HEUER
UNTERNEHMENSBERATUNG

Sicher durch die digitalen Lebenswelten

Impulsvortrag 6. Februar 2023, Klaudia Heuer

Unternehmerinnen-Stammtisch Osnabrück

Überblick digitale Lebenswelten

Online dabei sein und ins Netz starten

Online vernetzen und austauschen

Online einkaufen und bezahlen

Online sein in Haus und Freizeit

Online Reisen planen und vernetzt mobil sein

Überblick digitale Kompetenzen

Digitale Kompetenzen
 Sichere Interneteinstellungen - Zuhause und unterwegs - Browser sicher einrichten
 Geräte und Software sicher einrichten und pflegen - Software aktuell halten - Benutzerkonten sicher einrichten - Schutzprogramme nutzen - Software auswählen und sicher einrichten - Cloud-Nutzung abwägen - Das smarte Zuhause sicher einrichten
 Sichere Logins nutzen - Einrichtung sicherer Passwörter - Einrichtung eines Passwortmanagers - Zwei-Faktor-Authentisierung
 Daten schützen und sichern - Backup planen - Daten verschlüsseln - Datensparsamkeit

Digitale Kompetenzen
 Sicher digital kommunizieren - Nachrichten verschlüsseln - Kommunizieren über E-Mail - Kommunizieren über Messenger - Kommunizieren über soziale Netzwerke
 Sichere Transaktionen - Online-Banking - Online Geld bezahlen - Kontaktloses bezahlen
 Extra: Risiken verstehen - Schadprogramme - Onlinebetrug - Missbrauch von sensiblen Daten - Belästigung und Beleidigung

Sichere Interneteinstellungen – Zuhause und unterwegs

Router:

- Starkes Passwort
- Zweiter Faktor
- Firewall nutzen
- Daten verschlüsseln
- Updates installieren
- Offline sein

Unterwegs:

- Mit VPN einen Tunnel bauen
- Sichere Verbindung nutzen
- Offline sein

Sichere Interneteinstellungen – Browser sicher einrichten

Web-Browser:

- Stets die neueste Version eures Browsers verwenden
- Trennung von Browser und Passwortmanager
- Phishing- und Malware-Schutz aktivieren

Geräte und Software sicher einrichten und pflegen

Software aktuell halten

- Updates installieren
  - → Nicht nur Erweiterung der Funktion der Software.
  - → In den meisten Fällen werden dadurch auch Sicherheitslücken geschlossen.

Was ist beim Patch Management zu beachten?

- Überblick verschaffen
- Automatische Updates nutzen
- Eigenständige Updates regelmäßig durchführen
- Schwachstellen erkennen, z. B. über Newsletter „Sicher informiert“ des BSI

Geräte und Software sicher einrichten und pflegen

Software auswählen und sicher einrichten

- Notwendigkeit prüfen
- Ungenutztes löschen
- App-Berechtigungen hinterfragen
- Berechtigungen regelmäßig kontrollieren
- Side-Loading vermeiden

Geräte und Software sicher einrichten und pflegen

Cloud-Nutzung abwägen

- Weitergabe von Daten geklärt haben
- Rechtliche Bestimmungen berücksichtigen (Stichwort EU DSGVO)
- Cloud-Zugang sichern
  - Durch starkes Passwort und wenn möglich durch 2-Faktor-Authentisierung.
- Schützenswerte Daten verschlüsseln vor der Übertragung in die Cloud

Daten schützen und sichern – Backup planen

Warum?

- Schadsoftware hat alle Daten verschlüsselt
- Smartphone wurde gestohlen
- Laptop wurde beschädigt

NO BACKUP
NO MERCY

Fragestellungen:

- Welche Daten sollen gesichert werden?
- Wo sollen sie gesichert werden?
- Welcher Speicherplatz wird benötigt?
- Gibt es eine Software, die die Auswahl meiner Daten sichern kann?
- Wann und wie regelmäßig wird das Backup angelegt?
- Sind alle gewünschten Daten im Backup abgelegt?
- Lassen sie sich öffnen und prüfen?

Sicher digital kommunizieren – Per E-Mail

Risiko:

Weiterhin das Einfallstor Nummer eins bei Cyber-Sicherheitsvorfällen.

→ Drei-Punkte-Sicherheits-Check

- Ist die Absenderadresse bekannt? Ist der Betreff sinnvoll? Wird ein Anhang oder Link erwartet?
- Vorsicht: Absenderadressen können auch gefälscht werden!

Schutzmaßnahmen:

- Virenschutzprogramm aktivieren
- Text-Format nutzen
  - Im Quellcode von HTML-formatierten E-Mails kann auch ein schädlicher Code versteckt sein, der bereits beim Öffnen der Nachricht auf dem Computer ausgeführt wird.
- Inhalte verschlüsseln
- Digitale Unterschrift einsetzen

Extra: Risiken verstehen - Schadprogramme

„Infektionswege“:

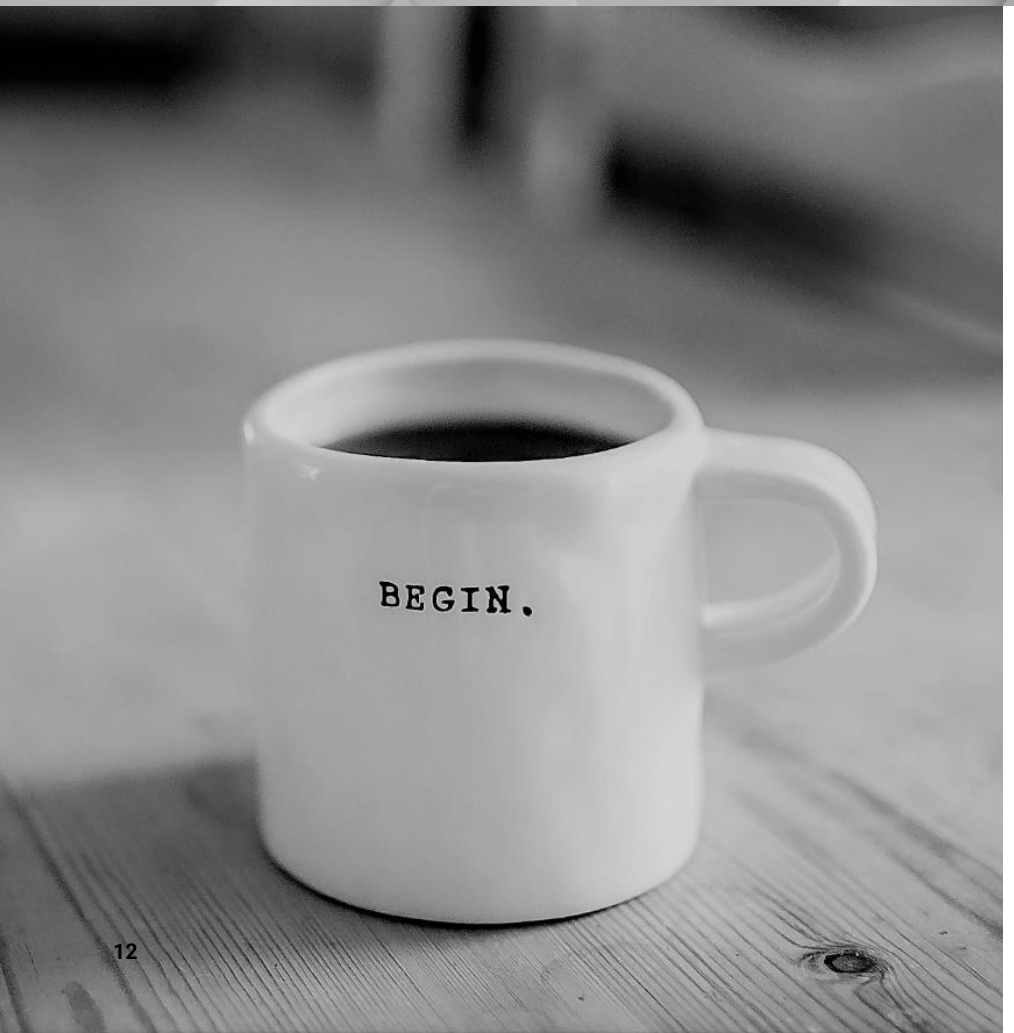
- E-Mail-Anhänge
- Software (Trojaner)
- Webseite

Häufigste Auswirkungen:

- Fernsteuerung, z.B. für den Aufbau eines Botnetzes
- Erpressung, sogenannte Ransomware, bei Unterbindung des Zugriffs auf Daten
- Ausspionieren von Daten
- Anzeige von Werbung

Schutzmaßnahmen:

- Führt regelmäßig Updates von Betriebssystemen und Programmen auf allen Geräten durch, um Sicherheitslücken zu schließen.
- Installiert ein Virenschutzprogramm und eine Firewall um Schadprogramme bereits beim ungewollten Download zu erkennen.
- Seid vorsichtig beim Öffnen von E-Mails.
- Nutzt nur vertrauenswürdige Quellen, um Daten herunterzuladen.
- Legt Backups wichtiger Daten an, um euch vor deren Verschlüsselung zu schützen und verlorene Daten selbst wiederherstellen zu können.



Fazit

- Cybersicherheit ist ein Thema das für uns alle als Gesellschaft auch in Zukunft an Relevanz gewinnen wird.
- Eine Auseinandersetzung damit hilft euch, euch sowohl als Privatperson als auch als Unternehmerinnen widerstandsfähiger aufzustellen und so die Vorteile der Digitalisierung sicher nutzen zu können.
- Meine Empfehlung:
  Richtet mindestens folgende Basis-Schutzmaßnahmen ein:
  - Spielt Updates regelmäßig ein
  - Führt regelmäßig Backups eurer Daten durch
  - Sorgt für eine sichere E-Mail-Nutzung
  - Und … seid auf den Fall der Fälle vorbereitet

Zum Nachlesen und weiteren Eintauchen ins Thema

Quellen:

- Cyberfibel – Digitale Lebenswelten
- Cyberfibel – Digitale Kompetenzen

https://www.cyberfibel.de/digitale-lebenswelten/

Sonstige weiterführende Informationen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

https://www.sicher-im-netz.de/

HEUER
UNTERNEHMENSBERATUNG

Ich arbeite als Botschafterin für eine sichere Digitalisierung.

Daher unterstütze ich euch sehr gerne dabei, im Bereich Cyber-Sicherheit euren Bedarf zu ermitteln und spezifische Kompetenzen zu entwickeln um dadurch euer Unternehmen besser zu schützen.

Ihr profitiert dabei von meiner über 13-jährigen Berufserfahrung mit kleinen, mittelständischen und großen Unternehmen in den Bereichen IT-Prüfung, IT-Beratung und Risikomanagement sowie von meinen Berufszertifizierungen.

Kontakt:
Klaudia Heuer
Mobil 0170 4847 506
kheuer@heuer-unternehmensberatung.de