zollabfertigung, die kontrolliert, was hinein- oder hinausgeht.

Die zentralen Sicherheitsaspekte sind dabei:

Schutz der Geschäftsintegrität vor

- Nicht-arbeitsrelevantem, unproduktivem Surfen.
- Dem Verlust vertraulicher Unternehmensinformationen und Geschäftsgeheimnisse.
- Unerwünschten oder illegalen Internetinhalten.

Schutz der Netzwerkintegrität vor

- Unangemessener Bandbreitennutzung.
- Übermäßiger Beanspruchung von Speicherkapazität.
- Netzwerkstaus.

Wozu dient eine Content-Security-Richtlinie?

Da viele Mitarbeiter den Internetzugang am Arbeitsplatz auch für private Zwecke, u. a. Online-Spiele, E-Mail, Online-Banking usw. nutzen, sind Kenntnisse über internetspezifische und rechtliche Rahmenbedingungen wichtige Grundvoraussetzungen für einen gewissenhaften Umgang mit dem Internet am Arbeitsplatz. Ohne eine geregelte Internet- und E-Mail-Nutzung sind Rechte und Pflichten von Mitarbeitern nicht klar und eindeutig definiert.

So entstehen neben den Vorteilen des Internet-Zugriffs unterschiedlichste Risiken:

Produktivitätseinbußen

Unbeschränkter Zugang zum Internet stellt für einige Mitarbeiter eine große Versuchung dar, diesen zu nicht-geschäftsrelevanten Zwecken zu nutzen – das Ablenkungspotenzial ist vielfältig. Untersuchungen zufolge nutzen drei von vier Mitarbeitern ihren Dienst-PC auch zum privaten Surfen. Zumeist schreiben sie E-Mails oder lesen Nachrichten.
Auch private Geschäfte werden oftmals vom Arbeitsplatz aus abgewickelt. 31 % derjenigen, die den Online-Zugang im Büro für private Zwecke nutzen, buchten Reisen oder reservierten Plätze. 28 % der Befragten regelten im Büro ihre Bankgeschäfte.

Insgesamt geht man davon aus, dass die private Nutzung des Internets am Arbeitsplatz allein die deutsche Wirtschaft jährlich bis zu dreistelligen Millionenbeträgen kostet. Die folgenden Daten untermauern dies:

- Laut IDC[1] sind 30 – 40 % der Internetaktivitäten von Angestellten nicht arbeitsbezogen.

- Ferris Research[2] hat in den USA ermittelt, dass der durchschnittliche E-Mail-Benutzer 25 % seiner täglichen Arbeitszeit für das Bearbeiten von E-Mails aufwendet – Tendenz steigend.

[1] IDC ist der weltweit führende Anbieter der IT-Marktbeobachtung und Beratung.
[2] How E-Mail Affects Productivity, Ferris Research, Document ID: 20000202SM, (02/2000).

- Laut Gartner Institute[3] sind die meisten Benutzern von der Flut ihrer E-Mails überfordert, außerdem geht ein hoher Anteil des E-Mail-Aufkommens nach einer Untersuchung von vault.com auf das Konto privater Nutzung – so gaben 30 % der Arbeitnehmer mit Internetzugang an, täglich bis zu zehn private E-Mails zu versenden.

- Marktforschungsstudien von Taylor Nelson Sofres zufolge surfen 93 % der deutschen Arbeitnehmer privat am Arbeitsplatz.[4]

- Eine Studie der Finanzzeitschrift „Capital" ergab, dass falls jeder der 5000 Mitarbeiter einer Bausparkasse pro Tag 15 Minuten im Internet surft Personalkosten in Höhe von rund 6,5 Millionen Euro jährlich entstehen.[5]

Berechnen Sie, wie viel privates Surfen Ihr Unternehmen kostet - unter **www.cobion.com/roi_calculator_de.htm.**

ROI-Calculator

Engpässe oder Überlastung im Netzwerk

Wenn privates Surfen mit bandbreitenintensiven Aktivitäten, wie z. B. MP3-Downloads, DVDs oder dem Download von Bildern einhergeht, so bedeutet dies eine verstärkte Belastung der Netzwerkleistung innerhalb des Unternehmens.
Geschieht dies während der üblichen Bürozeiten, kann es zu ernsthaften Engpässen bis hin zur Behinderung der Netzwerkfunktion und des geschäftlichen Internet-Verkehrs führen.
In Deutschland werden z. B. die Kosten, die der bundesweite Download des Moorhuhn-Computerspiels verursachte, laut ZDNet Deutschland auf mehr als 50 Millionen Euro geschätzt.
Eine weitere typische Ursache sind unaufgeforderte E-Mails-Sendungen, sogenannte Spam-E-Mails, die zusätzlich Zeit- und Netz-Kapazitäten beanspruchen.
Ferris Research geht davon aus, dass der Spam-Anteil von eingehenden E-Mails in den nächsten fünf Jahren von heute etwa 10 % auf 40 % ansteigen wird.

[3] Survey of Internet Use in the Workplace, Vault.com, (2000).
[4] Chip Online (2001).
[5] Techchannel (2001).

Ein Bericht der Europäischen Kommission[6] besagt, dass allein durch Spam-E-Mails Kosten von rund zehn Milliarden Euro weltweit entstehen (dieser Wert basiert auf den errechneten Downloadzeiten für E-Mails). Und laut einer Umfrage von Gartner, in der 13.000 E-Mail-Benutzer befragt wurden, gaben rund 50 % an, sechsmal oder häufiger täglich Spam-E-Mails am Arbeitsplatz zu erhalten.

Gesetzliche Haftung

Arbeitgeber sind verantwortlich und haftbar für die Tätigkeiten („illegale Surftrips") ihrer Mitarbeiter am Arbeitsplatz. Mit zunehmender Internet-Nutzung in Unternehmen zeigte sich das Problem der gesetzlichen Haftung, zunächst ausgehend aus den USA, mittlerweile rund um den Globus.
Einer Studie von SexTracker zufolge erfolgen beispielsweise etwa 70 % aller Zugriffe auf Pornoseiten an Werktagen zwischen 9.00 und 17.00 Uhr. Die Folgen können Klagen der Mitarbeiter sein, die sich durch solche Inhalte, zum Beispiel auf dem Bildschirm des/der Kollegen/in, belästigt fühlen.

Probleme mit dem Urheberrecht können durch Downloads von Software, Fotografien oder urheberrechtlich geschützten Dokumenten entstehen und rechtliche Konsequenzen mit sich bringen – und das nicht nur bei illegalen Inhalten wie z. B. Kinderpornografie.

Kann ein Unternehmen eine "Sorgfaltspflicht" nachweisen, um inakzeptables Verhalten von Mitarbeitern zu verringern, so kann das Haftungspotenzial auf ein Minimum beschränkt werden.

Vertrauensmissbrauch

Laut einer Studie des F.B.I. (2000) geht jeder zweite aktive oder passive, sprich ungewollt ausgelöste, Angriff auf ein Unternehmen auf das Konto eines Mitarbeiters.

[6] Informationen im Internet http://europa.eu.int/comm/index_de.htm.

In den USA beträgt der Anteil der internen Anschläge nach dieser Studie bereits 63 %. Eine Umfrage der PC Week (1999) ergab, dass 31 % der Befragten, absichtlich oder versehentlich vertrauliche Informationen an Adressaten außerhalb ihrer Organisationen verschickt haben. Unbeabsichtigt oder beabsichtigt – die Verletzung der Geheimhaltungspflicht stellt eine Bedrohung für Unternehmen dar, deren Folgen verheerende Auswirkungen auf das Vertrauen von Kunden und Märkten haben.

Ein Beispiel:
Sendet ein Mitarbeiter versehentlich eine E-Mail an alle in der Verteilerliste vorhandenen Empfänger, ohne die unternehmensfremden Adressaten auszusortieren, können so vertrauliche Daten das Unternehmen verlassen und verbreitet werden. Die vorsätzliche Verbreitung einer Kundendatenbank wäre gar ein geplanter Sabotageakt.
Apple Computer klagte z. B., weil ein Mitarbeiter Bilder von zwei Neu-Produkten vor deren offizieller Markteinführung im Internet veröffentlicht hatte. Dadurch war der Kurs der Apple-Aktie an der NASDAQ stark abgefallen.[7]

Imageschäden

Neben den strafrechtlichen Folgen für die verantwortlichen Unternehmer gehen Fälle von Missbrauch eines allgemeinen Internetzugangs meist mit einer massiven Rufschädigung einher.

Die gleiche Problematik besteht durch die Nutzung von E-Mail. Aktionen durch verärgerte Mitarbeiter oder auch unbeabsichtigt versendete Informationen per E-Mail, die durch Mitarbeiter ausgelöst werden, können zu negativen Meldungen über ein Unternehmen führen und deren Außenwirkung und Reputation nachhaltig beeinträchtigen.
Daraus resultiert nicht nur ein langfristiger Imageverlust, sondern auch ein Vertrauensverlust bei den Verbrauchern und eventuell sogar ein Absturz des Aktienkurses. Die Schädigung des Ansehens des Unternehmens kann somit zu einer ernsthaften Bedrohung werden.

Der Arbeitgeber hat die rechtliche Verantwortung für die Inhalte, die durch seine Mitarbeiter übermittelt werden. Aus diesem Grund ist die Möglichkeit eine Gewährausschlusserklärung an E-Mails anzuhängen immer wichtiger geworden.

[7] Reuters English News Service (August 2000).

Tipp

Beispiel:
„Diese E-Mail, einschließlich sämtlicher mit ihr übertragenen Dateien, ist vertraulich und für die ausschließliche Verwendung durch die Person oder das Unternehmen vorgesehen, an die/das sie adressiert ist. Für den Inhalt dieser E-Mail ist allein der Autor verantwortlich, Inhalt und Meinung müssen nicht die Ansicht der Firma (Name) wiedergeben."
(Vergleiche Anlage B, Position 1.3, Gewährausschlusserklärung)

Weitere Maßnahmen sind:

- Flankierende Maßnahmen zur Aufklärung und Information aller Mitarbeiter.
- Nutzung von E-Mail- und Internet-Management Lösungen zur Prävention.

Gefährdung der allgemeinen Datensicherheit

Neben den Sicherheitsrisiken von außen, werden die meisten sicherheitsrelevanten Vorfälle durch die eigenen Mitarbeiter verursacht.

Ein Großteil davon hängt eng mit dem Internet zusammen: Der Download von gefährlichen Codes wie etwa Viren, Trojanern und Würmern oder das Versenden von unternehmensinternen Informationen per E-Mail sollen als Beispiele dafür stehen.

2 Einführung von Content-Security-Richtlinien

Mit keiner anderen Kommunikationstechnik können Informationen so schnell, so weitreichend und in so komplexer Form verbreitet und genutzt werden. Viele Unternehmen haben dies erkannt und setzen die neuen Techniken ein, um ihre Ziele zu erreichen.
Die Frage ist, ob dabei die Interessen der Mitarbeiter und ihrer Interessenvertretungen ausreichend berücksichtigt werden.

Dieses setzt voraus, dass sowohl Mitarbeiter, Betriebs- und Personalräte als auch Gewerkschaften gleichberechtigten Zugang zu den Kommunikationsmitteln erhalten.

Neben den Vorteilen eines allgemeinen Internetzugangs ist es Unternehmen zu empfehlen, ihre ganz individuelle Vereinbarung zur E-Mail- und Internet-Nutzung am Arbeitsplatz zu entwickeln und diese in ihre Unternehmensstruktur einzubinden.

Begleitend dazu ist es sinnvoll, die Einhaltung dieses Regelwerks durch professionelle E-Mail- und Content-Security-Lösungen zu unterstützen.

Das Anliegen des Arbeitgebers besteht im Hinblick auf Internet- und E-Mail-Nutzung in der Schaffung und Aufrechterhaltung der Systemsicherheit. Aus diesem Grund hat der Arbeitgeber das Recht den Datenverkehr zu filtern. Hierbei sollen entsprechend allgemeiner Vorschriften die verwendeten Protokolle des Internets, E-Mail-Adressen, der Zeitpunkt etc. protokolliert werden. Beispielhaft sei hier das Scannen von sogenannten E-Mail-Attachments genannt.

Gewerkschaftliche Kommunikation

Es ist zu berücksichtigen, dass die Überwachung der Arbeitnehmer mittels technischer Einrichtungen der Mitbestimmung des Betriebsrates unterliegt
(§ 87 Absatz 1 Nr. 6 BtrVG).

Bedeutung des Datenschutzes für den Arbeitnehmer

Eine pauschale und undifferenzierte Überwachung des E-Mail-Verkehrs von Mitarbeitern verstößt grundsätzlich gegen das allgemeine Persönlichkeitsrecht (§ 823 Absatz 1 BGB).

Der Persönlichkeitsschutz ist durch betriebliche Interessen des Arbeitgebers begrenzt. Der Arbeitgeber hat einerseits die Sicherheit seines EDV-Systems zu gewährleisten und muss außerdem dafür sorgen, dass bei krankheits- oder urlaubsbedingter Abwesenheit eines Mitarbeiters die (elektronische) Post eingesehen werden kann (§ 9 BDSG).

Betriebliche Regelungen

Ob der Arbeitnehmer das Telekommunikationssystem des Arbeitgebers benutzen darf, richtet sich nach dem Inhalt des Arbeitsvertrages oder einer entsprechenden Betriebsvereinbarung.

Unter Umständen liegt eine betriebliche Übung (Gewohnheitsrecht) vor, die voraussetzt, dass die entsprechende Praxis für den Arbeitgeber wenigstens erkennbar war und die Arbeitnehmer darauf vertrauen konnten, dass es auch in Zukunft beim aktuellen Zustand bleiben werde.

Ebenso ist auch eine konkludente Lösung[8] möglich:
Wenn z. B. privates Telefonieren erlaubt ist, kann der Arbeitnehmer davon ausgehen, dass in vergleichbarem Umfang auch private E-Mail-Nutzung oder privates Surfen möglich ist.

[8] Konkludente Handlungen: Handlungen, die als (nicht ausdrückliche) Willenserklärung angesehen werden, alles das gelten zu lassen, was nach der Lebens- und Rechtserfahrung aus eben solchen Handlungen gefolgert werden kann.

3 Ziele einer Content-Security-Richtlinie

Ziele

Die Vereinbarung sollte...

- Eine klare Definition der Unternehmenspolitik bezüglich des Gebrauchs von Internet und E-Mail am Arbeitsplatz wiedergeben. Je detaillierter die Richtlinien, desto klarer sind später jedem Einzelnen Rechte und Pflichten.
- Sicherheitsrisiken durch Anregung zu Umsicht und professioneller Praxis vermeiden.
- Den Schutz des Unternehmens vor rechtlicher Haftung gewähren.
- Die Mitarbeiter zu einem effektivem und positivem Gebrauch der Netzwerk-Ressourcen anhalten.

Alle Mitarbeiter müssen die Folgen einer Zuwiderhandlung kennen, d. h. Sanktionen für ein- und mehrmalige Verstöße müssen definiert und Konsequenzen dargestellt werden.
Nach Verabschiedung einer Betriebsvereinbarung sollte Augenmerk auf die Pflege der Richtlinien gelegt werden. Ständige Veränderungen im Geschäftsleben z. B. beim Mitarbeiterstand, in den Geschäftspraktiken oder in der Internet-Technologie machen dies notwendig. Um auf Dauer zu bestehen, sollte Ihre Vereinbarung dies alles unterstützen. Der Anspruch, dass die einmal gewählten Regeln für Ihr Unternehmen sinnvoll und richtig sind, kann sich erst in der täglichen Arbeit erweisen.

Siehe auch Verwaltung von Richtlinien

Um die Einhaltung des Regelwerks zu überprüfen, ist es wichtig, technische Lösungen zu implementieren, die dessen Einhaltung sehr wahrscheinlich machen. Viele Unternehmen nutzen die dynamische Lösung einer E-Mail- bzw. Web-Filtersoftware. Deren Vorteile sind hohe Differenzierungsmöglichkeiten in Fragen der individuellen und kollektiven Zugangsrechte.

4 Die Umsetzung einer Richtlinie

Umsetzung

Vereinbarungen zur E-Mail- und Internet-Nutzung am Arbeitsplatz sind auf jeden Fall umzusetzen! Zum einen dienen sie als Absicherung des Arbeitgebers, zum anderen erhalten die Mitarbeiter ein schriftliches Regelwerk, woran sie sich bei Fragen rund um E-Mail- und Internet-Nutzung orientieren können.

Bitte beachten

Was Sie vor Einführung von Content-Security-Richtlinien beachten sollten:

- Sensibilisierung aller Mitarbeiter.
  Für den Umgang von E-Mail und Internet am Arbeitsplatz ist Information und Aufklärung wichtig, um Verständnis für mögliche Einschränkungen zu wecken.

- Teamorientierte Ausarbeitung der Richtlinien.
  Erarbeiten Sie ein Richtlinienpaket, welches von einer breiten Basis im Unternehmen getragen wird. Sinnvoll ist es ein paritätisch besetztes Gremium zu bilden, welches aus Vertretern der Geschäftsführung, der Mitarbeiter sowie des Betriebsrates zusammengesetzt ist.

- Klären Sie den Umfang der privaten Internet-Nutzung.
  Es ist evtl. durchaus sinnvoll, die private Nutzung des Internet im Rahmen der Freizeit, z. B. vor und nach der Arbeit oder während der Mittagspause, zu gestatten.

- Wer kann was?
  Die Frage des Internetzugangs am Arbeitsplatz muss nicht für alle Arbeitnehmer gleich behandelt werden. Je nach Abteilung und Arbeitsaufgabe macht es durchaus Sinn, Einzelpersonen weitergehende Rechte im Umgang mit ihrem Internetzugang zu gewähren als anderen.

- An welcher Stelle wird für uns der Verwendungszweck einer Content-Security-Software sichtbar und an welcher nicht?

- Sorgen Sie für eine schriftliche Ausarbeitung und deren Verbreitung im Unternehmen.
  Die Nutzungs-Richtlinien sollten eindeutig, allgemein verständlich und ohne Fachbegriffe formuliert sein. Legen Sie wert auf positive Formulierungen.

- Definieren Sie Sanktionen bei Verstößen gegen die Content-Security-Richtlinien.
  Erstellen Sie Regelungen für den Fall von einmaligen oder mehrmaligen Zuwiderhandlungen. Weisen Sie auch darauf hin, dass illegale Internet-Aktivitäten behördlich angezeigt werden.

- Implementierung der unterstützenden Maßnahmen.

5 Einhaltung der Nutzungsrichtlinien durch Content-Security-Lösungen

Das Ziel einer Internet-Nutzungsvereinbarung ist es, dass sich alle Mitarbeiter eines Unternehmens nach ihr richten und diese einhalten. Daher sollte sich das Unternehmen überlegen, mit welchen zusätzlichen Maßnahmen sie die Einhaltung der Nutzungsrichtlinien unterstützen bzw. gewährleisten kann.

Der Markt bietet unterschiedlichste Filterlösungen an, die ein hohes Maß an Sicherheit in allen Fragen der Internet-Nutzung am Arbeitsplatz generieren.

Content-Security-Lösungen sind technische Werkzeuge, die sich an den individuellen Richtlinien anlehnen sollten und nicht umgekehrt.

Je detaillierter das Unternehmen seine Richtlinien ausgearbeitet hat, desto einfacher ist es, sie mit modernen Filter-Lösungen umzusetzen.

! Tipp

Ein Test der angedachten Lösung im Vorfeld der Einführung ist dringen anzuraten.

6 Was sollte Ihre Content-Security-Lösung heute bieten?

Individuelle Konfigurationsmöglichkeiten

In einem Unternehmen existieren vielfältige Arbeitsplätze mit vollkommen unterschiedlichen Bedürfnissen, was den Zugriff auf Informationen aus dem Internet angeht.
Eine geeignete Filterlösung sollte dies berücksichtigen können und individuell konfigurierbare Benutzerprofile und ein hohes Maß an Differenzierungsmöglichkeiten bieten.

Dazu gehört z. B. sowohl eine zeitliche Staffelung als auch die Berücksichtigung von Einzel- oder Gruppeninteressen. Überprüfen Sie daher, ob individuell konfigurierbare Profile angelegt werden können nach:

- Benutzern
- Benutzergruppen
- IP-Adressen
- Rechnernamen

Aktualität der Filterliste

Um mit dem rasanten Wachstum des Internets standhalten zu können, sollten dynamische E-Mail- und Internet-Filter-Lösungen implementiert werden.
So kann über eine wachsende URL-Filterdatenbasis[9] eine hohe Abdeckung und Aktualität gewährleistet werden. Viele Anbieter von Filtersoftware arbeiten an diesem Punkt ausschließlich mit dem Faktor „Mensch", das heißt sie beschäftigen Personen, die Internetinhalte manuell klassifizieren – eine langwierige Arbeit, die nur einen Bruchteil der täglichen Veränderungen abbilden kann.

[9] Uniform Resource Locator, Abk. URL, die Adresse, durch die ein Dokument im World Wide Web eindeutig gekennzeichnet wird.

Cobion beispielsweise setzt dagegen in diesem Zusammenhang vollautomatische Verfahren ein, um Internetseiten zu analysieren. Mit Hilfe der inhaltsbezogenen Analyse werden Bilder, Symbole, grafische Abbildungen, Gesichter und Texte auf Webseiten erfasst, analysiert und entsprechend bewertet. Dabei kommt eine Kombination von Text- und Bilderkennung zum Einsatz, die durch Verbinden von semantischer und bildbezogener Analyse ein exaktes Klassifizieren ermöglicht.
Zusätzlich werden Seiten manuell überprüft. Das sorgt für eine niedrige Fehlerquote und eine hohe Qualität der Filterkategorien. Hinzu kommt, dass die Cobion-Filterliste permanent in elf Sprachen gepflegt wird und deutschsprachige Inhalte berücksichtigt. Über ein tägliches Update der Filterliste wird garantiert, dass die implementierte Nutzungsrichtlinie stets zuverlässig umgesetzt und eingehalten werden kann.

Lernendes System

Unterschiedliche Unternehmen weisen ein unterschiedliches Surfverhalten auf. Eine intelligente Content-Security-Lösung sollte dies berücksichtigen und nutzen können. Die Cobion–Filterliste passt sich optimal an das Surfverhalten von Unternehmen oder Organisationen an. Über „WebLearn" können Unternehmen alle aufgerufenen Seiten, die in die Rubrik „nicht kategorisierte Seiten" fallen, automatisiert an das Cobion-Rechenzentrum übermitteln. Die URLs werden dort mit erhöhter Priorität dem maschinellen Kategorisierungsprozess zugeführt und in die entsprechenden Kategorien eingetragen. Insgesamt stehen 58 Haupt- und Unterkategorien zur Verfügung, um Internet-Inhalte zu klassifizieren. Die Resultate werden - zusätzlich zu den neuen URLs, die der Cobion Filterliste täglich hinzugefügt werden - in die globale URL-Datenbank aufgenommen.
Innerhalb des täglichen Aktualisierungsprozesses werden diese der gesamten Cobion-Benutzergemeinde zur Verfügung gestellt. Die Filterdatenbasis wird so permanent um firmenindividuelle Internetanfragen erweitert und optimiert.

Hohe Skalierbarkeit

Die geeignete Content-Security-Lösung sollte zukünftige Entwicklungen des Unternehmens, wie z. B. Expansion oder den Aufbau von Niederlassungen, berücksichtigen können. Daher sollte die Lösung auch eine große Anzahl von Benutzern oder Benutzergruppen handhaben und managen können.

Die Umsetzung der Nutzungsrichtlinien ist zentral auf weitere Niederlassungen oder Filialen zu übertragen.
Stellen Sie daher sicher, wie weit die Content-Security-Lösung mit Ihrem vorhandenen Netzwerk harmonisiert.

Tipp

Setzen Sie in Ihrem Unternehmen vorab nur eine E-Mail oder Internet-Filter-Lösung ein, ist darauf zu achten, dass die gewählte Software kompatibel zu weiteren Content-Security-Produkten ist.

Umfassender Support

Verlässlicher Support ist ein entscheidender Erfolgsfaktor! Überprüfen Sie daher, ob Ihr Software-Anbieter Ihnen diesen bieten kann und in welchem Umfang dieser angeboten wird (First-, Second-, Third-Level-Support, Hotline, 24 Std.-Support)?

Bitte beachten

Ihre gewählte Filter-Lösung wird über Reporting-Tools verfügen, die Ihnen nach vorab erstellten Regeln Auswertungen über die Nutzung des Internet-Zugangs liefern. Die Möglichkeit solcher Reportings bei Filter-Programmen ruft immer wieder Kritiker auf den Plan.
Wie detailliert allerdings ein Reporting ist, hängt von der gewählten Lösung und von der Zustimmung des Betriebsrates, sowie von der Rechtslage am Einsatzort ab. So gelten in den USA beispielsweise gänzlich andere Regelungen als in der Bundesrepublik Deutschland. Generell ist es allerdings auch ohne eine Filter-Lösung möglich, über das Log-file die Internet-Aktivitäten von Mitarbeitern zu dokumentieren und auszulesen. Hier setzen aber die rechtlichen Regelungen Grenzen, die auch bei einem Einsatz von Filterlösungen zu beachten sind.

Prävention statt Kontrolle

Intelligente Filter-Lösungen haben nicht das Ziel, eine personenbezogene Auswertung der Internet-Zugriffe bereitzustellen. Vielmehr liefern diese einen Bericht über die Nutzung des Internets, um mögliche Schwachstellen in den Nutzungs-Richtlinien aufzuzeigen und um notwendige Modifizierungen aufzuzeigen.

7 Verwaltung von Content-Security-Richtlinien

Verwaltung

Mit der Implementierung von Richtlinien zur privaten E-Mail- und Internet-Nutzung am Arbeitsplatz ist die Aufgabe für die Beteiligten NICHT erledigt – es handelt sich hier vielmehr um einen fortlaufenden Prozess! Warum?
Eine Übereinkunft über die Entwicklung und Einführung von Nutzungsrichtlinien und die Umsetzung durch intelligente E-Mail- und Internet-Management-Lösungen sind die ersten Schritte – die heutige Zeit ist aber geprägt von permanenten Veränderungen, sowohl die Internet-Technologie als auch die Anzahl Ihrer Mitarbeiter oder deren Zugehörigkeit zu Abteilungen oder Projekten.

Bitte beachten

Ihre Richtlinie sollte daher in regelmäßigen Abständen auf folgende Punkte hin überprüft werden:

- Ist die Nutzungsrichtlinie angesichts permanenter Internetinhalte noch aktuell? Überarbeiten Sie Ihre Richtlinien regelmäßig. Lassen Sie die Änderungen durch das leitende Management bestätigen und machen Sie diese Bestätigung im Unternehmen bekannt.

- Werden Ihre Mitarbeiter ausreichend über die Nutzungsrichtlinie informiert? Kommunizieren Sie die Nutzungsrichtlinien regelmäßig im Unternehmen. Schulen Sie Ihre Mitarbeiter in den Richtlinien und geben Sie Gelegenheit zu Fragen und Anmerkungen.

- Erhalten sie in regelmäßigen Abständen Updates Ihrer Filter- und Antivirenlösungen?
  Schützen Sie sich vor neuen Gefahren, indem Sie ihre Unternehmenslösung für Content-Security in regelmäßigen Abständen aktualisieren. Stellen Sie sicher, dass Sie die neueste Version ihrer Content-Security-Software besitzen.

- Ist Ihre Nutzungsrichtlinie individuell abgestimmt – oder werden Mitarbeiter bei der Verrichtung von Tätigkeiten behindert?

- Löschen Sie die Nutzungsrechte von Ex-Mitarbeitern zeitnah.

- Lassen Sie sich bei Neueinstellung von Mitarbeitern per Unterschrift die Kenntnisnahme und Akzeptanz der Nutzungs-Richtlinien bestätigen, bevor er Internet-Zugang erhält.

- Benötigen einzelne Mitarbeiter/Projektgruppen/Abteilungen geänderte Zugriffsrechte? Überprüfen Sie in regelmäßigen Intervallen die Benutzerrechte für Einzelpersonen, Gruppen oder Abteilungen.

- Erhalten Sie Rückmeldung und arbeiten diese in Ihre Nutzungsvereinbarung um?

- Welche eventuellen Gesetzesänderungen sind aufgetreten?

! Tipp

Bei Modifizierungen Ihrer Nutzungsrichtlinien sind diese offen im Unternehmen zu kommunizieren, das heißt sowohl alle Mitarbeiter als auch der Betriebsrat sollten umfassend informiert werden, eventuelle Unklarheiten sind eindeutig zu klären.

8 Rechtliche Eckdaten

- Die Internet-Nutzung am Arbeitsplatz berührt Fragen des Arbeitsrechts und des Datenschutzes sowie unter Umständen strafrechtliche Aspekte. Diese ergeben sich beim illegalen Verhalten im Umgang mit dem Internet.
  Besonders wichtig ist dabei der Schutz minderjähriger Auszubildender. Hier müssen die Inhalte den Richtlinien des Jugendschutzes entsprechen, da sonst Haftungsrisiken durch eventuelle Belästigung für den Arbeitgeber entstehen (StGB § 86a, § 130f, § 184).

- Es gibt keinen gesetzlichen Anspruch auf Internet-Nutzung am Arbeitsplatz. Die Entscheidung hierüber obliegt dem Arbeitgeber.

- Eine Rücknahme der Erlaubnis ist prinzipiell möglich. Relativ problemlos kann allerdings nur die Betriebsvereinbarung gekündigt werden.

- Entscheidend ist immer die Frage nach dienstlicher oder privater Nutzung des Internets. Ist die Nutzung privater Natur, stellt sich die Frage, ob diese erlaubt ist, stillschweigend geduldet oder grundsätzlich untersagt ist.

- Auch für die private Nutzung von E-Mail am Arbeitsplatz existiert kein gesetzlicher Anspruch. Der Arbeitgeber kann einseitig bestimmen, ob eine private Nutzung durch den Arbeitnehmer erlaubt bzw. untersagt ist. Wird die private Internet-Nutzung jedoch wissentlich geduldet, kann eine betriebliche Übung bestehen. Diese erlaubt es dem Arbeitnehmer, das Internet für private Zwecke zu benutzen.

- Bei den Kontrollmöglichkeiten der Internet-Nutzung durch den Arbeitgeber ist entscheidend, ob eine dienstliche oder private Nutzung vorliegt. Bei einer privaten Nutzung des Internets muss des weiteren unterschieden werden, ob dies mit oder ohne Erlaubnis des Arbeitgebers erfolgt. Der Arbeitgeber ist grundsätzlich berechtigt, die Leistung eines Arbeitnehmers zu überprüfen und sich darüber zu informieren, wie der Arbeitnehmer seine Arbeitsleistung erbringt. Zu diesem Zweck darf er z. B. den Inhalt geschäftlicher E-Mails des Arbeitnehmers einsehen.

- Anders ist es bei der erlaubten privaten Nutzung der E-Mail. Falls die private Nutzung zulässig ist, greifen die Vorschriften des Telekommunikationsgesetzes (§ 85 Absatz 1 TKG) sowie Vorschriften zum Allgemeinen Persönlichkeitsrecht des Arbeitnehmers (§ 823 Absatz 1 BGB)[10]. Daraus ergeben sich kaum Kontrollmöglichkeiten. Ausnahme: Schwerwiegende strafbare Handlungen des Arbeitnehmers.

- Bei einer unerlaubten privaten Nutzung sind die Kontrollmöglichkeiten umfassender. Es geht in diesem Fall um die Abwägung zwischen dem Interesse des Arbeitgebers und dem Persönlichkeitsrecht des Arbeitnehmers. Dieses kann z. B. zutreffen, wenn es um den Schutz von Geschäftsgeheimnissen geht.

- Verstößt der Arbeitnehmer gegen das Verbot der privaten Nutzung, riskiert er arbeitsrechtliche Sanktionen von einer Abmahnung bis hin zur Kündigung. Die Art der Sanktion ist grundsätzlich von der Schwere des Verstoßes und von der Zulässigkeit der Kontrollmöglichkeiten abhängig. Hierzu ist immer eine Einzelfallbetrachtung notwendig. Wichtig in diesem Zusammenhang: Informationen, die z. B. unter Missachtung des Persönlichkeitsrechts des Arbeitnehmers oder des Mitbestimmungsrechts des Betriebsrats[11] gewonnen werden, dürfen nicht gegen den Arbeitnehmer verwendet werden.

- Rechtliche Grundlagen der Internet-Nutzung stellen unter individualrechtlichen Gesichtspunkten z. B. Arbeitsverträge oder einseitige Bestimmungen des Arbeitgebers dar. Kollektivrechtliche Grundlage kann beispielsweise eine Betriebsvereinbarung sein.

- Sollen die Einführung technischer Maßnahmen zur Regelung der Internet-Nutzung im Unternehmen eingeführt werden, ist auch hier wieder zwischen individualrechtlichen Aspekten, die sich aus der bisherigen Nutzung im Unternehmen ergeben, und kollektivrechtlichen Aspekten zu unterscheiden. Darunter sind die Informations- und Mitbestimmungsrechte des Betriebsrates zu verstehen.

---

[10] Vgl. „Möglichkeiten des Arbeitgebers zur Überwachung der E-Mail-Kommunikation des Arbeitnehmers", Pos. 4. Das Fernmeldegeheimnis des Telekommunikationsgesetzes, www.afs-rechtsanwaelte.de/artikel13.htm.

[11] Die Überwachung der Arbeitnehmer mittels technischer Einrichtungen der Mitbestimmung des Betriebsrates unterliegt § 87 Abs. 1 Nr. 6 BtrVG.

- Im Falle der Einführung einer Content-Security-Lösung muss, nach derzeit geltendem Recht, der Betriebsrat vor deren Implementierung zustimmen.[12]
  Fehlt die Zustimmung des Betriebsrates, kann der Betriebsrat vom Arbeitgeber verlangen, dass eine weitere Nutzung unterlassen wird, bis eine Einigung erreicht ist. Schlussfolgerung dessen kann nur sein, dass bevor die Content-Security-Lösung eingeführt werden soll, die Entwicklung und Verabschiedung einer Betriebsvereinbarung zur Internet-Nutzung im Konsens notwendig ist.

[12] Siehe auch Ausführung zu: Konludente Handlungen, betriebliche Regelungen, S.11

9 Die derzeitige Rechtsprechung

Fristlose Kündigung aufgrund privaten Surfens oder E-Mailings in...

Deutschland

Arbeitsgericht Düsseldorf
Einem Arbeitnehmer wurde ohne vorherige Abmahnung fristlos gekündigt, weil er abredewidrig während der Arbeitszeit Dateien mit pornografischem Inhalt in erheblichem Umfang vom Netz heruntergeladen und auf dem betriebseigenen PC gespeichert hatte.

Arbeitsgericht Hannover
Fall 1
Einem Arbeitnehmer wurde ohne vorherige Abmahnung fristlos gekündigt, weil er den Internetzugang seines Arbeitgebers benutzt hatte, um private Pornografie-Webseiten zu unterhalten. Der Arbeitgeber ist zudem ein Verband mit Schwerpunkt in der Jugendförderung.

Fall 2
Einem Angestellten wurde fristlos gekündigt, weil er während der Arbeitszeit Dateien mit pornographischem Inhalt auf seinen Dienst-PC heruntergeladen hatte (CHIP Online, Arbeitsgericht Hannover, Az.: 1 Ca 504/00B).

Veröffentlichungen zu diesem Fall in der (Fach-)Presse (Auszug)

- Capital, Heft 24/2001, S. 130.
- FOCUS, Heft Nr. 48/2001, S. 182.
- Neue Zeitschrift für Arbeitsrecht 2001, S. 1022 - 1024.
- Neue Juristische Wochenschrift 2001, S. 3500 - 3502.

Arbeitsgericht Wesel
Fristlose Kündigung ohne vorherige Abmahnung wurde für unwirksam erklärt, da kein ausdrückliches Verbot privaten Internetsurfens bestand (ArbG Wesel Urteil vom 21.03.01- 5 Ca 4021/00).

Die Rechtsprechung zu diesem Fall
Was passieren kann, wenn keine Regelung getroffen wird, zeigt das Urteil des Arbeitsgerichts Wesel vom 21.03.01:
Die Klägerin arbeitet seit circa sechs Jahren als Buchhalterin bei der Beklagten. Im August/September1999 wurde im Betrieb eine neue Computeranlage installiert. Der Arbeitgeber behauptet, die AN habe zwischen September 1999 bis September 2000 circa 80 – 100 Stunden während der Arbeitszeit im Internet zu Privatzwecken gesurft.
Der Arbeitgeber sprach im September 2000 eine ordentliche Kündigung aus. Mit Schreiben vom 15.12.00 kündigte der Arbeitgeber das Arbeitsverhältnis fristlos, ohne vorherige Abmahnung.

Die fristlose Kündigung ist unwirksam.

Ein Arbeitsverhältnis kann nur dann fristlos gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann.
Ob ein wichtiger Grund im Einzelfall vorliegt, muss in zwei Schritten geprüft werden:

1. Es ist festzustellen, ob ein Sachverhalt an sich geeignet ist, einen wichtigen Kündigungsgrund abzugeben. Das ist der Fall, wenn der Sachverhalt zu einer konkreten Beeinträchtigung des Arbeitsverhältnisses geführt hat.

2. In einer zweiten Stufe ist zu erörtern, ob nach Abwägung aller in Betracht kommenden Interessen der Parteien die konkrete Kündigung gerechtfertigt ist.

Inwieweit eine private Nutzung des betrieblichen Internetanschlusses eine arbeitsvertragliche Pflichtverletzung darstellt, die eine Kündigung rechtfertigt, ist bislang durch die Rechtsprechung noch nicht geklärt. Bei vergleichbaren arbeitsvertraglichen Pflichtverletzungen (z. B. privates Telefonieren am Arbeitsplatz) ist anerkannt, dass eine Kündigung dann gerechtfertigt sein kann, wenn ein ausdrückliches Verbot des Arbeitgebers vorliegt und der Arbeitnehmer diesem Verbot auch nach einschlägiger Abmahnung zuwiderhandelt.
Überträgt man diese Rechtsprechung auf Fälle des privaten Internetsurfens, ergeben sich folgende Grundsätze:

1. Nutzt der Arbeitnehmer das Internet entgegen einem ausdrücklichen Verbot des Arbeitgebers für private Zwecke, so stellt dies eine arbeitsvertragliche Pflichtverletzung dar, die eine Kündigung rechtfertigen kann.

2. Hat der Arbeitgeber die private Nutzung genehmigt bzw. über einen längeren Zeitraum hinweg widerspruchslos geduldet, ist eine Kündigung nur im Ausnahmefall möglich, nämlich dann, wenn die Nutzung in einem Ausmaß erfolgt, von dem der Arbeitnehmer nicht mehr annehmen durfte, diese sei noch vom Einverständnis des Arbeitgeber gedeckt.

3. Vor Ausspruch einer Kündigung bei Störungen im Vertrauensbereich ist aber immer eine Abmahnung erforderlich, wenn es sich um steuerbares Verhalten des Arbeitnehmers handelt und eine Wiederherstellung des Vertrauens erwartet werden kann.

Im entschiedenen Fall gab es weder ein ausdrückliches Verbot noch eine Abmahnung. Das Gericht geht davon aus, dass privates Surfen von 80 bis 100 Stunden im Jahr noch nicht ein Ausmaß erreicht, das eine Abmahnung überflüssig macht: "Der Arbeitgeber muss in der ersten Zeit der Nutzungsmöglichkeit einer neuen Einrichtung damit rechnen, dass im Vergleich zum üblichen Gebrauch eine intensivere Nutzung in einer Anlernphase erfolgt. Die Arbeitnehmerin befindet sich in einer "spielerischen Lernphase". Zudem durfte die Arbeitnehmerin davon ausgehen, dass es durchaus im Interesse des Arbeitgebers ist, möglichst schnell durch intensive Nutzung aus beliebigen Themenbereichen den Umgang mit dem Internet zu erlernen.

Europa

Großbritannien
HP suspendierte mehr als 100 Angestellte. Nachdem ein Vorstandsmitglied eine E-Mail mit pornografischem Inhalt erhielt, wurden die Mitarbeiter suspendiert, ihre Laptops beschlagnahmt und sie selbst aus der Firma eskortiert.
(Juli 2002, news.zdnet.de/story/0,,t101-s2119394,00.html)

Frankreich
Inzwischen liegt eine höchstrichterliche Entscheidung zur Frage der Kontrollmöglichkeiten des Arbeitgebers in bezug auf private Dateien (also z. B. private E-Mails) der Arbeitnehmer vor. Ein Unternehmen legte in einem Kündigungsverfahren dem Gericht Dateien vor, die auf dem Arbeitsplatz-Computer des von Kündigung bedrohten Arbeitnehmers im Verzeichnis „Persönlich" gespeichert waren. Der Kassationsgerichtshof kam zu dem Ergebnis, dass hier eine gravierende Verletzung der privaten Sphäre des Arbeitnehmers vorliege. Auch am Arbeitsplatz habe der Arbeitnehmer Anspruch auf den Schutz des Privatlebens.

Der Kassationsgerichtshof stellt ferner klar, dass dieser Schutz unangetastet bleibt, auch wenn der Arbeitgeber ausdrücklich die private Nutzung untersagt und der Arbeitnehmer das Verbot nicht beachtet hat (Cour de Cassation, Urteil Nr. 4164, 02.10.2001, AZ 99-42.942).[13]

USA

New York
Die New York Times hat 23 Mitarbeiter wegen Internet-Missbrauchs entlassen.
www.spiegel.de/netzwelt/technologie/0,1518,55733,00.html

Evanston, Illinois
Kündigung wegen 2.000 MP3-Dateien.
Sekretärin wurde gefeuert, weil sich etwa 2.000 MP3-Dateien auf dem Computer in ihrem Büro befanden (New York Times).
www.chip.de/news_stories/news_stories_208394.html

[13] Unter anderem unter Berufung auf europäisches Recht.

Weitere Urteile wegen Missbrauch des Internets...

Pornografie

- Das Mobilfunkunternehmen Orange entließ 30 bis 40 Mitarbeiter, weil sie pornografische Inhalte heruntergeladen und im Büro verbreitet hatten.
  (August 2000, www.msn.co.uk)

- Dow Chemical entließ circa 40 Mitarbeiter wegen der Versendung von E-Mails mit pornografischen Inhalten. Seit Juli 2000 hat das Unternehmen Berichten zufolge wegen obszöner E-Mails nahezu 300 Mitarbeiter entlassen oder diszipliniert.
  (August 2000, Computerworld)

- Personal und Beamte des Weißen Hauses wurden dabei überführt, als sie umfangreiche Dateien mit Hardcore-Porno-Videos auf die Computer der Regierung herunterluden.
  (August 2000, www.worldnetdaily.com)

Vertrauensmissbrauch

- Siemens verklagte zwei frühere Mitarbeiter, die vertrauliche Unternehmensinformationen und Geschäftsgeheimnisse, zu denen sie während ihrer Firmenzugehörigkeit Zugang hatten, für auswärtige Geschäftsaktivitäten verwendeten.
  (Januar 2000, Sun-Sentinel Ft. Lauderdale)

- Apple Computer verklagte eine Person, die Bilder von zwei neuen Produkten im Internet vor deren offizieller Einführung veröffentlicht hatte, wodurch der Kurs der Apple-Aktie an der NASDAQ gefallen war.
  (August 2000, Reuters English News Service)

- Borland International Inc. klagte gegen einen ihrer früheren Mitarbeiter, da dieser mit Hilfe des firmeneigenen E-Mail-Systems vertrauliche Geschäftsdaten an seinen neuen Arbeitgeber gesendet hatte. Der frühere Mitarbeiter sowie der Nachrichtenempfänger wurden wegen Diebstahls von Geschäftsgeheimnissen verklagt.
  (Oktober 1996, The American Employment Law Council Conference)

Rufschädigung

- Norton Rose, eine angesehene Anwaltskanzlei, wurde als vermeintlicher Urheber der E-Mail "Claire Swire" in ihrem Ansehen geschädigt. Es handelte sich dabei um eine E-Mail mit pornografischem Inhalt, die an mehr als zehn Millionen Menschen weltweit verschickt worden war.
  (Heise-online, „Fütter mein Email-Ego", Dezember 2000, www.heise.de/tp/deutsch/inhalt/co/4494/1.html)

- Edward D. Jones & Co, USA, leitete Maßnahmen gegen 60 Mitarbeiter ein, nachdem ein Firmenangehöriger sich über eine E-Mail eines Kollegen mit anstößigem Inhalt beschwert hatte.
  (Oktober 1999, The Columbus Dispatch, USA)

- First Union Corp. USA entließ sieben Mitarbeiter, weil sie pornografische und andere anstößige E-Mails über ihre Firmen-Accounts verschickt hatten.
  (August 1999, Knight Ridder News Service; www.kri.com)

Gesetzliche Haftung

- Zwei Mitarbeiter von Nissan wurden aufgrund der Versendung sexuell eindeutiger E-Mails entlassen. Sie erhoben Klage wegen ungerechtfertigter Entlassung und machten die Verletzung ihrer Privatsphäre geltend. Nissan gewann den Prozess, weil das Unternehmen E-Mail-Richtlinien aufgestellt hatte, die die Verwendung firmeneigener Computersysteme für firmenfremde Aktivitäten untersagte.
  (Januar 2000, Human Rights, USA / Computer Weekly)

- Zwei Mitarbeiter von Kwick Fit wurden entlassen, nachdem entdeckt worden war, dass sie vulgäre E-Mails über das firmeneigene E-Mail-System miteinander ausgetauscht hatten.
  (August 1999, News of the World, Großbritannien)

- Die Vertriebsfirma BG leistete eine Zahlung in Höhe von 161.000 US $ an den Konkurrenten Transco zur Beilegung einer Verleumdungsklage. Ein leitender Mitarbeiter von BG hatte eine diffamierende E-Mail an Transco-Mitarbeiter geschickt, in der fälschlicherweise behauptet wurde, dass Exoteric Gas Solutions (von BG) vertrauliche Informationen von Transco missbraucht hätte.
  (Januar 1999, Human Rights, USA)

10 Weiterführende Informationen

! Tipp

Hier finden Sie eine Liste mit Literaturangaben und weiterführenden Links zum Thema:

- Ver.di-Forum zum Thema „Onlinerechte für Beschäftigte“ www.onlinerechtefuerbeschaeftigte.de
- Prof. Dr. Peter Wedde (Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Fachhochschule Frankfurt sowie wissenschaftlicher Leiter des Projektes quid!, virtuelles Interview abrufbar unter tool.wegewerk.com/verdi/onlinerechte/quest/overview.php3?id=1&)
- Private Nutzung der Kommunikationssysteme am Arbeitsplatz www.tse-hamburg.de/Papers/Internet/Recht/daeubler.html
- Möglichkeiten des Arbeitgebers zur Überwachung der E-Mail-Kommunikation des Arbeitnehmers www.afs-rechtsanwaelte.de/artikel13.htm
- Grundsätze für „Benutzerrichtlinien für den Umgang mit Internet“ www.datenschutz-bayern.de/technik/orient/ibenrili.htm
- „Onlinerechte für Beschäftigte“, Beispiele, Fragen und Antworten, Meinungen, Live-Chat mit Michael Sommer (stellvertretender Vorsitzender der ver.di) www.onlinerechtefuerbeschaeftigte.de/more
- Arbeitsrecht Kompakt – Blitzdienst für Arbeitgeber, Fachverlag für Recht und Führung, Bonn www.arbeitsrechtsinfos.de
- Technischer Jugendschutz im Internet www.jugendschutz.net
- Verantwortlichkeit für Medien- und Teledienste; Bundeskriminalamt Wiesbaden www.bka.de/aktuell/agenda98/vtr98/vtr_heyl98.html

- Wir brauchen weltweite Mindeststandards, Dr. Christine Bergmann, Bundesministerin für Familie, Senioren, Frauen und Jugend, im Politik-Digital-Interview über wirksame Maßnahmen zum Kinder- und Jugendschutz, Politik digital www.politik-digital.de/netzpolitik/jugendschutz/bergmann.shtml

- Förderverein Informationstechnik und Gesellschaft e. V. (FITUG) www.fitug.de/bildung/index.html

- Private Nutzung der Kommunikationssysteme am Arbeitsplatz www.tse-hamburg.de/Papers/Internet/Recht/daeubler.html

- Grundsätze für „Benutzerrichtlinien für den Umgang mit Internet" www.datenschutz-bayern.de/technik/orient/ibenrili.htm

- Möglichkeiten des Arbeitgebers zur Überwachung der E-Mail-Kommunikation des Arbeitnehmers www.afs-rechtsanwaelte.de/artikel13.htm

- „Netlaw Library", Prof. Dr. Thomas Hoeren, Institut für Informations-, Telekommunikations- und Medienrecht der Universität Münster www.jura.uni-muenster.de/netlaw/default.cfm?RNr=0,133,122&opened=122&Lang=de - 122

- Verband der deutschen Internetwirtschaft www.eco.de/index_de.htm

- quid! - Das Gütesiegel für Qualität im betrieblichen Datenschutz quid.fh-frankfurt.de/kurzbeschreibung.html

11 Wer hilft weiter?

Hilfe

Cobion AG

Mit inhaltsbezogenen Sicherheitslösungen - genannt „Content-Security-Lösungen" - trägt Cobion den hohen Anforderungen des Marktes an lückenlose Sicherheitskonzepte Rechnung.

1997 in Kassel gegründet, hat sich die Cobion AG schnell als technologisch führender Anbieter durchgesetzt. Die OrangeBox-Produktfamilie garantiert serverbasierende Kontrolle, Monitoring und Sicherheit für Internet-Nutzung, E-Mail-Verkehr und E-Commerce-Anwendungen in Unternehmen und Organisationen.

Die Produktgruppierung erfolgt in 3 Kategorien:

Cobion Produktpalette

- Internet Security (OrangeBox Web)
- E-Mail Security (OrangeBox Mail)
- Intranet Security (OrangeBox LAN)

Ungewollte oder illegale Informationen gelangen so weder in ein Firmennetzwerk noch können vertrauliche Unternehmensdaten dieses verlassen. Eine produktive Internet-Umgebung am Arbeitsplatz wird geschaffen, Haftungs- und Sicherheitsrisiken werden reduziert und es wird verhindert, dass vertrauliche Daten in falsche Hände geraten.

PriceWaterhouseCoopers Veltins – Rechtsberatung in Deutschland

PriceWaterhouseCoopers Veltins

PriceWaterhouseCoopers Veltins, nachfolgend PWC genannt, gehört mit circa 150 Anwälten zu den größten wirtschaftsberatenden Anwaltsfirmen in Deutschland. Damit kann PWC das gesamte Spektrum des Wirtschaftsrechts abdecken und Kunden umfassend und kompetent beraten.

Einen Schwerpunkt von PWC bildet das Arbeitsrecht (Employment & Human Resources), wobei auch in diesem Bereich nochmals nach Branchenschwerpunkten unterschieden wird. Auch hier geht man bei PWC davon aus, dass Rechtsprobleme nur dann erfolgreich analysiert und gelöst werden können, wenn man die Branchen verstanden hat. Alle Fachbereiche sind überörtlich organisiert, wobei der Kunde in jeder Niederlassung einen persönlichen Ansprechpartner erreichen kann. Die Kommunikationswege (Telefon/Telefax/E-Mail/Internet) sind durch Firewall-Systeme auf höchster Sicherheitsstufe abgesichert, so dass die Kommunikation mit dem Kunden geschützt ist und die Vertraulichkeit der Daten gewährt wird. Das international orientierte Profil von PWC wird dadurch unterstrichen, dass die Rechtsanwälte ihre Dienstleistungen nicht nur auf Deutsch, sondern auch auf Englisch, Französisch, Italienisch, Spanisch, Griechisch, Niederländisch, Schwedisch, Russisch und Arabisch erbringen.

Die Cobion AG steht u. a. in engem Kontakt mit RRef. Stefan Schröcker der PricewaterhouseCoopers Veltins Rechtsanwaltsgesellschaft mbH in München. Herr Schröcker ist seit vier Jahren Mitarbeiter von PWC-Veltins und derzeit als Rechtsreferendar und Mitglied der ICT (Information and Communication Technology) Group in München beschäftigt. Schwerpunktmäßig ist Herr Schröcker in den Bereichen Datenschutz- und IT-Recht sowie im gesamten Internetrecht und Recht der neuen Medien tätig.

Kontaktdaten
Tel. +49(0)89 29097-0
Fax +49(0)89 29097-200

Cobion

Anlage A: Checkliste zur Entwicklung von Content-Security-Richtlinien für den Internet-Zugriff

Diese Checkliste zur Entwicklung von Content-Security-Richtlinien für den Internet-Zugriff soll Ihnen bei der Erstellung Ihrer individuellen Content-Security Richtlinie helfen.

1. Erkennung von Internet-Übertragungen nach Typ

Dies ist die Fähigkeit, das Heraufladen und Herunterladen von Dateien ins bzw. vom Internet zu steuern. Diese Funktion ermöglicht die Erkennung sämtlicher Dateien bestimmten Typs.

Dateityp: Bilder
Damit die Erkennung von Bildern Ihren Anforderungen entsprechend funktioniert, sollten
Sie folgende Dateitypen berücksichtigen:
JPEG, GIF, DXF, DWG, PSP, PNG, PIC, TIFF, PCX, FLI und BMP.

Mit der Tabelle unten können Sie zusammenfassen, wie mit bestimmten Bilddateien im Einzelnen verfahren werden soll, d. h. welche Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

Dateityp: Filme

Video-Dateien sind normalerweise groß. Der Transfer dieser Dateien könnte zur Überlastung der Netzwerkressourcen führen.

Sie sollten folgende Video-Dateien berücksichtigen: MPEG, AVI, RM QTM und MOV. Sie können festlegen, dass alle Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

Dateityp: Container- und Kompressionsformate

Sie sollten folgenden Typen von Container- und Kompressionsformaten berücksichtigen: PGP, BINHEX, RAR, TNEF, UUE, LZH, ARJ, CAB, CMP, ZIP, GZIP und TAR. Sie können festlegen, dass alle Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Sobald Sie sich zur Erkennung von Container- und Kompressionsdateien entschieden haben, können Sie festlegen, wie mit ihnen verfahren werden soll. Mit der Tabelle legen Sie diesen Bereich Ihrer Internet-Richtlinien fest.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

Dateityp: Ausführbare Dateien

Ausführbare Dateien können groß sein und haben normalerweise nichts mit der Arbeit zu tun. Ausführbare Dateien sind eine der wichtigsten Quellen für die Verbreitung von Viren. Daher müssen Sie dafür sorgen, dass Ihre Lösung für Content Security diesen Dateityp prüft. Benutzer, die ohne Berechtigung ausführbare Dateien herunterladen, können die Stabilität des Netzwerks beeinträchtigen und das Unternehmen Haftungsrisiken aussetzen, wenn die Software nicht lizenziert ist.

Sie sollten folgenden Typen von ausführbaren Anlagen berücksichtigen: JavaByte, DosExe, Win31Exe, Win32DLL und Win32exe. Sie können festlegen, dass alle ausführbaren Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Sobald Sie sich zur Erkennung von Container- und Kompressionsdateien entschieden haben, können Sie festlegen, wie mit ihnen verfahren werden soll. Mit der Tabelle legen Sie diesen Bereich Ihrer Internet-Richtlinien fest.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

Dateityp: Dokument-Dateien

Makros in Dokument-Dateien sind eine häufige Gefahrenquelle für Viren. Dokument-Dateien können auch vertrauliche Informationen eines Unternehmens enthalten.

Eine Content-Security-Lösung sollte über ein Dokumenten-Archiv verfügen, dass selbst Fragmente vertraulicher Informationen erkennt und verhindert, dass solche sensiblen Dokumente das Unternehmen verlassen.

Sie sollten folgende Typen von Dokument-Dateien berücksichtigen: Fax, Rich Text, CDA, Microsoft Projekt, Microsoft PowerPoint, Microsoft Word, Microsoft Excel, OLE Package 1-2-3. PDF, Text und HTML. Sie können festlegen, dass alle Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Sobald Sie sich zur Erkennung von Dokument-Dateien entschieden haben, können Sie festlegen, wie mit ihnen verfahren werden soll. Mit der Tabelle legen Sie diesen Bereich Ihrer Internet-Richtlinien fest.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

Dateityp: Audio-Dateien

Es gibt im Internet viele Quellen mit digitaler Musik und Audio-Dateien. Da diese Dateien im allgemeinen sehr groß sind, kann der Download schnell die Systemressourcen überlasten und das Untenehmen einem Haftungsrisiko aussetzen, wenn es sich um illegale Kopien von urheberrechtlich geschützten Aufnahmen handelt.

Sie sollten folgende Typen von Audio-Dateien berücksichtigen: MIDI, AIF, VOC, AU, WAV MP3 und RAM. Sie können festlegen, dass alle Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Sobald Sie sich zur Erkennung von Audio-Dateien entschieden haben, können Sie festlegen, wie mit ihnen verfahren werden soll. Mit der Tabelle legen Sie diesen Bereich Ihrer Internet-Richtlinien fest.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

Cobion

Dateien nach Namen

Sie können Dateien einerseits an ihrem Typ und andererseits an ihrem Namen erkennen.
So können Sie zum Beispiel verhindern, dass Dateien mit bekannten Namen in das Internet heraufgeladen oder vom Internet heruntergeladen werden.
Hierzu können Dateien mit Animationen gehören, die verstärkt zu ganz bestimmten Zeiten im Jahr in Umlauf gesetzt werden.

Sie sollten folgende Datei-Typen berücksichtigen: SWF (Shock-Wave/Flash); DXR.

Sie können festlegen, dass alle Dateien abgeblockt werden sollen oder nur von bestimmten Benutzergruppen oder Einzelbenutzern herauf- oder heruntergeladen werden dürfen.

Typ	Website	Benutzer	Download
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren
______	❑ Alle Websites ❑ Bestimmte URLs	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Zulassen ❑ Ablehnen ❑ PassLock ❑ Protokollieren

2. Internet-basierte E-Mail

Internet-basierte E-Mail-Dienste, wie HotMail, GMX oder Yahoo!, ermöglichen eine E-Mail-Verwendung, die die SMTP-Sicherheit am Gateway umgeht.
Aus diesem Grund werden Internet-basierte E-Mail-Dienste häufig zum Versenden von privater E-Mail und zum heimlichen Versenden von vertraulichen Informationen verwendet.

Legen Sie mit der Tabelle unten fest, wie Ihre Content-Security-Lösung mit Internet-basierter E-Mail verfahren soll.

Benutzer	Verwaltung von internen E-Mails
❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ablehnen ❑ Warnmeldung ❑ Protokollieren

3. Steuern der Internet-Verwendung nach Inhalt und Tageszeit

Durch die Möglichkeit die Internet-Verwendung durch inhaltliche Analyse zu steuern, können Unternehmen den Inhalt von Internet-Übertragungen exakt bestimmen.

Außerdem sollte der Zugriff auf bestimmte Internet-Inhalte während der Arbeitszeit beschränkt und zu anderen Zeiten zugelassen werden.

Legen Sie mit der Tabelle unten fest, welcher Typ von Inhalt zu welcher Tageszeit wie gesteuert werden soll.

URLs	Website	Tageszeit	Download	
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	_____	❑ Zulassen ❑ Ablehnen	❑ PassLock ❑ Protokollieren
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	_____	❑ Zulassen ❑ Ablehnen	❑ PassLock ❑ Protokollieren
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	_____	❑ Zulassen ❑ Ablehnen	❑ PassLock ❑ Protokollieren

4. Festlegen von Ausnahmen

Ihre Content-Security-Lösung sollte Ihnen die Einstellung user-spezifischer Richtlinien erlauben.
Sie können für Benutzergruppen und einzelne Benutzer festlegen, dass bestimmte Benutzer während der Arbeitszeit normalerweise keinen Zugang zum Internet erhalten, jedoch auf einzelne Seiten zugreifen können, die sie für ihre Arbeit benötigen.

Kategorie	Tageszeit	Genemigter Zugriff in Ausnahmefällen
_____	_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person
_____	_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person
_____	_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person

Cobion

Anlage B: Checkliste zur Entwicklung von Content-Security-Richtlinien bei E-Mail

Diese Checklisten zur Entwicklung von Content-Security-Richtlinien für den E-Mail-Verkehr sollen Ihnen bei der Erstellung Ihrer individuellen Content-Security-Richtlinie helfen.

Cobion

1. Erkennung von Anlagen nach Typ

Erkennung nach Typ

Dies ist die Fähigkeit, ein- und ausgehende E-Mails auf der Basis des an der Nachricht angehängten Anlagen-Typs zu prüfen. Der Anlagen-Typ muss durch die Datei-Signatur und nicht alleine durch die Dateierweiterung erkennbar sein, damit Benutzer die Dateien nicht umbenennen, um die Prüfung zu umgehen.

Dateityp: Bilder
Sie sollten folgende Typen von Bilddateien berücksichtigen: JPEG, GIF, DXF, DWG, PSP, PNG, PIC, TIFF, PCX, FLI und BMP.

Mit der Tabelle unten können Sie zusammenfassen, wie mit bestimmten Bilddateien im Einzelnen verfahren werden soll, d. h. welche Dateien abgeblockt werden sollen oder nur zwischen bestimmten Benutzergruppen oder Einzelbenutzern versendet werden dürfen.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

Dateityp: Filme/Audio

Audio- und Video-Dateien sind normalerweise groß und können zur Überlastung der Ressourcen führen.

Sie sollten folgende Typen von Audio-Dateien berücksichtigen: MIDI, AIF, VOC, AU, WAV und MP3.

Bei Filmdateien sollten Sie folgende Typen berücksichtigen: AVI, QTM, MPEG, RM, MOV und WMV.

Mit der Tabelle unten können Sie zusammenfassen, wie mit bestimmten Audio- und Video-Dateien im Einzelnen verfahren werden soll.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

Dateityp: Kompressionsformate

Um sicherzustellen, dass von komprimierten Dateien keine Gefahr ausgeht, müssen die Content-Security-Tools rekursive Analyse beherrschen, d. h. die Dateien wiederholt und beliebig entpacken, um die komprimierten Daten im Rohzustand zu prüfen.

Sie sollten folgende Typen von Kompressionsformaten berücksichtigen: TAR, ZIP, GZIP,CMP, CAB, ARJ, LZH und RAR

Sobald Sie sich zur Erkennung von komprimierten Dateien entschieden haben, können Sie festlegen, wie mit ihnen verfahren werden soll. Mit der Tabelle legen Sie diesen Bereich Ihrer Internet-Richtlinien fest.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

Dateityp: Ausführbare Anlagen
Ausführbare Dateien sind eine der wichtigsten Quellen für die Verbreitung von Viren. Daher müssen Sie dafür sorgen, dass Ihre Lösung für Content Security diesen Dateityp prüft.

Sie sollten folgende Typen von ausführbaren Anlagen berücksichtigen: JavaByte, DosExe, Win31Exe, Win32unknown, Win32DLL und Win32exe.

Mit der Tabelle unten können Sie zusammenfassen, wie mit bestimmten ausführbaren Anlagen im Einzelnen verfahren werden soll.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

Dateityp: Dokument-Dateien

Damit nur die Personen und Abteilungen die Dateien erhalten, die mit den normalen Geschäftsaktivitäten zu tun haben, wünschen Sie möglicherweise, dass Ihr Content Security-Lösung die Anlagen nach Dokument-Typ prüft.

Sie sollten dabei sämtliche Datei-Typen berücksichtigen und den Datenaustausch zwischen den Benutzern entsprechend Ihrer Content-Security-Richtlinien festlegen.

Mit der Tabelle legen Sie fest, wie mit einzelnen Datei-Typen verfahren werden soll.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

2. Dokumenten-Depot

Neben der Funktion, durchlaufende E-Mails oder deren Anhänge in Echtzeit auf verbotene oder unerwünschte Inhalte zu scannen sollte eine Content-Security-Lösung über ein Dokumentenarchiv verfügen:
Über dieses Dokumentenarchiv wird sicher verhindert, dass selbst kleinste Fragmente vertraulicher Dokumente das Unternehmen per E-Mail verlassen und in Hände gelangen, in die sie nicht gelangen sollten wie z. B. Quellcode, Entwicklungsentwürfe, betriebliche Kennzahlen, Auszüge aus Meetings, Vertragsdokumente, persönliche Daten von Angestellten u. v. m.

3. Gewährausschlusserklärung

Die vermehrte Internet-Nutzung hatte zur Folge, dass die rechtliche Verantwortung für die Inhalte einer E-Mail vom Mitarbeiter auf den Arbeitgeber übergegangen ist. In dieser Hinsicht ist die Fähigkeit, eine Gewährausschlusserklärung an E-Mails anzuhängen immer wichtiger geworden.
Außerdem wird die Fähigkeit, E-Mail-Haftungsausschlüsse für das ganze Unternehmen, eine Abteilung oder Einzelbenutzer anzupassen, zunehmend als Teil effizienter Sicherheits-Richtlinien implementiert. Daher muss eine Content-Security-Lösung das Anhängen einer Textnachricht am Anfang oder Ende eines E-Mail-Nachrichtentextes ermöglichen, idealerweise für alle ausgehenden E-Mails automatisch.

Beispiel:
„Diese E-Mail, einschließlich sämtlicher mit ihr übertragenen Dateien, ist vertraulich und für die ausschließliche Verwendung durch die Person oder das Unternehmen vorgesehen, an die/das sie adressiert ist. Für den Inhalt dieser E-Mail ist alleine der Autor verantwortlich, Inhalt und Meinung müssen nicht die Ansicht der Firma [Name] wiedergeben.“

Die Gewährausschlusserklärung für Ihr Unternehmen:

Gewährausschlusserklärung für Abteilung:

Gewährausschlusserklärung Für Einzelbenutzer:

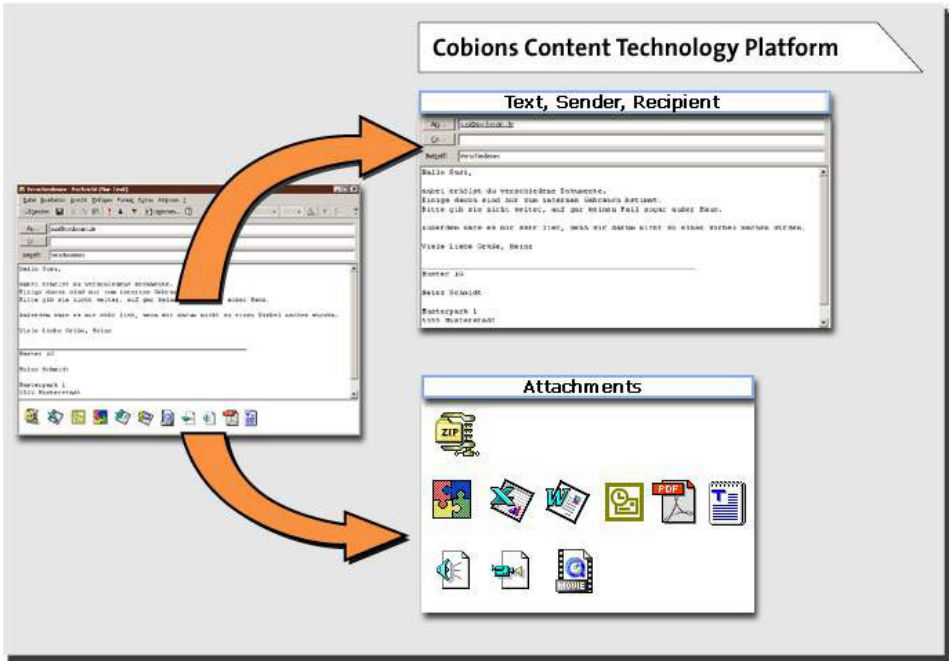
4. Bild- und Textanalyse

Durch die Möglichkeit beliebige Dokumente nach vordefinierten Texten und Bildern zu durchsuchen, können Unternehmen den Inhalt von E-Mails und Attachments exakt bestimmen und Gefahren abwehren.

Eine Content-Security-Lösung sollte in der Lage sein, eine *intelligente* Analyse der Daten in der Betreffzeile, dem Textkörper und in den Anlagen von E-Mails durchzuführen.

E-Mails können durch verschiedene Anlagen wie ZIPs, HTML und sonstige Dateien komplexer Natur sein. In manchen Fällen ist es nicht mehr offensichtlich, um welchen Dateityp es sich handelt, da z. B. jemand die Dateiendung umbenannt haben könnte.

Jedes Dateiformat (z. B. eine ZIP- oder eine Word-Datei) hat eine spezielle Signatur, die dazu dient, den Typ eindeutig zu bestimmen.
Eine binäre Analyse der E-Mail-Anlagen ermöglicht den angefügten Dateityp aufgrund des tatsächlichen Inhalts zu erkennen.



Die entscheidende Fähigkeit der verwendeten Content-Security-Lösung ist die Inhaltsanalyse der E-Mail-Anlage, unabhängig des verwendeten Dateiformats.

Die meisten Dateien beinhalten mehr als einen Inhaltsteil. Archiv-Dateien beinhalten zum Beispiel mehrere Dateien mit verschiedenem Inhalt. Manchmal speichern sie hunderte oder mehr verschiedene Text-Dateien, Bilder, Excel-Blätter etc.
So können z. B. Word-Dateien neben Bildern auch eingebettete Objekte beinhalten.

Der nächste Schritt zerlegt nun jede Datei oder jeden Anhang in seine Teile.
Betrachten Sie eine ZIP-Datei, die eine Word-Datei enthält, die wiederum eine andere ZIP-Datei beinhaltet. Ihre Content-Security-Lösung analysiert diese einzelnen Dateien und bewertet den Inhalt mit Hilfe passender „Werkzeuge" in Beziehung zueinander.
Neben einer Text-Anlage können ebenso *Bilder* Textinformationen enthalten.
Durch eine integrierte OCR[14] wird der Inhalt eines Bildes nach Text durchsucht und indentifizierte Zeichen und Zeichenfolgen in Text-Inhalt überführt. Auf diese Weise ist die Content-Security-Lösung in der Lage, Schlüsselwörter in Bildern zu finden.
Dies erlaubt Ihnen zum Beispiel, alle Inhalte, die das Wort „vertraulich" enthalten, zu blockieren. Es spielt keine Rolle, ob das Wort in der Betreff-Zeile einer E-Mail, in einer Word-Datei oder innerhalb eines Bildes erscheint.

Die Kombination der Schlagwörter ermöglicht durch komplexe Textmuster inhaltliche Unterscheidungen zu erkennen (extended regular expressions).

Hier einige Beispiele:

or	**porn; XXX; adult**	Identifiziert den Inhalt der die Worte „porn", „XXX" oder „adult" enthält.
near	**vertraulich; Vertrag**	Identifiziert den Inhalt eines Dokuments, in dem das Wort "vertraulich" in der Nähe des Wortes „Vertrag" erscheint.
porn*		Identifiziert jedes Wort, das mit der Vorsilbe „porn", wie „pornografisch", „pornsite" etc. beginnt.

Sie können die Inhaltsanalyse von Dateien individuell und sämtliche Kriterien benutzerspezifisch einrichten.

[14] Optical Character Recognition (OCR).

Cobion

Notieren Sie in der Tabelle unten die Wörter, nach denen Sie E-Mails durchsuchen möchten.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

5. Anti-Spam

Der Begriff „Spam" bezeichnet unerwünschte oder Junk-E-Mail. Derartige E-Mails verschwenden Ressourcen und die Zeit des E-Mail-Empfängers.

Der übliche Weg ist die Sperrung der IP-Adresse, der Spam-Quelle. Eine effektivere Möglichkeit ist die Analyse des Headers, um die E-Mail einer bekannten Spam-Quelle zuordnen zu können. Eine intelligente Textanalyse bietet weitere Kontrollmöglichkeiten, um Phrasen wie „schell reich werden" zu erkennen.

Beispiele für die Spam-Erkennung über die Textanalyse:

- „wenn Sie von unserer Anschriftenliste gestrichen werden möchten"
- „wenn Sie innerhalb von 3 Tagen antworten, erhalten Sie ein Geschenk"
- „zahlt sich garantiert aus"
- „werden Sie schnell reich"

Notieren Sie in der Tabelle die Spam-Wörter oder -Phrasen, die Ihr Unternehmen in E-Mails suchen möchte.

Bild-Typ	Benutzer	Eingehende E-Mails	Ausgehende E-Mails
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

__________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
__________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite
__________	❑ Alle ❑ Nach Ab-teilung ❑ Nach Per-son	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leiten	❑ Ausliefern ❑ Weiterleiten ❑ Antwort an Absender ❑ Löschen ❑ Warnmeldung ❑ Protokollieren ❑ An Dritte leite

6. Steuern der E-Mail-Verwendung nach Inhalt und Tageszeit

Durch die Möglichkeit die E-Mail -Verwendung durch inhaltliche Analyse zu steuern, können Unternehmen den Inhalt von Internet-Übertragungen exakt bestimmen.

Außerdem sollte der Empfang bestimmter E-Mail-Inhalte während der Arbeitszeit beschränkt und zu anderen Zeiten zugelassen werden.

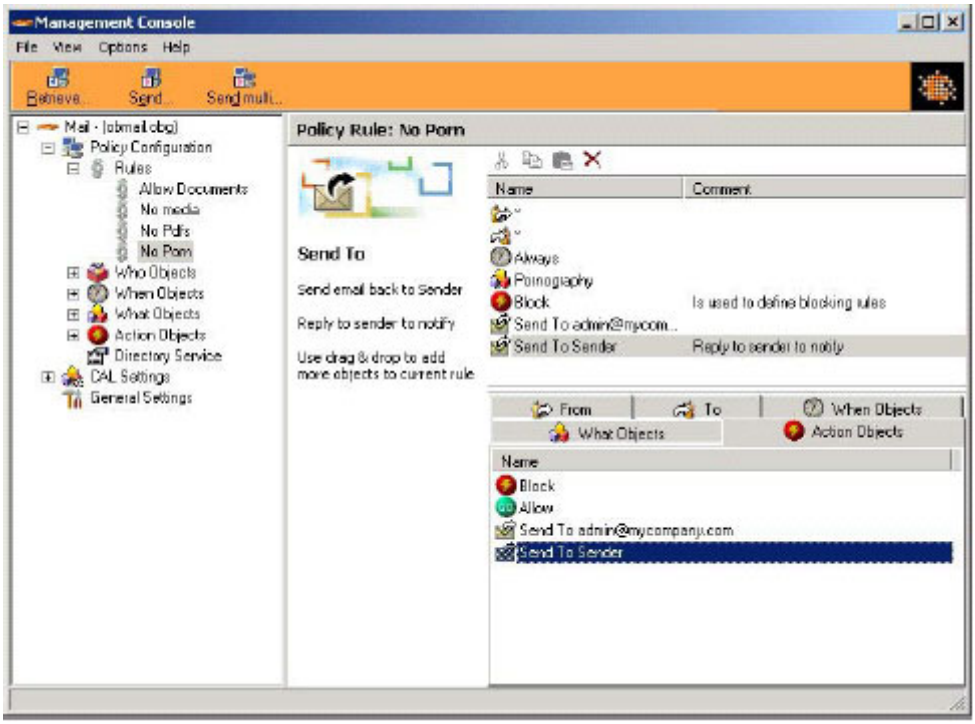
Legen Sie mit der Tabelle unten fest, welche Kategorie zu welcher Tageszeit wie gesteuert werden soll.

Typ	Benutzer	Tageszeit	Download
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	_____	❑ Zulassen ❑ Ablehnen ❑ Warnmeldung ❑ Protokollieren
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	_____	❑ Zulassen ❑ Ablehnen ❑ Warnmeldung ❑ Protokollieren
_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person	_____	❑ Zulassen ❑ Ablehnen ❑ Warnmeldung ❑ Protokollieren

7. Festlegen von Ausnahmen

Ihre Content-Security-Lösung sollte Ihnen die Einstellung benutzerspezifischer Richtlinien erlauben.
Sie können für Benutzergruppen und einzelne Benutzer festlegen, dass bestimmte Benutzer während der Arbeitszeit normalerweise keine E-Mails mit Anlagen bestimmten Typs erhalten, jedoch einzelne Dateien verschicken können, die sie für ihre Arbeit benötigen.

Benutzer / Abteilung	Tageszeit	Genemigter Zugriff in Ausnahmefällen
_____	_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person
_____	_____	❑ Alle ❑ Nach Abteilung ❑ Nach Person



Cobion

Anlage C: Musterbetriebsvereinbarung zur E-Mail- und Internet-Nutzung am Arbeitsplatz

Die folgende Nutzungsvereinbarung gilt als Anregung.
Diese Musterbetriebsvereinbarung erhebt keinen Anspruch auf Vollständigkeit, allgemeine Übertragbarkeit und Rechtsverbindlichkeit.[15]

Bitte beachten Sie!
Beim Abschluss einer Nutzungsvereinbarung ist immer die konkrete Situation im Unternehmen zu berücksichtigen.

Der folgende Entwurf ist keine für alle Unternehmen gleichermaßen anwendbare Regelung, sondern ist entsprechend anzupassen!

[15] Die aufgeführte Musterbetriebsvereinbarung ist übernommen von ver.di, der Vereinten Dienstleistungsgewerkschaft. Sie kann im Internet unter **www.onlinerechtefuerbeschaeftigte.de/more/solutions/020218184345** heruntergeladen werden.

§ 1 Geltungsbereich und Gegenstand

Diese Vereinbarung gilt für alle Beschäftigten der Firma XXX Die Vereinbarung umfasst alle Betriebsstätten des Unternehmens. Die Vereinbarung regelt die Einführung und Anwendung der Intranet/Internet- und E-Mail-Nutzung im Unternehmen.

§ 2 Ziel- und Zweckbestimmung

1. Durch den Einsatz von Intranet- und Internettechniken soll die interne und externe Kommunikation sowie der Informationsaustausch verbessert werden.
2. Mit dem Ermöglichen der Internet/Intranet und E-Mail Nutzung und dem Abschluss dieser Vereinbarung werden folgende Zwecke verfolgt:
a) die Beschäftigten bei der Nutzung von Informations- und Kommunikationsdiensten sowie von Internetdienstleistungen zu unterstützen
b) den Schutz der persönlichen Daten und der Gesundheit der Beschäftigten bei der Nutzung von Intranet/Internet und E-Mail zu gewährleisten.

§ 3 Grundsätze der Nutzung

Arbeitsorganisatorische Einheit im Sinne dieser Vereinbarung ist.... oder andere räumlich selbstständige Verwaltungseinheiten. Internet und E-Mail werden primär für dienstliche Zwecke eingesetzt. Die gelegentliche Nutzung dieser Systeme für private Zwecke wird gestattet, sofern der betriebliche Ablauf nicht gestört wird und keine zusätzlichen Kosten entstehen. Das Recht zur Internet-Nutzung darf nicht missbraucht werden. Ein Missbrauch liegt vor, wenn das Internet für strafbare, diffamierende, rassistische, gewaltverherrlichende oder sexistische Aktivitäten genutzt wird. Das Unternehmen sorgt für einen systemseitigen dem Stand der Technik entsprechenden Schutz vor Viren oder sonstigen Sicherheitsrisiken bei der Intranet/Internet und E-Mail Nutzung. Die Berechtigung zur Nutzung von Intranet/Internet und E-Mail wird programmtechnisch geregelt. Die Abgabe einer Verpflichtungserklärung auf das Datengeheimnis nach § 5 BDSG einschließlich der Bestätigung der Kenntnisnahme eines Merkblattes über die Bestimmungen des Rechts über Ordnungswidrigkeiten und Straftaten (Anlage 1) sind ausnahmslos unverzichtbar.

§ 4 Systembeschreibung

Die für den Intranet/Internet-Zugang verwendeten Programme werden in der aufgeführt > Verweis auf Anlage. Darin enthalten ist auch eine Kurzbeschreibung der verwendeten Programme, aus denen sich die wesentlichen Funktionen ergeben. Durch die zugriffsberechtigten Systemadministratoren darf nur Einsicht in solche Daten genommen werden, die für die Betriebsfähigkeit und Sicherheit des Netzwerkes und der dezentralen Einheiten von Bedeutung sind.

§ 5 Leistungs- und Verhaltenskontrolle

Die mit dem Intranet/Internet/E-Mail-Nutzung zusammenhängenden Hard- und Software-Systeme werden nicht zum Zwecke der Leistungs- und Verhaltenskontrolle der Beschäftigten genutzt. Die bei der Nutzung erfassten Benutzerdaten dürfen ausschließlich von den zugriffsberechtigten Personen für Zwecke der Systemsicherheit und der Systemintegrität verwendet werden.

§ 6 Personenbezogene und – beziehbare Daten

Protokolliert wird ausschließlich der das Unternehmensnetzwerk verlassende Datenverkehr. Bei der Nutzung des Internet werden ausschließlich folgende Daten protokolliert und gespeichert:
a) Benutzerkennung und Rechner, von dem aus zugegriffen wurde,
b) Datum und Uhrzeit,
c) Adresse des Zielrechners auf den zugegriffen wurde,
d) URL (interner Pfad auf dem Zielrechner, der angibt, wo sich dort die abgerufene Information befindet)
e) Dauer der Datenübertragung
f) Menge der übertragenen Daten.
Die Protokolle dienen ausschließlich den Zwecken der Gewährleistung der Systemsicherheit, der Steuerung der Lastverteilung im Netzwerk, der Abrechnung und der Optimierung des Netzes sowie der Analyse und Korrektur von technischen

Fehlern und Störungen. Ergibt sich ein begründeter Missbrauchsverdacht erhält der Arbeitgeber nach Zustimmung des zuständigen Betriebsrates unter Hinzuziehung eines Mitglieds des Betriebsrats Zugriff auf die pseudonymisierten Nutzungsdaten, die zur Aufklärung des Verdachts erforderlich sind. Erhärtet sich der Verdacht bei dieser pseudonymisierten Untersuchung, erhält der Arbeitgeber nach Zustimmung des Betriebsrats unter Hinzuziehung eines Mitgliedes des Betriebsrats und im Beisein des betroffenen Mitarbeiters oder Mitarbeiterin Zugriff auf die reidentifizierten Daten dieser Personen für den entsprechenden Zeitraum. Zu diesem Zweck wird eine Berechtigung geschaffen, die an ein geteiltes Passwort gebunden ist und unter Eingabe der Benutzer- oder Gerätekennung die notwendigen personenbezogenen Informationen für den ausgewählten Zeitraum anzeigt. Über eines der beiden Passwörter verfügt der jeweils zuständige Betriebsrat. Es werden dabei keine Protokolldaten verwendet, die älter als 30 Tage sind. Erhärtet sich der Verdacht nicht, sind die gewonnenen Daten unverzüglich zu löschen. Die Protokolldateien werden jeweils für 60 Tage geführt und danach automatisch gelöscht. Auswertungen, die personenbezogene oder – beziehbare Daten enthalten, sind als Anlage XXX abschließend aufgeführt. Dabei sind die folgenden Angaben zu dokumentieren:
a) Bezeichnung des erstellenden Programms,
b) Zweck der Auswertung,
c) Form der Auswertung,
d) Aussagefähiges Muster der Auswertung.
Eine Übermittlung von Daten an Dritte findet nicht statt.

§ 7 Zugriffsberechtigungen

Die Zugriffsberechtigungen mit Systemprivilegien zu den Programmen und Daten im Zusammenhang mit der Intranet/Internet/E-Mail-Nutzung werden organisatorisch und programmtechnisch geregelt. Die Zugriffs- und Verfügungsbefugnisse sind möglichst eng zu fassen. Die zugriffsberechtigten Personen sind nach § 5 BDSG auf das Datengeheimnis zu verpflichten und haben eine entsprechende Verpflichtungserklärung zu unterschreiben. Die Verantwortung aus dieser Verpflichtung ist ihnen angemessen zu erläutern. Bei Bedarf sind diese Personen vor diesem Hintergrund zu schulen.

§ 8 Qualifizierung

Die zugriffsberechtigten AdministratorInnen werden für die neuen Funktionen auf Kosten des Arbeitgebers geschult. Die Schulungen finden während der Arbeitszeit statt. Die NutzerInnen des Intranet/Internet werden ausreichend qualifiziert, um ihre mit Zugriffsberechtigung verbundenen Aufgaben kompetent ausführen zu können. Die Schulungen finden während der Arbeitszeit auf Kosten des Arbeitgebers statt. Dazu gehören:
a) in anwendungstechnischer Hinsicht die effektive Nutzung und arbeitsorganisatorisch optimale Einbindung in die übrigen Tätigkeiten,
b) die Information über mögliche gesundheitliche Risiken,
c) Grundfragen des Datenschutzes und der Persönlichkeitsrechte,
d) Daten- und Systemsicherheitsfragen und rechtliche Hinweise in Zusammenhang mit dem Zugriff auf Internetseiten mit strafrechtlich relevanten Inhalten
e) Aufklärung über Art und Umfang der Protokollierungen
f) die Regelungen dieser Vereinbarung.
Die entsprechenden Informations- und Qualifizierungsmaßnahmen werden mit dem
zuständigen Betriebsrat abgestimmt. Der Arbeitgeber verpflichtet sich, eine kurze und übersichtliche Handlungsanweisung zur Verfügung zu stellen.

§ 9 Rechte des Gesamtbetriebsrats und der Gewerkschaften

Der GBR hat das Recht, jederzeit unter Wahrung der Persönlichkeitsrechte der Beschäftigten die Einhaltung dieser Vereinbarung zu kontrollieren. Ihm sind, soweit nicht anders geregelt, auf Anforderung die erforderlichen Unterlagen zur Verfügung zu stellen. Der GBR kann auch in unregelmäßigen Abständen und unangemeldet Kontrollausgaben zu allen personenbezogenen Daten der Beschäftigten verlangen. Er hat das Recht, sämtliche Unterlagen der Systemdokumentation einzusehen und sich erläutern zu lassen. Der GBR kann hierfür dem Arbeitgeber einen Beauftragten benennen, der die Kontrollen durchführt. Ihm sind auf Verlangen alle Unterlagen zur Prüfung der Einhaltung dieser Vereinbarung zu übergeben. Der GBR ist darüber hinaus berechtigt, einen Sachverständigen seiner Wahl zur Kontrolle dieser Daten hinzuzuziehen. Der GBR erhält ebenso die Möglichkeit sich und seine Arbeit im Intranet zu präsentieren. Eine Verlinkung mit den zuständigen Gewerkschaftsseiten ist zulässig. Der GBR hat die Möglichkeit alle Beschäftigten über E-Mail zu informieren. Die zuständigen Gewerkschaften erhalten die Möglichkeit, die Beschäftigten über E-Mail bzw. Newsletter zu informieren. Die Rechte der örtlichen Betriebsräte bleiben unberührt.

§ 10 Änderung, Ergänzung und Erweiterung

1. Änderungen, Ergänzungen und Erweiterungen der technischen Umgebung, der dazugehörenden Software-Systeme, insbesondere von Funktionen sowie der Auswertung personenbezogener bzw. personenbeziehbarer Daten dürfen nur nach vorheriger Zustimmung des Gesamtbetriebsrates erfolgen. Dieser ist dann rechtzeitig und umfassend zu informieren. Die Rechte der örtlichen Betriebsräte bleiben unberührt.

§ 11 Sanktionen

Personelle Maßnahmen, die auf einer missbräuchlichen oder unzulässigen Anwendung der mit dem Internetzugang zusammenhängenden Hard- und Softwaresysteme basieren, sind unwirksam. Personenbezogene Erkenntnisse und Maßnahmen aus einer solchen Anwendung dürfen weder bei internen Beurteilungen noch bei arbeitsgerichtlichen Verfahren als Beweismaterial verwendet werden. Weitere Rechte des Betriebsrats bleiben von dieser Regelung unberührt. Werden die mit der Intranet/Internet/E-Mail-Nutzung zusammenhängenden Hard- und Softwaresysteme entgegen den hier vereinbarten Regelungen anderweitig genutzt, wird der entsprechende Teil dieser Systeme so lange nicht genutzt, bis durch geeignete Maßnahmen sichergestellt ist, dass eine Wiederholung ausgeschlossen ist.

§ 12 Information des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist unverzüglich über Missbräuche und Missbrauchsversuche des E-Mail-/Intranet-/Internet-Systems zu unterrichten. Alle Beschäftigten haben das Recht, vermutete oder tatsächliche Verstöße dem Betriebsrat und dem Datenschutzbeauftragten mitzuteilen. Das Beschwerderecht nach §§ 84 und 85 BetrVG bleibt davon unberührt.

§ 13 Schlussbestimmungen

1. Alle angeführten Anlagen zu dieser Vereinbarung sind Bestandteil dieser Vereinbarung.
2. Diese Vereinbarung tritt mit Unterzeichnung in Kraft. Sie kann von beiden Vertragsparteien mit einer Kündigungsfrist von sechs Monaten zum Monatsende gekündigt werden.
3. Nach Eingang der Kündigung müssen unverzüglich Verhandlungen über eine neue Vereinbarung aufgenommen werden.
4. Bis zum Abschluss einer neuen Vereinbarung gilt diese Vereinbarung weiter.

5. Sollten Sachverhalte, die in der praktischen Anwendung dieser Vereinbarung bzw. durch Nutzung von Intranet/Internet/E-Mail oder durch die technische Entwicklung regelungsbedürftig sein, so verpflichten sich die Vertragsparteien schnellstmöglich eine Regelung ergänzend zu vereinbaren, die den Grundsätzen dieser Vereinbarung entspricht.