Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitsrichtlinie für die Internet- und E-Mail-Nutzung

- Beispiel -

Stand: Dezember 2008

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

INHALTSVERZEICHIS

1 Einleitung

Diese Sicherheitsrichtlinie basiert auf den IT-Grundschutz-Katalogen des BSI. In der rechten Spalte befinden sich Verweise zu Hintergrundinformationen und zu Maßnahmenvorschlägen innerhalb der IT-Grundschutz-Kataloge.

M x.xx

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist in weiten Bereichen zur Selbstverständlichkeit geworden. Folge ist das Ausrüsten immer mehr PCs mit einem Internet-Zugang. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Mit Hilfe von Attachments (Anhängen) können Dateien effizient transportiert und E-Mail als Groupware-Lösung genutzt werden.

Dadurch können jedoch weitere Bedrohungen für die Institution entstehen: Neben dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener, vertraulicher und weiterer sensitiver Informationen während des Versands über das Internet ist auch die Sicherheit der intern abgespeicherten Informationen durch Angriffe von außen bedroht.

z. B. G 1.1, G 2.24, G 3.45 G 4.22, G 5.9

Diese Risiken müssen durch entsprechende – dem angestrebten Sicherheitsniveau angemessene – Maßnahmen auf ein tragbares Maß reduziert werden.

M 2.192

Hinweis:
Bemerkungen und Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung der Musterrichtlinie besonders empfiehlt, sind gelb hinterlegt.

2 Geltungsbereich

Diese Richtlinie zur Nutzung von E-Mail- und Internet-Diensten gilt für alle Beschäftigten ohne Ausnahmen. Die Richtlinie umfasst Vorgaben zur Organisation, zur Administration und zur Nutzung von E-Mail- und Internetdiensten.

Die Regelungen haben verbindlichen Charakter, so dass Verstöße gegen die Inhalte der Richtlinie zu arbeitsrechtlichen Konsequenzen führen können.

Sie gilt für alle Betriebsteile, d. h. auch bei Tele(heim)arbeit oder bei mobiler Arbeit außerhalb der Geschäftsräume. Darüber hinaus sind die Vorschriften auch für externe Mitarbeiter – soweit anwendbar – gültig und vertraglich sicherzustellen.

Für die inhaltliche Bearbeitung sowie für die Pflege und Änderung der Texte ist der IT-Sicherheitsbeauftragte im Namen der Leitung verantwortlich.

3 Organisation

3.1 Stellen

Die Internet- und E-Mail-Dienste sind durch fachkundiges Personal zu administrieren und zu warten. Zu diesem Zweck sind die Internet-Dienste durch Administratoren und nicht von normalen IT-Benutzern zu betreuen. Auch für die Überprüfung der Sicherheit des Netzes sind die Administratoren zuständig. M 2.26 und M 3.10

Administratoren haben sich regelmäßig über sicherheitsrelevante Patches, Updates oder sonstige Informationen zu informieren und die notwendigen Maßnahmen zu ergreifen. Im Rahmen ihrer Tätigkeit arbeiten sie eng mit dem IT-Sicherheitsbeauftragten zusammen und unterstützen und informieren ihn. M 2.35

3.2 Grundsätzliche Anforderungen

Die Empfehlungen des BSI zur Internet-Sicherheit sind zu berücksichtigen.

Alle Sicherheitseinstellungen sollten zentral steuerbar sein und nicht von IT-Benutzern abgeschaltet oder verändert werden können.

Hinweis: Es folgt ein Beispiel, wie eine Regel zum Schutz eines besonders gefährdeten Fachbereichs formuliert werden kann:

In Bereichen mit sehr hohem Schutzbedarf bezüglich Vertraulichkeit ist nur E-Mail-Nutzung erlaubt. Weitere Internet-Dienste (WWW, FTP usw.) sind zu deaktivieren. Zur Zeit ist hiervon die Entwicklungsabteilung für Prototypen betroffen.

Aktive Inhalte, die als gefährlich gelten, sind im Produktivnetz nur nach Genehmigung durch den IT-Sicherheitsbeauftragten zugelassen. Die Genehmigung darf nur bei vertrauenswürdigen Seiten einzeln erteilt werden. M 5.69

Alle Mitarbeiter müssen Seiten mit aktiven Inhalten, die aufgrund der Sicherheitseinstellungen am Arbeitsplatz nicht korrekt oder unvollständig dargestellt werden können, trotzdem nutzen können. Wenn keine andere technische Lösung zur Verfügung steht, werden Internet-PCs, die nicht an das interne Netz angebunden sind, in ausreichender Anzahl zur Verfügung gestellt. M 5.46, M 2.234

Bei der Auswahl eines Internet Service Provider bzw. eines Mailproviders sind Sicherheitsaspekte zu berücksichtigen. M 2.176, M 2.123

3.3 Schulungen

Die IT-Benutzer sind vor der erstmaligen Nutzung von E-Mail- und Internet-Programmen zu schulen. Dabei sind Ihnen die aus der Nutzung der Internet- M 3.4

und E-Mailnutzung resultieren Gefahren und die entsprechenden Sicherheitsregelungen näher zu bringen.

3.4 Zugriff

Der Zugriff auf Internet- und E-Mail-Dienste muss für jeden Mitarbeiter individuell geregelt werden. M 2.220

4 Konfiguration

4.1 Allgemeines

Die E-Mail- und Internet-Programme, die Mail- und Internet-Server sowie die Hardwarekomponenten sind durch die Administratoren möglichst so zu konfigurieren, dass ohne weiteres Zutun der IT-Benutzer optimale Sicherheit erreicht werden kann. M 2.174 und M 5.56 M 2.60 M 5.32

Änderungen an den Sicherheitseinstellungen durch die IT-Benutzer sind nicht gestattet.

4.2 Schutz gegen Computer-Viren

Bei jeglicher Kommunikation über das Internet muss an den Schutz vor Computer-Viren gedacht werden. Einzelheiten sind dem Virenschutzkonzept zu entnehmen.

Hinweis: Die nachfolgenden Regeln in Kapitel 4.2 sind redundant zum Virenschutzkonzept. An dieser Stelle kann daher auf sie verzichtet werden, wenn das Viren-Schutzkonzept so wie vom BSI vorgeschlagen übernommen wurde. Auch wenn auf ein eigenes Viren-Schutzkonzept verzichtet wird, empfiehlt es sich, das Muster des BSI zur Information zu lesen.

Ein- und ausgehende E-Mails sind zentral am Gateway auf Computer-Viren hin zu prüfen.

Es ist für einen Schutz gegen Dialerprogramme zu sorgen.

Innerhalb der Default-Einstellungen ist sicher zu stellen, dass Datei-Endungen nicht unterdrückt werden. Andernfalls wird es dem Nutzer erschwert, Dateiarten zu unterscheiden und Gefährdungspotentiale einzuschätzen.

4.3 Internet-Browser und E-Mail-Client

Es sind bei Browsern und E-Mail-Clients nur die Funktionen und Programme zu aktivieren, die zwingend benötigt werden. Die Zuteilung der verwendeten Programme und Dienste ist zu dokumentieren. M 5.45 und M 5.93f M 5.72 M 2.7

Cookies sind aus datenschutzrechtlichen Gründen zu unterdrücken oder regelmäßig zu löschen. M 5.45

Wenn der Cache des Browsers genutzt wird, ist dieser regelmäßig (nach der Sitzung) zu löschen. M 5.45

Die Funktion des Browsers, heruntergeladene Daten automatisch zu öffnen, ist zu deaktivieren. Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden (Vorschaufunktion deaktivieren). M 5.94 M 5.94

Von der Funktion automatischer Lesebestätigungen ist abzusehen, da dies unerwünschte E-Mail-Versender unterstützen kann (Spam). M 5.94

Bei einer automatischen Weiterleitung von E-Mails ist die Vertraulichkeit zu wahren, indem sichergestellt wird, dass alle Empfänger die E-Mails auch lesen dürfen.

Die Funktion des Browsers ist zu deaktivieren, die das automatische Ausfül-

len von Formularen auf Internetseiten durch abgespeicherte persönliche Informationen oder Passwörter ermöglicht. M 5.93

Die Funktion des E-Mail-Clients, die Adresse eines E-Mail-Empfängers automatisch zu vervollständigen, sollte nicht verwendet werden.

4.4 Sicherheitsgateway (Firewall)

Erst nach Einführung einer geeigneten Firewall darf der Anschluss an ein externes Netz erfolgen. Die Firewall ist so zu konfigurieren und zu administrieren, dass sie einen effektiven Schutz darstellt und Manipulationen verhindert werden. M 2.78 und M 4.100f

Aktive Inhalte sind zentral an der Firewall zu filtern.

Bei der Firewall sind die Filterregeln so restriktiv wie möglich zu wählen („alles was nicht erlaubt ist, ist verboten“). Die IT-Benutzer dürfen jedoch nicht durch eine Vielzahl von Meldungen belästigt und in ihrer Arbeit beeinträchtigt werden. M 2.76 und M 2.78

Alle weiteren Komponenten, die der Kommunikation zwischen geschütztem internen und ungeschützten externen Netz dienen, müssen sicher angeordnet werden. M 2.77

Laptops dürfen nur mit dem Internet verbunden werden, wenn sie mit einer Personal Firewall ausgestattet sind. M 5.91

4.5 Revision

Der Fernzugriff von Benutzern auf E-Mail-Accounts ist zu kontrollieren und sicher zu gestalten. M 2.109

Es sind die sicherheitsrelevanten Ereignisse zu protokollieren. Der Datenverkehr ist ebenfalls automatisch zu protokollieren. Bei Verdacht auf einen Sicherheitsverstoß sind die Protokolle durch eigens hierfür Berechtigte auszuwerten. Datenschutz- und Mitbestimmungsrechte sind zu beachten. M 4.47 und M 4.106 M 2.110

5 Nutzung

5.1 Private und dienstliche Nutzung

Ob Internet und E-Mail privat genutzt werden dürfen, muss geregelt werden, um unklare Situationen und Streitigkeiten zu verhindern. Auch wenn Seiten mit bestimmten Inhalten nicht angesehen werden dürfen, muss es an dieser Stelle festgeschrieben werden. Das BSI kann zu diesem Punkt aber keine Empfehlung abgeben, da bei der Regelung der privaten Nutzung nicht nur die Unternehmenskultur, sondern auch umfangreiche rechtliche Aspekte zu berücksichtigen sind. Rechtliche Informationen zu diesem Thema bietet z. B. der Bundesbeauftragte für den Datenschutz. Die "einfachste" Lösung ist es, private Nutzung von E-Mail und Internet zu untersagen.

Beim dienstlichen Gebrauch ist darauf zu achten, dass geltende Gesetze (insbesondere das Urheberrecht) eingehalten werden.

Auch bei der E-Mail-Nutzung sind die üblichen Geflogenheiten in der Kommunikation zu wahren. Alle nach außen gehenden E-Mails sind daher mit Absenderangabe (Name und Telefonnummer) zu versehen. M 2.118

Beiträge in Internet-Newsgroups oder Diskussionsforen unterliegen den gleichen Regelungen wie sonstige öffentliche Meinungsbekundungen und Veröffentlichungen im Namen des Arbeitgebers und sind vom Pressesprecher vorab freizugeben.

5.2 Übertragung schützenswerter Daten

Die Übertragung von vertraulichen Informationen an Externe mittels E-Mail ist ausschließlich in verschlüsselter Form zulässig. E-Mails dürfen nicht an externe Stellen übermittelt werden, wenn diese nicht in der Lage sind, verschlüsselte E-Mails zu lesen. M 5.108

Wenn es auf die Integrität von E-Mails ankommt, sollte die Verwendung elektronischer Signaturen geprüft werden. M 5.108

Interne E-Mails mit vertraulichem Inhalt, dürfen das interne Netz nicht verlassen (Versand über eigene Standleitung). M 2.118

5.3 Herunterladen von Dateien

Dateien und Programme sind nur durch Berechtigte von vertrauenswürdigen Quellen herunterzuladen.

5.4 E-Mail-Adressen

Jeder Mitarbeiter erhält eine mitarbeiterspezifische E-Mail-Adresse. Zusätzlich werden funktionsbezogene E-Mail-Adressen eingerichtet, die für dienstliche Angelegenheiten verwendet werden müssen. Auf der Internetseite sollten nach Möglichkeit nur funktionsbezogene E-Mail-Adressen genannt werden. M 2.122 M 2.275

Es muss durch Vertretungsregeln gesichert werden, dass E-Mails im Abwesenheitsfall beantwortet werden. Diese Pflicht gilt insbesondere für funktionsbezogene E-Mail-Adressen. M 2.274

Die Adressierung von E-Mails muss eindeutig erfolgen. Es sind Adressbücher und Verteilerlisten zu erstellen und zu pflegen. Es ist sicherzustellen, dass diese Listen nicht extern zugänglich sind. M 2.119 M 5.55

Sofern E-Mails an mehrere Empfänger versandt werden, sind nach Möglichkeit Verteilerlisten oder die „BCC-Option“ zu nutzen, so dass der Empfänger nicht die komplette Empfängerliste einsehen kann.