Empfehlungen zum sicheren Umgang mit E-Mails

Die schriftliche Kommunikation und der Austausch von Daten zwischen zwei Kommunikationspartnern oder innerhalb einer Gruppe erfolgt heute bevorzugt per E-Mail. Das, obwohl der Übertragungsweg als unsicher gilt und auch mancher Speicherort für E-Mails nicht als ausreichend sicher angesehen werden kann. Dies ist besonders problematisch, wenn es sich bei den ausgetauschten Informationen um vertrauliche Daten handelt. Einen besonderen gesetzlichen Schutz erfahren hierbei die personenbezogenen Daten.

Im folgenden sollen Hinweise zum sicheren Umgang mit E-Mails und der mit ihnen übermittelten vertraulichen Daten gegeben werden.

1 Situation

1.1 Gesetzeslage

Obwohl E-Mail als unsicheres Medium zur Übertragung von Daten gilt, werden häufig vertrauliche Daten, zu denen auch die personenbezogenen Daten[1] zählen, per E-Mail verschickt. Vertrauliche Daten sind besonders zu schützen, insbesondere wenn dies sogar vertraglich mit einem Kooperationspartner vereinbart wurde. Abgesehen davon verlangt das Niedersächsische Datenschutzgesetz (NDSG) den besonders sorgsamen Umgang einer öffentlichen Stelle des Landes mit personenbezogenen Daten. Entsprechende Anforderungen an den Umgang mit E-Mails, die personenbezogene Daten beinhalten, ergeben sich insbesondere aus den Paragrafen des NDSG:

§ 7 Abs. 2.10 (Technische und organisatorische Maßnahmen, hier Übertragung von Daten),

§ 14 Abs. 1 (Übermittlung an Personen oder Stellen in Staaten außerhalb des europäischen Wirtschaftsraums).

E-Mails mit personenbezogenen Daten dürfen hiernach nicht per E-Mail verschickt werden, wenn die Gefahr besteht, dass diese *unbefugt gelesen, kopiert, verändert oder gelöscht werden können.* E-Mails mit personenbezogenen Daten dürfen hiernach auch nicht zur Verarbeitung, und hierzu zählt auch die Speicherung, in Staaten außerhalb des europäischen Wirtschaftsraums geschickt werden.

1.2 Sicherheit von E-Mails

Die Sicherheit der E-Mail-Übertragung ist abhängig vom Raum, in dem die E-Mails übertragen werden.

1.2.1 Innerhalb der TU Braunschweig-Domäne

Die E-Mail-Konten der TU Braunschweig werden in dem zentralen E-Mail-Serversystem im GITZ verwaltet und gespeichert. Das Serversystem steht im geschützten Maschinensaal des GITZ. E-Mails die zwischen zwei Konten der TU Braunschweig Domäne „@tu-braunschweig.de“ (TU-Domäne) ausgetauscht werden, verlassen nicht das Serversystem. Der Zugriff auf das Serversystem geschieht inner-

[1] § 3 das Niedersächsische Datenschutzgesetz (NDSG) definiert personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (Betroffene).

halb der TU Braunschweig über das geschlossene Datennetz der TU Braunschweig. Der Zugriff von außerhalb ist nur Berechtigten und nur über ein verschlüsselndes Protokoll (ssl) möglich.

Die Übertragung und die Speicherung von E-Mails werden, nach dem Stand der Technik, innerhalb der TU-Domäne als sicher angesehen. Entsprechend kann der Versender einer E-Mail von einem E-Mail-Konto der TU-Domäne davon ausgehen, dass seine E-Mail an einen Adressaten in der TU-Domäne den sicheren Bereich nicht verlässt und die E-Mails damit nicht *unbefugt gelesen, kopiert, verändert oder gelöscht werden können.*

1.2.2 Außerhalb der TU Braunschweig-Domäne

Verlassen E-Mails die TU-Domäne, so kann die Übertragung nicht mehr als sicher angenommen werden. Dienstliche E-Mails mit vertraulichem Inhalt dürfen an externe E-Mail-Adressen nur verschlüsselt geschickt werden. Befinden sich die vertraulichen Daten in einer angefügten Datei, so muss zumindest der Inhalt dieser Datei verschlüsselt sein.

2 Umgang mit vertraulichen Daten in E-Mails

Wenn die Gefahr besteht, dass E-Mails *unbefugt gelesen, kopiert, verändert oder gelöscht werden können* dürfen diese nur verschlüsselt übertragen werden. Für E-Mails, die außerhalb des EU-Wirtschaftsraums gespeichert, oder verarbeitet werden, gelten besonders strenge Maßstäbe.

2.1 Verschlüsselung

E-Mails mit vertraulichem Inhalt lassen sich insgesamt verschlüsseln. Befindet sich der vertrauliche Inhalt in einem Anhang, genügt es u. U., den Anhang zu verschlüsseln.

2.1.1 Verschlüsselung der gesamten E-Mail

Die Verschlüsselung einer gesamten E-Mail erfordert eine PKI (Public Key Infrastructure)[2], die dem Absender den öffentlichen Schlüssel zum Verschlüsseln und dem Empfänger den privaten Schlüssel zum Entschlüsseln liefert. Aktuell verfügt die TU Braunschweig über keine PKI, sodass die Verschlüsselung der gesamten E-Mail nicht unterstützt werden kann.

2.1.2 Verschlüsselung von Anhängen

Anhänge lassen sich mit symmetrischen Schlüsseln[3] verschlüsseln. Viele Anwendungen bieten proprietäre Verschlüsselungsverfahren (MS-Word, Adobe PDF,…). Darüber hinaus lassen sich mit kostenlose Datenkompressionsprogramm wie z. B. 7Zip Dateien verschlüsseln. In der Vergangenheit galt die Verschlüsselung der MS-Office Dokumente (≤ Office 2003) als schwach. Die Verschlüsselung von MS-Office 2007-Dokumente und später gilt heute aber als ausreichend stark und lässt sich nur noch mit Brute-Force-Angriffen[4] knacken. Auch 7Zip bietet mit 256 Bit AES eine starke Verschlüsselung an.

PDF-Dateien lassen sich inzwischen mit 256 Bit AES sowohl mit symmetrischen als auch mit asymmetrischen Schlüsseln sichern. Adobe Acrobat und Reader bieten ab Version X (10) die Möglichkeit selbstsignierte Zertifikate mit asymmetrischen Schlüsselpaaren zu generieren. Der Empfänger der Nachricht schickt sein Zertifikat mit seinem öffentlichen Schlüssel an den Versender der Nachricht. Dieser verschlüsselt die Nachricht mit dem öffentlichen Schlüsseln des Empfängers. Durch ein besonderes

---

[2] Eine PKI erzeugt die für alle Teilnehmer asymmetrische Schlüsselpaare, bestehend aus einem öffentlichen und einem privaten Schlüssel, übergibt jedem Teilnehmer seinen privaten Schlüssel und macht den öffentlichen Schlüssel allen Teilnehmern bekannt. Nachrichten werden dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur vom Empfänger mit seinem privaten Schlüssel gelesen werden. Die sichere Zuordnung des öffentlichen Schlüssels zum Empfänger wird dabei von der PKI über Zertifikate abgesichert.
[3] Bei einer symmetrischen Verschlüsselung wird bei Ver- und Entschlüsselung derselbe Schlüssel verwendet.
[4] Bei Brute-Force Angriffen werden alle möglichen Zeichenkombinationen getestet, bis der passende Schlüssel gefunden wurde.

Verfahren lassen sich dabei in einem PDF-Dokument gleichzeitig mehrere Personen angeben, die das PDF-Dokument mit ihrem privaten Schlüssel entschlüsseln können.

In der Regel muss der Absender selbst einen Schlüssel festlegen. Für alle diese Schlüssel gelten hierbei die gleichen Regeln wir für sichere Passwörter[5].

2.2 Cloud-Storage

Das Gauß-IT-Zentrum betreibt einen zentralen Cloud-Storage Dienst als Kollaborationsplattform. Der Dienst umfasst die Bereitstellung und den Zugriff auf einen zentralen Datenspeicher (Cloud), dessen Sicherung und Wiederherstellung.

Anstatt Dateien per E-Mail zu verschicken, lassen sich Dateien in der Cloud der TU Braunschweig speichern, von der sie vom Empfänger der Nachricht heruntergeladen werden können. Der Zugriff auf die Cloud ist nur über Protokolle, die eine Verschlüsselung beinhalten, möglich. Jeder Mitarbeiter der TU Braunschweig hat einen Zugang zur Cloud über https://cloudstorage.tu-braunschweig.de.

2.2.1 Datenübergabe mithilfe der Cloud-Storage

Arbeitsgruppen, Gremien und andere Gruppen können in der Cloud der TU Braunschweig gemeinsame Verzeichnisse anlegen, in denen sich Dateien zur gemeinsamen Nutzung ablegen lassen. Dabei lassen sich für einzelne Verzeichnisse die berechtigten Personen und deren Zugriffsrechte (Lesen/Schreiben) festlegen. In den Verzeichnissen lassen sich auch vertrauliche Daten sicher ablegen und die Partner dann z. B. per E-Mail über das neu abgelegte Dokument informieren.

2.2.2 Datenübergabe per Link

Handelt es sich um datenschutzrechtlich unkritische Daten und geht es nur darum, den gleichzeitigen Versand von Dateien an eine Vielzahl von Empfängern zu vermeiden, so genügt es, statt die Datei anzuhängen, in der Nachricht einen (kryptischen) Link auf die Datei mitzuschicken. Der Empfänger kann dann nach einem Klick auf den Link die entsprechende Datei auf seinen Rechner herunterladen. Die Vorgehensweise verbietet sich für vertrauliche Daten, da jeder, der den Link kennt, Zugriff auf die entsprechende Datei bekommt. Denn jeder der Zugriff auf die E-Mail erlangt, kennt damit auch den Link.

3 Weiterleitungen

Weiterleitungen von E-Mails und Abruf von E-Mails unterliegen den gleichen Gefahren wie der direkte Versand von E-Mails an Adressen außerhalb der TU Braunschweig-Domänen.

3.1 Automatische Weiterleitung

Gehören Sender und Empfänger einer E-Mail zur TU Braunschweig-Domäne, so kann der Sender davon ausgehen, dass die E-Mail den geschützten Bereich der Domäne nicht verlässt und darf damit auch vertrauliche Daten unverschlüsselt versenden. Bei einer automatischen Weiterleitung zu einer Adresse außerhalb der TU Braunschweig-Domäne leitet der Empfänger die E-Mail ohne Prüfung des Inhalts auf Vertraulichkeit und ohne Kenntnis des Absenders auf unsicherem Weg in einen möglicherweise unsicheren Bereich.

Normalerweise haftet beim Datenaustausch per E-Mail der Sender für eventuelle Schäden, die durch den Missbrauch sensibler Daten verursacht werden. Bei einer Weiterleitung haftet der Weiterleitende. Werden alle eingehenden E-Mails automatisch weitergeleitet, so ist die Gefahr sehr groß, dass auch vertrauliche unverschlüsselte Nachrichten den geschützten Raum der TU-Domäne verlassen.

[5] Siehe auch https://www.tu-braunschweig.de/datenschutz/wissen/passwoerter/index.html

3.2 Automatischer Abruf von E-Mails vom TU-Konto

E-Mails lassen sich nicht nur automatisch aus dem dienstlichen E-Mail-Konto an ein externes Konto weiterleiten. Umgekehrt besteht technisch genauso die Möglichkeit, von einem externen E-Mail-Konto automatisch alle E-Mails eines dienstlichen Kontos abzurufen. Viele E-Mail-Provider unterstützen dies und motivieren ihre Kunden geradezu, einen automatischen Abruf einzurichten. Die datenschutzrechtliche Problematik ist hier noch verheerender, da zusätzlich zur oben geschilderten Problematik in diesem Fall beim Provider die Zugangsdaten zu einem IT-System der TU Braunschweig hinterlegt werden müssen. Dies ist aus Sicherheitsgründen nicht zulässig. Daher wird von jedem Nutzer, bei den regelmäßig erforderlichen Passwortänderungen die Bestätigung abverlangt, dass er anerkennt, sein Passwort nicht an Dritte weitergeben zu dürfen.

3.3 Mailinglisten und Verteiler (Reflektoren)

Um die Kommunikation und den Datenaustausch innerhalb von Forschergruppen oder Arbeitsgruppe zu vereinfachen, werden auch als Reflektoren bezeichnete Mailinglisten oder Verteiler eingerichtet. Der Benutzer ist sich bei der Nutzung einer solchen Verteilerliste bewusst, dass er seine E-Mail nicht an eine einzelne Person schickt und sich nicht alle adressierten E-Mail-Konten in der TU-Domäne befinden.

Werden über solche Reflektoren vertrauliche oder personenbezogene Daten ausgetauscht, so ist darauf zu achten, dass die Daten verschlüsselt sind. Eine Ausnahme bilden Verteiler mit bekannterweise ausschließlich E-Mail-Adressen des zentralen E-Mail-Systems der TU Braunschweig.

3.4 Alternativen zur automatischen Weiterleitung

Automatische Weiterleitungen werden häufig eingerichtet, um auch von zuhause oder auf Dienstreisen auf dienstliche E-Mails zugreifen zu können. Einigen mag nicht bewusst sein, dass auch das zentrale E-Mail-Konto der TU Braunschweig weltweit erreichbar ist. Dies ist per Web- oder per E-Mail-Client möglich. Bei Zugriff über einen E-Mail-Client wird die Verbindung zwischen Client und Host zwangsweise verschlüsselt, sodass auch vertrauliche Daten auf diesem Wege sicher ihr Ziel erreichen. Vorsicht ist dagegen bei Web-Clients trotz https-Verschlüsselung geboten, insbesondere wenn das genutzte Endgerät, wie PC, Laptop, Smartphone etc., über einen öffentlichen Hotspot oder den Hotspot eines Hotels mit dem Internet verbunden ist.

3.4.1 Benachrichtigung über eingehende E-Mails

Einige Mitarbeiter wollen von ihren mobilen Endgeräten über den jeweiligen Eingang wichtiger E-Mails informiert werden. Dies ist auch mit dem zentralen E-Mail-System der TU Braunschweig[6] möglich. Werden im zentralen E-Mail-System weniger wichtige Nachrichten vorab per Regel aussortiert, sieht der Mitarbeiter im Posteingang seines mobilen Endgeräts nur die verbliebenen relevanten Nachrichten.

[6] Communigate Pro oder abgekürzt CGP