CyberXScape

Zwischenbericht | Call 15 | Projekt ID 5203

Inhalt

1 Einleitung

CyberXScape wird eine digitale spielbasierte interaktive Lernerfahrung zum Thema Cybersecurity. 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 will dabei die Barriere möglichst geringhalten und eine web-basierte Schulung schaffen, die jeder ohne Download einer neuen App durchführen kann. Sei es zuhause im Wohnzimmer oder gemeinsam mit den Kollegen im Büro. Dabei wird CyberXScape WebXR als Alternative zu in native Apps eingebundene XR-Lösungen enthalten welches die Interaktion räumlich, spannend und interaktiv macht.

2 Status der Arbeitspakete

2.1 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.

2.2 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 Szenario
- Beschreibung Geschichte & Spielablauf

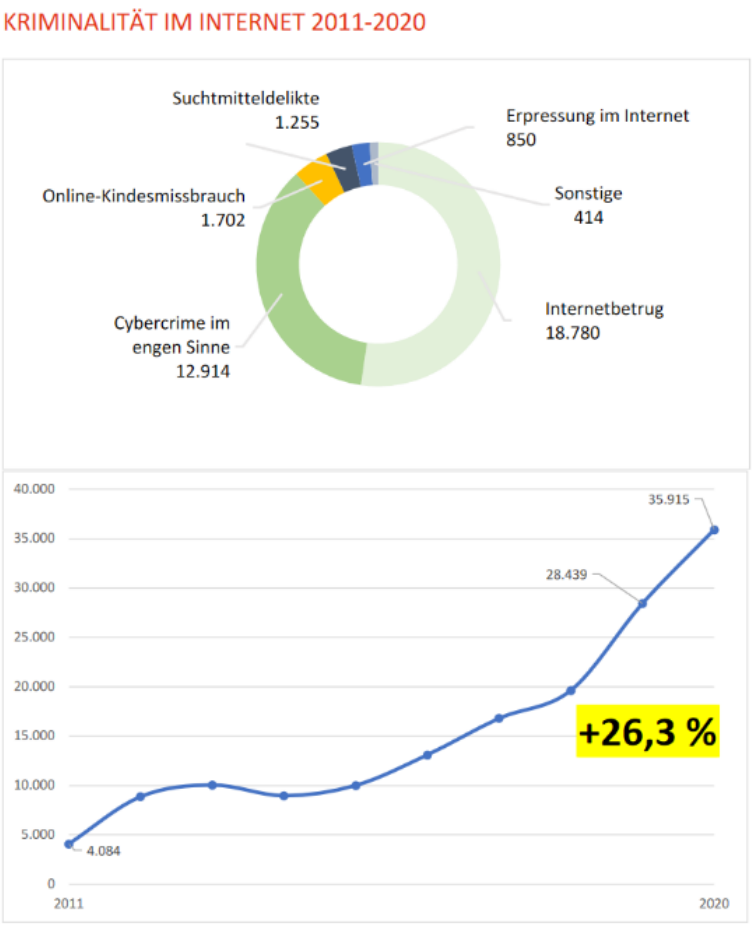
Festlegung der Detail-Themen

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.

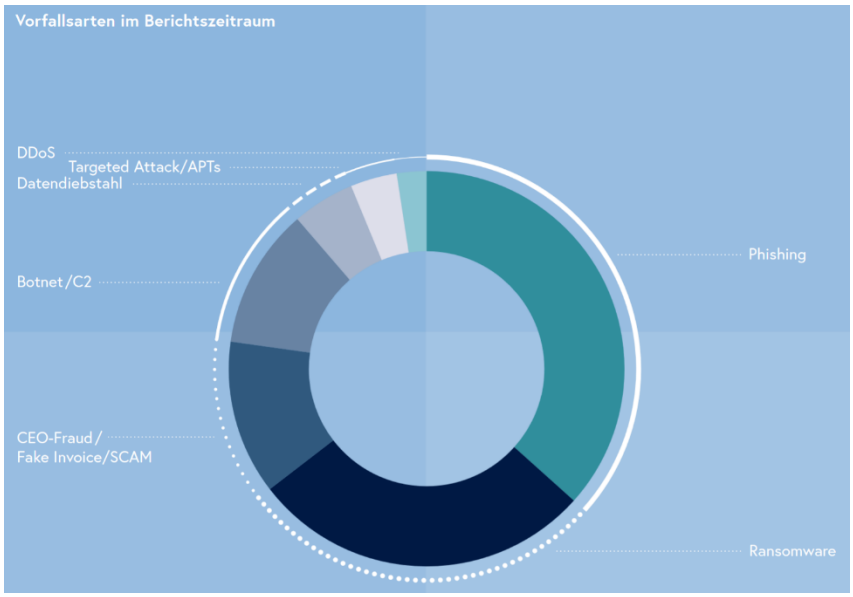
Weitergehend haben wir uns in aktuelle wissenschaftliche Publikationen und Statistiken eingelesen, welche sich mit dem Thema Cyber Security befassen. Folgend ein Auszug der Erkenntnisse aus den Publikationen.

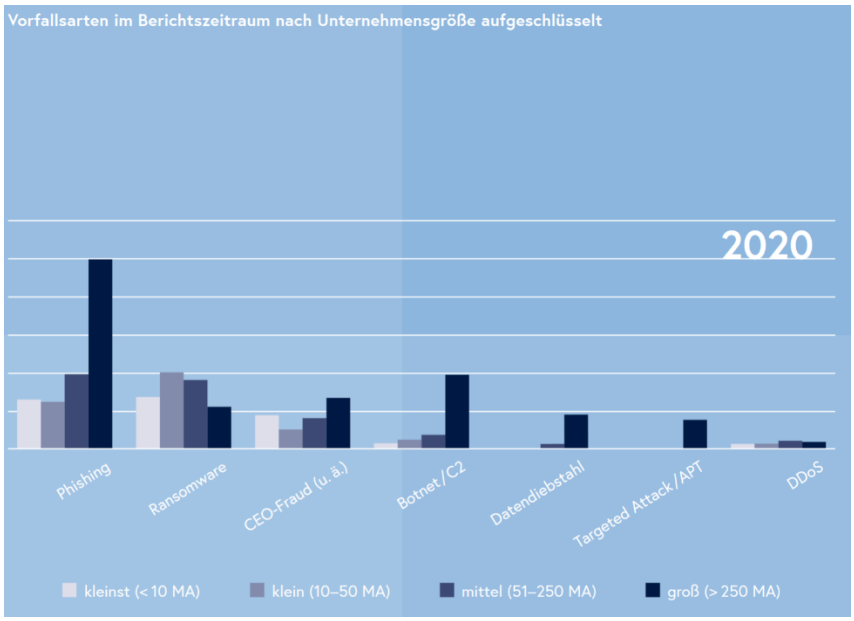
Österreich



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.



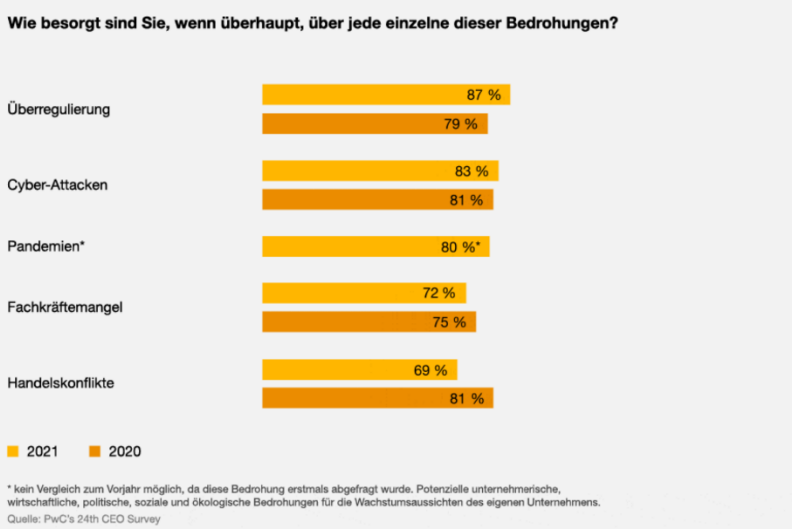


Quelle: Bericht Cyber Sicherheit für das Jahr 2020 (https://www.onlinesicherheit.gv.at/Services/Publikationen/Sicherheitsberichte/2020-BKA-Bericht-Cyber-Sicherheit-fuer-das-Jahr-2020.html)

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



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

1. Kennen der 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?
2. Phishing & E-Mails
   Sensibilisierung der Aufmerksamkeit für Phishing und Erkennen von gefälschten E-Mails. Vorschlag von getrennten E-Mail-Adressen (Accounts / Kommunikation).
3. Sichere Passwörter und sicherer Umgang
   Eine unzureichende Absicherung oder ein zu einfaches Passwort ist immer noch eines der einfachsten Einfallstore.
4. Social Engineering
   Warum schreibt mir mein Chef eine SMS für diese dringende Überweisung?
5. Risiken von gemischter Gerätenutzung
   Wie konnte mein Sohn ein Abo auf dem Firmenaccount abschließen?
6. Erkennen & Melden von Vorfällen
   Die Wichtigkeit einer schnellen Reaktion. Was passiert, wenn das Wochenende erst noch verstreicht?

Unsere Wahl der Detail-Themen ist derzeit noch nicht final. Wir haben eine Fragerunde vorbereitet die wir derzeit mit 3 – 5 Expertinnen und Experten im Gespräch diskutieren. Diese Gespräche

helfen uns die Detail-Themenwahl zu finalisieren. Die Gespräche sind ebenfalls auch Teil unseres Marketingkonzepts.

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

Beschreibung Szenario, Geschichte & Spielablauf

Unsere Ideen zum Szenario, Geschichte & Spielablauf sind derzeit noch nicht final. Wir planen in den nächsten 2 Wochen eine interne Runde in welcher wir das gemeinsam als Team finalisieren.

2.3 Arbeitspaket 3 – *Prototyp*

Haupttätigkeiten:

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

Die WebXR API ist Stand heute (August 2021) 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 Fokus der WebXR Schnittstelle lag in den letzten Jahren vermehrt auf VR Anwendungen. Aktuell wandelt sich der Fokus aber auch in Richtung des 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 sein könnte.

Aufgrund dieser Gegebenheit wird unser Produkt auf AR.js eine unabhängige Bibliothek für AR im Web setzen. Unsere Tests haben gezeigt, dass derzeit AR.js die besten Ergebnisse liefert.

Aufgrund der Schwierigkeiten mit WebXR für AR Anwendungen wird unser Produkt womöglich nur einen kleineren AR Anteil als ursprünglich gedacht beinhalten und verstärkt auf andere Ansätze von WebXR setzen. Damit wir trotzdem das Thema Cybersecurity gut abdecken können und ein Produkt liefern können, das über einen reinen Prototypenstatus hinausgeht, müssen wir diesen Kompromiss eingehen.

2.4 Arbeitspaket 4 – *Entwicklung*

Wir befinden uns aktuell erst am Anfang der Entwicklungsphase. Unsere Frontend Architektur wird auf das Framework A-Frame in Zusammenhang mit AR.js setzten. Wir haben aktuell ein internes Frontend Projekt zum Start der Entwicklung bereitstehen.

Unser Backend wird das für uns bereits bewährte Framework Phoenix (Elixir) verwenden.

2.5 Arbeitspaket 5 – *Marketing*

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

In Phase 2 werden wir aktiv Unternehmen, die wir bereits zu unseren Kunden zählen als Teil einer Produkt Beta-Phase mit in unsere Entwicklung mit aufnehmen. Dadurch wird bereits vor der Veröffentlichung an der Bekanntheit von CyberXScape gearbeitet.

In Phase 3 unseres Marketingkonzepts 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.

Die eigene Projektwebsite (cyber-x-scape.at) ist online. Kontaktherstellung zu mehreren Experten (Thema IT-Sicherheit) ist derzeit am Laufen. Das Projekt wurde auf unserer eigenen Website mit angeführt (polycular.com/portfolio/cyberxscape).

Wir sind bereits am Sammeln von zusätzlichen Nutzern die Lust haben in unser Beta-Phase CyberXScape zu testen.

2.6 Arbeitspaket 6 – *Dokumentation und Formales am Projektende*

Im Arbeitspaket 6 haben wird aktuell noch keine Fortschritte zu berichten.

3 Umsetzung Förderauflagen

Im Marketingkonzept Pilot cases im Bildungsbereich überlegen, um Verwertungschancen zu erhöhen

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.

4 Zusammenfassung Planaktualisierung

- Projektergebnisse: Ergänzung von weiteren Webadressen der Veröffentlichung
- Projektergebnisse: Anpassung der Fertigstellungsgrade
- Arbeitspakete: Anpassung der Fertigstellungsgrade
- Stundendokumentation: Eintrag der zwischenzeitlich geleisteten Stunden

Im Arbeitsplan kam es zu einer kleinen Anpassung. Der für Ende Juli geplante Zwischenbericht wurde erst mit September fertiggestellt, da erst jetzt 50% der Projektkosten angefallen sind. Um einen guten Abschluss für das Projekt zu gewährleisten ist nun Dezember 2021 das geplante Projektende. Nach Möglichkeiten wird versucht mit Ende Dezember auch noch den Endbericht einzureichen, es kann allerdings dazu kommen, dass der Endbericht erst Anfang Jänner fertiggestellt wird.

5 Öffentlichkeitsarbeit/ Vernetzung

- Kontaktaufnahme und Interviews mit Experten ist derzeit am Laufen
- Eigene Projektwebsite ist online: *cyber-x-scape.at*
- Projekt wurde auf unserer Firmenwebsite ebenfalls angeführt: *polycular.com/portfolio/cyberxscape*
- Der Plan künftiger Aktivitäten ist bereits im Punkt 3. – Umsetzung Förderauflagen als Teil des Marketingkonzeptes erläutert.

6 Eigene Projektwebsite

→ *cyber-x-scape.at*