Große Kreisstadt
Öhringen

Fachstelle
Bildung-Beteiligung-Jugend

AZ: 453.033 Datum: 28.07.2016

Information über Schadsoftware und Internetbetrüger

Quelle: csm_Bild_TK-Pressefoto_8512002088_03e26447
Zu finden unter Google Bilder

Liebe Freunde,
da die Nutzung vom Internet mit der Zeit immer gefährlicher wird. Geben wir euch ein paar Tipps damit ihr euch Sicherer im Internet bewegen könnt.

Mit freundlichen Grüßen
Jugendreferat Stadt Öhringen

Schadsoftware Locky und Ranscem

Die Software Avira berichtet über eine neue Vision der Locky-Ramsomware: *https://blog.avira.com/locky-goes-offline/*.
Diese Version richtet Schaden an, wenn der Anwender offline ist. Sie erschwert es die Rechner abzusichern, wenn es der Version allerdings nicht gelingt den Command-and-Control Server zu erreichen schaltet die Ransomware(Ransomware sind Krypto- oder Erpressungstrojaner) automatisch nach kurzer Zeit in den Offline-Modus und beginnt mit der Verschlüsselung der Daten.
Auch Ranscam scheint auf den ersten Blick eine weitere Form von Ransomware zu sein. Sie droht ebenfalls mit Verschlüsselung von Dateien und fordert Lösegeld von 0,Bitcoins (Bitcoins ist eine virtuelle Geldeinheit). Erhält der Anwender so eine Nachricht, hat die Version bereits begonnen Dateien zu löschen. Die Dateien kommen auch nicht mit der Bezahlung des Lösegeldes zurück. Weitere Infos über Ranscam finden sie unter:
http://www.zdnet.de/88274607/neue.ransomware-loescht-dateien-trotz-loesegeldzahlung/

Apple: Erpressung mit Sperrfunktion für iPad und iPhone

Besonders in den USA und Europa verwenden Internet-Betrüger erworbene Account-Daten von Apple-IDs, um Nutzer von iPads und iPhones wie auch Sperrfunktion zu erpressen. Sie drohen mit Löschung aller Daten auf dem Smartphone oder Tablet, wenn keine Zahlung zwischen 30 und 50 US-Dollar erfolgt. Eine Schutzmaßnahme vor solchen Angriffen sind unterschiedliche und neue Passwörter für verschiedene Onlinedienste. Niemals die Gleichen! Nach zu lesen sind diese Informationen auf folgenden Seiten:

http://www.notebookcheck.com/Apple-iPhone-und-iPad-Sperrfunktion-wird-missbraucht.169150.0.html.de
http://support.apple.com/en-us/HT204145
http://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Sicherheitsupdates für Apple Handys und Computer

Apple veröffentlicht Sicherheitsupdates für sein mobiles Betriebssystem, sein Stationäres Betriebssystem und auch für den Webbrowser Safari und iTunes. Da diese Sicherheitslücken ein Risiko für die Geräte sind sollte man die Updates so schnell wie möglich installieren. Hier die Seiten für die Sicherheitsupdates:

https://www.bsi-fuer-buerger.de/SharedDocs/Warnmeldungen/DE/TW/warnmeldung_tw-t16-0078.html?nn=6775642
http://www.bsi-fuer-buerger.de/SharedDocs/Warnmeldungen/DE/TW/warnmeldung_tw-t16-0077.html
http://www.bsi-fuer-buerger.de/SharedDocs/Warnmeldungen/DE/TW/warnmeldung_tw-t16-0075.html?nn=6775642
https://www.bsi-fuer-buerger.de/SharedDocs/Warnmeldungen/DE/TW/warnmeldung_tw-t16-0076.html?nn=6775642

Pokémon Go

Auch in Deutschland ist ein riesiger Hype um das Augmented-Reality-Spiel Pokémon Go entstanden. Spieler die sich mit einem Google Konto für die App anmeldeten, gewährten dem Spielehersteller zwischenzeitlich vollen Zugriff auf das eigene Konto. Unter einem solchen Zugriff ist es möglich E-Mails zu lesen, Einblicke in den Suchverlauf und Standorte oder die Dokumente von Google Drive. Um sich zu schützen sollte man Pokémon Go nur aus Quellen wie Google Play oder Apple App Store installieren. Da es für Spieler unmöglich scheint in dieser App anonym zu sein, hat der Bundesverband nun die Entwickler adressiert. Weitere Infos zu Pokémon Go und seine Risiken findet man auf folgenden Seiten:

https://www.heise.de/security/meldung/Pokemon-Go-Android-Versionen-mit-Trojaner-im-Umlauf-3262816.html
http://www.heise.de/security/meldung/Pokemon-Go-greift-sich-alle-Google-Rechte-3263813.html
http://www.vzbv.de/pressemitteilung/vzbv-mahnt-entwickler-von-pokemon-go-ab