Konzept cyberXscape

Game Design

cyberXscape sieht eine Abfolge von Micro-Games mit der Aufgabe des Findens von Sicherheitslücken oder Angriffsflächen im Themenbereich Cyber Security vor. Eine einfache Aufforderung erklärt in jedem Micro-Game die jeweilige Aufgabe.

Beispiele:

- Unsicher platziertes Passwort finden!
- Unversperrtes Gerät finden!
- Umgang mit sensiblen Dokumenten!

Die Aufgaben sind in einer zufälligen Abfolge zu bewältigen. Jeder Aufgabe ist ein Zeitlimit gesetzt. Aufgaben werden in 3 unterschiedlichen Schwierigkeiten erstellt. Das Spiel steigert sukzessiv die Schwierigkeit. Nach Erfolg oder Scheitern einer Aufgabe wird dem Spieler oder der Spielerin eine Risiko-Lernkarte präsentiert, welche durch einen Konzentrationstest bestätigt werden muss.

Szenerie der Micro-Games

Die Micro-Games sind einzelne virtuelle 3D Szene in der Form eines Schreibtisch Arbeitsplatzes. Szenen sind im Spiel wiederkehrend jedoch jeweils mit geänderten Details und Bedingungen.

Risiko-Lernkarten

Risiko-Lernkarten nach jedem Micro-Game vermitteln welchen Risiken Unternehmen durch Cyber Attacken ausgesetzt sind.

Konzentrationstest

Jede Risiko-Lernkarte muss durch einen Konzentrationstest bestätig werden. Angedacht ist eine eigene Testart pro Lernkarte. Testarten sollten sich durch kreative ungewöhnliche Interaktion unterscheiden.

Beispiele:

- Schüttle dein Smartphone um zu bestätigen das du das Risiko verstanden hast
- Drehe dein Telefon im Kreis um zu bestätigen das du das Risiko verstanden hast

Verfasser: Christoph Wögerbauer <christoph.woegerbauer@polycular.com>

Version: 2022-01-28

Motivationsmechanismen

Ziel des Spiels ist es möglichst viele Tage ohne Zwischenfälle zu erreichen.
→ X Tage ohne Zwischenfall!
Wobei sich die Tage als einzelne Micro-Games umschlüsseln.

Micro-Games werden mit einem Timer versehen (30 Sekunden). Der Zeitdruck kann gegebenenfalls sukzessive erhöht werden. Das heißt nach X Durchläufen verringert sich die Zeit auf z.B. 20 Sekunden.

Spielmodi

Endlos Modus mit Highscore

Im Falle eines Fehlers wird der Score (X Tage ohne Zwischenfall) einfach wieder auf 0 gesetzt. Arbeitsplatz kann aber auch als "sicher" markiert werden, sofern kein Risiko vorhanden ist oder das Risiko nicht gefunden wird.

Risiko-Lernkarten Modus

Eventuell einen Risiko-Lernkarten Modus. Durchklicken der Lernkarten alleine mit deren lustigen interaktiven Methoden zur Bestätigung.

Technische Herangehensweise

Die technische Herangehensweise beinhaltet die Evaluierung welche Webbasierten 3D Frameworks oder welche Game Engines mit Web-Exportmöglichkeiten in Frage kommen. Im weiteren Schritt wird evaluiert inwieweit Augmented Reality (AR) mit dem gewählten Framework / Game Engine über die WebXR API angesprochen werden kann.

Didaktische Herangehensweise

- Interner Workshop zur Konzeptfindung
- Recherche über Mitbewerber für Schulungen im Bereich Cyber Security, inklusive welche Themenbereiche diese behandeln
- Interne Themenwahl
- Durchführen von Expertengesprächen
- Interner Workshop zur Finalisierung des Konzepts
- Programmierung

Verfasser: Christoph Wögerbauer <christoph.woegerbauer@polycular.com>