SafeWise
17.06.2022

Modul 1: Grundlagen der Cyber- und IT-Sicherheit

IT-Sicherheitsvorfälle

IT-Sicherheitsvorfälle (IT-Security-Incidents) sind Geschehnisse, die die Vertraulichkeit, Verfügbarkeit und/oder Integrität einer IT-Komponente versehen, oder von denen eine Versehrung Gefahr in der Zukunft ausgeht.

Beispiel:
Eine Phishing Mail, ist eingegangen, auf deren bösartigen Link aber nicht reagiert wurde. Bei Klicken auf den Link würde eine Schadsoftware heruntergeladen werden, über die Hacker in das Rechenzentrum gelangen können.

Erklärung:
Auch wenn kein Schaden entstanden ist, handelt es sich bei der eingegangenen Mail um ein IT-Security-Incident, da die Mail gut möglich noch weiter im weiter Umlauf ist und es ohne Gegenmaßnahmen in Zukunft gut absehbar ist, dass ein Mitarbeiter auf den Link darin klicken wird.

Schwachstelle:
Einem Sicherheitsereignis wird der Weg durch eine Schwachstelle bereitet.
Eine Schwachstelle ist ein Zustand, der als Eintrittspforte für Sicherheitsgefahren dient. Wird diese Pforte durch die Gefahren genutzt kommt es zu einem IT-Security-Incidents.

Merke:
Sowohl Schwachstellen, als auch IT-Security-Incidents sind je nach unternehmensinternen Richtlinien einem vom Unternehmen gestellten Beauftragten oder Vorgesetzten zu melden.

Passwortsicherheit

Sichere Passwörter sind nicht nur ein wichtiger Bestandteil um das Unternehmen vor Angreifern zu schützen, sondern auch ein fester und wichtiger Bestandteil des Alltags geworden. Denn das Passwort ist oft die einzige Hürde, die Angreifer haben, um deine persönlichen Daten zu klauen und deine Identität zu missbrauchen. Wenn ein Angreifer Zugriff auf eines deiner Konten bekommt, kann er dir und deinem Arbeitgeber ernsthaften finanziellen Schaden zufügen.

Folgende Punkte musst du beim Umgang mit deinen Passwörtern beachten:

- Regeln beim erstellen des Passwortes beachten, welche aber immer Unterschiedlich sind (z.B. mindestens eine Groß- und Kleinbuchstaben, mindestens ein Sonderzeichen, mindestens eine Ziffer und mindestens acht Zeichen).
    - Des Weiteren sollten keine Namen wie z.B. die von Familienmitgliedern Firmennamen oder Namen/ Bezeichnungen der Anlage verwendet werden
    - keine Wörter verwenden, die im Wörterbuch stehen
- Passwörter nicht aufschreiben
- Passwortmanager verwenden
- Passwörter verwenden die du dir nicht merken kannst
- Kein Passwort mehrmals verwenden

Sicheres-WiFi

Beim Benutzen eines WiFi Netzwerkes sollte man beachten, dass man keine unsicheren und dubiosen Netzwerke verwendet. Da hier die Gefahr besteht, dass Angreifer versuchen deine Daten zu klauen, dir Schadsoftware einzuschleusen oder dein Smartphone, Tablet oder PC zu übernehmen.

Unsichere WiFi-Netzwerke sind:

- Offene Netzwerke
- Mit WEP “verschlüsselte” Netzwerke

Unter Dubiosen WiFi-Netzwerken versteht man:

- Netzwerke die auf Channel 14 laufen
- Netzwerke die Verbunden mit offenen bekannten Netzwerken sind

Umgang mit mobilen Datenträgern und externer Hardware

Beim Umgang mit mobilen Datenträgern und externer Hardware gibt es einige Punkte zu beachten, die bei Nichtbeachtung zu existenzbedrohenden Problemen führen können.

Folgende Punkte musst du beachten:

- Regeln zum Umgang mit Datenträgern beachten, diese sollten vom Arbeitgeber vorgegeben werden.
- Die Komponenten/Datenträger sollten zur Benutzung auf einige Geräte beschränkt werden (Device Control).
    - Umsetzbar durch Funktionen auf Betriebssystem oder spezieller Software.

- Speichermedien aus nicht vertrauenswürdigen Quellen, müssen vor Benutzung mittels Quarantäne PC und zusätzlichen Manuellen Scan auf Schadcode/-programme geprüft werden.
    - Hierzu zählen auch externe Dienstleister
    - Notebooks vor Zugriff auf eigentliches System.
- Autorun-Funktion sollte auf allen ICS (Engl.: Industrial Control System, Deut.: industrielle Kontrollsystem) deaktiviert sein, um zu verhindern, dass sich Schadprogramme automatisch weiterverbreiten.
- Wechseldatenträger Schleuse verwenden.
- Ausschließlich unternehmenseigene Wechseldatenträger verwenden.
- Diese unternehmenseigenen Wechseldatenträger sollten nur im ICS-Netz verwenden werden.
- Physische Sperren gegen unbefugte Wechseldatenträger einbauen.
    - USB-Schlösser
    - Entfernen der Platinen
- Vollverschlüsselung der Datenträger und Wartung von Notebooks.

Phishing

Mittels Phishing versucht ein Angreifer an deine persönlichen oder firmeninternen Daten zu gelangen. Dies passiert oft per E-Mails, gefälschte Webseiten, SMS oder anderen soziale Medien. Der Angreifer versucht sich als vertrauenswürdige Person auszugeben (z.B. Kollege, Administrator, Amazon, Interpol, usw.) und anschließend dem Benutzer Informationen zu entlocken, oder ihn dazu zu bringen auf einen Link zu klicken, der auf eine mit Schadcode infizierte Seite verweist.

Folgende Punkte musst du beachten:

- Zum einen ist es wichtig bei E-Mails oder andere Nachrichten erstmal kritisch zu hinterfragen und erstmal die Nachricht auf Auffälligkeiten zu überprüfen, bevor man auf Links klickt oder Antwortet.
    - Rechtschreibfehler
    - Grammatik
    - Absender
    - Links
        - wo führen sie hin
        - sieht die URL vertrauenswürdig aus
    - Anrede
    - Was will der Absender von mir
- Oft reichen diese Punkte aber noch nicht, da die Angreifer immer professioneller werden. Deshalb gibt es Punkte die man zur Prävention davor schon beachten sollte:

- Awareness-Training mit Bedacht durchführen.
- Sich an die vom Arbeitgeber erstellten Sicherheitsrichtlinien halten. z.B.:
    - Informationen, die für das Unternehmen wichtig sind, geheim halten.

    - Datensicherungskonzept beachten.
    - Verschwiegenheitserklärung/Datenschutzerklärung für Mitarbeiter, Partner und Dienstleister.
    - Vorfälle schon bei geringstem Verdacht melden.
- Alarmierungswege die vom Arbeitgeber vorgegeben sind, kennen und nutzen.
    - Diese sollten keine negative Konsequenzen für den Arbeitnehmer haben.
- Technische Sicherheitsmechanismen verwenden
    - Diese erkennen Fehlverhalten und Angriffe
- Regelmäßige Datensicherung, um nach Angriff Daten wiederherzustellen.

Quellen

Sicherheitsvorfälle

- BSI ICS Kompendium
    - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=3

Passwortsicherheit

- Cyber-Sicherheitsempfehlungen BSI; Sichere Passwörter erstellen
    - https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Sicheres-WiFi

- https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-invisible-rogue-access-point-siphon-off-data-undetected-0148031/
- https://www.okta.com/identity-101/evil-twin-attack/

Umgange mit mobilen Datenträgern und externer Hardware

- BSI ICS Kompendium
    - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=3

Phishing

- BSI ICS Kompendium
    - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=3
- BSI: Industrial Control System Security, Top 10 Bedrohungen und Gegenmaßnahmen 2019
    - https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=1