technische universität
dortmund

Betriebsregelung zum Umgang mit E-Mails an der TU Dortmund

Präambel

Vor dem Hintergrund, dass eine erhöhte Gefährdungslage durch Schadsoftware besteht und E-Mails nach wie vor einen der populärsten Wege für die Verbreitung von Schadsoftware darstellen, werden in dieser Betriebsregelung Regelungen zur E-Mail-Sicherheit getroffen. Das ITMC verfolgt effektive Maßnahmen zum Schutz der IT-Infrastruktur. Zusätzlich sind bei der Nutzung von E-Mail-Diensten besondere Sorgfalt und eine persönliche Mitwirkung erforderlich, um Angriffe auf die IT und Daten und somit auf die Campus IT der TU Dortmund zu vermeiden. Die Betriebsregelung umfasst Maßnahmen nach dem BSI Grundschutz, die in der angehängten Handlungsempfehlung näher erörtert werden.

§ 1
Geltungsbereich und Zweck

I. Diese Betriebsregelung gilt für die Benutzung der zentralen Postfächer von den E-Mail-Diensten Unimail und Exchange sowie der Postfächer auf Fakultäts-Servern.

II. Diese Betriebsregelung zielt sowohl auf die Reduzierung der Infektionsgefahr mit Schadsoftware, welche von aktiven Inhalten und ausführbaren Dateien in E-Mails ausgeht als auch auf die Reduzierung der Gefahr für die Entwendung von persönlichen Zugangsdaten über manipulierte Webmails in E-Mails ab. Somit dient sie dem Schutz der Campus IT und der digitalen Daten der TU Dortmund.

III. Diese Betriebsregelung gilt für alle Nutzer*innen von E-Mail-Diensten gemäß § 2 der ITMC Benutzungsordnung.

§ 2
Allgemeines

I. Die automatisierte, zentrale Filterung der eingehenden E-Mails identifiziert verdächtige Mail-Anhänge, welche ausführbare Dateien, MS Office und PDF-Dokumente mit aktiven Inhalten enthalten.

II. Die identifizierten Attachments werden gekennzeichnet, verpackt und die verdächtige E-Mail wird im Anhang an eine Informationsmail an den/die Empfänger*in zugestellt, welche über die potentielle Gefährdung informiert und einen Ansprechpartner für Rückfragen nennt.

III. Als verdächtig klassifizierte Weblinks werden in E-Mails automatisch deaktiviert.

§ 3
Verantwortlichkeit und Zuständigkeit

I. Alle Nutzer*innen, die gemäß § 2 der ITMC Benutzungsordnung einen E-Mail Account der TU Dortmund erhalten, sind verpflichtet, sich über die Bestimmungen zur E-Mail-Sicherheit an der TU Dortmund zu informieren sowie die Vorgaben dieser Betriebsregelung einzuhalten.

II. Empfänger*innen von Informationsmails (gemäß § 2/II.) über verdächtige E-Mails sind verpflichtet, der Meldung nachzugehen und mit dem/der Absender*in Rücksprache zu halten, um so einerseits den/die tatsächliche/n Absender*in, andererseits den Inhalt des Anhangs zu verifizieren. Ist eine Rücksprache nicht möglich, wendet sich der/die Nutzer*in an die vorhandenen Ansprechpartner*innen für Rückfragen, um die E-Mail-Verifikation sicherzustellen. Erst wenn die Echtheit der E-Mail gesichert ist, darf das beigefügte Dokument entpackt und geöffnet bzw. der angegebene Weblink separat in einem Browser aufgerufen werden.

III. Das ITMC verantwortet die zusätzlichen Sicherheitsfunktionen der Email Security Appliance der TU Dortmund, um die eingehenden Mails an die unter § 1 Abs. 1 genannten Postfächer zu erfassen und Mails mit verdächtigen Inhalten mit Warnhinweisen für die Empfänger*innen zu kennzeichnen.

IV. Der Service Desk, erreichbar unter **service.itmc@tu-dortmund.de**, und das Sicherheits-Informationscentrum (SIC), erreichbar unter **info.sic@tu-dortmund.de**, des ITMC sind in Zweifelsfällen von verdächtigen E-Mails als Ansprechpartner für Rückfragen zuständig. Verdächtige E-Mails sollen an die obigen E-Mail-Adressen weitergeleitet werden, um potentiell infizierte Mails frühzeitig zu erkennen. Nach dem Weiterleiten soll die E-Mail in den Spam-Ordner oder Papierkorb des E-Mail-Programms verschoben werden.

§ 4
Inkrafttreten

Diese Betriebsregelung tritt mit sofortiger Wirkung in Kraft.

Erstellt durch das ITMC

Freigabe durch den Rektor