Cybersicherheit in Zeiten des Coronavirus

Die IT-Infrastruktur ist derzeit einer besonderen Belastung ausgesetzt. Überdies nutzen Cyberkriminelle die Krisensituation gezielt aus, um daraus Profit zu schlagen. Achten Sie gerade jetzt auf Cybersicherheit und informieren Sie Ihre MitarbeiterInnen über Gefahren!

Risiken

- Überlastung der privaten, unternehmensinternen und öffentlichen Infrastruktur
- Einsatz privater Hardware und Software mit geringeren Sicherheitsstandards für Unternehmenszwecke
- Phishing-Angriffe und Social Engineering
- Remote-Logins werden über Internet durch Bots attackiert

Maßnahmen

- ✓ **Virus-Schutz und Firewall**

Aktivieren bzw. installieren Sie Antiviren-Schutz und Firewall.

- ✓ **Geräteschutz**

Verwenden Sie Zugriffsbeschränkungen für Ihre Geräte. Sperren Sie Ihr Gerät in jedem Fall, wenn Sie Ihren Home-Office-Arbeitsplatz verlassen.

- ✓ **sichere Verbindungen**

Verwenden Sie idealerweise VPN-Dienste, um eine geschützte Verbindung zu Ihrem Firmennetzwerk von außen aufzubauen. Sorgen Sie dafür, dass WLAN oder LAN-Verbindungen entsprechend abgesichert sind (Routereinstellungen, Verschlüsselung mittels WPA2 oder WPA3).

- ✓ **aktuelle Software und Updates**

Installieren Sie Sicherheitsupdates bei Betriebssystemsoftware, wichtigen Programmen und Apps umgehend um Sicherheitslücken zu schließen.

- ✓ **Datensicherung**

Sichern Sie Ihre Daten regelmäßig auf einem geeigneten Medium (z.B. externe Festplatte, USB, Cloud). Ohne Backups können Sie wertvolle Daten verlieren und sind z.B. Angriffen durch Ransomware (Erpressertrojaner) schutzlos ausgeliefert.

- ✓ **sichere Passwörter**

Verwenden Sie ausreichend sichere Passwörter.

Nützen Sie für jeden Zugang ein eigenes Passwort.

Greifen Sie dabei auf geeignete Passwort-Manager zurück, die Sie mit einem ausreichend sicheren Passwort oder anderen Authentifizierungsmethoden schützen.

Aktivieren Sie die sichere Multi-Faktor-Authentifizierung, wenn es möglich ist.

- ✓ **Social Engineering und Phishing**

Rechnen Sie damit, dass Cyberkriminelle versuchen, sich als vertrauenswürdige Quellen (z.B. IT-Abteilung, Gesundheitsbehörde) auszugeben.

Phishing-mails stellen eine besondere Gefahr da: Überprüfen Sie bei ungewöhnlichen E-Mails stets die Identität der Absenderadresse.

Halten Sie im Zweifel immer Rücksprache mit geeigneten Ansprechpersonen (IT-Verantwortliche, Vorgesetzte, KollegInnen).

Geben Sie unter keinen Umständen Benutzerdaten oder Passwörter weiter, wenn Sie dazu aufgefordert werden. Geben Sie online vertrauliche und persönliche Daten ausschließlich über SSL-verschlüsselte Seiten bekannt (erkennbar an "https://" und an einem Schlosssymbol am unteren Bildschirmrand).

Führen Sie nur vertrauenswürdige Programme aus zweifelsfrei seriösen Quellen aus.

Beispiele für Social Engineering Versuche:

• Sie erhalten eine E-Mail mit der Aufforderung, Ihre Benutzerdaten oder Passwörter einzugeben, damit Sie aktuelle Informationen über das Coronavirus erhalten.

• Es öffnet sich ein Pop-Up. Ein Sicherheitsteam informiert Sie über die neueste Anzahl von Infektionsfällen und fordert Sie auf, eine „Nachrichtensoftware“ zu installieren.

• Sie erhalten einen Anruf. Der Unbekannte gibt sich als Mitarbeiter der IT-Abteilung aus und fordert Sie auf, Zugangsdaten herauszugeben.

Links:

Cybersicherheit für Unternehmen www.it-safe.at

IT-Security Experten https://www.wko.at/site/it-safe/suche-nach-it-security-expert-inn-en.html

Home-Office https://www.onlinesicherheit.gv.at/service/news/532326.html

Gefahren im Internet
https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy__sicher_durch_die_digitale_welt/3.html

Phishing
https://www.ombudsmann.at/schlichtung.php/cat/45/aid/264/title/Was_ist__Phishing__und_was_kann_ich_dagegen_tun_

Passwortsicherheit
https://www.onlinesicherheit.gv.at/praevention/konten_und_passwoerter/passwort-auswahl/249589.html

Stand: 19.03.2020

IMPRESSUM: Medieninhaber, Herausgeber: WKÖ, Bundessparte Information und Consulting,
Wiedner Hauptstraße 63, 1045 Wien