Dokumentinformationen

TLP:GREEN

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Autor** | **Bemerkungen** |
| 25.05.2021 | 0.1 | Dr. Marius Mertens | Unter Mitwirkung von Stefan Beyer und Martin Zeiler |
| 17.06.2021 | 0.2 | AG IT-Sicherheit |  |
| 27.07.2021 | 0.3 | Dr. Marius Mertens | Unter Mitwirkung von Christoph Czychun |

Aktuellste Version abrufbar unter <https://www.uni-due.de/ciso/intranet/dokumentation.php>

TLP:RED: Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/ Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

TLP:AMBER: Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln Traffic Light Protocol (TLP) einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:GREEN: Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

TLP:WHITE : Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

[https://de.wikipedia.org/wiki/Traffic\_Light\_Protocol]

Sicherheitsempfehlungen „Better E-Mail” der AG IT-Sicherheit

# Präambel

Die E-Mail wird als schneller und vielseitiger Kommunikationskanal geschätzt und gehört zum geschäftlichen wie privaten Alltag dazu. Dieses Medium birgt allerdings auch Gefahren: Angreifer versuchen, per E-Mail Schadprogramme einzuschleusen oder die Empfänger durch geschickte Formulierungen dazu zu bringen, sensible Informationen zu verraten.

Dieses Dokument soll Anregungen zum sicheren Umgang mit E-Mails geben und kann auch als Vorlage für eine verbindliche Regelung in Ihrem Bereich verwendet werden. Sie erhalten insbesondere auch Hinweise zum Umgang mit Angriffen per E-Mail und wie sie solche Versuche erkennen können. Dies kann allerdings nur gelingen, wenn legitime E-Mails möglichst keine Merkmale von schädlichen E-Mails aufweisen. Darum geben wir Ihnen außerdem Hinweise, welche unseriösen Merkmale Sie in Ihren eigenen E-Mails vermeiden sollten.

# Missgeschicke können passieren

* Sollen Sie einmal auf einen fragwürdigen Link geklickt haben, eine Datei versehentlich ausgeführt oder Ihr Passwort verraten haben: Das kann passieren!
* Bewahren Sie im Fall des Falles Ruhe. Fahren Sie im Zweifelsfall Ihren PC herunter, um die Aktivität eventueller Schadsoftware einzuschränken.
* Scheuen Sie sich nicht davor, schnell um Unterstützung zu bitten und über den Vorfall zu sprechen. In den allermeisten Fällen lässt sich durch eine kurzfristige Reaktion das Problem schnell lösen, ohne dass ein größerer Schaden entsteht.

# Grundlagen E-Mail-Verkehr

E-Mails sind das digitale Äquivalent von Postkarten. Insbesondere gilt:

* Die Inhalte können auf dem Transportweg von Dritten gelesen oder verändert werden.
* Die Absenderangabe wird nicht geprüft und kann auf einen beliebigen Namen bzw. eine beliebige E-Mail-Adresse gesetzt werden. Analogie: Auf einem Brief kann man als Absender eintragen, was man möchte. Der Absender einer E-Mail lässt sich nur durch eine digitale Unterschrift (siehe unten) eindeutig bestimmen.
* Jeder kann Ihnen einen Brief oder eine E-Mail schicken, egal ob Sie das möchten oder nicht.

# Digitale Unterschrift und Verschlüsselung

* Unterschreiben Sie Ihre E-Mails immer digital. Dies wird auch „digital signieren“ genannt und ermöglicht dem Empfänger, Sie eindeutig als Absender der E-Mail zu identifizieren. Dazu benötigen Sie ein Zertifikat des DFN-Vereins.
* Verschlüsseln Sie vertrauliche E-Mails bei Bedarf. So ist sichergestellt, dass vertrauliche Informationen nur vom gewünschten Empfänger gelesen werden können.
* Weitere Informationen und Anleitung finden Sie unter:  
  <https://www.uni-due.de/zim/services/e-mail/verschluesselung.php>

# Sicherer Umgang mit E-Mails

* Bei ungewöhnlichen Inhalten (sensible Themen, problematische Anhänge, etc.) stimmen Sie sich mit dem Empfänger vor dem Absenden der E-Mail über einen anderen Kommunikationskanal (z. B. telefonisch) ab.
* Überprüfen Sie vor dem Versand – insbesondere, wenn es sich um sensible Inhalte handelt – die Empfängerliste:
  + Sind ausschließlich die gewünschten Empfänger enthalten?
  + Nutzen Sie die Personensuche, um Tippfehler oder Irrläufer durch Namensgleichheiten zu vermeiden.
  + Verwenden Sie bei vielen sich gegenseitig nicht bekannten Empfängern das BCC-Feld zur Adressierung.
  + Nehmen Sie sich eine „Gedenkminute“ vor dem Absenden von kritischen E-Mails – einmal abgesendete E-Mails können Sie nicht wieder zurückholen.
* Beachten Sie bei Anhängen:
  + Anhänge sollten nicht zu groß sein (in der Regel kleiner als 50 MB). Manche Provider sind jedoch strenger und lassen nur noch kleinere E-Mails zu. Sie erhalten dann eine Fehlermeldung und müssen die E-Mail mit kleineren Anhängen erneut senden.
  + Verwenden Sie im Geschäftsverkehr übliche und sichere Formate, z. B. docx als Word-Dokument ohne Makros statt docm, das Makros und Schadsoftware enthalten kann.
  + Unverschlüsselte Anhänge können ebenso wie E-Mail-Inhalte von Dritten mitgelesen werden.
  + Wenn Sie ein Dokument nicht anhängen, sondern über einen Online-Speicherdienst teilen wollen, verwenden Sie dafür ein empfohlenes Angebot der Universität (z. B. GigaMove oder Sciebo) und keinen kommerziellen Drittanbieter. Siehe Leitlinien zur Nutzung von Cloud-Diensten:   
    <https://www.uni-due.de/imperia/md/content/zentralverwaltung/verkuendungsblatt_2019/vbl_2019_68.pdf>
* Wenn Sie externe Inhalte verlinken: Senden Sie nur leicht überprüfbare Links, idealerweise auf interne Seiten der UDE. Vermeiden Sie insbesondere Linkverkürzer. Eine Ausnahme stellt der Linkverkürzer „udue.de“ der UDE dar, der ausschließlich auf Angebote der UDE verlinkt.
* Verwenden Sie möglichst wenige Formatierungsoptionen und senden Sie E-Mails bevorzugt im Nur-Text-Format.
* Bei vielen und/oder gegenseitig unbekannten Empfängern sollten Sie aus Datenschutzgründen das BCC-Feld zur Adressierung verwenden. So werden die E-Mail-Adressen der weiteren Empfänger nicht ungewollt an Dritte weitergegeben.
* Das Anfordern von Lesebestätigungen wirkt invasiv, Sie sollten es daher vermeiden.
* Das Setzen einer „hohen Priorität“ wirkt invasiv, Sie sollten es daher vermeiden.
* In der Regel ist eine E-Mail eine digitale Geschäftskorrespondenz zu dienstlichen Vorgängen. Die äußere Form sollte dem entsprechen 🡪 Vgl. klassischer Geschäftsbrief
  + Verwenden Sie für dienstliche E-Mails ausschließlich Ihre dienstliche E-Mail-Adresse.
  + Unterschreiben Sie Ihre E-Mail digital mit Ihrem DFN-Zertifikat.
  + Sprechen Sie Ihre(n) Empfänger persönlich und zielgruppengerecht an.
  + Formulieren Sie das Thema der E-Mail aussagekräftig und leicht verständlich.
  + Die formalen Elemente eines Geschäftsbriefs (Betreff, Anrede, Textkörper, Grußformel) sollten enthalten sein. Nutzen Sie auch die Möglichkeit, in einer Signatur unter dem Textkörper automatisch Ihre Kontaktinformationen mitzuteilen.
  + Prüfen Sie, ob alle für das Verständnis erforderlichen Informationen enthalten sind (z. B. NICHT schreiben „Bitte öffnen Sie den Anhang“ ohne im E-Mail-Text auf den Zweck einzugehen)
* Automatische Abwesenheitsbenachrichtigungen
  + Bei E-Mails ist eine sehr zeitnahe Reaktion inzwischen üblich. Bei längerer Abwesenheit sollten Sie die automatische Abwesenheitsnotiz aktivieren. Informieren Sie ggf. über Vertretungsregelungen und/oder den Zeitpunkt Ihrer Rückkehr.
  + Unterschied zwischen internen und externen Absendern: Abwesenheitsbenachrichtigungen für interne Absender sind in der Regel unkritisch. Bei externen Absendern sollten Sie prüfen
    - Ob benannte Vertreter mit einer Offenlegung gegenüber externen einverstanden sind
    - Ob Sie Externen die Dauer Ihrer Abwesenheit mitteilen wollen.
    - Ob Sie Externen überhaupt Abwesenheitsnotizen senden wollen, weil diese Spammern unter Umständen verraten, dass das Postfach aktiv ist.
  + Hintergrund: Automatische Abwesenheitsnotizen können Angreifern wertvolle Informationen liefern, z.B. über die Abwesenheit einer zentralen Person.
* Versand von Massen-E-Mails über Listen und Mailverteiler
  + Vor allem Massen-E-Mails sollten wegen des unvermeidlichen unpersönlichen Charakters digital unterschrieben werden.
  + Das Vorgehen kann sich je nach Versandart unterscheiden. Informieren Sie sich vor dem Versand beim Betreiber Ihres Mailverteilers, wie die digitale Unterschrift erfolgt.
  + Je größer der spätere Verteiler, desto wichtiger ist ein vorheriger Test, ob alles wie gewünscht funktioniert.

# Schlechte E-Mails erkennen

* Melden Sie verdächtige E-Mails an [hotline.zim@uni-due.de](mailto:hotline.zim@uni-due.de). Senden Sie die E-Mail idealerweise als Anhang an Ihre Meldung, so dass die vollständigen Informationen inklusive Header zur Analyse erhalten bleiben. Anleitung:  
  <https://www.uni-due.de/zim/hilfecenter/faqs.php?id=800#a_800>
* Reagieren Sie nicht auf Spam: Antworten Sie nicht, klicken Sie keine Links an. Auch vermeintliche „Unsubscribe-Links“ teilen dem Absender in der Regel lediglich mit, dass Ihre E-Mail-Adresse aktiv ist und gelesen wird. Löschen Sie solche E-Mails ungelesen.
* Wenn Sie versehentlicher Empfänger einer E-Mail sind und diese eindeutig kein Spam ist, sollten Sie freundlicherweise den Absender darüber informieren.
* Das automatische Senden von Lesebestätigungen sollte deaktiviert werden.
* Konfigurieren Sie Ihr E-Mail-Programm so, dass es E-Mails im Nur-Text-Format anzeigt.
* Das ZIM informiert über aktuelle Phishingkampagnen und Häufungen von Spam auf  
  <https://www.uni-due.de/zim/sicherheitsmeldungen.php>
* Überprüfen Sie die digitale Unterschrift (Signatur) der E-Mail
  + Stimmt der Absender mit dem überein, was Sie erwarten?
  + Wird die Signatur vom E-Mail-Programm als gültig angezeigt?
  + Wurde das verwendete Zertifikat bei Absendern der UDE vom DFN-Verein ausgestellt? Dies gilt auch für viele andere deutsche Universitäten.
* Überprüfen Sie in der E-Mail enthaltene Links. Achten Sie dabei darauf, ob die URL plausibel erscheint, z.B. ob ein vermeintlich universitätseigenes Angebot auf die Domain uni-due.de oder uni-duisburg-essen.de verweist. Seien Sie insbesondere vorsichtig, wenn Sie zu einer Anmeldung oder sonstigen Eingabe von Login-Informationen aufgefordert werden. Verlassen Sie die Seite im Zweifel.
* Seien Sie misstrauisch, wenn Sie dazu aufgefordert werden Zahlungen zu leisten, Gutscheine oder Guthabenkarten zu erwerben, Dateien herunterzuladen oder auszuführen. Tun Sie im Zweifel nicht, was der Absender von Ihnen verlangt und erkundigen Sie sich zuerst bei der Hotline: [hotline.zim@uni-due.de](mailto:hotline.zim@uni-due.de).
* Seien Sie misstrauisch, wenn der Absender versucht, Druck auf Sie auszuüben. Oft behaupten Angreifer, Sie hätten Zugriff auf das Postfach oder Schadsoftware auf dem Rechner installiert. In der Regel treffen die Behauptungen nicht zu. Erkundigen Sie sich im Zweifel bei der Hotline: [hotline.zim@uni-due.de](mailto:hotline.zim@uni-due.de).
* Angreifer informieren sich über Ihre Ziele und verfassen erstaunlich realitätsnahe E-Mails. Personalabteilungen erhalten häufig fingierte Bewerbungen, Übungsgruppenleiter vermeintliche Nachfragen zu einer Prüfung. Seien Sie immer misstrauisch, wenn Sie eine Datei öffnen sollten oder einem externen Link folgen sollen.
* Leider gibt es keine Garantie oder unfehlbare Methode, eine E-Mail als nicht schädlich zu erkennen. Wenn Sie den geringsten Zweifel haben, fragen Sie beim Absender über einen anderen Kommunikationskanal nach, ob die erhaltene E-Mail legitim ist. Eine zusätzliche Nachfrage und deswegen eventuell verzögerte Bearbeitung einer legitimen E-Mail ist im Zweifel immer die bessere Alternative zur Ausführung von Schadsoftware einer Angriffsmail.