



netidee

PROJEKTE

KMU digi sicher: Digitale Selbstverteidigung für KMUs

Zwischenbericht | Call 18 | Projekt ID 6773

Lizenz: CC BY 4.0

Inhalt

1	Einleitung.....	3
2	Status der Arbeitspakete	3
1.1	Arbeitspaket 1 - <Detailplanung, Formales am Projektstart>.....	3
1.2	Arbeitspaket 2 - <Konzeption der E-Learning Inhalte>.....	3
1.3	Arbeitspaket 3 - <Konzeption des Workshops>.....	6
1.4	Arbeitspaket 4 - <Abhalten von Test Workshops>.....	6
1.5	Arbeitspaket 5 - <Erstellung der finalen Versionen>.....	7
1.6	Arbeitspaket 6 - <Dokumentation am Projektende>.....	7
3	Zusammenfassung Planaktualisierung.....	7
4	Öffentlichkeitsarbeit/ Vernetzung.....	7
5	Eigene Projektwebsite.....	8

1 Einleitung

Ob im Privaten oder in der Arbeit, wir hinterlassen überall Datenspuren, für die sich viele interessieren. Seit geraumer Zeit geraten KMUs zunehmend ins Visier von Kriminellen. Das bedeutet für betroffene Unternehmen: Betrug, Erpressung, finanzielle Verluste und, im schlimmsten Fall den Verlust von Geschäftsgrundlagen. Mit dem E-Learning-Tool (OER) & maßgeschneiderten Workshops zur „Digitalen Selbstverteidigung für KMUs“ bieten wir Wissen und Kompetenzvermittlung zum Selbstschutz. Praxisnah. Flexibel. Interaktiv.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 - <Detailplanung, Formales am Projektstart>

Das Arbeitspaket 1 wurde zeitgerecht Anfang Dezember 2023 abgeschlossen und mit dem Projektplan an netidee.at übermittelt. Dieses Paket umfasste speziell die Zeiteinteilung und Aufteilung an die mitarbeitenden Personen. Insgesamt arbeiten 6 Personen an dem Projekt, mit unterschiedlichen Fachbereichen wie Admin, E-Learning Inhalte und Workshop-Konzept. Zur Vorstellung des Projektes hat Daniel Lohninger den ersten Blogpost für netidee verfasst. Es wurden drei weitere Blogposts von Felix Riedl-Riedenstein veröffentlicht die einen Einblick in die Arbeit des Teams geben.

2.2 Arbeitspaket 2 - <Konzeption der E-Learning Inhalte>

Bei der Gründung der epicenter.academy war der Fokus auf Jugendliche gerichtet und deren Fähigkeiten ihre eigenen Daten durch digitale Selbstverteidigung zu schützen. Bei der Ausgestaltung der Workshop-Inhalte wurde darauf geachtet altersspezifische Methoden und Sprache zu verwenden. Die Zielgruppe ist hier zwischen 14 und 21 Jahren alt. Daher waren die Tätigkeiten im ersten Arbeitspaket auf die Weiterentwicklung unserer bestehenden Inhalte gerichtet. Wir haben analysiert welche Strukturen, Inhalte und Fallbeispiele wir ändern und ergänzen müssen.

Anfänglich wurden die Struktur-Elemente für die E-Learning Kapitel ausgearbeitet. Genauer ging es hier um die Frage wie die verschiedenen Angebote für Jugendliche und KMUs auf der Website epicenter.academy am besten präsentiert werden können. Ziel ist es das E-Learning so übersichtlich wie möglich für alle interessierten Personen zu gestalten. Egal ob Jugendliche oder Unternehmer:innen, der Weg zu den relevanten Kapiteln soll so einfach und niederschwellig wie möglich sein. Eine weitere strukturelle Entscheidung musste bei der Definition der verschiedenen Kapiteln getroffen werden. Da die

inhaltlichen Schwerpunkte anders sind wurde analysiert welche Kapitel gekürzt, zusammengelegt oder erweitert werden müssen.

Der arbeitsintensivste Tätigkeit im Arbeitspaket 2 war die Definition von inhaltlichen Schwerpunkten mit Relevanz für KMUs. Bei dieser hat das Team sowohl bestehende Inhalte weiterentwickelt als auch neuen Kapitel erstellt. Für KMUs liegt der Schwerpunkt von digitaler Selbstverteidigung bei Onlinekriminalität und ihren verschiedenen Formen, weshalb der Schutz von Daten im persönlichen Gebrauch etwas weniger Platz hat. Hier liegt auch der inhaltliche Unterschied zu dem bereits existierenden E-Learning für Jugendliche.

Daher hat das Team an Inhalten gearbeitet die Unternehmer:innen und Mitarbeiter:innen aufklären welche Arten von Angriffen auf IT-Infrastruktur es gibt und wie sich Unternehmer:innen und Mitarbeiter:innen selbst vor Angriffen auf die IT-Systeme der Unternehmen schützen können. Das inkludiert Kapitel wie Phishing, Passwörter, Verschlüsselung, Digitale Kriminalität, Geräte sicherer machen und sicher Kommunizieren. Während diese Kapitel weiterentwickelt wurden sind auch neue Kapitel entstanden um thematische Lücken zu schließen. Speziell sicheres, endgültiges Löschen von Daten und Künstliche Intelligenz haben sich aufgedrängt und wurden konzipiert.

KI ist in aller Munde aber für unser Projekt aus zwei Gründen relevant: Erstens, diese Technologie wird immer stärker von kriminellen Organisationen bei Angriffen auf Unternehmen eingesetzt. Zweitens, es gibt viele unterschiedliche Informationen über die KI-Produkte und Dienstleister die mit ihren Services viel versprechen. Nicht alle Angebote sind aber seriös und es gibt einige Gefahren für Personen und Unternehmer:innen die solche Produkte einsetzen. Ziel des neuen Kapitels ist es daher die Grundlagen der Technologie zu erklären, damit Personen fundierte Entscheidungen beim Einsatz von KI-Produkten treffen können. Zusätzlich wird es Inhalte zu Deepfake-Phishing geben um dieser neuen und rasant zunehmenden Betrugsvariante gerecht zu werden.

Neben der theoretischen Ausarbeitung war es wichtig konkrete Fallbeispiele aus der Praxis in die Kapitel einzuarbeiten, da wir das E-Learning und die Workshops so relevant wie möglich für KMUs gestalten wollen. Eine gute Informationsquelle für die Anzahl und Art der Angriffe ist der Cybercrime Report des Innenministeriums und größere Studien die Cybercrime untersuchen. Es gibt auch immer wieder Artikel in verschiedenen Fachzeitschriften und Tageszeitungen die konkrete Beispiele von Angriffen, Phishing und die Betroffenen darstellen. Anhand dieser Beispiele wurden möglichst anschauliche Fallbeispiele in die Kapitel aufgenommen um die theoretischeren, abstrakteren Hilfestellungen und Erklärungen des E-Learnings und der Workshops zu ergänzen.

Ein wichtiger Teil der jeweiligen Kapitel sind die Praxis- und Merkbboxen, da sie das Wissen aus den Texten ergänzen. Für die Zielgruppe der KMUs ist es wichtig diese Elemente in Hinblick auf beruflichen Alltag zu erweitern. Die Praxisboxen

sollten interaktiv sein und User:innen dazu bringen Dinge selber auszuprobieren. Teil solcher Boxen sind beispielsweise Übungen wie ein Phishingsimulator u.a. Übungsmöglichkeiten. Dadurch kann ein:e Unternehmer:in jetzt die verschiedenen Taktiken solcher Angriffe selber testen.

Wir melden mit Freude, dass wir durch die dargelegte Vorgangsweise das Arbeitspaket 2 erfolgreich abgeschlossen haben. Die technische Umsetzung auf unserer Website ist jetzt durch eine Lösung mit einer zusätzlichen Übersichtseite für das E-Learning umgesetzt. Diese ermöglicht eine Trennung von dem bisherigen E-Learning für die Zielgruppe Jugendliche und der neuen Umsetzung für Unternehmen. Das bedeutet neue Kapitel können laufend eingepflegt und live geschallten werden, wenn die Inhalte fertig an die Zielgruppe angepasst sind.

Ebenso ist die Struktur der Kapitel gemacht und definiert welche neuen Inhalte in für die KMUs angeboten werden. Zwei Lücken in unseren Kapitel wurden bei der Analyse gefunden und erfolgreich geschlossen. Die Kapitel „sicheres, endgültiges Löschen von Daten“ und Künstliche Intelligenz sind bereits online.

In dem Kapitel sicheres, endgültiges Löschen von Daten ist der Fokus auf die technisch sichere Vernichtung von digitalen Daten auf Datenträgern. Für Unternehmen ist es ebenso wichtig ihre Datenträger am Ende des Verwendungszeitraums richtig zu entsorgen und alle Daten zu löschen, wie während der Benutzung darauf zu achten. Ohne fachgerechtes Löschen kann nicht gewährleistet werden, dass sich „neugierigen Dritten“ Zugang zu Betriebsgeheimnissen, sensiblen Daten von Kund:innen oder Informationen von Mitarbeiter:innen verschaffen.

Das Kapitel Künstliche Intelligenz ist, wie bereits oben beschrieben, momentan in aller Munde und es gibt eine Flut an neuen Anwendungen. Durch die Veröffentlichung wollen wir Unternehmer:innen einen Anhaltspunkt geben anhand dem sie Entscheidungen treffen können. Daher wollen wir ein Grundwissen vermitteln damit selbständig gute Entscheidungen getroffen werden können. Da das Themenfeld sehr groß ist und sich laufend weiterentwickelt ist hier das Feedback von den Unternehmen im Arbeitspaket 4 besonders wichtig.

Neben den neuen Kapiteln sind auch bestehende Kapitel umgeschrieben und im Backend bereit veröffentlicht zu werden. Es fehlt wie in Arbeitspaketen 4 und 5 beschrieben noch Feedback von Unternehmen um diese abschließend zu veröffentlichen. Wir haben uns dazu entschlossen Passwörter und Sicher Kommunizieren neben den zwei Hauptkapiteln zu Kriminalitätsformen zu priorisieren, da sie einerseits die zentralen Informationen zum Absichern von Onlinekonten und Authentifizierungen enthalten. Außerdem ist das Kapitel zu sicher Kommunizieren besonders relevant um die Kommunikation firmenintern und mit Kunden und Geschäftspartnern vertraulich zu halten.

Ein weiterer Erfolg war die sehr interessante Recherche und Gespräche über praxisnahe Fallbeispiele im Bereich der digitalen Sicherheit. Mit

Unternehmer:innen und Arbeitnehmer:innen konnten wir häufig auftretende Probleme und Fragen definieren auf die wir in unserem E-Learning und Workshopkonzept eingehen wollen.

Insgesamt haben wir in dem Arbeitspaket unsere Ziele gut erreicht und mussten nicht von dem ursprünglichen Plan abweichen. Mit der Erstellung der neuen Kapitel, der Weiterentwicklung der bestehenden und dem stärkeren Fokus auf Praxisbeispielen haben wir ein gutes Konzept erarbeitet. Wie in Arbeitspaket geplant werden wir dieses Konzept 2025 testen und Feedback einholen. Anhand dessen können wir dann das finale E-Learning erstellen.

2.3 Arbeitspaket 3 - <Konzeption des Workshops>

Aufbauend auf den gewonnenen Erkenntnissen bei der Ausarbeitung der E-Learning Kapitel hat das Team angefangen das Konzept für Workshops mit Unternehmen zu erstellen.

Die spezielle Herausforderung bei der Konzeption des Workshops ist die zeitliche Begrenzung. In unserem E-Learning haben wir Platz und Zeit Themen ausführlich aufzubauen und gehen nicht davon aus das Besucher:innen den gesamten Inhalt auf Einmal durchgehen. Im Gegensatz dazu haben wir im Workshop nur eigenen ganz konkreten Zeitraum in dem wir die Inhalte vermitteln können.

Daher steht am Beginn die inhaltliche Analyse um festzulegen was im Workshop unbedingt behandelt werden muss und welche Punkte, mit Verweis auf das E-Learning, nicht. Für diesen Prozess haben wir für die Teilnehmer:innen des Workshops konkrete Lernziele definiert: Die Unternehmer:innen und Arbeitnehmer:innen von KMUs die unseren Workshop besuchen sollen durch grundlegendes Wissen in digitaler Selbstverteidigung bessere und sicherere Handlungsentscheidungen im Alltag treffen um sich und ihr Unternehmen zu schützen. Das inkludiert auch konkrete Tipps die sie in ihren beruflichen Alltag mitnehmen können. Hierfür haben wir eine Matrix mit den Lernzielen für die unterschiedlichen Kapitel definiert, die die unterschiedlichen Kompetenzbereiche berücksichtigt. Um die Zeit in den Workshops bestmöglich zu nutzen werden die Lernziele und Schwerpunktsetzung für jedes Unternehmen außerdem in einer Bedarfsanalyse mit den Verantwortlichen erhoben und ein maßgeschneidertes Bildungsangebot erstellt.

Nach rund einem Drittel der geplanten Stunden haben wir, neben den Lernzielen, auch die Struktur und die groben Inhaltsblöcke für die Kapitel festgelegt. Die Kapitel mit besonderem Fokus sind Passwörter, Phishing, Geräte sicher machen und sicher Kommunizieren. Andere wie warum Datenschutz werden weniger stark im Fokus sein.

2.4 Arbeitspaket 4 - <Abhalten von Test Workshops>

Bereits im Sommer haben wir an der Umsetzung von Arbeitspaket 4 begonnen. Damit wir für die Akquise von Unternehmen gut vorbereitet sind steht jetzt ein Buchungstool für die Akquise auf der Website zur Verfügung. Dieses Buchungstool ist wichtig um die Terminisierung und Koordination von Workshops im Arbeitspaket 4 effizient umzusetzen.

Bei der Recherche nach dem besten Buchungstool ist das Team auf einige Widerstände gestoßen, da es nicht einfach ist ein datenschutzkonformes Angebot zu finden. Es wurden über 50 Tools analysiert und nur zwei waren wirklich datensparsam genug um unseren Ansprüchen zu genügen. Das besser zu unseren Anforderungen passende haben wir ausgewählt, aufgesetzt. Die technische Implementierung hat auch funktioniert, weshalb das Buchungstool schon voll funktionstüchtig ist und wir jetzt voll ausgerüstet sind für den Start der Akquise Anfang 2025.

2.5 Arbeitspaket 5 - <Erstellung der finalen Versionen>

Das Arbeitspaket wurde noch nicht begonnen, es wird wie vorhergesehen Anfang 2025 gestartet.

2.6 Arbeitspaket 6 - <Dokumentation am Projektende>

Das Arbeitspaket wurde noch nicht begonnen, es wird wie vorhergesehen im am Ende der Konzeption im Herbst 2025 damit gestartet.

3 Zusammenfassung Planaktualisierung

Die einzige wirkliche Abweichung und Aktualisierung ist der etwas frühere Start für Arbeitspaket 4. Das Buchungstool ist wichtig für die Akquise der Unternehmen, weshalb wir uns genug Zeit geben wollten einen guten Anbieter zu finden und die technische Implementierung auf der Website umzusetzen. Hier hat sich der Sommer angeboten, da in den Schulferien mehr Kapazitäten im Team frei sind. Viele unserer momentan gebuchten Workshops finden in Schulen statt, weshalb der Herbst und Winter weniger Termine bietet um eine tiefgründige Recherche zu machen.

Weiter wird in dem zweiten Teil unserer Umsetzung eine Personaländerung merkbar werden. Leonie Brög hat mit Ende Oktober die epicenter.academy GmbH verlassen und Arthur Spiess ist neu eingestellt worden. Er wird zukünftig anstelle von frau Brög an dem Projekt arbeiten.

4 Öffentlichkeitsarbeit/ Vernetzung

Die Trainer:innen der epicenter.academy sind immer wieder auf Veranstaltungen und auf Podiumsdiskussionen wenn es um das Thema Digitalisierung und damit

verbunden die Sicherheit von Benutzern geht. Beispiel dafür war die Veranstaltung „Bildung und Ausbildung in Zeiten Künstlicher Intelligenz“¹. Im Zuge dessen tauscht sich das Team gerne mit Unternehmer:innen und Arbeitnehmer:innen über deren Herausforderungen im beruflichen Alltag aus. Auf den Social Media Kanälen von epicenter.academy werden solche Auftritte gerne kundgetan. Noch wichtiger sind Social Media Posts die unser E-Learning und die neuen Inhalte bewerben. Wir wollen das möglichst viele Personen auf die unser frei zugängliches E-Learning stoßen und von ihr Gebrauch machen. Auch durch unsere starke Präsenz in Schulen ist unser momentanes E-Learning gut besucht. Wir erhoffen uns ähnliche Zahlen für das neue E-Learning für KMUs. Im besten Fall werden sich die beiden Seiten gegenseitig Aufmerksamkeit bringen.

Ebenso haben wir unsere regelmäßigen Blogposts breit über unsere Social Media Kanäle beworben.

5 Eigene Projektwebsite

Wie bereits angesprochen wird das E-Learning auf der Website von epicenter.academy frei zugänglich sein: <https://epicenter.academy/>

1 <https://www.youtube.com/watch?v=eFTR-qKWrKo>