Technische Universität Berlin

Der Präsident

R U N D S C H R E I B E N

☒ ALLE (Prof., WM, SM, Tut)

Gruppe **G**

Bearbeiter: Fr. Hiller	
Stellenzeichen / Telefon: K3-DS / 21784	Datum: 26.03.2012

Schlagwort :
Datenschutzrechtliche Aspekte beim Umgang mit E-Mails, Teil 3

- Sicherheit bei der Übertragung/Versendung von E-Mails mit vertraulichem Inhalt

Dieses Rundschreiben ersetzt:

Datenschutzrechtliche Aspekte beim Umgang mit E-Mails, Teil 3
– Sicherheit bei der Übertragung / Versendung von E-Mails mit vertraulichem Inhalt

Sehr geehrte Kolleginnen und Kollegen,

sehr häufig erreicht mich die Frage „Was muss beachtet werden, wenn ich vertrauliche Daten über E-Mail versenden möchte?“ Ich weiß von Fachgebieten, die vertrauliche Inhalte nur in verschlossenen Umschlägen per Hauspost versenden. Dies ist eine löbliche Vorsichtsmaßnahme, aber zeitlich aufwändig und bei Beachtung einiger Vorsichtsmaßnahmen nicht wirklich nötig.

1. automatische Übertragungsverschlüsselung

In der ZUV galt früher der Grundsatz, dass personenbezogene Daten nur verschlüsselt versendet werden dürfen.

Dieser Grundsatz hat auch heute noch Bestand, allerdings wird er – zumindest soweit es die Übertragung innerhalb der Technischen Universität Berlin betrifft – zumeist automatisch erfüllt.

E-Mails innerhalb der Technischen Universität Berlin sind während der Übertragung vom E-Mail-Client zum E-Mail-Server und umgekehrt verschlüsselt. „Innerhalb der TU“ heißt dabei von TU-Adresse zu TU-Adresse, unabhängig vom Zugriffsort (also auch, wenn ich von zuhause auf meinen TU-E-Mail-Account zugreife). Im unwahrscheinlichen Fall, dass der Netzwerkverkehr zwischen E-Mail-Server und Client abgehört wird, ist durch die Transportverschlüsselung der Inhalt der E-Mail nicht lesbar.

Diese Absicherung besteht allerdings nur während des Transports der E-Mail. Auf dem E-Mail-Client und dem E-Mail-Server bleibt die E-Mail weiterhin unverschlüsselt. Der Fall, dass hier ein Lauscher von außen kommt, ist jedoch weitaus weniger wahrscheinlich als der Fall, dass die E-Mail in Ihrem Rechner von Unbefugten wahrgenommen wird.

2. Empfänger als eigentliches Datenschutzrisiko

Grundsätzlich ist beim Versand per E-Mail nämlich der Umgang des Empfängers von E-Mails mit vertraulichem Inhalt das eigentliche Datenschutzrisiko.

Es ist ungleich leichter, mal eben eine E-Mail weiterzuleiten, weil man eine Passage aus einem Protokoll mitteilen will, als den Weg zum Kopierer zu nehmen und dabei dann vielleicht zu überlegen, dass den Dritten eigentlich nur eine Seite des Dokuments interessiert (und interessieren darf).

…

Auch werden Rechner an der TU nach wie vor häufig von mehreren Personen genutzt, Sekretariate benutzen das persönliche Passwort des Professors oder von Kollegen und umgekehrt – das darf datenschutzrechtlich nicht sein (vgl. Teil 1 des Rundschreibens), ist aber häufig so. Eine E-Mail in einem Postfach ist daher weniger sicher vor Blicken Dritter als der Inhalt eines als vertraulich/verschlossen markierten Umschlages.

3. zusätzliche Endnutzer-Verschlüsselung

Gern wird daher eine zusätzliche Endnutzer-Verschlüsselung mittels eines kryptografischen Schlüssels als weitere Absicherung gefordert. Hier werden nicht die einzelnen Datenpakete verschlüsselt, sondern die E-Mail als Ganzes. Zusätzlich besteht die Möglichkeit die E-Mail mit einem weiteren kryptografischen Schlüssel zu signieren (d.h. der Empfänger kann SICHER sein, dass die Mail tatsächlich von dem Absender kommt, der als Absender in der Mail angezeigt wird).

Hilfe bei der Einrichtung für die zusätzliche Endnutzer-Verschlüsselung bzw. Signatur bietet der tubIT-Kundendienst.

Während bei der Verschlüsselung der Transportpakete die E-Mail auf dem Rechner des Empfängers im Klartext vorliegt und von jedem mit Zugang zu diesem System lesbar ist, bleibt die Endnutzer verschlüsselte E-Mail auch nach dem Empfang verschlüsselt und benötigt bei jedem Lesen den entsprechenden Schlüssel.

Was man aber immer bedenken muss, ist, dass nach Entschlüsselung – egal ob automatische oder Endnutzer-Verschlüsselung – die E-Mail wieder eine normale E-Mail ist, also auch ausgedruckt oder unverschlüsselt weitergeleitet werden kann. Datenschutzrechtlich ist die zusätzliche Endnutzer-Verschlüsselung im Regelfall nicht geboten, sie stellt aber unbestreitbar die sicherste Methode zur Übermittlung von schützenswerten Daten / E-Mails dar.

4. Dokumentenpasswortschutz

Eine Alternative zur Sicherung vor unberechtigtem Einsehen durch Dritte an den Empfänger-PCs ist die Versendung der zu schützenden Daten als passwortgeschütztes Dokument im Anhang. Auch hier kann nur derjenige, der das Passwort kennt, das Dokument öffnen. Das Verteilen des Passworts an mehrere berechtigte Empfänger ist in der Regel zwar einfacher als die Verteilung der kryptografischen Schlüssel, allerdings gilt die Verschlüsselung mittels eines kryptografischen Schlüssels als sicherer als eine Verschlüsselung mit Passwort .Außerdem ist bei der Passwort-Variante ausschließlich der Anhang verschlüsselt und nicht die gesamte E-Mail. Vielfach wird auch das Passwort direkt in der E-Mail mitgeteilt, wodurch der Schutz sofort aufgehoben ist.

5. Einführung von SharePoint

Zuletzt möchte ich darauf hinweisen, dass über tubIT in Kürze Sharepoint an der Technischen Universität Berlin zur Verfügung stehen wird - also eine Plattform, auf der schützenswerte Inhalte zur Einsicht und Bearbeitung für bestimmte autorisierte Mitglieder von Gruppen abgelegt werden können. Sharepoint ist dabei in erster Linie gedacht für die Anwendung im wissenschaftlichen Bereich, insbesondere bei Forschungskooperationen. Eingeschränkt ist auch ein datenschutzrechtlich sinnvoller Einsatz in der Verwaltung denkbar.

Näheres über die Einführung und Verwendungsmöglichkeiten von Sharepoint werden Sie zeitnah über tubIT erfahren.

Bei Rückfragen stehe ich Ihnen unter datenschutzbeauftragte@tu-berlin.de zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Annette Hiller
behördliche Datenschutzbeauftragte der Technischen Universität Berlin