Trier University of Applied Sciences | HOCHSCHULE TRIER

Informationssicherheit

Um die Informationssicherheit in einer Organisation strukturiert zu implementieren, wird ein Informationssicherheitsmanagementsystem (ISMS) benötigt. Dabei handelt es sich nicht um ein „fertiges" System, dass sich automatisiert aktualisiert oder aufbaut, sondern um eine Systematik, wie die Informationssicherheit aufzubauen ist.

Ein ISMS regelt und verwaltet Planungs-, Lenkungs- und Kontrollaufgaben, die erforderlich sind, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen bzw. zu verbessern.

Fabian Amon
Informationssicherheitsbeauftragter (ISB)
der Hochschule Trier

Phishing-Angriffe (Ausgabe 02/25)

Eine vermeintliche E-Mail der Präsidentin, ein vermeintlicher Anruf eines Lieferanten… Oft erfolgt so die erste Kontaktaufnahme durch Angreifer. Via Social Engineering wird Vertrauen aufgebaut, um weitere Kontaktdaten zu sammeln und dann gezielt anzugreifen.

Phishing erkennen (E-Mail)>>>

Prüfen Sie bei jeder E-Mail, die Sie erhalten, zunächst die Absendeadresse. Interne E-Mail-Adressen beinhalten immer die Domäne (…)hochschule-trier.de oder umwelt-campus.de. **Beispiel:** Sie erhalten eine E-Mail mit folgender Absenderadresse: praesidentin@hotmail.com und dem Anzeigenamen der Präsidentin. Auffällig ist hier die Domäne: hotmail.com. Dies ist keine hochschulinterne Domäne, daher handelt es sich bei dieser E-Mail um eine Phishing-E-Mail. Achten Sie bitte darauf, dass es sich hierbei nur um ein Beispiel handelt und Domänen wie @gmail.com usw. auch möglich sind. Lassen Sie sich nicht von dem Anzeigename beirren. Auch wenn der Anzeigename einem Namen eines Hochschulmitarbeiters übereinstimmt, kann die Absende-E-Mailadresse dennoch hochschulfremd sein. Achten Sie bei externen E-Mail-Adressen auf E-Mail-Adresse, Betreff und Inhalt. Klicken Sie auf keinen Fall auf einen Link in einer E-Mail, die Ihnen verdächtig vorkommt. Bei Unsicherheiten können Sie sich jederzeit an die untenstehende E-Mail-Adresse wenden.

Phishing erkennen (Anruf)>>>

Phishing-Angriffe können sich nicht nur auf E-Mail beschränken, sondern sich auch per Telefon ausbreiten. Oft geben sich die anrufenden Personen als Lieferanten, Dienstleister o. Ä. aus. Diese haben meist das Anliegen, Bankverbindungen oder Adressen ändern zu lassen. WICHTIG! Geben Sie keine personenbezogenen Daten über das Telefon bekannt. Lassen Sie sich alle Änderungen der Bankverbindungen o. Ä. per E-Mail bestätigen. Überprüfen Sie die (beauftragten) Änderungen mit den vorhandenen Stammdaten und kontaktieren Sie den Lieferanten, Dienstleister o. Ä. und lassen Sie sich die Änderungen nochmals von diesen bestätigen. Verwenden Sie dazu bereits hinterlegten und verifizierte Kontaktdaten.

Die Absenderadresse muss @hochschule-trier.de oder @umwelt-campus.de beinhalten

Opfer eines Phishing-Angriffs >>>

Falls Sie Opfer eines Phishing-Angriffs sind, bewahren Sie Ruhe. Kontaktieren Sie umgehend ihre/n Vorgesetzte/n. Brechen Sie den Kontakt zum Angreifer sofort ab.

Bitte beachten Sie auch folgende Inhalte auf den Hochschulwebseiten:
E-Mail-Hygiene und Schutz vor Phishing-Mails

Notfallkontakt bei IT-Vorfällen

Bei **IT- bzw. Informationssicherheitsvorfällen** wenden Sie sich umgehend telefonisch an die: **-777** oder per E-Mail an: **informationssicherheit@hochschule-trier.de**