SMT
SICHERHEITSMANAGEMENT-TEAM

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Allgemeine IT-Sicherheitsmaßnahmen

Wie erstelle ich ein sicheres Passwort?

Ist mein PC ausreichend geschützt?

Was ist Malware?

Woran erkannt man sichere Webseiten?

Woran erkannt man eine Phishing-Mail?

Uploads vs. Datenschutz

IT-Sicherheitsmanagement-Team der Goethe-Universität

IMPRESSUM

IT-Sicherheitsmanagement-Team (SMT)

Goethe-Universität Frankfurt am Main

Theodor-W.-Adorno-Platz 1, PA-Gebäude

60323 Frankfurt am Main

smt@uni-frankfurt.de
https://www.uni-frankfurt.de/smt

Stand: März 2020

INHALT

DEFINITION UND ZIELE

Definition (IT-Sicherheit): Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen, Diensten und Systemen.

- Integrität: ist gewährleistet, wenn schützenswerte Daten unversehrt und vollständig bleiben.
- Vertraulichkeit: ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis nehmen können.
- Verfügbarkeit: bezieht sich auf Daten und Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.

Quelle: © ArtemSam / Fotolia.com

Ziel: „Ausreichende und angemessene IT-Sicherheit“ an der Goethe-Universität Frankfurt am Main.

ALLGEMEINE SICHERHEITSMASSNAHMEN

Quelle: © adempercem / Fotolia.com

Quelle: © thodonal / Fotolia.com

- Regelmäßige Aktualisierung des **Virenschutzprogramms:**
  - Das Hochschulrechenzentrum (HRZ) bietet allen Angehörigen der Goethe-Universität einen **kostenlosen Virenscanner** zum Herunterladen (**Sophos** für Windows und Mac OS X).
- Regelmäßige Installation sämtlicher verfügbarer **Sicherheitsupdates**:
  - **Betriebssysteme** (z. B. Microsoft, MAC OS/iOS, Android, usw.).
  - **Programme** (z. B. Internetbrowser, Office, Flash Player, Adobe Reader, usw.).
- Software und Programme sollen ausschließlich aus **vertrauenswürdigen Quellen** bezogen werden:
  - Webseiten der **Softwarehersteller.**
  - Oder www.heise.de.
  - Beim Installieren zusätzlich auf **versteckte** Softwarekomponenten achten (Toolbars, Adware usw.).
- Surfen am sichersten mit **verschlüsselter Verbindung** (https).
- Online-Shopping erfordert hohe Aufmerksamkeit:
  - Betrugsversuche kommen sehr häufig vor.

- Am sichersten zahlen Sie mit aufladbaren Kreditkarten.
- Achten Sie darauf, dass **Seiten** zum Online-Banking oder von Internetshops **verschlüsselt** sind.

Quelle: © ArtemSam / Fotolia.com

- Für den **Zugriff auf das Internet**:
  - Benutzerkonto mit eingeschränkten Rechten.
  - Keinesfalls ein Administrator-Konto!
  - Das gilt auch beim Abrufen und Lesen von E-Mails.

- Auf Gültigkeit bzw. auf Vertrauenswürdigkeit des **Zertifikats** achten:
  - Digitale Zertifikate bescheinigen die Vertrauenswürdigkeit von Kommunikationspartnern im Internet.

- Weitere Informationen finden Sie in der **Handlungsempfehlung „Nutzung von Internetdiensten“** auf der **Hompage des SMT**.

SICHERE PASSWÖRTER

Quelle: © Maksym Yemelyanov / Fotolia.com

- Nur sichere Passwörter verwenden:
  - Empfohlen wird eine Länge von **16 Zeichen** (mindestens 10 Zeichen sollten es aber auf jeden Fall sein).
  - Das Passwort sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.
  - **Nicht** aus Nutzerkontext oder Wörterbuch wählen.
  - **Keine alten Passwörter** verwenden.
  - Das Passwort sollte **geheim** gehalten und regelmäßig **geändert** werden.
  - **Dienstliche Passwörter** dürfen **nicht** bei externen Diensten verwendet werden.
  - Weitere Informationen finden Sie in der **Handlungsempfehlung „Umgang mit Passwörtern“** auf der **Hompage des SMT.**

DATENSICHERUNG

Quelle: © momius / Fotolia.com

- Benutzer*innen sollten ihre **wichtigen Daten** ausschließlich auf dem Home-Laufwerk bzw. auf den Gruppenlaufwerken (Netzwerklaufwerken) speichern (falls vorhanden).

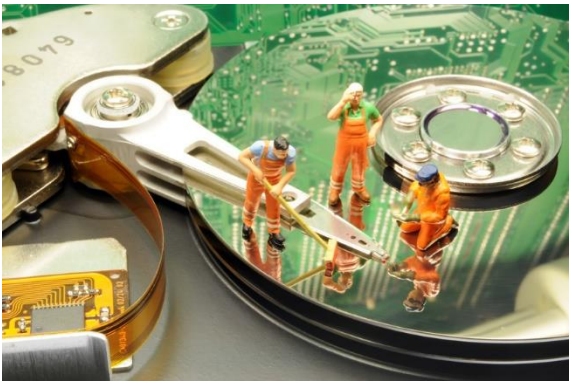
- Alle Daten auf den Fileservern des Hochschulrechenzentrums (HRZ) werden **täglich** durch den zentralen Backup-Service **gesichert.**

- **Regelmäßige Datensicherung** auf mindestens ein **externes Speichermedium** (empfohlen sind zwei Speichermedien), das nicht dauerhaft am PC angeschlossen ist.

- Bei **privaten Geräten** empfiehlt sich die Durchführung einer vollständigen Datensicherung.

- Bei der vollständigen Datensicherung werden neben Daten und Dokumenten Programme und das Betriebssystem gesichert.

SICHERES LÖSCHEN VON INFORMATIONEN



Quelle: © M. Johannsen / Fotolia.com

- **Gelöschte Daten** lassen sich meistens mit speziellen Tools **wiederherstellen**. Daher ist die Formatierung einer Festplatte oder eines Datenträgers als sicheres Löschverfahren ungeeignet.

- Bevor Sie Ihre Festplatten, USB-Sticks oder SD-Karten an **Dritte** oder zum **Elektroschrottrecycling** weitergeben, sollten Sie diese **löschen.** Alternativ sollten Sie sie vernichten.

- Mit spezieller **Software** lassen sich Daten auf Festplatten durch **Überschreiben** vollständig und nicht wiederherstellbar löschen.

- Wenn Sie eine Festplatte nicht überschreiben wollen oder wegen eines Defekts nicht können, so sollten Sie die Festplatte **physisch beschädigen oder zerstören**.

SICHERE NUTZUNG VON CLOUD-DIENSTEN

Quelle: © Vlad Kochelaevskiy / Fotolia.com

- Als Cloud-Dienst zur **Online-Speicherung von Dateien** wird u. a. die Sync-&-Share-Lösung **Hessenbox** (https://hessenbox.uni-frankfurt.de) empfohlen. Diese wird von der Goethe-Universität Frankfurt **betrieben und kostenlos angeboten**.
- Die Speicherung von **dienstlichen Informationen** mit personenbezogenen Daten auf externen Netzwerkspeicherlösungen (z. B. Apple iCloud, Amazon Drive, Microsoft OneDrive, DropBox) ist **untersagt!**
- Alternativen:
  - Home-Laufwerk bzw. Gruppenlaufwerke.
  - Netzwerkshare (z. B. Samba).
- **Private Daten** sollten auf externen Netzwerkspeicherlösungen verschlüsselt gespeichert werden.
- Weitere Informationen finden Sie in der **Handlungsempfehlung „Auslagerung von Daten in die Cloud“** auf der **Hompage des SMT**.

INFORMATIONSSICHERHEIT BEI MOBILEN GERÄTEN

Quelle: © Sergey Ilin / Fotolia.com

- Achten Sie beim Kauf von Geräten auf **Aktualität** des Betriebssystems sowie Verfügbarkeit von **Updates.**
- Das **Betriebssystem** und sämtliche installierte **Software und Apps** mit Sicherheitsupdates immer auf **dem neuesten Stand** halten.
- Der **Zugriff** auf mobile Geräte und deren Anwendungen muss durch **Schutzvorkehrungen** wie Passwort, PIN usw. **abgesichert** werden.
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen.
- Erstellen Sie regelmäßig Sicherungskopien.
- Aktivieren Sie **drahtlose Schnittstellen** nur bei Bedarf (wie z. B. GPS, Bluetooth, NFC, usw.).
- Weitere Informationen finden Sie in der **Handlungsempfehlung „Nutzung von mobilen Geräten“** auf der **Hompage des SMT.**

SICHERE NUTZUNG VON E-MAIL-DIENSTEN

- **Dienstliche E-Mail-Adressen** sollten **nicht** zur Nutzung **privater externer Dienstleistungen** (z. B. soziale Netzwerke, Online-Shopping usw.) verwendet werden.
- **Studierenden** wird aus Sicherheitsgründen empfohlen, die **Uni-Mail-Accounts** zur elektronischen Kommunikation mit Angehörigen der Universität zu verwenden.
- Verseuchte **E-Mail-Anhänge** und **Links** sind einer der häufigsten Wege, **Schadsoftware** in Computer einzuschleusen. Deshalb gilt stets erhöhte Aufmerksamkeit vor dem Klicken auf einen Link bzw. vor dem Öffnen eines Anhangs. Absender, Betreff und E-Mail-Text sollten stimmig und plausibel sein.
- **Bewerbungen** bzw. **Bewerbungsunterlagen** dürfen ausschließlich im **PDF-Format** eingereicht werden. Im Falle von Zip-Dateien oder Word-Dokumenten können Sie die Bewerber*innen dazu auffordern, Bewerbungen im PDF-Format noch einmal einzureichen.
- **Digitale Zertifikate** bescheinigen die **Vertrauenswürdigkeit** von Kommunikationspartner*innen. Achten Sie auf Gültigkeit und Vertrauenswürdigkeit des Zertifikats, wenn Sie eine signierte E-Mail erhalten.
- Weitere Informationen finden Sie in der **Handlungsempfehlung „Nutzung von E-Mail-Diensten“** auf der **Hompage des SMT**.

SOCIAL ENGINEERING

Bei Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Die Angreifer verleiten die Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

Schutzmaßnahmen gegen Social Engineering

Um das Risiko von Social-Engineering-Betrügereien zu mindern, sollten in jedem Fall die folgenden Grundregeln beachtet werden:

- Gehen Sie verantwortungsvoll mit **sozialen Netzwerken** um. Überlegen Sie genau, welche persönlichen Informationen Sie dort offenlegen, da diese von Kriminellen gesammelt und für Täuschungsversuche **missbraucht** werden können.
- Geben Sie in privaten und beruflichen sozialen Netzwerken keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis.
- Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen **niemals per Telefon oder E-Mail** mit. Banken und seriöse Firmen fordern ihre Kunden nie per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf.
- Lassen Sie bei E-Mails **von unbekannten** Absender*innen besondere Vorsicht walten.
- Sollte eine Reaktion zwingend erforderlich sein, **vergewissern Sie sich durch einen Anruf beim Absender oder der Absenderin,** dass es sich um eine legitime E-Mail handelt.

ARTEN DER SCHADSOFTWARE (MALWARE)

Quelle: © TAlex / Fotolia.com

- **Virus**
  - Löschen oder Beschädigung von Informationen, Daten und Systemen.
- **Trojaner**
  - Erpressung (Verschlüsselungs-Trojaner).
  - Spionage und Aufzeichnen (Tastatureingaben, Mikrofon, Webcam und Anmeldeinformation).
  - Missbrauch von Systemen und Geräten für illegale Aktivitäten.
- **Wurm**
  - Verbreitet sich extrem schnell im Netzwerk.
  - Ziel: Sicherheitslücken öffnen bzw. schaffen für andere Malwaresorten (Viren, Trojaner).

- **<u>Verbreitung der Schadsoftware erfolgt durch:</u>**
  - das Öffnen von verseuchten E-Mail-Anhängen.
  - Spam- und Phishing-Mails mit getarnten Links.
  - das Besuchen von kompromittierten Webseiten.
  - die Ausführung von infizierten Dateien/Downloads.

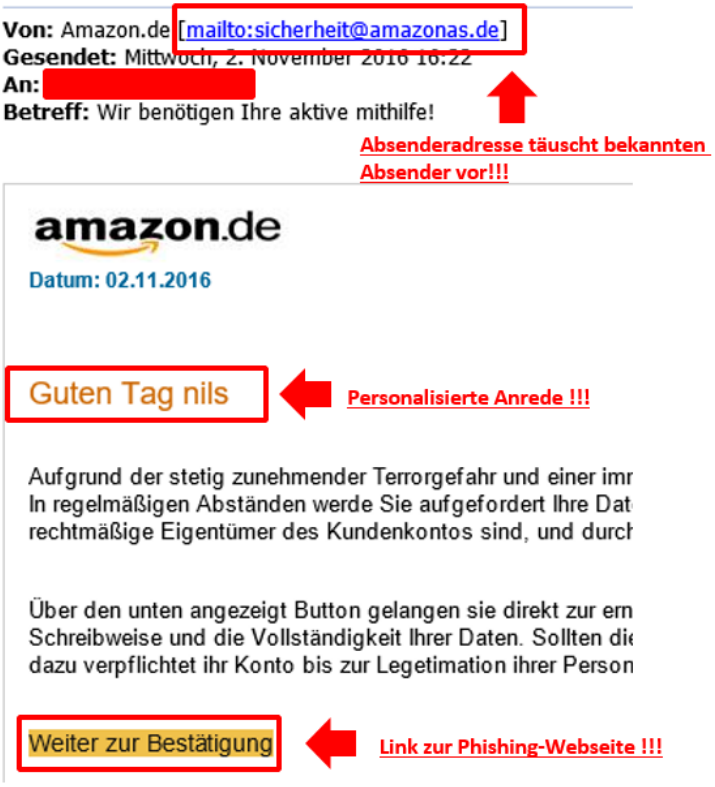
PHISHING- UND SPAM-MAILS

Quelle: © weerapat1003 / Fotolia.com

- Unerwünschte Mails, die Werbematerial und/oder Schadsoftware enthalten.
- **Woran erkennt man <u>Phishing- und SPAM-Mails</u>?**
  - Die Absenderadressen sind zumeist gefälscht.
  - Es wird nach vertraulichen Daten wie Passwörtern, PINs, Kontoverbindung gefragt.
  - Die E-Mails verwenden oft eine nichtpersonalisierte Anrede wie „Sehr geehrte Damen und Herren“ oder „Lieber Kunde der x-Bank!“. Zunehmend werden aber auch personalisierte Anreden verwendet.
  - Dringender Handlungsbedarf wird signalisiert wie „Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren…“.

- Unaufgefordert zugeschicktes Werbematerial.
- Die Nachrichten sind manchmal in schlechtem Deutsch verfasst (Schreibfehler!).
- Hinweise auf Änderung der Abrechnungssysteme oder Software-Updates bei Online-Kaufhäusern wie Amazon oder Ebay oder bei Banken.
- Die Mails enthalten Links oder Formulare, die vom Empfänger verfolgt beziehungsweise geöffnet werden sollen.

Phishing-Mail: Beispiel 1



Phishing-Mail: Beispiel 2

Antworten Allen antworten Weiterleiten

Do 01.11.2018 21:32

HRZ-Beratung <anna.maria.becker@fau.de>

[HRZ] Universität Postfach-Quota Überschritten!

An [redacted]

Bitte betrachten Sie diese Angelegenheit als Vertraulich.
Diese Nachricht wurde mit der Priorität "Hoch" gesendet.

Absenderadresse täuscht bekannten Absender vor!!!

Bitte löschen Sie ein beliebiges Element, das Sie nicht benötigen aus Ihrem Postfach und Entfernen der gelöschten Elemente oder starten Sie unten, um eine automatische Erhöhung Ihres Mailbox-Speichers zu ermöglichen.

http://hrz-frankfurt.ga/
Klicken oder tippen Sie, um dem Link zu folgen.

Ablegen

Link zur Phishing-Webseite !!!

Das Amt des Inforamtion Sicherheit halten dies aktualisiert, wenn Informationen ändern sollten, aber wir empfehlen allen Anwendern ihre Aktualisierungen nach der erwarteten Version dieses Patches ausgeführt.

Mit freundlichen Grüßen
Ihr HRZ Service Center Team

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

--
Goethe-Universität Frankfurt am Main.
Hochschulrechenzentrum (HRZ)

ERPRESSUNG PER E-MAIL

- **Merkmale von <u>Erpressungsmails</u>:**

  - Unbekannte Absender*innen behaupten unter anderem,
    - die Webcam des Empfängers oder der Empfängerin sei gehackt und man habe ihn oder sie bei „sexuellen Handlungen an sich selbst“ gefilmt.
    - sie hätten den Computer des Empfängers oder der Empfängerin mit einer Software infiziert, die pornografische Dateien gefunden habe und drohen damit, Freunde und Familienmitglieder darüber zu informieren.
  - Der Empfänger oder die Empfängerin soll eine gewisse Summe in Bitcoins überweisen oder das Video werde veröffentlicht.
  - Um den Druck zu erhöhen, können die Mails auch persönliche Daten wie Handynummer, Postanschrift oder Bankverbindung enthalten.

Beispiel: Erpressungsmail

Hallo!

Ich bin ein Hacker, der Zugriff auf Ihr Betriebssystem hat.
Ich habe auch vollen Zugriff auf Ihr Konto.
Ich beobachte dich jetzt seit ein paar Monaten.
Tatsache ist, dass Sie über eine nicht jugendfreie Website, die Sie besucht haben, mit Malware infiziert wurden.

Wenn Sie damit nicht vertraut sind, werde ich erklären.
Mit Trojan Virus kann ich auf einen Computer oder ein anderes Gerät uneingeschränkt zugreifen und diese steuern.
Das bedeutet, ich kann alles auf Ihrem Bildschirm sehen, die Kamera und das Mikrofon einschalten, aber Sie wissen nichts darüber.

Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre gesamte Korrespondenz.

Warum hat Ihr Antivirus keine Malware erkannt?
Antwort: Meine Malware verwendet den Treiber. Ich aktualisiere die Signaturen alle 4 Stunden, damit Ihr Antivirus-Programm nicht verwendet wird.

Ich habe ein Video gemacht, das zeigt, wie Sie sich in der linken Hälfte des Bildschirms zufrieden geben, und in der rechten Hälfte sehen Sie das Video, das Sie gesehen haben.
Mit einem Mausklick kann ich dieses Video an alle Ihre E-Mails und Kontakte in sozialen Netzwerken senden.
Ich kann auch den Zugriff auf Ihre gesamte E-Mail-Korrespondenz und die von Ihnen verwendeten Messenger veröffentlichen.

Aber keine Sorge, wir können dieses Datenschutzproblem auf verschiedene Weise beheben. Alles, was wir benötigen, ist eine Bitcoin-Zahlung von **£7,960.00 GBP**, was meines Erachtens angesichts der Umstände ein fairer Preis ist.

Die Bitcoin-Adresse für die Zahlung lautet: 1E3d8UbjCQ3z4DGX1PoYMCbDB1egsjTBDJ

BETRUGSMASCHEN PER E-MAIL

- **CEO-Fraud-Betrugsmasche**
  - Der CEO Fraud ist eine Betrugsmasche, bei der Unternehmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden.
  - Vorrangig werden Mitarbeitende aus der Buchhaltung oder dem Rechnungswesen adressiert, die berechtigt sind, Finanztransaktionen für das Unternehmen durchzuführen.
  - Diese Mitarbeiter*innen werden vermeintlich vom Vorstand, der oder dem Geschäftsführer*in oder einer sonstigen Führungskraft des eigenen Unternehmens per E-Mail angewiesen, eine größere Summe von einem Geschäftskonto auf ein fremdes Konto zu überweisen, oder den Code eines Zahlungsdienstes wie Google Pay Card zu versenden.
  - Dabei wird das Opfer oft unter Zeitdruck gesetzt und zur Verschwiegenheit angewiesen, da es sich vorgeblich um ein geheimes oder vertrauliches Projekt handelt.
  - Die Kontaktdaten der Zielpersonen und der vorgetäuschten Absender*innen werden häufig durch öffentlich verfügbare Informationen auf der Webseite des Unternehmens, in Online-Karriereportalen, in sozialen Netzwerken, in Handelsregistereinträgen oder auch durch direkte Anrufe im Unternehmen gewonnen.
  - Die Angreifer*innen nutzen diese Informationen, um den Inhalt der E-Mail sowie den Stil der Kommunikation im Unternehmen glaubwürdig nachzuahmen und den/die Empfänger*in dazu zu verleiten, die Geldbeträge zu überweisen.

ALLGEMEINE SCHUTZMASSNAHMEN

Quelle: © Kurt Kleemann / Fotolia.com

- Nicht automatisch auf die Links oder Dateianhänge klicken, die per E-Mail gesendet werden.
  - Immer zunächst nachdenken, ob Anhang und Inhalt plausibel sind.
  - Gegebenenfalls aktiv per Telefon bei der/dem angegebenen Absender*in nachfragen.
- Regelmäßige Datensicherung.
- Regelmäßige Aktualisierung:
  - des Virenschutzprogramms.
  - des Webbrowsers.
  - des Betriebssystems.
  - der installierten Software und Anwendungen.
- Immer mit Benutzerkonto arbeiten ohne Administratorrechte:
  - Administratorrechte sind nur für die Installation von Programmen notwendig.
- Die Firewall nie ausschalten.

Quelle: © Vlad Kochelaevskiy / Fotolia.com

- Nutzuen Sie eine Webcam- bzw. Kameraabdeckung.

- WLAN-Verbindungen sollten nicht bedenkenlos genutzt werden, da diese nicht immer eine sichere, verschlüsselte Verbindung zur Verfügung stellen. Gerade beim Umgang mit sensiblen Daten (z. B. Online-Banking, Shopping etc.) ist eine verschlüsselte Verbindung unerlässlich.

- Bei Verdacht auf Krypto-Trojaner, wenn z. B. Ihre Daten verschlüsselt werden oder eine Lösegeldforderung auf Ihrem Bildschirm angezeigt wird:

  - PC ausschalten und vom Netz trennen.
  - Den zuständigen Support informieren.
  - Bei Privatgeräten System neu installieren und die Sicherung aufspielen.

- Bei Fragen können Sie sich an Ihren zuständigen IT-Support bzw. Ihre IT-Sicherheitsbeauftragten wenden.

WICHTIGE LINKS UND QUELLEN

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - www.bsi.bund.de
  - www.bsi-fuer-buerger.de
- DFN Computer Emergency Response Team (DFN-CERT)
  - www.dfn-cert.de
- IT-Sicherheitsmanagement-Team (SMT)
  - www.smt.uni-frankfurt.de
  - smt@uni-frankfurt.de
    - Rechtliche und organisatorische Aspekte
- Goethe-Universität Computer Emergency Response Team (GU-CERT)
  - www.rz.uni-frankfurt.de/gu-cert
  - gu-cert@rz.uni-frankfurt.de
- Hochschulrechenzentrum (HRZ)
  - www.it-sicherheit.rz.uni-frankfurt.de
  - it-sicherheit@rz.uni-frankfurt.de
    - Technische Beratung
    - Meldung von IT-Sicherheitsvorfällen

ABKÜRZUNGEN

App: Application (Applikation, Anwendungssoftware)

BSI: Bundesamt für Sicherheit in der Informationstechnik

CEO: Chief Executive Officer (Geschäftsführer)

CERT: Computer Emergency Response Team

DFN: Deutsches Forschungsnetz

GPS: Global Positioning System

HRZ: Hochschulrechenzentrum

HTTPS: HyperText Transfer Protocol Secure
(Sicheres Hypertext-Übertragungsprotokoll)

IT: Information Technology (Informationstechnik)

NFC: Near Field Communication (Nahfeldkommunikation)

OS: Operating System (Betriebssystem)

PC: Personal Computer (Einzelplatzrechner)

PIN: Personal Identification Number (Persönliche Identifikationsnummer)

SD-Karte: Secure Digital Memory Card (Sichere Digitale Speicherkarte)

SMT: Security Management Team (Sicherheitsmanagement-Team)

USB: Universal Serial Bus (Serielles Bussystem)

VPN: Virtual Private Network (Virtuelles Privates Netzwerk)

WLAN: Wireless Local Area Network (Drahtloses Lokales Netzwerk)

IT-Sicherheitsmanagement-Team der Goethe-Universität

IMPRESSUM

IT-Sicherheitsmanagement-Team (SMT)

Goethe-Universität Frankfurt am Main

Theodor-W.-Adorno-Platz 1, PA-Gebäude

60323 Frankfurt am Main

smt@uni-frankfurt.de
https://www.uni-frankfurt.de/smt