CMS Info

Sicherheit in der IT: Vertrauen bei der E-Mail-Kommunikation

1. E-Mails prägen den beruflichen Alltag: Welche häufigen Bedrohungen gibt es?

Besonders häufig auftretende Bedrohungen sind: Spam, Scam und Phishing. Spam-E-Mails sind unerwünschte Nachrichten, oft mit dem Ziel, unnötige Werbung zu verbreiten. Scam-E-Mails verfolgen verschiedene betrügerische Absichten, wie z. B. falsche Rechnungen oder auch Erpressung. Phishing ist spezialisiert auf die Sammlung von sensiblen Daten, z. B. Benutzernamen, Passwörter bzw. Zugangsdaten. Alle drei Bedrohungen nutzen E-Mails, um als seriöser Absender wahrgenommen zu werden. Eine digitale E-Mail-Signatur stellt jedoch stets sicher, wer eine Nachricht tatsächlich geschrieben hat und dass der Inhalt unverändert ist. Zum Schutz gegenüber den genannten Bedrohungen rät der CMS deshalb zur Verwendung digitaler E-Mail-Signaturen bei der E-Mail-Kommunikation.

Weitere Infos zum Thema Phishing-Bedrohungen:
https://informationssicherheit.hu-berlin.de/de/Phishing
https://hu.berlin/phishing

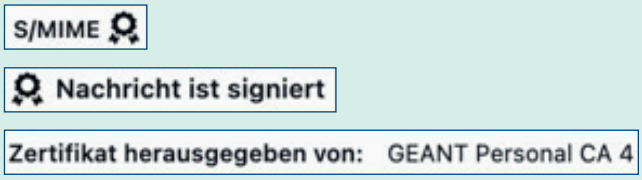
2. Was ist eine digitale E-Mail-Signatur?

Eine digitale E-Mail-Signatur ist ähnlich wie eine beglaubigte Unterschrift mit zusätzlichen Sicherheitsmerkmalen, die die Authentizität bestimmter Informationen offiziell bestätigt. Sie nutzt kryptographische Mechanismen, um die Identität des Absenders zu verifizieren und zu bestätigen, dass der Inhalt der Nachricht seit dem Versand unverändert ist. Die digitale E-Mail-Signatur stellt somit die Echtheit des Absenders sowie die Integrität des Inhalts einer E-Mail sicher.

3. Woran erkenne ich eine digital signierte E-Mail?

Die sichere Erkennung und Überprüfung digital signierter E-Mails sollte eine Routine sein. E-Mail-Clients kennzeichnen in der Regel signierte Nachrichten entsprechend, z. B. durch einen Hinweis „Sicherheit: Signiert (Max Mustermann)“.

Beispielhafte Kennzeichnung einer gültigen digitalen E-Mail-Signatur (Thunderbird):



Beispiele für ungültige digitale E-Mail-Signaturen sowie Praxistipps und Anleitungen:
https://hu.berlin/nutzerzertifikat-faq

4. Woher bekomme ich meine Zertifikatsdatei und wie mache ich das?

Sie können sich im Self-Service nach Anmeldung mit Ihrem HU-Account und Passwort ein Nutzer*innenzertifikat (Zertifikatsdatei) erstellen. Beachten Sie die Hinweise auf dem Antragsformular und die dortige Anleitung zum Download und zur Installation Ihrer Zertifikatsdatei. Ein weiterer Identifizierungsprozess ist nicht erforderlich.

Zum Self-Service:
https://hu.berlin/nutzerzertifikat (Antragsformular)

5. Wie funktioniert die Installation im E-Mail-Programm?

Sie müssen Ihr Zertifikat in allen E-Mail-Clients installieren, die Sie nutzen möchten. Es gibt Anleitungen für: Thunderbird, Outlook und Apple-Mail. Nach erfolgter Installation sowie Aktivierung sind zukünftig die eigenen E-Mails automatisch signiert und es ist kein weiterer Aufwand mehr notwendig.

https://hu.berlin/nutzerzertifikat-anwendungen

Fazit: Die Erstkonfiguration digitaler E-Mail-Signaturen ist unkompliziert und erhöht langfristig das Sicherheitsniveau der E-Mail-Kommunikation.

Stand: 20.2.2024

https://www.cms.hu-berlin.de