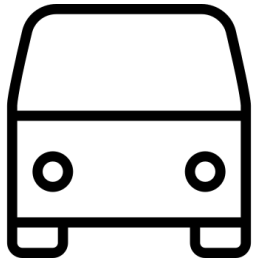
Technische Universität Braunschweig

Informationssicherheit im Homeoffice

Arne Windeler, 08.11.2024

Datenschutz auf dem Weg zwischen Dienststelle und Heimarbeitsplatz



- Ein abschließbarer Transport ist aus IT-Sicherheits- sowie Datenschutzgründen zwingend erforderlich

- Die Aktentasche sollte einen verdeckten Anhänger haben, um im Falle des Verlustes die Unterlagen nicht einsehen zu müssen.

- Lassen Sie die Akten und den Rechner nie aus den Augen

Datenschutz Zuhause

- Papierakten, Unterlagen und Datenträger nur im verschlossenen Rollcontainer, Schrank, Sideboard etc. lagern
- Keine Unterlagen in Hausmüll entsorgen

- Keine mobilen Datenträger
- Dienstliches Endgerät sollten nur mit verschlüsseltem Datenträger betrieben werden
- Führen Sie regelmäßig eine Datensicherung durch, Z.B. durch einen automatischen Backup.
- Arbeitsdaten nur auf Netzlaufwerk oder in TU-Cloud speichern

Schutz vor Zugang von Dritten

- Stellen Sie sicher, dass kein Unbefugter Zugang zum geöffneten Bildschirm hat.
- Bildschirme sollten mit Blickschutzfolie ausgestattet sein
- Aktivieren Sie den Bildschirmschoner wenn sie den Arbeitsplatz verlassen und andere Mitmenschen sich im Umfeld bewegen (Tasten: Windows + L).

- Telefongespräche oder Videokonferenzen sollten nicht von Dritten mitgehört werden können
- Erstellen Sie sichere Kennworte - mindestens 12 Zeichen- mit einer Kombination aus Groß- und Kleinschreibung, Sonderzeichen und Zahlen.

Meldeweg bei Sicherheits-/ Datenschutzverstoß

- Informieren Sie sich über den Meldeweg, für den Fall, dass sich ein Sicherheits-/ Datenschutzverstoß ereignet.

- Legen Sie Wert darauf, dass alle Verstöße unverzüglich gemeldet werden.

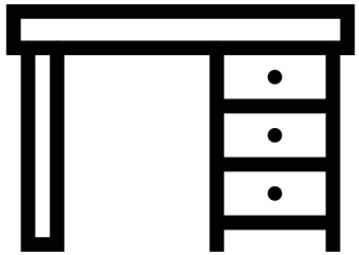
- Ob es sich dabei dann um einen Meldepflichtigen Verstoß nach Art. 33, 34 DSGVO handelt, können Sie gemeinsam mit Ihrem administrativen Datenschutz und Ihrem/Ihrer Datenschutzbeauftragten bewerten.

- datenschutz@tu-braunschweig.de

- soc@tu-braunschweig.de

Privat vs. Dienstlich

- Trennen Sie die betrieblichen Unterlagen von den privaten Gegenständen und Ablagen.
- Nutzen Sie dienstliche Hardware nicht für private Zwecke.
- Private Hardware nicht für dienstliches



Geräte am Heimarbeitsplatz

- Wie wird gedruckt?
  - Wird eine Ferneinbindung des Bürodruckers mit VPN-Tunnel benötigt?
  - Hinweis: Alternative Lösungen sind nur in Form eines lokalen USB-Druckers denkbar und müssen im Einzelfall mit der Stabsstelle CISO geklärt werden.

- Soweit Sie am heimischen Arbeitsplatz einen Drucker betreiben, achten Sie darauf, keine unnötigen Ausdrucke zu erstellen.
  - Die Mehrfachhaltung der Daten bringt neue datenschutzrechtliche Probleme mit sich. Ausdrucke müssen sicher verwahrt und sicher entsorgt werden, wenn sie nicht mehr benötigt werden.

- Schalten Sie bei dienstlichen Gesprächen die »Smart-Home« Geräte ab.

Internet am Heimarbeitsplatz

- Internet Router muss aktuelle Sicherheitsupdates erhalten
  - Das beinhaltet, dass sichergestellt werden muss, dass nur Geräte verwendet werden, die überhaupt noch Sicherheitsupdates vom jeweiligen Hersteller erhalten.

- Besteht eine Kabelverbindung zum Router?

- Alternativ: Besteht eine verschlüsselte (WPA2, besser WPA3) W-LAN-Verbindung zum Router?

- Für die Internetverbindung muss ein VPN-Tunnel zur Universität aufgebaut werden und dabei „tunnel all traffic“ als Modus verwendet werden

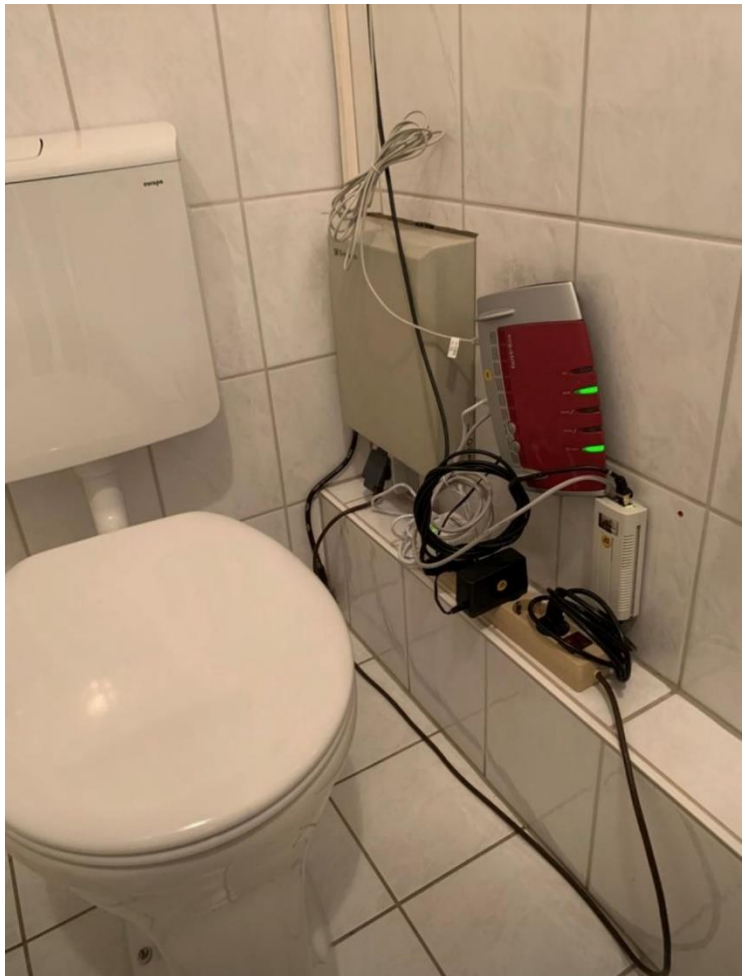
WLAN für alles und jede/n

Standardmäßig ”nur” ein (W)LAN.

- Alle Geräten können miteinander kommunizieren.
- Hängt hinter der Standard Firewall.

Sekundäres Netz

- Auf vielen WLAN Routern lassen sich *Gästenetze* einrichten
  - ➢ Trennung von Geräten.
  - ➢ Keine Kommunikation zwischen Geräten im Gästenetz erlaubt



Phishing

Di 09.07.2024 09:39

TU Braunschweig <admin@nicht-tu-bs.de>

Sie haben 1 Benachrichtigung von Ihrem Admin

An Mitarbeiter TU Braunschweig

Technische Universität Braunschweig

Sehr geehrter Nutzer,

Wir schließen alle alten Versionen Ihres E-Mail Kontos ab dem 09. Juli 2024.

Bitte Folgen Sie dem Link unten, um Ihr Konto zu aktualisieren.

Klicken Sie hier: Neue Version!

http://fake-website.nicht-tu-bs.de/
Klicken oder tippen Sie, um dem Link zu folgen.

Danke.

Die an diese Adresse gesendete Nachricht kann nicht beantwortet werden.

Technische Universität Braunschweig ©2024 Alle Rechte vorbehalten

Achten Sie besonders auf die Mailadresse

Häufig keine direkte Anrede aber teilweise legitime Signatur

Es wird häufig Zeitdruck erzeugt

Aufforderung Daten einzugeben oder sich anzumelden

Überprüfen Sie die Zieladresse des Links in der E-Mail

Angriffsszenarien

Wie kann es zu einem Informationssicherheits-Ereignis/-vorfall kommen?

Angriffsszenarien

Bedrohung	Schwachstelle
Diebstahl von Hardware der Hochschule	Unangemessen Aufbewahrung der Hardware
	Der Arbeitsplatz ist für Dritte frei zugänglich
Offenbarung personenbezogener Daten	Informationen sind für Dritte einsehbar
	Unverschlüsselte Speicherung personenbezogener Daten
Verlust personenbezogener Daten	Personenbezogene Daten werden nicht redundant gespeichert
Nicht-autorisierte Zugriff auf EDV	Nutzung schwacher Passwörter
	Kompromittieren von Passwörtern
	Benutzung eines Rechners durch mehrere Personen

Angriffsszenarien

Bedrohung	Schwachstelle
„Abhorchen“ von personenbezogenen Daten bei der Übermittlung	Nutzung öffentlicher Netze mit unverschlüsselter Leitung
Malware	Infizierte Software
	Veraltete Hardware oder Software
	Update oder Patch wurde nicht installiert
Ausfall der Infrastruktur	Einsatz eines einzigen Service-Providers
Falsche Nutzung der Dienste der Hochschule	Mangelhafte Regulierung
Aushorchen der Mitarbeitenden	Social Engineering

Quiz

Finden Sie die Fehler

Finden Sie die möglichen Gefahren auf diesem Bild!

Lösung 1/2

Telefon:

- Sensible Informationen sollten niemals laut ausgesprochen werden, wenn sich andere in der Nähe befinden. Besprich solche Themen, wenn andere nicht zuhören können, oder ergreife geeignete Maßnahmen, um nur begrenzte Informationen weiterzugeben.

Bildschirm:

- Wenn sensible Informationen auf dem Bildschirm deines PCs gut sichtbar sind, können unbefugte Personen auf diese Daten zugreifen. Achte darauf, wer um dich herum ist, und sperre deinen Computer immer, wenn du deinen Schreibtisch verlässt, indem du die Tasten Strg+Alt+Entf drückst.

Notizen:

- Notizen mit Daten auf dem Schreibtisch zu belassen, ist riskant, da die Informationen in die falschen Hände geraten könnten. Sei daher vorsichtig, welche Art von Informationen du auf Papier notierst. Wenn es notwendig ist, schriftliche Notizen aufzubewahren, wähle einen sicheren Ort. Schreibe auch keine Passwörter auf Notizzettel.

Lösung 2/2

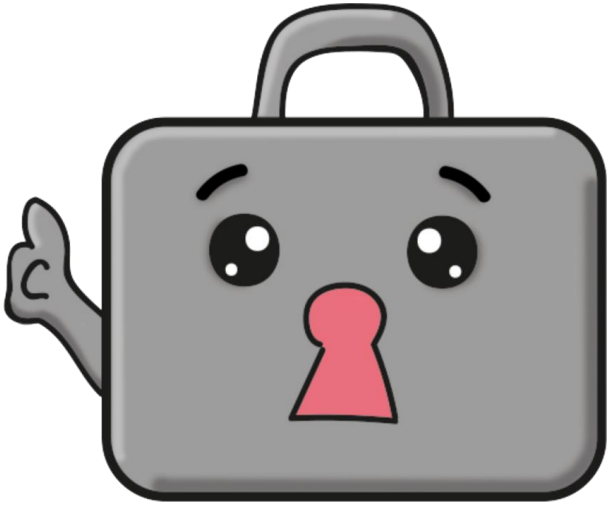
Mülleimer:

- Wenn sensible Informationen entsorgt werden, ist ein unsicherer Papierkorb nicht der richtige Ort und kann für ein Unternehmen ein erhebliches Risiko bedeuten. Eine Entsorgung muss auf sichere Art und Weise entsprechend den Unternehmensrichtlinien erfolgen.

Dokumente:

- Sensible Informationen auf dem Schreibtisch zu belassen, kann für die Daten eine Gefahr darstellen. Sperre solche Dokumente weg, wenn du vom Schreibtisch weggehst.

Vielen Dank für Ihre Aufmerksamkeit



Fragen, Wünsche, Anregungen
können Sie jetzt mit uns teilen
oder schreiben Sie an:
informationssicherheit@tu-braunschweig.de