Informationsblatt der Datenschutzbehörde

Datensicherheit und Home-Office

Aufgrund der derzeitigen Epidemie (Coronavirus, COVID-19) kommt es im öffentlichen und privaten Bereich vermehrt zum Umstieg auf Home-Office. Darüber hinaus wird die aktuelle Situation und die damit verbundene allgemeine Verunsicherung von Cyberkriminellen missbraucht. Vor diesem Hintergrund hat die Datenschutzbehörde ein Informationsblatt zum Thema Datensicherheit und Home-Office erstellt, welches am Arbeitsplatz geteilt werden kann.

Allgemeines zum Thema Home-Office

Bitte bewahren Sie Hardware (insbesondere Diensthandy, Dienstlaptop) sicher auf. Verwenden Sie nach Möglichkeit eine geschützte WLAN- oder LAN-Verbindung und sofern vorhanden, eine verschlüsselte VPN-Verbindung. Bei der Nutzung einer offenen ungeschützten WLAN-Verbindung ist jedenfalls der Einsatz einer verschlüsselten VPN-Verbindung empfohlen. Ist ausnahmsweise ein öffentlicher Transport der Hardware nötig, sollte eine erhöhte Aufmerksamkeit gegenüber Diebstahl bestehen und sichergestellt werden, dass bei Geräten eine Hardware- oder softwarebasierte Verschlüsselung zum Einsatz kommt.

Cyberkriminalität und Social Engineering

Die aktuelle Ausnahmesituation und die Verunsicherung werden von Kriminellen missbraucht. Rechnen Sie damit, dass Kriminelle versuchen, sich als vertrauenswürdige Quellen (etwa als Gesundheitsbehörde) auszugeben. Geben Sie unter keinen Umständen Benutzerdaten oder Passwörter weiter, wenn Sie dazu aufgefordert werden. Installieren Sie auch nicht eigenmächtig Software auf Ihrem (Dienst-) Laptop. Hinterfragen Sie stets Anweisungen, die Sie zu ungewöhnlichen Handlungen oder der Installation von diversen Programmen auffordern.

Bitte berücksichtigen Sie, dass eine Identität gefälscht werden kann. Überprüfen Sie bei ungewöhnlichen E-Mails daher stets die Identität der Absenderadresse und vergleichen diese mit der Absenderadresse von vertrauenswürdigen E-Mails Ihrer KollegInnen.

Bitte halten Sie im Zweifel Rücksprache mit der Ansprechperson für IT-Angelegenheiten Ihres Arbeitgebers.

Beispiele:

- Sie erhalten eine E-Mail mit der Aufforderung, eine Home-Office-Software zu installieren.

- Sie erhalten eine E-Mail mit der Aufforderung, Ihre Benutzerdaten oder Passwörter einzugeben, damit Sie aktuelle Informationen über das Coronavirus (COVID-19) erhalten.
- Es öffnet sich ein Pop-Up. Ein angebliches 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 einer Gesundheitsbehörde aus und fordert Sie auf, Ihre Kreditkartendaten bekannt zu geben, damit Ihnen ein Impfstoff zugeschickt werden kann.

Allgemeine Informationen zu Gefahren und Kriminalität im Internet finden Sie auch unter:

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

und https://www.onlinesicherheit.gv.at/gefahren_im_netz/startseite.html