16.09.2025

Wie gefährlich sind E-Mail, SMS, WhatsApp & Co.?

Die verschiedenen heute gebräuchlichen Nachrichten-Anwendungen bringen unterschiedliche Gefahren mit sich. Diese zu kennen ermöglicht eine sichere Nutzung.

Die elektronische Post, kurz E-Mail, gehört zu den meistgenutzten Nachrichtendiensten schlechthin. «Mails» können nebst Text verschiedene Inhalte wie Bilder, Webseiten- und Multimedia-Elemente sowie Dateianhänge enthalten. Zudem kann der Absender bestimmte Metadaten hinterlegen, etwa seine Absenderadresse, eine Betreffzeile, die Dringlichkeit oder eine Lesebestätigung.

Dementsprechend bergen E-Mails verschiedene Gefahrenquellen. Das grösste Risiko geht von angehängten Dateien aus, den sogenannten Attachments. Da einer Mail grundsätzlich beliebige Dateien beigefügt werden können, lassen sich auf diese Weise auch schädliche Inhalte mitschleusen, etwa Malware oder Microsoft-Dokumente (Word, Excel etc.) mit gefährlichen Makros.

Ähnliches gilt für Links in E-Mails. Diese können auf eine Phishing-Website oder eine mit Malware verseuchte Seite führen. Auch die Absenderadresse (Feld «From» bzw. «Von») von E-Mails kann gefälscht werden, sodass die Nachricht von einer vertrauten Person oder Institution zu kommen scheint. **Links, Anhänge und Absender sollten daher mit grosser Vorsicht behandelt werden.** Als weitestgehend gefahrenfrei wird heute dagegen der eigentliche Textinhalt (Body) von E-Mails angesehen.

Bei Messenger-Diensten wie WhatsApp, Telegram oder Facebook Messenger handelt es sich meist um proprietäre Anwendungen des jeweiligen Herstellers, die entsprechend ganz unterschiedliche Sicherheitsstandards verfolgen. Eine generelle Risikoabschätzung ist daher nicht möglich. Da diese Apps verschiedene Inhalte wie Bilder, Videos, Links oder auch Dateianhänge zulassen, gelten grundsätzlich die gleichen Vorsichtsmassnahmen wie bei E-Mails.

Vergleichsweise harmlos erscheinen dagegen Short Message Service Nachrichten, kurz SMS. Da es sich dabei in Reinform nur um Textmeldungen handelt, lassen sich keine schädlichen Inhalte einschleusen. Links in SMS können aber natürlich trotzdem auf eine schädliche Website führen. Doch Achtung: Hersteller-spezifische Formate wie iMessage von Apple oder Samsung Message können zusätzliche Inhalte enthalten, deren Gefahrenpotenzial schlecht abgeschätzt werden kann. Analog zur Absenderadresse von E-Mails lässt sich auch die Rufnummer einer SMS fälschen, sodass die Nachricht von einer bekannten Person oder Firma zu kommen scheint. Dies gilt übrigens auch für WhatsApp-Nachrichten.

Bei allen Nachrichten-Typen gilt: Bei Unsicherheiten keine Links oder Anhänge öffnen und nicht direkt auf die Nachricht antworten, sondern beim vermeintlichen Absender über einen anderen Kanal den Versand und Inhalt bestätigen lassen. Zum Beispiel telefonisch über die offizielle Rufnummer der Person, der Bank oder der betreffenden Firma.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik