Stammgemeinschaft eHealthAargau | emedo

Handout
Grundlagen der Informationssicherheit

Öffentliches WLAN

Verschlüsselung
Viele öffentliche WLANs sind nicht verschlüsselt. Sie müssen sich daher selbst um die Verschlüsselung kümmern. Am besten rufen Sie vertrauliche Daten erst gar nicht ab oder nutzen ein VPN (Virtual Private Network).

Honeypots
WLAN-Namen sind frei wählbar. Angreifer können vertrauenerweckende WLAN-Namen (SSIDs) einrichten und den Datenverkehr mitlesen. Das ist besonders beliebt auf Messen, öffentlichen Plätzen und in Hotels.

Passwortsicherheit

Nicht 2x dasselbe
Am besten für jede Website und Anwendung ein eigenes Passwort nutzen. Wenn eine Anwendung gehackt wird, kann sich der Angreifer nicht in eine andere einloggen.

Lang statt kompliziert
Es schadet nicht, komplizierte Passwörter zu verwenden, falls Sie sich diese merken können bzw. sicher verwahren. Noch wichtiger ist aber eine entsprechende Länge.

Wörterbuch
Verwenden Sie keine Wörter, die im Wörterbuch stehen, auch wenn Sie diese leicht verfremden oder um Zahlen ergänzen.

Social Engineering

Was ist Social Engineering?
Unter Social Engineering versteht man den **Versuch, Personen zu beeinflussen, um an sensible Informationen zu kommen.** Manche Angreifer geben sich als vertrauenswürdige Personen aus und versuchen Hilfsbereitschaft und Gutgläubigkeit auszunutzen. Andere dringen in Büros ein und suchen nach unbesetzten Schreibtischen oder betreiben Dumpster Diving.

Schutzmassnahmen
- Seien Sie bei jeder Kommunikation mit Unbekannten misstrauisch.
- Passen Sie auf, wenn Sie Ihre IT-Geräte in der Öffentlichkeit entsperren. Ihre Eingabe könnte gesehen oder abgefilmt werden.
- Achten Sie auf einen aufgeräumten Arbeitsplatz.
- Leeren Sie regelmäßig Ihren Papierkorb.
- Lassen Sie sich zu nichts unter Zeitdruck drängen, wenn Sie sich unsicher sind.

Stammgemeinschaft eHealth Aargau
Laurenzenvorstadt 11
5000 Aarau
info@emedo.ch
www.emedo.ch
062 836 40 10

Phishing

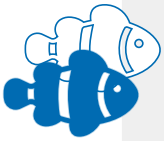
Was ist Phishing?

Beim Phishing versuchen Angreifer, mittels **E-Mail**, Anruf oder Messengernachricht **an vertrauliche Informationen des Opfers zu kommen, um schädliche Aktivitäten durchzuführen**. Die Betrüger treten dabei als vertrauenswürdige Personen auf und kontaktieren die Betroffenen mit dringlichen Anliegen. Dadurch sollen diese dazu gebracht werden, bestimmte Handlungen zu vollziehen, die es den Angreifern ermöglichen, Zugriff auf vertrauliche Daten oder den PC zu erlangen.

Merkmale von Phishing Mails

- Ungewöhnliche Absenderadresse
- Unpersönliche Anrede
- Falsche Rechtschreibung bzw. ungewöhnliche Sprache
- Dringliches Anliegen
- Aufforderung zu einer Handlung (zum Beispiel Anklicken von Links oder Öffnen von Anhängen)
- Die Kontaktperson erkundigt sich nach firmeninternen Details oder sensiblen Informationen.

Arten von Phishing



Spear-Phishing
Die Betroffenen werden ausgespäht und erhalten eine persönlich zugeschnittene E-Mail mit der Aufforderung, einen Link oder Anhang zu öffnen.

Erpressungsmails
Bei dieser Betrugsmasche versenden die Täter Mails, in denen sie angeben, dass sie im Besitz von belastendem Material sind – etwa Beweisen, dass man pornographische Webseiten besucht hat. Damit sie diese nicht veröffentlichen, fordern sie ein Lösegeld.

Dynamite-Phishing (z.B. EMOTET)
Bei diesem Angriffstyp werden automatisch personalisierte Phishing-Mails erzeugt. So erhalten Sie zum Beispiel eine angebliche E-Mail von einem Geschäftspartner, mit dem Sie erst kürzlich in Kontakt waren. In dieser werden Sie aufgefordert, einen Link oder ein Dokument zu öffnen.

CEO-Fraud
Bei einem solchen Angriff geben sich die Täter meist als Geschäftsführer (CEO) oder als ein höher positionierter Mitarbeiter aus und versuchen das Opfer zu überreden, hohe Zahlungen ins Ausland zu tätigen.

Ransomware
Diese Art von Schadsoftware kann Daten auf einzelnen Rechnern oder im ganzen Netzwerk vollständig verschlüsseln und fordert Lösegeld für deren Entschlüsselung. Der einzig sichere Schutz ist das regelmäßige Erstellen von externen Backups.

Umgang mit Phishing

- Öffnen Sie keine Links oder Anhänge in Nachrichten von unbekannten
- Absendern. Klicken Sie auch in SMS- oder Messenger-Nachrichten nicht auf Videos o.Ä.
- **Löschen Sie verdächtige Nachrichten oder leiten Sie sie – mit einer Warnung versehen – an Ihre IT-Abteilung weiter.**
- Erlauben Sie bei heruntergeladenen Dateien auf keinen Fall die Ausführung (auch nicht von Makros etc.).
- Glauben Sie, Opfer eines Angriffs geworden zu sein, trennen Sie Ihren PC sofort vom Firmennetzwerk (LAN-Kabel ziehen, WLAN-Verbindung trennen).
- Geben Sie auch am Telefon keine sensiblen Informationen an unbekannte Personen weiter, sondern bitten Sie den Anrufer stattdessen um eine Rückrufnummer und überprüfen Sie seine Identität.