How-not-to-get-hacked

Festplattenverschlüsselung: Bevor das Betriebssystem hochfährt, muss die Festplatte entschlüsselt werden. Windows bietet hier *BitLocker* an.

2-Faktor-Authentifizierungen (2FA): Erzwingen Sie wo möglich 2FA, um eine zusätzliche Sicherheitsebene zu schaffen (Betriebssysteme, Bankaccounts usw.).

Sichere Passwörter und Passwort Manger: Ein Passwort sollte aus einer zufälligen Kombination aus mind. 12 Zeichen (Groß, Klein, Zahlen, Sonderzeichen) bestehen und nicht mehrfach verwendet werden. Ein Passwort-Manager wie *KeePass* hilft dabei für jeden Account ein einzelnes, starkes Passwort zu erzeugen.

Prinzip der geringsten Privilegien: Benutzen Sie, nach Möglichkeit, für Ihre tägliche arbeiten Benutzeraccounts ohne Privilegien. Administrative Accounts sollten nur im Bedarfsfall genutzt werden. Legen Sie IT-Assets so an das deren Privilegien nicht über den produktiven Bedarf hinausgehen.

Backups: Backups helfen nicht nur nach Hacker-Angriffen, sondern auch bei Geräteverlust und sollten immer zu festgelegten Zeiten durchgeführt werden. Es sollte verschiedene Backups erstellt werden (z. B. wöchentlich, monatlich, halbjährlich). Backups sollten teilweise offline & extern gelagert werden. Die 3-2-1-Regel wird oft empfohlen.

Phishing: Das größte Einfallstor. Prüfen Sie die E-Mail-Absender Adresse. Dokumente können Schadcode enthalten und sollten in einer isolierten Umgebung (Sandboxing) geöffnet werden. Klicken Sie keine Links an und geben Sie dort keine sensiblen Daten ein, wenn Sie nicht sicher sind. Lassen Sie sich nicht unter Druck setzen. Im Zweifelsfall einfach alles ausschalten/ auflegen und spazieren gehen.

Updates: Halten Sie Ihre IT-Assets auf dem neusten Stand. Veraltete IT-Assets sind anfällig für Sicherheitslücken und ein leichter Gewinn für Angreifer.

IT-Asset-Management: Behalten Sie einen Überblick über Ihre IT-Assets (Software, Geräte, Benutzer usw.). Löschen Sie nicht mehr benötigte Software. Deaktivieren Sie Benutzer, wenn diese das Unternehmen verlassen. Unterbinden Sie das anschließen von nicht genehmigten Geräten an Ihr Netzwerk.

Notfallplan: Was passiert, wenn morgen meine Geräte verschlüsselt sind oder mein Büro abgebrannt ist?

</> ETHICAL HACKING

Jonas Borgartz
Ethical Hacker
+49 177 7094537
jonas.borgartz@it-sicherheit.io
www.it-sicherheit.io