MOBILE ENDGERÄTE RICHTIG SCHÜTZEN

Bei Cybersicherheit denkt man oft nur an den Schutz der Informationen, die auf einem Computer oder Server gespeichert sind. Doch auch bei Smartphones und Tabletts wird es zunehmend wichtiger Vorkehrungen zu treffen, um den Schutz der Daten zu gewährleisten.

? FRAGE

! ERKLÄRUNG

Sind Ihre mobilen Endgeräte mit Sperrcodes und Passwörtern ausgestattet?

Ob Code-Sperre, Passwort-Sperre, Muster-Sperre, Fingerabdrucksensor oder Gesichtserkennung: Es gibt eine Vielzahl an Möglichkeiten, um Unbefugten den Zugang zu mobilen Geräten zu versperren und somit auch den Zugang zu Ihren Daten.

- Passwörter bieten den besten Schutz für Geräte. Sie sollten lang und einzigartig sein und Buchstaben, Groß- und Kleinschreibung, Zahlen und Sonderzeichen beinhalten.
- Allgemein gilt: Je länger die Code-, Muster- oder Passwortkombination, desto besser.
- Um Geräte optimal zu schützen, kann eine Kombination der oben genannten Entsperrungsmethoden genutzt werden.
  - Aktivieren Sie den PIN Ihrer SIM-Karte.
  - Richten Sie auf all Ihren mobilen Endgeräten Bildschirmsperren ein.
  - Schützen Sie sensible Anwendungen mit einem PIN oder Passwort.
  - Benutzen Sie einen Passwort-Manager, um komplexe Passwörter zu generieren und diese sicher zu verwalten.

Sind alle Ihre Geräte mit einem Basisschutz versehen?

Alle mobilen Endgeräte benötigen einen zuverlässigen Basisschutz:

- **Antivirus-Apps** durchleuchten die Daten und Anwendungen auf den Geräten und suchen nach Schadsoftware.
- **Echtzeitvirenschutz-Apps** erkennen Viren in Echtzeit und leiten sofortige Gegenmaßnahmen ein.
- **Firewall-Apps** überwachen die Netzwerkaktivitäten aller Anwendungen und können bei Bedarf Verbindungen unterbinden. Somit erhält der Nutzer die Kontrolle über den Datenfluss seines Endgerätes.

Auch diese Anwendungen müssen regelmäßig aktualisiert werden, um den Schutz zu gewährleisten.

Benötigen Sie alle Applikationen, die auf Ihren Geräten installiert sind?

Alle Applikationen, egal ob Social Media, Wetter, Messenger oder sonstige, sind an Ihren Daten interessiert und sammeln diese.

- Löschen Sie alle Applikationen, die Sie nicht mehr benötigen oder benutzen.

Auf welche Informationen haben Ihre Apps Zugriff?

- **Vor dem Kauf:**
  - Informieren Sie sich bereits im App-Store, noch vor dem Herunterladen, über die Anwendungen. Viele Apps sind Datenfresser.
  - Lesen Sie die Nutzerbedingungen, um herauszufinden, auf welche Funktionen des Smartphones oder Tablets (Kamera, Mikrofon, Ortungsdienste, Kontakte, etc.) die Anwendung zugreift und welche persönlichen Daten sie speichert und teilt.
- **Nach dem Kauf:**
  - Kontrollieren Sie die Zugriffsrechte der Anwendung und schalten Sie alle Funktionen, die nicht benötigt werden, ab.
  - Überprüfen Sie regelmäßig die Zugriffsrechte der Anwendungen, denn bei jedem Update können sich diese ändern oder erweitern.
  - Nutzen Sie kein bestehendes Konto aus sozialen Netzwerken, um sich anzumelden. Wenn Apps mit Social Media-Konten verknüpft werden, können diese Daten austauschen.

Auch Webbrowser greifen auf Ihre Daten zu und werten diese aus. Nutzen Sie einen Webbrowser, der Wert auf Ihre Privatsphäre legt und Ihre persönlichen Daten nicht sammelt.

FRAGE

ERKLÄRUNG

Aktualisieren Sie regelmäßig die Betriebssysteme und Apps Ihrer mobilen Endgeräte?

Bei Betriebssystemen und Apps tauchen ständig neue Schwachstellen auf, die eine Gefahr für die Datensicherheit darstellen können. Die Herausgeber versuchen, diese Sicherheitslücken durch die Veröffentlichung neuer Versionen zu schließen.

- Aktualisieren Sie Ihre Betriebssysteme und Applikationen, sobald ein Update verfügbar ist.

Haben Sie Schnittstellen aktiviert?

Drahtlosschnittstellen wie Bluetooth, WLAN oder NFC können Schwachstellen darstellen und Cyberkriminellen ermöglichen, Datenübertragungen mitzulesen. Deswegen sollten sie bei Nichtnutzung deaktiviert werden.

- Öffentliche WLANs stellen eine Sicherheitslücke für Geräte dar:
  - Nutzen Sie ein virtuelles privates Netzwerk (VPN), um den Schutz der Daten zu steigern.
  - Informieren Sie sich bei Gratisversionen von VPNs, inwiefern die Daten verschlüsselt übertragen werden.
- Wenn Sie Ihr mobiles Endgerät nutzen, um einen eigenen Hotspot einzurichten:
  - Sichern Sie diesen mit guten Passwörtern ab.
  - Filtern Sie den Zugang einzelner Geräte.
  - Bestätigen Sie Geräte beim ersten Kontakt.
  - Schalten Sie den Hotspot nach der Nutzung wieder ab.

Hardwareschnittstellen (z.B. USB-Verbindungen)

- Benutzen Sie diese nur, wenn Sie deren Besitzer vertrauen.
- Legen Sie in den Einstellungen der mobilen Geräte fest, ob beim Anschließen per USB eine Datenübertragung erfolgt oder das Gerät nur aufgeladen werden soll.
- Nutzen Sie zum Aufladen möglichst nur das mit dem Gerät gelieferte Netzteil.

Sind Ihre Daten geschützt?

Das Backup

- Speichern Sie eine Kopie der Daten, um deren Verlust zu verhindern. Hierfür bieten sich Cloud-Lösungen oder USB-Speicher an.
- Speichern Sie möglichst wenig Daten auf den Geräten.

Die SD-Karte

- Bei modernen Smartphones ist die Verschlüsselung des internen Speichers in der Regel voreingestellt. Daten, die auf einer SD-Karte gespeichert sind, sind jedoch meist nicht durch die Speicherverschlüsselung des Geräts geschützt.
- Formatieren Sie die SD-Karte als „intern", damit sie nicht außerhalb des mobilen Endgerätes lesbar ist und die Daten verschlüsselt sind.

Sind Ihre Mitarbeiter für die sichere Nutzung der mobilen Endgeräte sensibilisiert?

Kennen Ihre Mitarbeiter die Sicherheitsrisiken und Tricks von Cyberkriminellen? Informieren Sie sie über die häufigsten Gefahren und sensibilisieren Sie sie, kritisch zu bleiben, wenn per E-Mail, SMS oder Anruf persönliche Daten (Passwörter, Berechtigungen, Kontonummern, etc.) abgefragt werden.

Wissen Sie, was bei Verlust des mobilen Endgerätes zu tun ist?

- Legen Sie schon im Vorfeld fest, welche Anwendungen gesperrt und welche Konten deaktiviert werden müssen. Machen Sie sich eine Liste der installierten Anwendungen und notieren Sie sich Notfallnummern.
- Stellen Sie sicher, dass Sie verlorene oder gestohlene Geräte aus der Ferne sperren können. Hierfür gibt es beispielsweise Apps, die es Ihnen ermöglichen, per Textnachricht einen Code an das Gerät zu schicken, um Ortungsdienste einzuschalten, Daten zu verschlüsseln oder zu löschen. Achten Sie bei der Auswahl einer App darauf, dass der Anbieter vertrauenswürdig ist.
- Notieren Sie sich die IMEI-Nummer (Seriennummer) des Gerätes. Sie gilt als Eigentumsbeweis im Falle eines Diebstahls und kann unter bestimmten Bedingungen genutzt werden, um das Gerät zu orten.
- Nachdem Sie die Daten Ihres Gerätes gesperrt haben, sollten Sie auch die SIM-Karte beim Anbieter sperren lassen.

Allgemeine Richtlinien:

- Geben Sie Ihren mobilen Endgeräten nur Zugriff auf die Firmendaten, die Sie zur Arbeit benötigen.
- Geben Sie Ihre Geräte nie aus der Hand. Mobile Geräte sind persönliche Gegenstände und sollten nicht an Fremde übergeben werden, auch nicht für einen kurzen Anruf.
- Bereinigen Sie alle Speicher und setzen Sie das Gerät in den Werkszustand zurück, bevor Sie es verkaufen oder entsorgen. Vergessen Sie nicht, zusätzliche Speichermedien wie externe SD-Karten oder SIM-Karten zu entfernen.

CHAMBRE DES MÉTIERS
LUXEMBOURG

Haben Sie noch Fragen?
Möchten Sie weitere Informationen zu den bestehenden Angeboten erhalten?
Dann zögern Sie nicht, die Abteilung eHandwierk der Chambre des Métiers zu kontaktieren:
E-Mail: **ehandwierk@cdm.lu**
Tel.: **42 67 67 - 305 / 306**