



hochschule mannheim

Konzept

Awareness von OT-Mitarbeitern zu Nutzen und Grenzen von IT-Security-Maßnahmen

Projektsemester Cyber Security SS 2022

Team: **SafeWise** 

Philipp Feil
Bogdan Kotikov
Athanasios Aritzis
Zehra Aydin

Dozenten:

Sandro Leuchter
Thomas Smits

Inhaltsverzeichnis

1 Einleitung	2
2 Ziel und Zielgruppe	2
3 Umsetzung:	2
3.1 Lernthemen	2
3.2 Ablauf der Schulung	3
3.3 Mnemotechnische und didaktische Mittel	5
3.4 Setting	6
3.5 Belohnungssystem	7
Anhang Berechnung Belohnungssystem	9

1. Einleitung

Die Zunahme von Cyberangriffen in der Industriebranche stellt eine erhöhte Herausforderung an geeignete Gegenmaßnahmen. Die Sensibilisierung von Mitarbeitern ist dabei von zentraler Bedeutung.

Wie diese Sensibilisierung umgesetzt werden kann, um ein Höchstmaß an Effektivität zu erreichen, beschreibt das vorliegende Konzept.

2. Ziel und Zielgruppe

Die Schulung richtet sich an Ingenieure aus der OT.

Um die Schulung noch näher an der Zielgruppe zu gestalten wurde sie exemplarisch auf den Energie-Sektor zugeschnitten.

Die darauf zugeschnittenen Elemente (bspw. das Belohnungssystem mit dem Energiekonto in Gigajoule) lassen sich mit etwas Kreativität analog auf andere Sektoren übertragen.

OT-Security-Awareness im Energiesektor ist besonders wichtig, da das Produkt Energie bzw. Strom für jeden anderen Sektor ein Betriebsmittel ist. Durch diese Abhängigkeit ist der Energiesektor ein besonders beliebter Angriffspunkt für Hacker, und das auch im Rahmen von Cyber-Kriegshandlungen.

Die Wandlung dieses Sektors durch den Ausbau erneuerbarer Energien, erhöht außerdem die Angriffsfläche für Hacker.

3. Umsetzung:

3.1. Lernthemen

Im Anhang I sind alle Lernthemen gelistet, und es wird genauer aufgeführt, was der Lernende zu diesen Themen an Wissen erwirbt.

Die Themenauswahl basiert auf industriellen Standards und Fachartikeln zur IT-Security (im ICS-Kontext):

- [Industrial Control System Security, Top 10 Bedrohungen und Gegenmaßnahmen 2019 vom BSI](#)
- [Best Practices aus dem BSI ICS-Security-Kompendium](#)
- [OPS.1.2.5 Fernwartung vom BSI](#)
- [Cyber-Sicherheitsempfehlungen BSI: Sichere Passwörter erstellen](#)

Folgende Themen sind vorgesehen, implementiert wurden die fett markierten:

- **Sicheres Verhalten am Arbeitsplatz**
- **Allgemein Vorsicht beim Surfen im Internet und Downloads**

- Phishing
- Social Engineering
- **Passwortsicherheit**
- **Secure Wifi**
- Umgang mit mobilen Datenträgern und externer Hardware
- Regelmäßige Updates und Patches
- Fernzugriff
- Netzwerksegmentierung
- Überwachung der Anlage (Logging/ Monitoring)
- **IT-Security-Incidents**
- Feldgeräte absichern
- Absicherung von Diensten und Protokollen (Zeitsynchronisierung
DNS-Namensauflösung)
- Internet of Things

3.2. Ablauf der Schulung

Nach einer Einleitung, in der der Nutzer mit seiner Rolle und Umgebung vertraut gemacht wird, werden nacheinander drei Module freigeschaltet.

Module:

In den Modulen werden die Schulungsthemen als kleine Spiele oder Kurzgeschichten gehalten.

Ein Modul ist abgeschlossen, wenn alle Spiele darin erfolgreich (- d.h. mit mindestens 75% richtigen Entscheidungen -) abgeschlossen wurden.

Innerhalb eines Moduls kann der Nutzer die Reihenfolge der Spiele/Lernthemen frei bestimmen.

Die Abfolge der Module imitiert den Gang durch das Unternehmen bzw. durch das Purdue Modell von oben nach unten.

Da Angriffe über die oberen Ebenen weniger technische Virtuosität von Angreifern erfordern, über die Zeit am Arbeitsplatz hinaus erfolgen können, und sich ebenso destruktiv auswirken können, kommen diese frühzeitig an die Reihe.

Nach Abschluss des Moduls wird eine PDF freigeschaltet, in der aus jedem Lernthema die wichtigsten Regeln noch einmal kurz zusammengefasst sind.

Modul Nr.	Thema
1	Sicheres Verhalten am Arbeitsplatz

	Cyber Security Incidents
	Surfen im Internet und Downloads
	Phishing
	Social Engineering
	Passwortsicherheit
	Secure Wifi
	Umgang mit mobilen Datenträgern und externer Hardware
2	Überwachung der Anlage
	Updates und Patches
	Fernzugriff
	Netzwerksegmentierung
3	Feldgeräte Absichern
	Absicherung von Diensten und Protokollen
	Internet of Things

3.3. Mnemotechnische und didaktische Mittel

Im Anhang II Mnemotechnische und didaktische Mittel findet sich eine detaillierte Dokumentation zum Einsatz der mnemotechnischen und didaktischen Mittel innerhalb der Anwendung.

Um eine höchstmögliche Schulungseffektivität zu erreichen wurden mnemotechnische und didaktische Mittel bedacht, die schließlich zu Anforderungen wurden und im Design der Schulung berücksichtigt sind.

Folgende didaktische Mittel wurden an mnemonischen Mentalfaktoren orientiert eingesetzt:

Mnemotech- nischer Mentalfaktor	Didaktisches Mittel	Umsetzung
Lokalisation	Ordnung und Struktur der Lerninhalte, Vorgabe der Lehrroute.	<ul style="list-style-type: none"> - Aufteilung in Module, themenspezifische Bündelung darin. Dadurch Verhinderung von Überwältigung des Nutzers.
	Wiederholung	<ul style="list-style-type: none"> - Anreiz zur Wiederholung, da neue Belohnungen warten und Neugier wecken (Eindrücke aus E-City). - PDF mit Zusammenfassung.
Logik	Deduktives Denken fördern.	<ul style="list-style-type: none"> - Regel erklären, und ein konkretes Beispiel lösen lassen.
Aufmerksamkeit	Abwechslung	<ul style="list-style-type: none"> - Durch viele verschiedene Minispiele bzw. Kurzgeschichten. - Durch die unterschiedlichen Eindrücke aus E-City als Belohnung.
	Entdeckendes Lernen	<ul style="list-style-type: none"> - In den als Kurzgeschichten gehaltenen Spielen.
	Learning by	<ul style="list-style-type: none"> - In den als Kurzgeschichten

	mistakes	gehaltenen Spielen.
	Interaktion	<ul style="list-style-type: none"> - In allen Spielen, vor allem in Kurzgeschichten bei einem Gegenüber zum interagieren.
Emotion	Belohnung	<ul style="list-style-type: none"> - Spielfortschritt bei erfolgreichem Absolvieren. - Lob von Joules. - Siehe Abschnitt "Belohnungssystem".
	Selbstwirksamkeit	<ul style="list-style-type: none"> - Der User kann innerhalb eines Modules die Reihenfolge , wann der Spiele selbst wählen. - Durch frei bestimmbaren Einsatz und Dosierung der Belohnung (Energie). - Abhängigkeit von E-City und den dort lebenden Menschen wird visuell vorgeführt durch die angehenden Lichter in E-City, und die Eindrücke. - Die Spiele/Stories verlaufen in Abhängigkeit der Benutzeraktionen.
Fantasie	Gamification	<ul style="list-style-type: none"> - In Form der Meta-Story/ des Spiel-Universums - In Form von Simulationsspiel - In Form des Belohnungssystems

3.4. Setting

Schauplatz

denn nur mit dem Wissen aus der Schulung kann er die richtigen Maßnahmen gezielt zum Schutz des E-Werks einsetzen .

Der Spieler findet sich in der Rolle des Ingenieurs wieder.

Sein Schauplatz ist das fiktive Kraftwerk "E-Werk", in welchem er arbeitet, und welches die fiktive Stadt "E-City" mit Strom versorgt.

Die Verfügbarkeit der Anlage stellt der Nutzer sicher, indem er sich schult, 6

User Guide

Als Guide durch die Schulung gibt es einen Charakter, der Hilfestellung und Erklärung gibt und den Spieler durch das Spiel begleitet.

3.5. Belohnungssystem

Durch das Spielen und besonders das erfolgreiche Spielen erhält der Benutzer Energie in Form von Gigajoule (Geschult-Sein impliziert Anlagenverfügbarkeit impliziert Energieproduktion) da seine Anlage durch seine Awareness verfügbar und produktiv ist.

Somit ist die Energie, die der Nutzer sammelt ist gleichzeitig ein Indikator für seine Awareness zur OT-Security, und damit für die Ausprägung der Schwachstelle, die durch die Schulung gepatched wird: mangelndes Bewusstsein beim Ingenieur.

Bei Weiterentwicklung der Software kann dieser Indikator womöglich auch eine gute Anwendung als KPI finden.

Belohnung	Beschreibung	Auslöser
Energie	50 GJ	Bei jedem vollständigen Durchklicken eines Spieles, unabhängig von richtigen oder falschen Antworten.
	100 GJ	Bei Abschließen eines Spieles für jedes Prozent ab dem 51. Prozent.
Einsatz der Energie für E-City	Ausschüttungsoption der Energie für E-City: Der Nutzer kann Energie an die Stadt E-City spenden und bekommt ein Feedback, wie lange die gespendete Energie die Stadt versorgt.*	Der Nutzer steuert selbst seinen Energievorrat an, und entscheidet wie viel Energie er E-City zuführen will - er muss die Energie vorher durch Spielen gewonnen haben.

Belohnung visuelles Feedback des Energieeinsatzes	a) Stadt, die zuvor im Dunkeln lag und bei Energieversorgung leuchtet.	Energiespende an E-City.
	b) Eindruck aus E-City Ein Bild einer Momentaufnahme davon, wie in E-City die Energie eingesetzt wird	Energiespende an E-City.
	c) Sammlung der "Eindrücke aus E-City"	Bei Komplettierung der Schulung (alle Module durch).
Fortschritt / Freischaltung	Spiel gilt als erfolgreich abgeschlossen und muss nicht wiederholt werden.	Über 75% der Entscheidungen in einem Spiel wurden richtig getroffen.
	Modul gilt als abgeschlossen und muss nicht wiederholt werden, nächstes Modul wird freigeschaltet.	Alle Spiele im Modul wurden erfolgreich abgeschlossen.

* Die Berechnung zur Energieversorgung basiert auf echten Daten und ist im Anhang III Belohnungssystem beschrieben.

Anhang: Berechnung Belohnungssystem

Berechnung der Energie:

Quelle für die zugrunde liegenden Daten:

<https://www.sonnenseite.com/de/energie/120-staedte-studie-stromverbrauch-das-sind-deutschlands-stromverschwender-staedte/>

Durchschnittlicher Energieverbrauch pro Kopf jährlich (in Deutschland): 1700 kWh

Durchschnittlicher Energieverbrauch in einer 100 000 Seelen-Stadt im Jahr:

$100\,000 \times 1700 \text{ kWh im Jahr}$

Durchschnittlicher Energieverbrauch in einer 100 000 Seelen-Stadt am Tag:

$(100\,000 \times 1700 \text{ kWh}) / 360$ für die Stadt

$= 472\,222 \text{ kWh}$ $= 472 \text{ MWh}$
 $= 1699\,999\,000 \text{ kJ}$ $= 699\,200 \text{ MJ}$
 $= 1699 \text{ GJ}$

Durchschnittlicher Energieverbrauch in einer 100 000 Seelen-Stadt am Tag:

$1699 \text{ GJ} / 24 \text{ h} = 71 \text{ GJ/h}$

- wir runden der Einfachheit halber auf 70.
Mit 70 GJ kann man also die Stadt für eine Stunde mit Energie versorgen.

-> Für eine Minute Energie in der Stadt braucht man also:
 $70 \text{ GJ} / 60 \text{ m} = 1,2 \text{ GJ (gerundet)}$

- Mit einem GJ erzeugt man Strom für:
 $60 \text{ m} / 70 \text{ GJ Minuten} = 0.9 \text{ Minuten (gerundet)}$.

Wir runden:

1 GJ entspricht 1 Minute Energie in E City.