CyberXScape

Endbericht | Call 15 | Projekt ID 5203

Inhalt

1 Einleitung

Das Thema Cybersecurity trifft immer häufiger Unternehmen, deren Mitarbeiterinnen und Mitarbeiter und uns alle als Privatpersonen. Die bisherigen Sicherheitsstrategien alleinstehend, wie abgeschlossene Firmennetzwerke und strikte Firewalls, funktionieren in der immer weiter vernetzten Welt nicht mehr ausreichend. Der Mensch ist immer öfter das Einfallstor für gezielte Cyberangriffe, welche auch zusehends personalisierter und ausgefeilter werden.

Gerade jetzt, wo Remote Arbeit- und Lernen immer mehr zum Alltag gehört, benötigt es Schulungsmaßnahmen, die jede Einzelne und jeden Einzelnen für das Cybersecurity Thema sensibilisieren. CyberXScape hält dabei die Barriere möglichst gering als web-basierte Schulung, die jeder ohne Download einer neuen App durchführen kann. Sei es zuhause im Wohnzimmer oder gemeinsam mit den Kollegen im Büro.

2 Projektbeschreibung

cyberXscape ist eine digitale spielbasierte interaktive Lernerfahrung zum Thema Cybersecurity.

In der aktuellen Fassung behandelt cyberXscape die Themen:

- Passwörter
- unversperrte Geräte
- sensible Daten

cyberXscape funktioniert als webbasierte XR Anwendung ganz ohne Download einer App.

2.1 Projektziele

Ziel ist ein webbasiertes Escape Game zur Sensibilisierung im Bereich Cyber Security. Das Spiel soll Basiswissen als Crashkurs in unterhaltsamerer weiße nachhaltig vermitteln. Anwendern sollen durch cyberXscape mehr Bewusstsein für die Risiken eröffnet werden. Auf unterhaltsame Weise sollen verschiedene Einfallstore im täglichen Büro-Alltag kennengelernt und mit kleinen Tipps und Tricks Strategien zur Vermeidung aufgezeigt werden.

Weiters solle das Projekt cyberXscape die Möglichkeiten für Extended Reality (XR) und im speziellen Augmented Reality (AR) und) im Web evaluieren. Die Hoffnung bestand, dass die WebXR Schnittstelle noch während der Projektlaufzeit einen Standard und entsprechende Verbreitung in den gängigen Browsern erreicht.

2.2 Zielgruppe

Zur Zielgruppe zählen alle die mit einem digitalen Umfeld in Berührung kommen. Ein Fokus liegt auf jenen, die im betrieblichen Kontext damit arbeiten, da dies der Bereich mit den höchsten

wirtschaftlichen Risiken und Schäden ist. Grundsätzlich soll cyberXscape für alle jene funktionieren, die Spaß an Unterhaltung und am Spielen haben. Es soll eine niederschwellige Einladung sein, sich mit dem Thema auseinander zu setzen und mögliche eigene Verhaltensmuster zu erkennen und zu verändern.

2.3 Projektergebnis

Das Projektergebnis ist ein kostenlos verfügbares online Spiel in einem Spielumfang von bis zu 10 Minuten. Das Spiel ist für die unterschiedliche Nutzung auf folgenden Geräten optimiert:

- Desktop Geräte mit Navigation mittels Tastatur + Maus
- Smartphones mit Navigation mittels Gyroskop Sensor + Touch (immersive Web)

Aufgrund des aktuellen Stands der Standardisierung sowie Stabilität in den Browser Implementierungen von Augumented Reality (AR) im WebXR Standard beinhaltet cyberXscape derzeit leider keine AR Funktionalität. Die Stabilität dieser Funktion ist für den produktiven öffentlichen Einsatz noch unzureichend. Die Entwicklung in Richtung Virtual Reality (VR) mittels WebXR Standard erscheint vielversprechender und wäre bereits möglich.

3 Verlauf der Arbeitspakete

3.1 Arbeitspaket 1 - *Detailplanung und Formales am Projektstart*

Der Projektstart verlief Dank des Kick-Offs, der Unterstützung der in Polycular in der Projektabwicklung bereits erfahrenen Kollegen und der zur Verfügung gestellten Vorlagen problemlos. Die Vorlage für das Projektcontrolling selbst bot eine gute Struktur und klare Anweisungen. Dadurch konnte das Thema von neuen Mitarbeitern eigenständig übernommen werden, die zwar schon ausreichend Projekterfahrung mitbringen, aber ursprünglich noch weniger Erfahrung mit dem Projektcontrolling und der Projektabwicklung hatten.

3.2 Arbeitspaket 2 - *Konzeption*

Beim Spielkonzept handelt es sich um die Beschreibung zu Handlung, Ablauf und Geschichte im finalen Spiel.

Haupttätigkeiten:

- Festlegung der Detail-Themen
- Festlegung Zielgruppenfokus
- Beschreibung Spielablauf
- Beschreibung Szenario
- Beschreibung Spielmotivation

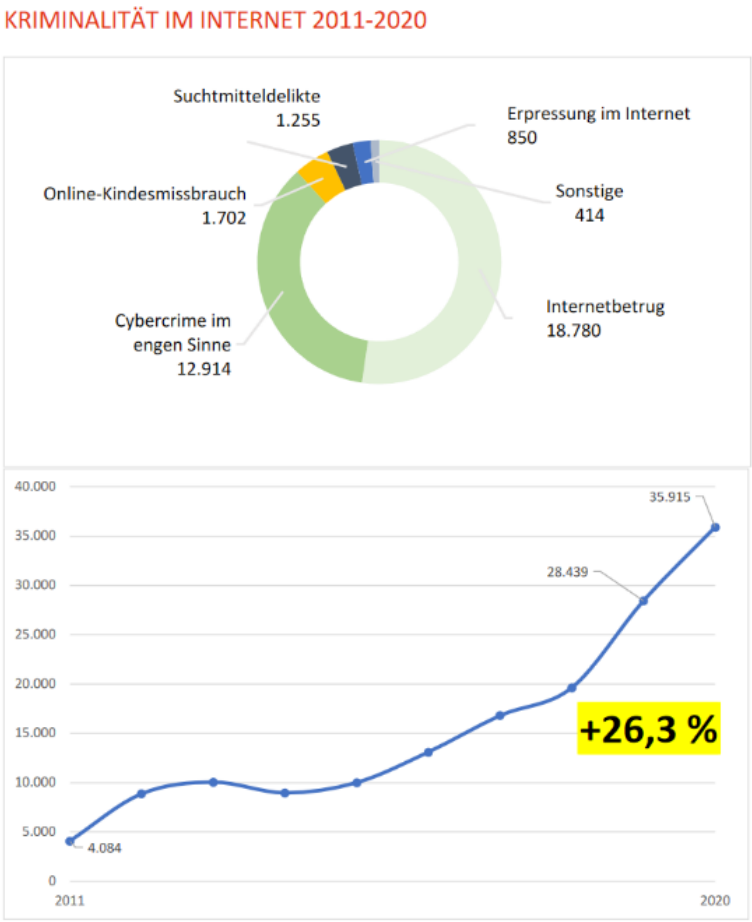
Festlegung der Detail-Themen

Für die Festlegung der Detail-Themen wurde eine umfangreiche Recherche unternommen, über welche Themen andere Anbieter von Schulungsmaßnahmen im Bereich Cyber Security behandeln. Dabei konnten wir rund 20 Anbieter eruieren bei welchen die Themen in ihrem Webauftritt oder ihrer Unterlagen ausreichend ersichtlich war.

Zusammenfassend bieten viele Anbieter zu ihren Schulungen auch Phishing Simulationen an. Ansonsten sind die Themenbereiche sehr vielfältig vom Datenschutz bis zu sicherem Umgang mit Social Media. Viele der Anbieter scheinen eine Tendenz zu technischen Details zu haben. Viele der Anbieter kommen auch aus dem klassischen IT-Bereich. Aber es gibt durchaus auch schon Anbieter mit gamifizierten Ansätzen.

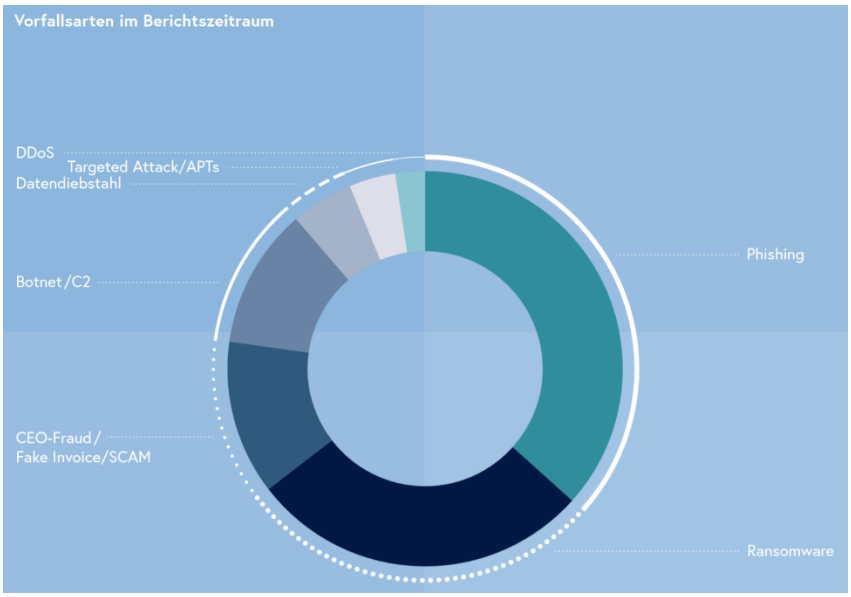
Weitergehend haben wir uns in aktuelle wissenschaftliche Publikationen und Statistiken eingelesen, welche sich mit dem Thema Cyber Security befassen. Folgend ein Auszug der Erkenntnisse aus den Publikationen.

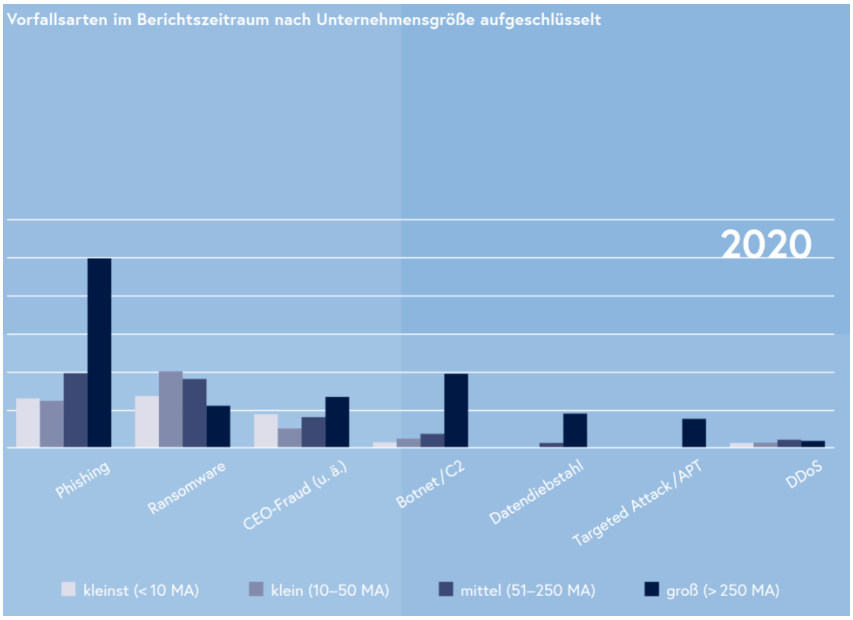
Österreich



Quelle: Überblick Kriminalitätsentwicklung 2020 (https://www.bmi.gv.at/bmi_documents/2607.pdf)

Als Hauptrisikofaktor wird nach wie vor der Mensch, d. h. „die Mitarbeitenden", angesehen. In den nächsten Jahren wird nach Einschätzung der befragten Unternehmen der Bedarf an Bewusstseinsbildung (Cyber-Awareness) für die Mitarbeiterinnen und Mitarbeiter stark steigen und es wird zu einer Weiterentwicklung der IT-Security-Services von derzeit eher technisch geprägten Bereichen hin zu einem gesamtheitlichen System mit Trainings- und Schulungsmaßnahmen kommen müssen.



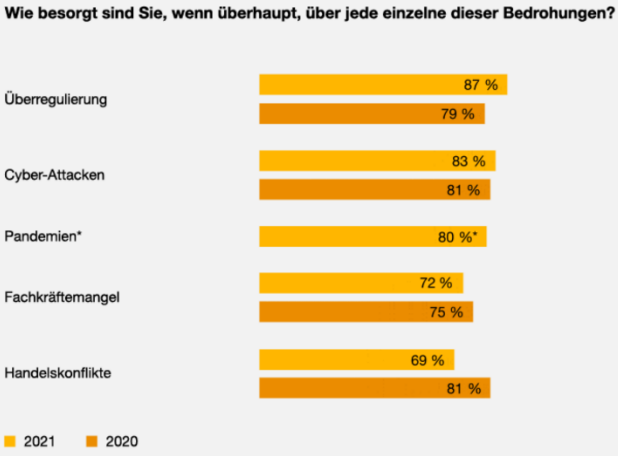


Quelle: Bericht Cyber Sicherheit für das Jahr 2020 (https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitsberichte/2020-BKA-Bericht-Cyber-Sicherheit-fuer-das-Jahr-2020.html)

Deutschland

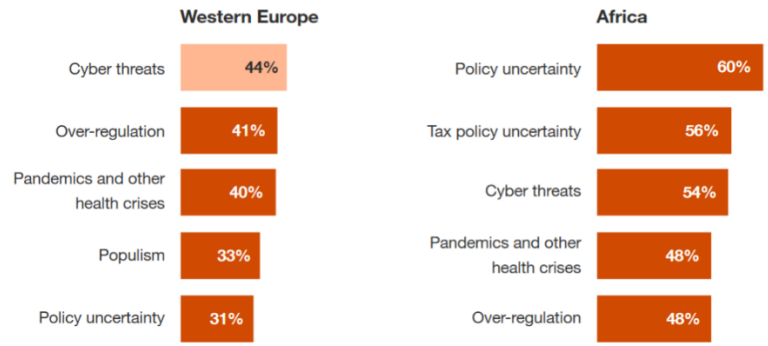
„Cybersicherheit kommt endlich dort an, wo sie hingehört: Ganz oben auf der CEO-Agenda. Die erhöhte Alarmbereitschaft ist ein gutes Zeichen, jedoch ist jetzt auch Handeln gefragt. Die Sicherstellung und Stärkung der Cyber-Resilienz durch regelmäßige Simulationen und Trainings sollte für jedes Unternehmen obligatorisch sein."

Holger Herbert, Cyber Security Leader bei PwC Deutschland



Question

How concerned are you, if at all, about each of these potential economic, policy, social, environmental and business threats to your organisation's growth prospects? (Showing only 'extremely concerned' responses)



Quellen:

https://www.pwc.de/de/im-fokus/cyber-security/ceosurvey.html

https://www.pwc.de/de/ceosurvey/pwc-24th-global-ceo-survey-2021.pdf

Von besonderem Interesse waren für uns auch noch folgende Publikationen:

- **Kennwortsicherheit**
  https://www.onlinesicherheit.gv.at/Services/Publikationen/Broschueren-und-Leitfaeden/2021-BVT-Kennwortsicherheit.html
- **Cyberangriffe gegen Unternehmen in Deutschland**
  https://kfn.de/wp-content/uploads/Forschungsberichte/FB_158.pdf

  Folgebefragung: *https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf*
- **Cybercrime Report 2019**
  https://bundeskriminalamt.at/bmi_documents/2552.pdf
- **CYBERSICHERHEIT ALS CHANCE – Cyberkriminalität und ihre Prävention bei kleinen und mittleren Unternehmen in Österreich**
  https://www.kfv.at/wp-content/uploads/2019/12/Cybercrime_KMU_2019-_HP.pdf
- **Cyber Security in Österreich 2021 – KPMG**
- **Bundeslagebild Cybercrime 2020**
  https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf?__blob=publicationFile&v=4

Vorauswahl von Detail-Themen

Kenne die Risiken

Das Bewusstsein der Risiken für Mitarbeiter ist essenziell, um dem Thema auch mit Verständnis entgegenzutreten. Warum muss mich das interessieren? Kann mein Job dadurch gefährdet werden?

Phishing & E-Mails

Sensibilisierung der Aufmerksamkeit für Phishing und Erkennen von gefälschten E-Mails. Vorschlag von getrennten E-Mail-Adressen (Accounts / Kommunikation).

Sichere Passwörter und sicherer Umgang

Eine unzureichende Absicherung oder ein zu einfaches Passwort ist immer noch eines der einfachsten Einfallstore.

Social Engineering

Warum schreibt mir mein Chef eine SMS für diese dringende Überweisung?

Risiken von gemischter Gerätenutzung

Wie konnte mein Sohn ein Abo auf dem Firmenaccount abschließen?

Erkennen & Melden von Vorfällen

Die Wichtigkeit einer schnellen Reaktion. Was passiert, wenn das Wochenende erst noch verstreicht?

Finale Auswahl von Detail-Themen

Zentral für das Game-Konzept wurden folgende 3 Themen ausgewählt:

- Kenne die Risiken
- Sicherer Umgang mit Passwörtern
- Versperren von Geräten

Ergänzend wurde versucht die anderen Themen im Kontext des Spielerlebnisses mitzutransportieren, ohne eine dedizierte Spielszene dafür zu entwickeln.

Festlegung Zielgruppenfokus

Grundsätzlich orientiert sich unsere Zielgruppe an der breiten Masse. Mit dem Thema sind Schüler*innen, Familien sowie Unternehmen allesamt betroffen. In weiterer Folge und für die Nachhaltigkeit des Projekts sehen wir für uns jedoch eine Chance den Fokus auf Mitarbeiterinnen und Mitarbeiter in kleinen und großen Unternehmen zu legen.

Aufgrund der umfangreichen Analyse der aktuellen Cybercrime Lage wissen wir, dass das Thema in Zukunft vor allem für Unternehmen, aufgrund der dadurch entstehenden Risiken, noch mehr an Brisanz gewinnen wird. Gemeinsam mit der Zielgruppe haben wir auch die Risiken eruiert mit welchen Unternehmen mit Cyber-Crime konfrontiert werden.

Risiken für Unternehmen

Betriebsstillstand

- verschlüsselte Daten
- gesperrte Systemzugänge (Accounts / Datenbanken / ...)
- Dienstverweigerung (Denial of Service - DoS)
  Beispiel: Ausfall Onlineshop.

Rechtliche Konsequenzen

- Veröffentlichung von sensiblen oder persönlichen Daten
- Schädigung der Kunden durch eingeschleusten Code (Viren, Trojaner, Malware, Ransomware, Spyware, Rootkits, Bots, ...)
  Beispiel: Bei Verkauf von digitalen Produkten / Maschinen / Geräten (SolarWinds).
- Weitere Strafzahlungen durch nachgewiesene Missstände
  Beispiel: DSGVO

Vorteil der Konkurrenz

- Wettbewerb gelangt durch Kauf oder aktiven Einbruch an Betriebsgeheimnisse (Spionage)

Finanzieller Verlust

- Entwendung von Geldern (Diebstahl)

Personenschäden

- Beeinträchtigung der Sicherheit von Maschinen oder Anlegen durch Manipulation

Fehlentscheidungen

- Durch Manipulation und gezielten Falschinformationen

Imageschaden

Game Design

Eine Abfolge von Micro-Games mit der Aufgabe des Findens von Sicherheitslücken oder Angriffsflächen zu einem der Themen.

Eine einfache Aufforderung erklärt 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

Virtuelle 3D Szene von Schreibtisch Arbeitsplatzen. Szenen sind im Spiel wiederkehrend jedoch jeweils mit geänderten Details und Bedingungen.

Motivation

Ziel des Spiels ist es möglichst viele Tage ohne Zwischenfälle zu erreichen.
→ X Tage ohne Zwischenfall!

Der Zeitdruck kann gegebenenfalls sukzessive erhöht werden.

3.3 Arbeitspaket 3 - *Prototyp*

Haupttätigkeiten:

- Eruieren der Limitationen der WebXR Schnittstellen
- Eruieren der möglichen technischen Herangehensweisen

Die WebXR API ist Stand heute (Jänner 2022) leider immer noch nicht standardisiert. Das heißt der Standard befindet sich immer noch in Entwicklung. Die Browser Hersteller arbeiten jedoch

schon an Implementierungen, diese wiederum können sich aber aufgrund des fehlenden Standards immer noch jederzeit ändern. Nur der Brower Chrome liefert bereits eine Implementierung, die ohne Zutun für Anwender aktiviert ist. Diese Implementierung erfordert jedoch ein ARCore fähiges Gerät sowie den Download der „Google Play Services for AR“ über den App Store. Der geschätzte Markt an ARCore fähigen Geräten scheint jedoch mit rund einer Milliarde bereits ansehnlich. Der Download der zusätzlichen „Play Service for AR“ aber eine große Hürde für die Nutzer:innen.

Der Fokus der WebXR Schnittstelle lag in den letzten Jahren vermehrt auf Virtual Reality (VR) Anwendungen. Aktuell wandelt sich der Fokus aber auch in Richtung des Augmented Reality (AR) Bereich. Die AR Implementierungen zeigen immer noch große Schwachstellen auf, die es für einen Produktiveinsatz einer größeren Anwendung im aktuellen Stadium noch in den Hintergrund rücken lässt. Die Verwendung von WebXR bereitet sich damit schwierig und ist leider immer noch nicht da angelangt, wo wir hofften, dass es im Jahr 2021 / 2022 sein könnte.

Aufgrund der Schwierigkeiten mit WebXR für AR Anwendungen beinhaltet unser Produkt derzeit keine AR Möglichkeit.

Als Kompromiss nutzt cyberXscape in der aktuellen Fassung auf mobilen Geräten zusätzlich den Gyroskop Sensor (immersive Web) als Navigationselement, was das Erlebnis interaktiver und spannender macht.

Für den Frontend 3D Teil wurden insgesamt die folgenden Frameworks evaluiert:

- PlayCanvas
- Wonerlandengine
- Godot
- Defold
- A-Frame (three.js)
- Babilon.js
- Phaser

3.4 Arbeitspaket 4 – *Entwicklung*

Die derzeitige Fassung von cyberXscape setzt auf das für uns bewährte Framework Phoenix (Elixir). Dabei kommt eine Technik zum Einsatz die Spielfortschritte mittels Websocket an das Backend kommuniziert. Der Frontend Teil der Anwendung setzt auf das 3D Framework A-Frame. Dieser Teil ist aber ebenfalls nahtlos in den Phoenix Backend Teil integriert. Das ermöglicht uns in der ersten Produktphase eine schnellere Weiterentwicklung.

3.5 Arbeitspaket 5 – *Marketing*

Unser Marketingkonzept sah vor, das wir in Phase 1 Experten im Bereich IT-Sicherheit mit ins Boot holen. Dies fand in der Form der bereits erwähnten Expertengesprächen statt. Über den Zugang von Experten an unserer Seite sehen wir eine größere Empfehlungschance unserer Lösung als Schulungs- / Bildungsmaßnahme für vernetzte Unternehmen / oder Kunden des Experten.

In Phase 2 haben wir aktiv Unternehmen, die wir bereits zu unseren Kunden zählen als Teil einer Produkt Beta-Phase mit in unsere Entwicklung mit aufgenommen. Dadurch war bereits vor der Veröffentlichung für der Bekanntheit von CyberXScape gesorgt.

In Phase 3 unseres Marketingkonzepts, nach Ende des Projekts, wollen wir Unternehmens-Trainer für das Thema gewinnen und ihnen unsere Lösung als attraktive Schulungsmaßnahme anpreisen.

Einen Pilot-Case im klassischen Bildungsbereich (Schulen) sehen wir im aktuell Projektzeitraum noch nicht vor. Um hier eine Überschneidung unserer Interessen zu gewährleisten, sehen wir mit dieser Ausrichtung Chancen für eine weitere nachhaltige Wertschöpfung, die es dann auch über den Kontakt mit Firmen ermöglichen wird mit einem Piloten im klassischen Bildungsbereich (Schulen) oder außerschulischen Bildungsbereich für Jugendliche Fuß zu fassen.

Wir haben in Summe vier Expertengespräche geführt welche uns enorm geholfen haben die wichtigsten Themen für cyberXscape dingfest zu machen. Die Experten waren angesiedelt im universitären Beriech, Dienstleistung IT-Sicherheit, IT-Leitung im Konzern sowie im Bereich Marketing Consulting spezialisiert für IT-Sicherheitsanbieter.

Über eine Beta-Phase von mehreren Monaten konnten wir internes, wie auch externes sammeln und gleich in den iterativen Entwicklungsprozess mit einfließen lassen.

3.6 Arbeitspaket 6 – *Dokumentation und Formales am Projektende*

Im Arbeitspaket 6 wurden die finalen Projektabgaben fertiggestellt und an netidee übermittelt. Alle öffentlichen Abgaben wurden auf die Projektwebsite hochgeladen. Mit dem Abschluss von Arbeitspaket 6 ist somit das Projekt vollständig dokumentiert und abgeschlossen.

4 Umsetzung Förderauflagen

Siehe Arbeitspaket 2 (Zielgruppe) und 5 (Marketing).

Zusammengefasst wollen wir über Projektabschluss hinaus auch mit Piloten im klassischen Bildungsbereich (Schule) Fußfassen und es wird an einem Marketing- und Businesskonzept gearbeitet, dass über Einnahmen und Unterstützung von Betrieben auch Workshops und Material in Form von Toolkits für den Bildungsbereich ermöglicht. Wir haben hier aus vorangegangenen Projekten (ÖkoGotschi, Escape Fake) positive Erfahrungen gemacht, dass besonders Unternehmen mit einer thematischen Nähe zum Projektthema Workshops und potenziell auch Weiterbildungen für Lehrende unterstützen.

Über dem Ansatz „Teach the Teacher“ können Bedenken abgebaut werden und so zu einer guten Verbreitung führen. Einen ähnlichen Ansatz verfolgen wir bereits mit unserem Projekt „Escape Fake“. Hier können wir die inhaltliche Nähe (im weitesten Sinne Digital Media Literacy) und Synergien der 2 Projekte nutzen.

5 Liste Projektendergebnisse

1	*Projektzwischenbericht*	*CC-BY-3.0 AT*	*netidee.at/cyberxscape*
2	*Projektendbericht*	*CC-BY-3.0 AT*	*netidee.at/cyberxscape*
3	*Entwickler_innen-DOKUMENTATION*	*CC-BY-3.0 AT*	*netidee.at/cyberxscape*
4	*Anwender_innen-DOKUMENTATION*	*CC-BY-3.0 AT*	*netidee.at/cyberxscape*
5	*Veröffentlichungsfähiger Einseiter*	*CC-BY-3.0 AT*	*netidee.at/cyberxscape*
6	*Externkommunikation*	*CC-BY-3.0 AT*	*netidee.at/cyberxscape*
7	*Konzept*	*CC BY 4.0*	*netidee.at/cyberxscape*
8	*Sourcecode cyberXscape / Cybercrime Escape Game*	*LGPL 3.0*	*github.com/polycular/cyber-x-scape_game*
9	*3D Asset Bundle*	*CC BY SA 4.0*	*netidee.at/cyberxscape*
10	*Website*	*CC BY 4.0*	*cyber-x-scape.at*
11	*Sourcecode placeholder website*	*ISC*	*github.com/polycular/cyber-x-scape_placeholder_website*

6 Verwertung der Projektergebnisse in der Praxis

Wir konnten bisher von allen Spielern viel positives Feedback sammeln. Die geringe Barriere das Spiel einfach mittels eines Browsers starten zu können kommt sehr gut an. Die Steigerung der Schwierigkeit schafft Lust zum Weiterspielen.

7 Öffentlichkeitsarbeit/ Vernetzung

- Interviews mit Experten
- Anführen des Projekts auf unserer Firmenwebsite: *polycular.com/portfolio/cyberxscape*
- Live schalten des Spiels: *cyber-x-scape.at*
- Aussenden des Spiels an die Expert:innen
- Aussenden des Spiels an interessierte Beta-Tester

Weitergehend ist die Vernetzung zu ÖIAT und der Plattform Saferinternet geplant. Erste Gespräche wurden im Dezember 2021 mit ÖIAT bereits geführt.

8 Eigene Projektwebsite

→ *cyber-x-scape*.at

9 Geplante Aktivitäten nach netidee-Projektende

Wir (Polycular) planen durch Vernetzung und Firmensponsorings weitere Cybersecurity Themen in cyberXscape behandeln zu dürfen sowie aber auch die aktuellen Themen durch weitere spannende Rätsel ergänzen zu können. Wir haben noch viele weitere gute Ideen in petto die cyberXscape noch spannender machen können.

Mit der aktuellen Pilot-Entwicklung wurde die Basis für einen weitere Entwicklungen innerhalb von Polycular geschaffen. Ein Teil der Ergebnisse können vor allem inhaltlich weiterverarbeitet werden.

Wir konnten rund um das Themengebiet digitaler Arbeitsplatz, Cyber-Security und Cyber-Crime und Desinformation zwei weiterführende Förderungen auf österreichischer-Ebene- ebenso wie auf EU-Ebene auf die Beine stellen. Damit ergibt sich die Möglichkeit über die Schiene digitaler Arbeitsplatz, schlussendlich mit weiteren Unternehmen in Kontakt zu kommen und so auch Unterstützung für cyberXscape zu erhalten. Zum anderen mit einem kommenden EU-Projekt zur Weiterentwicklung von „Escape Fake“ nicht nur diese App in der Entwicklung voran zu treiben, sondern mit unseren Partner auch die Vermarktung von „Escape Fake 2.0“ aber auch

cyberXscape in Schulen, Bibliotheken und außerschulischen Bildungseinrichtungen in der gesamten EU voran zu treiben.

10 Anregungen für Weiterentwicklungen durch Dritte

cyberXscape würde natürlich davon profitieren, wenn es in weiteren Sprachen übersetzt wird. Es bietet sich aber auch an cyberXscape im Bereich WebXR weiterzuentwickeln.

Der Bereich Virtual Reality (VR) sollte relativ einfach zu erschließen sein. Im Bereich Augmented Reality (AR) sind leider seitens der WebXR Standardisierung und Browser Implementierungen noch Hürden zu überwinden.

Als Game Development Studio würden wir uns aber natürlich auch freuen, wenn sich Entwickler aus unserem Umfeld an der Weiterentwicklung von A-Frame beteiligen oder ihnen die Möglichkeit besteht an der Standardisierung von WebXR mitzuwirken.