Die externe Kommunikation erfolgt in der Landesverwaltung zu großen Teilen durch das Versenden von E-Mails, z. B. über Microsoft Outlook. Der Datenverkehr per E-Mail ist ein neuralgischer Punkt für Angriffe von außen.

Befall mit Schadsoftware

Durch E-Mails mit Schadsoftware wird versucht, Ihr dienstliches IT-System zu infizieren. Dies wird üblicherweise mithilfe von dubiosen Links und Dateianhängen versucht. Datenverlust und ggf. eine Beeinträchtigung des Dienstbetriebs sind mögliche Folgen.

Falsche (Versand-)Adressen

Beim Versand von dienstlichen Daten per Mail kann die Vertraulichkeit bedroht werden, wenn man falsch adressiert oder nicht geschützte Dokumente verschickt.

Täuschung durch falschen Absender

Es kommt vor, dass der Name des Absenders einer E-Mail nicht mit der Mailadresse des Absenders übereinstimmt. Betrügerische Mails nutzen das oft bewusst, um dem Empfänger eine falsche Identität des Absenders anzuzeigen. Genauso kann es passieren, dass eine Link-Adresse nicht der angezeigten Bezeichnung dieses Links entspricht.

Fehlerhafte Makroprogrammierung und Missbrauch selbst programmierter Makros

Durch infizierte Makros kann die Sicherheit in Microsoft Outlook nachhaltig gestört werden, es droht automatisierter Datenabfluss.

Unbeabsichtigte Verifizierung der Mailadresse durch aktivierte Abwesenheitsmeldung

Wenn der Abwesenheitsagent für alle eingehenden Mails aktiviert ist, kann Ihre dienstliche Mailadresse durch Spammails verifiziert werden.

www.thueringen.de

digitale Services
verwaltung.thueringen.de

Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, © Jakub Krechowicz (Titel), ©vegefox.com (innen oben), ©4zevar (innen Laptop Grafik)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Kommunikation per E-Mail

Wie man Risiken in der elektronischen Kommunikation vermeidet

Informationssicherheit

Ihr Outlook-Account ist ein dienstliches Werkzeug, das Sie mit Sorgfalt verwenden und schützen müssen. Unachtsamkeit oder Bequemlichkeit kann schwerwiegende Folgen für die Sicherheit der Landesverwaltung haben.

Im Zweifel Sicherheit zuerst

Wenn Ihnen eine E-Mail verdächtig vorkommt, dann nichts herunterladen, keinen Link betätigen, keinen Anhang öffnen, nicht weiterleiten. Von Ihnen als Spam oder Phishing identifizierte E-Mails sofort löschen. Bei Unklarheiten informieren Sie zuerst den IT-Sicherheitsbeauftragten.

Vertrauliches Verschlüsseln

Schützen Sie vertrauliche Inhalte vor dem Versenden. Nutzen Sie dazu unter anderem die Möglichkeiten bei Office-Produkten, den Zugriff auf Dokumente mit einem Passwort zu schützen. Übermitteln Sie das Passwort möglichst auf einem anderen Wege (z. B. per Telefon), aber mindestens zeitversetzt in einer anderen Mail.

Abwesenheitsmeldung richtig einstellen

Legen Sie beim Aktivieren der Abwesenheitsinformation fest, dass nur Absender innerhalb der Landesverwaltung informiert werden. Senden Sie keine Abwesenheitsmitteilungen an Externe.

Keine Autovorschau oder Vorschaufenster nutzen

Prüfen Sie, ob Ihre Mails voreingestellt als Text und nicht im HTML-Format angezeigt werden können. Die Deaktivierung der E-Mail-Vorschau erhöht die Sicherheit wesentlich, weil dadurch keine aktiven Inhalte ausgeführt werden können. Bei Fragen wenden Sie sich bitte an Ihren Administrator.

Niemals selbstprogrammierte Makros einsetzen

Nutzen Sie im Bereich der Mailkommunikation ausschließlich vorinstallierte oder dienstlich bereitgestellte Makros.

Double Check bei der Adresse

Überprüfen Sie vor dem Versenden vertraulicher Daten noch einmal die Mailadresse. Achten Sie darauf, dass es sich um die richtige Person handelt, damit Sie nicht einen anderen Empfänger mit demselben oder einem ähnlichen Namen anschreiben.

Keine privaten Mails in dienstlichen Mailkonten

Private Mails, die Sie an Ihren dienstlichen Account weiterleiten, könnten mit Schadsoftware infiziert sein und Ihr Outlook-Konto befallen.

Keine Weiterleitung dienstlicher Informationen in den privaten Bereich

Das Weiterleiten dienstlicher Informationen in den privaten Bereich stellt eine Dienstpflichtverletzung dar, da Sie dadurch Daten und Informationen dem Zugriff der Behörde entziehen.

Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:	
Dienststelle:	
Telefon:	
E-Mail:	