LEITFADEN

ZUR CYBERSICHERHEIT IM UNTERNEHMEN

WELABS

Dank unserer Erfahrung bei der Umsetzung von Projekten, begleiten wir Euch gerne in der Thematik zur Cybersicherheit und stehen Euch zur Seite – hierfür haben wir einen kompakten Leitfaden zusammengetragen, der einige der wichtigsten Punkte auflistet:

Welche Maßnahmen sind bereits im Unternehmen umgesetzt worden oder geplant? Hierbei ist es wichtig, bereits die Basis wie z.B. aktive Firewalls & aktualisierte Antivirenprogramme etc. zu haben:

- Implementierung einer Firewall, um unautorisierten Zugriff zu blockieren
- Aktualisierung von Antivirensoftwares auf allen Endgeräten
- Aktualisierung der Betriebssysteme und Anwendungen auf allen Geräten
- Empfehlung von regelmäßigen Netzwerkscans und Überwachung auf Anomalien
    - Einsatz von Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS)
- Verschlüsselung für Daten & Dokumente

Umgang mit Externe Geräte, Verbindungen & Zugangskontrollen – Egal ob im Office, Hybrid oder Remote, es sollten Regelungen zur Nutzung und die Sicherheit erstellt werden:

- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
- Kontrolle und Überwachung von externen Geräten, die mit dem Unternehmensnetzwerk verbunden sind
    - Nutzung von Virtual-Personal-Network (VPN)
- Vermeidung von Verwendung persönlicher Endgeräte oder Zubehör z.B. USB-Sticks & externe Laufwerke

Richtlinien für Cybersicherheit aufsetzten - Dies bietet einen gut dokumentierten und strukturierte Prozess und erste Grundlage zur Sensibilisierung für das Thema:

- Einführung von Richtlinien für …
    - Passwörter
    - sicheren Umgang mit Unternehmensdaten

    - Nutzung von externen Geräten und öffentlichen Netzwerken
- Implementierung von Multi-Faktor-Authentifizierung (MFA)
- Festlegung von Verantwortlichkeiten und Kontakten für den Notfall.

Einführung einer Notfallplanung und Wiederherstellung – Die Technologie ist ständig im Wandel, und somit sind die damit verbundenen Gefahren. Es ist also wichtig im Falle eines Falles einen sicheren Plan aufzustellen:

- Regelmäßige Backups wichtiger Daten
- Erstellung eines umfassenden Notfallplans für Cyberangriffe
- Regelmäßige Überprüfung der Einhaltung von Sicherheitsstandards und Vorschriften
    - Ggf. Sicherheitsbeauftragen oder zuständiges Team aufstellen und schulen

Schulung und Sensibilisierung für alle anbieten – Es ist bedeutend, dass im Unternehmen in regelmäßigen Abständen das Thema behandelt wird, um potenzielle Gefahren und Wichtigkeit zu verdeutlichen:

- Schulungen für Mitarbeiter & Leads zum Thema Sicherheitsbewusstsein
- Testphasen für Phishing-Simulationen
- Regelmäßige Notfallübungen mit den Mitarbeitern durchführen
- Aktualisierung der Schulungen bei Einführung neuer Sicherheitsrichtlinien

Darf es ein wenig mehr sein?

Gerne beraten wir Euch bei weiteren Fragen zum Thema Cybersicherheit oder besucht unsere Webseite, um erste Eindrücke zu bekommen. Lass uns zusammen eine sichere digitale Reise starten und Deine Welt vor den unsichtbaren Bedrohungen schützen.