Sehr geehrte Kolleginnen und Kollegen!

Aktuell handelt es sich für alle ArbeitnehmerInnen um eine besondere Situation:

Die enorme Zunahme an Teleworking und die geringe Vorort-Besetzung für Notbetrieb bedeuten leider auch fehlende persönliche Kommunikation und vermehrt schriftliche Kommunikation via E-Mail, WhatsApp usw.

Das haben leider auch Betrüger und Cyberkriminelle erkannt und nutzen diese ungewöhnliche Situation und Erwartungshaltung von MitarbeiterInnen aus. Seien Sie deshalb in folgenden Situationen besonders wachsam!

**1. Gefälschte E-Mail-Absender:**

Als MitarbeiterIn rechnen Sie aktuell mit primär schriftlichen Aufträgen und Sie können sich nicht -  wie gewohnt -  kurzfristig persönlich abstimmen. E-Mails und Absender der E-Mail können gefälscht sein. E-Mail-Anhänge können auf dem Weg von Empfänger zu Absender verändert oder ersetzt werden.

**Seien Sie daher bei E-Mails wachsam:**

* mit ungewöhnlichen und/oder vertraulichen Aufträgen, die eine Änderung der üblichen Vorgehensweise bedeuten (auch wenn die E-Mail scheinbar von einem Ihnen gut bekannten Absender stammt);
* von Absendern, mit welchen Sie vielleicht üblicherweise nicht direkt kommunizieren (z.B. Geschäftsführung);
* mit Überweisungsaufträgen in ungewöhnlicher Höhe oder mit geänderten Kontoverbindungen (auch wenn die Rechnung tatsächlich erwartetwird);
* mit Aufträgen von externen Auftraggebern (Behörde, Rechtsanwalt oÄ);
* mit dem Auftrag Zugangsdaten/Passwörter herauszugeben oder einzugeben.

**2. E-Mails zum Thema Corona**:

Aktuell ist der Informationsbedarf an „Corona/Covid-19“ sehr hoch. Als MitarbeiterIn rechnen Sie mit E-Mails zu Thema von Geschäftsführung und Führungskräften. Aktuell kursieren daher bereits gefährliche E-Mails mit Schadprogrammen und Phishing-Links.

**Seien Sie bei E-Mails oder anderen elektronischen Anfragen wachsam**:

* wenn Sie E-Mail-Anhänge zu „Corona/Covid-19“ öffnen sollen.
* wenn Sie auf externe Links zum Thema „Corona/Covid-19“ klicken sollen.

**3. Fernzugriffe auf Ihre Geräte**

Aktuell rechnen Sie damit, dass sich Ihre IT, IT-Dienstleister oder Programmhersteller bei Ihnen melden.

**Seien Sie wachsam – auch wenn bekannte Namen genutzt werden:**

* wenn jemand einen Fernzugang zu Ihrem System/Laptop wünscht z.B. über Teamviewer.
* wenn Sie jemand auffordert einen Fernzugriff zu genehmigen oder zu beantragen.
* wenn Sie Programme installieren sollen, die Sie angeblich für Homeoffice-Zwecke oder Schadprogramm-Abwehr benötigen.

**3. Telefonische Kontaktaufnahme**

Betrüger können versuchen, Sie telefonisch unter Druck zu setzen, indem Sie auf Teleworking-Erfordernisse Bezug nehmen.

**Seien Sie bei telefonischen Kontakten wachsam**:

* Geben Sie keine Zugangsdaten/Passwörter heraus, weil Sie sich sonst angeblich nicht mehr in das System einloggen können oder nicht mehr über Teleworking arbeiten können oÄ. Es gibt keinen legitimen Grund für die Weitergabe von Zugangsdaten/Passwörtern, auch wenn Sie der Anrufer noch so sehr unter Druck setzt.
* Erteilen Sie keine Zugangsberechtigungen ohne Prüfung der Identität des Anfordernden (bzw. in Einhaltung der erforderlichen Prozessschritte).

**4. Wie gehen Sie in solchen Fällen richtig vor?**

* Kommen Sie dem Auftrag nicht ohne Abklärung nach, jeder versteht dies in der aktuellen Situation.
* Akzeptieren Sie Zeitdruck nicht, wenn das von Ihnen verlangt, Vorgaben und Regeln zu brechen.
* Notieren Sie sich Name und ggfs. Unternehmen des telefonisch Anfragenden und prüfen Sie dessen Identität/Berechtigung.
* Halten Sie sofort telefonisch Rücksprache mit dem Absender (sofern Kollegin/Kollege), mit Ihrer Führungskraft, oder mit Ihrer IT-Abteilung.
* Allgemein gilt für Teleworking: Achten Sie darauf, dass Sie interne/vertrauliche Unternehmensdaten in einem geschützten Bereich (indoor) bearbeiten. Zugriff auf Hard-/Software und Daten dürfen aus rechtlichen Gründen nur Sie als MitarbeiterIn haben (auch nicht Ihre privaten Vertrauenspersonen). Bitte beachten Sie die ggfs. geltende Teleworking-Policy.