L 3.1 Gefahren und Risiken

Im Internet:
Man muss sich bewusst sein, dass Streifzüge im Netz Spuren hinterlassen. Mit allen Besuchen auf Homepages sind mittels Cookies Daten im Internet gespeichert. Vorsicht ist geboten bei Computer Updates, damit wird auch eine Verbindung zum eigenen Rechner erstellt die genutzt wird, damit ist der Betrüger dann online dabei.

Mit Telefon und Emails:

Folgende Merkmale sollten Sie alarmieren:
Emails in fehlerhafter oder fremder Sprache. Dringender Handlungsbedarf. Aufforderung zur Eingabe mit Daten – oder öffnen einer Datei.

„Enkeltrick“
Mit diesen Tricks wird ein betrügerisches Vorgehen bezeichnet, bei dem sich die Betrüger über Telefon, Emails meist gegenüber älteren und /oder hilflosen Personen, als deren Verwandte ausgeben, um unter Vorspiegelung falscher Tatsachen an deren Bargeld oder Wertgegenstände zu gelangen.

„SMS oder WhatsApp“
Hallo Mama, mein Handy ist kaputt, das ist meine neue Nummer. Diese Nachricht ist ein Teil einer Betrugsmasche, das läuft immer gleich ab. Jemand mit unbekannter Nummer meldet sich, der Sohn oder Tochter zu sein. Danach folgen Geldforderungen mit der Begründung: ich muss eine Rechnung bezahlen, das geht aber nur mit dem neuen Handy. Ich gebe dir das Geld morgen wieder zurück.

„Schockanruf“
Der unbekannte Anrufer ist angeblich von der Polizei, von der Staatsanwaltschaft oder arbeitet im Spital. ER erzählt zum Beispiel, dass die Tochter oder der Sohn einen schweren Unfall hatte. Danach wird dringend Geld gefordert für eine Kaution oder angeblich medizinische Leistung, die nicht von der Versicherung gedeckt sind.

„Polizeianruf ab Band“
Am Telefon wird ein Tonband abgespielt, das angeblich von der Polizei stammt. Eine Computerstimme fordert die angerufene Person auf, die Taste 1 zu drücken. Hier meldet sich dann ein falscher Polizist, der versucht mit erfundenen Geschichten einen Geldbetrag für eine angeblich begangene Straftat zu erpressen.

„Bankbetrug“
Diese Art von Betrug hat zum Ziel, an sensible Informationen von Bankkunden zu gelangen. Die Betrüger lassen sich kreative Geschichten einfallen, um potentielle Opfer zu Zahlungen oder zur Herausgabe von Bankdaten zu bewegen. Wo werden beispielsweise vermeintlich fehlgeleitet Zahlungen hinterfragt.

„QR-Code“
Ist ein zweidimensionaler Code, welcher zur mobilen Datenerfassung entwickelt wurde. Weil der Inhalt eines QR-Codes nicht auf den ersten Blick ersichtlich ist, ist es möglich, in ihm einen Link zu verstecken, der den Betrachter nach dem Scannen auf eine schädliche Seite führt oder sogar ungewollt Funktionen seines Smartphones ausführt, darum sollte man beim Scannen kontrollieren, ob die Adresse mit dem Titel Anbieters übereinstimmt.