Mit der zunehmenden Digitalisierung steigt das Bedrohungspotenzial durch Cyberattacken deutlich an.
Der erfolgreiche Umgang mit diesen Risiken erfordert ein Bewusstsein für Cybersicherheit sowie Kenntnisse im Management effektiver Schutzmaßnahmen.

DEFINITION DER CYBERSICHERHEIT

Cybersicherheit bezieht sich auf eine Reihe von Technologien, Prozessen und Praktiken, die Netzwerke, Geräte, Programme und Daten vor Angriffen, Beschädigungen oder unbefugtem Zugriff schützen sollen. Cybersicherheit kann auch als Informationstechnologiesicherheit bezeichnet werden.

So schützen sie Ihre Daten

-  ***Software Updates***

  Sollte man immer machen, wenn sie angeboten werden
  In den Einstellungen der Geräte, wie z.B. Smartphone, Tablet oder Notebook hinterlegen das die Updates immer automatisch installiert werden.

-  ***Virenschutz aktualisieren***

  Der Virenschutz auf Computer, Tablet etc. sollte sich immer auf einem aktuellen Stand befinden.
  Somit ist die Wahrscheinlichkeit auch neuere Varianten von Schadprogrammen aufzudecken gegeben.

-  ***Apps, Programme installieren***

  nur aus seriösen Quellen installieren.
  Zum Beispiel die Website des Herstellers bzw. beim Smartphone
  aus dem aktuellen App-Store.

-  ***Daten verschlüsseln***

  besonders sensible Daten sollten verschlüsselt werden:
  Dafür gibt es Apps oder Programme. Manche Geräte (z.B. Smartphones) sind schon ab Werk mit einer solchen Funktion ausgestattet.

-  ***Datenschutzvorkehrungen***

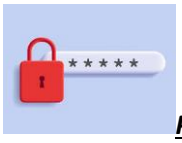
  Datenschutz bei tragbaren Geräten immer mal wieder prüfen
  Es kann bei Updates Änderungen bei den Zugriffsrechten auf Daten eines gekoppelten Gerätes wie z.B. einer Fitnessuhr kommen.

-  ***Bildschirmsperre einrichten***

  Die Freigabe des Smartphones o.a. Geräten ist so erst nach der Eingabe einer Tastenkombination, dem persönlichen Fingerabdruck oder die Gesichtserkennung möglich.

-  ***WLAN – Bluetooth***

  WLAN bzw. Bluetooth werden meist nur vorübergehend gebraucht, von daher sollte die Funktion bei nicht Nutzung deaktiviert werden, was recht einfach über die Einstellung der Geräte zu bewerkstelligen ist.

-  ***Password***

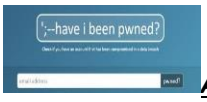
  Man sollte immer ein starkes Passwort benutzen. Hierfür kann man auf dem Handy oder PC einen Passwortmanager nutzen.
  Zudem sollten Passwörter möglichst nur einmal vergeben werden.

-  ***Zwei-Faktor Authentifizierung***

  Hiermit bestätigt man seine Identität über zwei verschiedene Quellen.
  Das heißt z.B. über den PC und das Smartphone.
  Erst dann wird der Zugriff auf ihre Daten gewährt.

-  ***Regelmäßiges Backup***

  Die Daten auf digitalen Geräten sollten regelmäßig gesichert werden.
  Im Ernstfall kann man dann immer auf eine Kopie zurückgreifen und schützt sich somit vor kompletten Datenverlust.

- 

Auf Datenlecks prüfen

Sie sollten regelmäßig z.B. ihre E-Mail-Adresse (n) dahingehend untersuchen ob Sie Opfer eines Datenlecks geworden sind:
Das geht u.a. sehr gut auf den Seiten:
https://haveibeenpwned.com
oder
https://sec.hpi.de/ilc.