Empfehlung für den Versand von dienstlichen E-Mails, E-Mail-Rundschreiben und Statusmails an der WWU

Zielgruppe: IT-Administratoren der WWU *IV-Sicherheitsteam, Januar 2018*

Einleitung

Die folgende Empfehlung gibt Standards für den Versand von dienstlichen E-Mails, E-Mail-Rundschreiben und Statusmails an der WWU vor.

Empfehlung für den Versand von dienstlichen E-Mails, E-Mail-Rundschreiben und Statusmails an der WWU

- Einleitung
- Hintergrund
- Empfehlungen für dienstliche E-Mails
- Empfehlung für E-Mail-Rundschreiben
  - Beim Versand von E-Mail-Rundschreiben sollten die folgenden Punkte eingehalten werden:
- Empfehlung für Statusmails

E-Mail-Rundschreiben sind von Einrichtungen der WWU als E-Mail verschickte Rundschreiben an Empfängergruppen.

Statusmails sind von zentralen Systemen der WWU automatisch generierte und verschickte E-Mails an Nutzer (z.B. von Nutzerverwaltung, Druckabrechnung, SAP, sciebo etc.).

Hintergrund

Die Verbreitung aktueller *Schadsoftware* erfolgt hauptsächlich per Internet-Browser und per E-Mail. Insbesondere die seit Anfang 2016 wachsende Zahl von Verschlüsselungstrojanern setzt als Infektionsweg hauptsächlich auf E-Mails und Nutzerinteraktion beim Öffnen von E-Mail-Anhängen. Daneben stellt *Phishing* ein ernstes Problem dar, da mit abgefangenen Kennungen und Passwörtern noch weitergehender Schaden für die WWU angerichtet werden kann. Phishing-E-Mails werden immer professioneller und zielgerichteter versendet (sog. *Spear-Phishing*), so dass hier dringend Handlungsbedarf besteht.

Es wird u. a. von den IV-Sicherheitsbeauftragten großer Aufwand zur Nutzersensibilisierung durch Flyer, Webseiten und Weiterbildungs-Angebote betrieben. Ein wichtiger Punkt darin ist, Nutzer für gefälschte E-Mails zu sensibilisieren. Dabei wird stets davon abgeraten auf Links oder Anhänge in verdächtigen E-Mails zu klicken.

Es ist daher essentiell, dass offizielle E-Mails möglichst wenig Spam-Merkmale aufweisen!

Empfehlungen für dienstliche E-Mails

Dienstliche E-Mails sollten nach Möglichkeit generell digital signiert werden. Angehörige der WWU können bei der WWUCA entsprechende Digitale IDs beantragen, mit denen ein sicherer E-Mail-Verkehr ermöglicht wird. Informationen zur Beantragung und Verwendung finden sich auf den Webseiten der WWUCA [11]. Die E-Mail-Verschlüsselung sollte nicht generell, sondern nur bei personenbezogenen oder sensiblen Daten verwendet werden.

Empfehlung für E-Mail-Rundschreiben

Alle Einrichtungen der WWU sollten beim Versand von E-Mails die folgenden Mindestanforderungen erfüllen, um den Nutzer tatsächlich zu erreichen und den gängigen IT-Sicherheits-Empfehlungen gerecht zu werden.

Bei der Weiterleitung von Informationen an eine Empfängergruppe ist zu beachten, dass E-Mail-Adressen personenbezogene Daten sind und nicht einfach an Dritte weitergegeben werden dürfen [1]. Daher sollen keine großen Adresslisten in den sichtbaren Empfängerfeldern (`To:` oder `Cc:` Feld) verwendet werden. In Einzelfällen ist das `Bcc:` Feld zu verwenden und bei Wiederholungsfällen eine Mailingliste im ZIV einzurichten [2].

Im Nutzerportal MeinZIV wird ein Tool zum Versenden von E-Mail-Rundschreiben mit persönlicher Anrede und digitaler Signatur angeboten [3].

Beim Versand von E-Mail-Rundschreiben sollten die folgenden Punkte eingehalten werden:

1. **Verwenden einer digitalen Signatur**

Nur durch die Verwendung einer „digitalen Signatur“ [4] kann die *Echtheit* einer E-Mail eindeutig überprüft werden. Für die Absenderadresse muss eine entsprechende Digitale ID (auch „Nutzer- oder Gruppenzertifikat“ genannt) [5] vorliegen bzw. bei der WWUCA [6] beantragt werden.

2. **Gleicher Aufbau und Format der E-Mails**

Durch diese Punkte soll verhindert werden, dass E-Mails aufgrund der fehlerhaften Form als Spam eingestuft und gelöscht werden.

a) Anrede

- bei personenbezogenen Inhalten mit Namen
- ansonsten mit Nennung der Zielgruppe [TK1] (Mitarbeiter, Studierende, Professoren, Dekane etc.). Die Zielgruppe sollte so klein wie möglich gewählt werden, um Mitarbeiter und Studierende nicht durch zu viele E-Mails zu belästigen.

b) Inhalt (siehe dazu 3.)

c) Textsignatur[7] mit Ansprechpartner (*dabei konsistente und sinnvolle Absenderangaben* [TK2] *)*.

3. **Verwendung von HTML, Links und E-Mail-Anhängen**

Es kann nicht davon ausgegangen werden, dass HTML-E-Mails und Anhänge bei jedem Empfänger und auf jedem Gerät wie gewünscht angezeigt werden. Daher ist der Verweis auf eine zur E-Mail passende Webseite (z.B. im Mitarbeiter- oder Studierendenportal) mit weiteren Informationen und Dokumenten zu bevorzugen [8].

a) HTML-E-Mails und Anhänge sollten *nur in Ausnahmefällen* verwendet werden.

b) Links sollten nur zu Webseiten der Uni Münster (uni-muenster.de/wwu.de) verweisen, dabei sind vorrangig `https`-Links zu verwenden. Mit dem Link-Verkürzer `go.wwu.de` [9] können kurze Links oder Links zu externen Seiten realisiert werden.

c) Es sollten keine direkten Links zu mit HTTP Auth Passwort-geschützten Webseiten verwendet werden, da der Nutzer dann die Echtheit der aufgerufenen Seite nicht überprüfen kann. Für den Single-Sign-On-Bereich (SSO) des zentralen Webserverparks gibt es eine extra SSO-Eingangs-Seite [10].

Empfehlung für Statusmails

Statusmails enthalten in der Regel personenbezogenen Inhalt und sollten daher mit persönlicher Anrede verschickt werden.

Es wird empfohlen, die Regelung für E-Mail-Rundschreiben soweit wie möglich auch für Statusmails umzusetzen. Allerdings kann dies technisch bedingt nicht in jedem Punkt möglich sein.

Mittels Signing-Milter [12] lassen sich E-Mails automatisch digital signieren, auch wenn die Anwendung das selbst nicht unterstützt.

---

[1] Vgl. https://heise.de/-1902442

[2] Siehe https://www.uni-muenster.de/ZIV/Technik/Server/Listenserver.html

[3] Die Nutzung kann auf Anfrage beim ZIV eingerichtet werden (E-Mail an wwwadmin@uni-muenster.de).

[4] Siehe https://de.wikipedia.org/wiki/Digitale_Signatur

[5] Siehe https://de.wikipedia.org/wiki/Digitales_Zertifikat

[6] Siehe https://www.uni-muenster.de/WWUCA

[7] Es ist etablierte Konvention, eine Signatur durch einen Signaturtrenner vom Nachrichtentext abzutrennen. Dieser besteht aus einer Zeile, die nur die Zeichenfolge „-- “ (zwei Bindestriche und ein Leerzeichen) enthält. Dadurch wird es den meisten E-Mail-Programmen und Newsreadern ermöglicht, eine Signatur automatisch zu erkennen und beim Antworten nicht zu zitieren.

[8] Das BSI empfiehlt die Darstellung von HTML in E-Mails abzuschalten: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Sicherheitsirrtuemer/Irrtuemer_E-Mail-Sicherheit.html

[9] Siehe: https://go.wwu.de/

[10] Vgl. https://www.uni-muenster.de/de/mywwu/index.shtml

[11] Siehe https://www.uni-muenster.de/WWUCA/

[12] Siehe https://www.uni-muenster.de/imperia/md/content/iv-sicherheit/signing-milter.pdf

---

[TK1] "Sie erhalten diese E-Mail als Mitarbeiter/Studierender der Uni Münster..."

"Diese E-Mail richtet sich an alle Mitarbeiter etc."

[TK2] "Rundmail der Verwaltung/Online-Redaktion" etc.

Keine unbekannten Personen