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.

Zusätzlich zu den hier vorgeschlagenen Maßnahmen empfiehlt die Datenschutzbehörde, dass Arbeitgeber eine weiterführende und an den jeweiligen Betrieb angepasste Checkliste („Do's and Don'ts") erstellt, die ArbeitnehmerInnen beim Home-Office einzuhalten haben.

Allgemeine Hinweise 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.
- Bitte laden Sie keine beruflichen Daten auf private Geräte oder die private Cloud. Dies gilt insbesondere für den Fall, wenn kein Betriebsequipment zur Verfügung steht.
- Verwenden Sie keine privaten Kommunikationsmittel (WhatsApp, Facebook, Instagram, o.ä.) für den Austausch von beruflichen Informationen.
- Vermeiden Sie das Ausdrucken von Unterlagen. Sollte dies dennoch notwendig sein, sollten Sie die ausgedruckten Unterlagen entsprechend vernichten und jedenfalls nicht in der Hausmülltonne entsorgen.
- 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.
- Stellen Sie sicher, dass auch im Home-Office regelmäßige Backups der Daten durchgeführt werden, um das Risiko eines Datenverlusts durch Diebstahl (oder durch eine defekte Festplatte) zu minimieren.

Cyberkriminalität und „Social Engineering"

Die aktuelle Ausnahmesituation und die Verunsicherung wird von Kriminellen missbraucht. Insbesondere ist ein Anstieg von Phishing-Attacken zu beobachten, mittels welcher Kriminelle versuchen über gefälschte Webseiten, E-Mails oder Kurznachrichten an Nutzerdaten zu gelangen. 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. Überprüfen Sie vor der Eingabe von Nutzerdaten auf einer Webseite die URL („die Webadresse“) und rufen Sie Login-Seiten lieber durch manuelle Eingabe auf, anstatt einem Link aus einem E-Mail zu folgen. 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.

Besondere Vorsicht ist auch geboten, wenn Sie in einer E-Mail zu dringenden Handlungen aufgefordert werden. Kriminelle versuchen oftmals unter Vorspielung besonderer Dringlichkeit zu bestimmten Handlungen zu verleiten *(„Falls Sie nicht innerhalb der nächsten 2 Tage eine Verifikation durchführen, wird ihr Konto/Zugang gesperrt.“)*

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 dringlichen Aufforderung ihren E-Mail-Account für den Home-Office-Einsatz zu verifizieren.
- 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.

Weiterführende Informationen

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