KMU digi sicher: Digitale Selbstverteidigung für KMUs

Endbericht | Call 18 | Projekt ID 6773

Inhalt

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.

Projektbeschreibung

Beschreibung der Projektziele / Zielgruppe und inhaltlicher Überblick über das Projektergebnis (max. 5 Seiten)

Die epicenter.academy GmbH entstand aus einem Vereinsprojekt von epicenter.works (Grundrechtsorgansiation), das vom AK NÖ Projektfonds "Arbeit 4.0" 2022/2023 finanziert wurde. Die Zielgruppe war damals ausschließlich Schülerinnen und Schüler (14-19 Jahre). Aufgrund der massiven Gefährdung von KMUs lt. Cybercrime Report 2022 des BMI, war es unser Ziel das Ausbildungsprogramm der epicenter.academy GmbH zu erweitern, um für die Zielgruppe der KMUs sowie auch NGOs eine Ressource zum Thema: „IT- und Datensicherheit“ zu schaffen.
KMUs, EPUs und auch Nichtregierungs-Organisationen bilden das starke Rückgrat der österreichischen Wirtschaft. Wir wollten mit dem Projekt einen niederschwelligen Wissenstransfer speziell für kleinere Unternehmen und Organisationen schaffen, um die Inhalte laufend, gemäß der digitalen Entwicklungen, ergänzen zu können.

Durch die netidee-Teilförderung des Projektes wurde bei Vertragsunterzeichnung gemeinsam mit der Geschäftsleitung der netidee vereinbart, die ursprüngliche Laufzeit von einem Jahr bis Ende 2025 zu strecken, um das Projekt neben dem laufenden Betrieb der epicenter.academy GmbH in Ruhe umsetzen zu können.

Um eine praxistaugliche E-Learning-Struktur für KMUs, EPUs und NGOs zu entwickeln, waren viele Gespräche mit den Zielgruppen sowie Recherchetätigkeiten nötig. Es war uns wichtig, die Struktur so zu konzipieren, dass sie einfach im Berufsalltag der Zielgruppen einsetzbar ist und trotzdem, durch Interaktionen, leicht verständlich bleibt.

Schlussendlich stellte sich heraus, dass neben der allgemeinen Einführung ins E-Learning und dem Glossar der wichtigsten Begrifflichkeiten zu dem Thema, ein Cluster von 4 Hauptgruppen für die gewünschte Zielgruppe am praktikabelsten ist.

1. Sicher kommunizieren
2. Gute und schlechte Passwörter
3. Phishing
4. Digitale Kriminalität
5. Sicheres, endgültiges Löschen von Daten

Das Kapitel **„Sicher kommunizieren“** vermittelt Unternehmen und deren Mitarbeiter:innen die grundlegenden Risiken unsicherer Kommunikationskanäle und erklärt, warum diese für vertrauliche Inhalte ungeeignet sind. Es führt in zentrale Verschlüsselungstechniken ein, insbesondere in die Ende-zu-Ende-Verschlüsselung, die verhindert, dass Dienstanbieter:innen oder Dritte Nachrichten mitlesen können. Zudem werden datenschutzfreundliche E-Mail-Anbieter, sichere Messenger-Dienste und die Nutzung von PGP für verschlüsselte E-Mails vorgestellt. Ergänzend beschreibt das Kapitel konkrete, praxisnahe Schritte, mit denen Unternehmen ihre interne und externe Kommunikation schützen können, darunter die Auswahl geeigneter Tools, die Sensibilisierung von Mitarbeiter:innen und die strukturierte Bewertung der bestehenden Kommunikationswege. Ziel ist es, Unternehmen in die Lage zu versetzen, ihre digitale Kommunikation nachhaltig vor unbefugtem Zugriff zu sichern.

Das Kapitel **„Gute und schlechte Passwörter“** erklärt, warum starke und gut verwaltete Passwörter eine zentrale Rolle für die IT-Sicherheit von Unternehmen spielen. Es behandelt, wie Authentifizierung grundsätzlich funktioniert — dass man sich entweder durch Wissen (Passwort/PIN), Besitz (z. B. Gerät, Token) oder biometrische Merkmale identifiziert — und stellt da hinein die Bedeutung sicherer Passwörter.
Weiterhin legt das Modul dar, wie Passwörter typischerweise geknackt werden — z. B. durch Brute-Force bzw. Wörterbuchattacken oder durch Phishing und Social Engineering — und warum einfache, kurze oder mehrfach verwendete Passwörter besonders gefährdet sind.

Als Antwort darauf leitet das Kapitel wichtige Kriterien für sichere Passwörter ab: Sie sollten lang, komplex (alphanumerisch, mit Sonderzeichen) und einzigartig pro Dienst sein; idealerweise als weniger merkbare, aber sichere Passphrase. Außerdem wird der Einsatz eines Passwortmanagers empfohlen, um viele unterschiedliche Passwörter sicher und bequem zu verwalten.

Zusätzlich erläutert das Kapitel Schutzmaßnahmen und gute Praktiken für den Fall, dass ein Zugang kompromittiert wurde — z. B. das Passwort ändern, alle Zugriffe prüfen, Zweifaktor-Authentifizierung aktivieren und gegebenenfalls andere verbundene Accounts absichern.

Insgesamt bietet „Gute und schlechte Passwörter“ Unternehmen ein klares Verständnis dafür, wie man sichere Zugangsdaten erstellt und verwaltet, wie

man häufige Angriffswege erkennt und wie man sich langfristig vor unberechtigtem Zugriff auf Unternehmens- oder Kundendaten schützt.

Das Kapitel **„Phishing“** erläutert, wie Online-Betrüger:innen mit fingierten Nachrichten oder Webseiten versuchen, Unternehmen, Organisationen oder auch Privatpersonen über Tricks und Täuschung dazu zu bringen, sensible Informationen (z. B. Passwörter, Zugangsdaten, Finanzdaten) preiszugeben oder Schadsoftware herunterzuladen. Es zeigt typische Angriffsformen auf — von Massen-E-Mails bis zu gezielten Attacken auf einzelne Personen oder Organisationen — und macht deutlich, warum Phishing besonders effektiv ist: Weil Täuschung durch vertrauenswürdige Aufmachung und Manipulation menschlicher Emotionen funktioniert.

Besonderes Augenmerk liegt darauf, wie solche Angriffe erkannt werden können: Das Kapitel beschreibt typische Merkmale von Phishing-Mails, erklärt wie betrügerische Webseiten aussehen können, und sensibilisiert dafür, wie manipulative Techniken — wie Täuschung, Druck, gefälschte Absender — eingesetzt werden.

Darüber hinaus gibt es konkrete Schutzempfehlungen: Das Modul vermittelt, wie Mitarbeitende im Unternehmen durch Aufmerksamkeit, kritische Prüfung von Nachrichten und URLs, skeptisches Verhalten bei unerwarteten Aufforderungen und durch technische Maßnahmen Risiken minimieren können. Auch wird der Einsatz von Schulungen und Tests — etwa Simulationen — zur Sensibilisierung und Erhöhung der Widerstandsfähigkeit gegen Phishing empfohlen.

Insgesamt schafft das Kapitel eine solide Grundlage, damit Unternehmen und ihre Mitarbeitenden die Gefahren von Phishing erkennen und eigenständig entscheiden können, wie sie Kommunikation und Zugangsdaten schützen — und stärkt damit deren Resilienz gegenüber einer der häufigsten Ursachen für Datenpannen und Cyberangriffe.

Das Kapitel **„Digitale Kriminalität“** gibt Unternehmen einen fundierten Überblick über die wachsende Bedrohung durch Straftaten im digitalen Raum. Es erklärt, was unter digitaler Kriminalität verstanden wird, wer betroffen sein kann und wie weit das Spektrum reicht — von Datendiebstahl und -verlust über Angriffe auf IT-Infrastruktur bis zu Sabotage, Spionage oder Erpressung. Dabei verdeutlicht das Modul, dass jede Organisation, jedes Unternehmen und auch Privatpersonen potenziell Ziel solcher Angriffe sein können.

Das Kapitel macht außerdem deutlich, dass Angriffe nicht nur technisch erfolgen — häufig werden psychologische Tricks und soziale Manipulation eingesetzt (z. B. Angst, Neugier, Hierarchie, Gewohnheit), um Menschen zur Preisgabe sensibler Daten zu verleiten. Es thematisiert, wie diese Methoden funktionieren und mit welchen Taktiken Kriminelle vorgehen.

Im Anschluss liefert das Kapitel praxisnahe Hinweise, wie sich Unternehmen wirksam schützen können — darunter klare Empfehlungen zu Datensicherung und Backups, Trennung von privaten und beruflichen Geräten, Zugangsbeschränkungen, sowie Sensibilisierung der Mitarbeitenden für aktuelle Betrugs- und Angriffsmuster. Es empfiehlt zudem, einen Notfall- und Krisenplan (Incident-Response-Plan) zu haben, um materiellen Schaden und Reputationsschaden zu begrenzen.

Insgesamt stärkt das Kapitel das Bewusstsein dafür, dass digitale Kriminalität ein reales, komplexes und ständig wachsendes Risiko darstellt — und gibt Unternehmen klare Werkzeuge und Strategien an die Hand, um ihre digitale Infrastruktur, Daten und Identität bestmöglich zu schützen.

Ein weiteres Kapitel behandelt das Thema **„Sicheres, endgültiges Löschen von Daten“**. Für Unternehmen ist es entscheidend, Datenträger am Ende ihres Einsatzzeitraums korrekt zu entsorgen und darauf befindliche Informationen vollständig zu entfernen. Dabei stellt sich auch die Frage, ob sich nur bestimmte Daten gezielt löschen lassen. Das Bewusstsein für die eigene Verantwortung im Umgang mit personenbezogenen und sensiblen Daten ist zentral für die Datensicherheit. Nur so lässt sich verhindern, dass unbefugte Dritte Zugriff auf Betriebsgeheimnisse oder Mitarbeiter:inneninformationen erhalten. Das neue Kapitel erläutert daher, wie Daten vollständig entfernt werden können, was „sicheres“ Löschen bedeutet und unter welchen Umständen es überhaupt möglich ist.

In Unternehmen existieren zahlreiche Dokumente mit sensiblen Inhalten, etwa Verträge oder Bankdaten. Was geschieht, wenn diese Unterlagen analog nicht mehr benötigt werden? Sie werden vernichtet – üblicherweise durch Schreddern. Für digitale Dateien gilt dasselbe Prinzip: Um Informationen tatsächlich zu löschen, sind – je nach Art des Datenträgers – unterschiedliche Verfahren erforderlich.

Neben der fachlichen Ausarbeitung wurden in das neue Kapitel zusätzliche Elemente wie interaktive Übungen und Merkfelder integriert. Sie dienen der Wiederholung zentraler Inhalte und erhöhen den Lerneffekt.

Schon parallel zum E-Learning entwickelte das Team ein Workshop-Design für kleine Unternehmen und Organisationen.

Die ersten Workshops konnten wir bei einem befreundenden Architekten, einer Steuerberatungskanzlei und einer Veranstaltungs-GmbH durchführen. Die wertvollen Inputs der teilnehmenden Mitarbeitenden flossen direkt in die Evaluierung des E-Learnings für Unternehmen und in die Struktur des Evaluierungstools für Teilnehmer:innen der Workshops mit ein.

Seit Frühjahr 2025 ist das KMU-Workshop-Angebot ein fixer Bestandteil des Ausbildungsprogramms der epicenter.academy GmbH. Mittlerweile konnten

wir das Angebot auch mit einer Webinar-Reihe ergänzen und bieten neben der klassischen „Digitalen Selbstverteidigung für KMUs“ auch KI-Workshops an, in dem die Unternehmen ihrer gesetzlichen Schulungspflicht nach dem EU AI Act nachkommen können.

Verlauf der Arbeitspakete

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 arbeiteten 6 Personen an dem Projekt, mit unterschiedlichen Fachbereichen wie Admin, E-Learning Inhalte und Workshop-Konzept.

Arbeitspaket 2 - <Konzeption der E-Learning Inhalte>

Zu Beginn der epicenter.academy standen Jugendliche im Fokus, weshalb die bestehenden Inhalte zunächst altersgerecht gestaltet und im ersten Arbeitspaket analysiert wurden, um notwendige strukturelle und inhaltliche Anpassungen vorzunehmen. Mit der Erweiterung der Zielgruppe um KMUs wurde anschließend eine neue E-Learning-Struktur entwickelt, die beide Angebote übersichtlich trennt und sowohl Jugendlichen als auch Unternehmer:innen einen einfachen Zugang zu relevanten Kapiteln ermöglicht. Der Schwerpunkt des zweiten Arbeitspakets lag auf der inhaltlichen Weiterentwicklung für KMUs, deren Bedarf vor allem im Bereich der Onlinekriminalität und des Schutzes betrieblicher IT-Systeme liegt. Dafür wurden bestehende Kapitel wie Passwörter, Verschlüsselung und sicheres Kommunizieren überarbeitet sowie die hinzukommenden Kapitel „Digitale Kriminalität“, „Phishing“ und „Sicheres, endgültiges Löschen von Daten“ erstellt. Letztere vermitteln Grundlagenwissen zu dem vor allem für KMUs existenzbedrohenden Gefahrenlage durch kriminelle Cyberangriffe; sowie darin Datenschutz und Löschpflichten auch tatsächlich durchführen zu können.

Um die Inhalte möglichst praxisnah zu gestalten, wurden Fallbeispiele aus Cybercrime-Berichten und Medien integriert und interaktive Praxisboxen entwickelt, die Nutzer:innen das eigenständige Erkennen und Ausprobieren typischer Angriffsmethoden ermöglichen, etwa durch Phishingbeispiele. Die technische Umsetzung der neuen Struktur auf der Website ist abgeschlossen; neue Kapitel können nun auch in Zukunft ergänzt werden. Zwei identifizierte inhaltliche Lücken wurden bereits geschlossen, weitere überarbeitete Kapitel stehen zur finalen Abstimmung durch Unternehmen bereit.

Die intensive Recherche zu realen Bedrohungsszenarien und der Austausch mit Unternehmer:innen haben das Konzept weiter geschärft und bestätigt. Insgesamt wurden die Ziele des Arbeitspakets vollständig erreicht: Die Inhalte

sind erweitert, vertieft und stark praxisorientiert ausgerichtet. 2025 wurden die Materialien wie geplant getestet und mit Hilfe des Unternehmensfeedbacks zur finalen E-Learning-Version weiterentwickelt.

Arbeitspaket 3 - <Konzeption des Workshops>

Auf Basis der Erkenntnisse aus der Entwicklung der E-Learning-Kapitel begann das Team mit der Konzeption eines Workshop-Designs für Unternehmen, wobei die zentrale Herausforderung die begrenzte Zeit der Zielgruppe im Vergleich zum umfangreichen E-Learning darstellte. Daher wurde zunächst analysiert, welche Inhalte unbedingt im Workshop behandelt werden müssen und welche mit Verweis auf das E-Learning ausgelagert werden können. Für die Teilnehmenden wurden klare Lernziele definiert: Unternehmer:innen und Mitarbeitende von KMUs und Organisationen sollen grundlegende Kompetenzen der digitalen Selbstverteidigung erwerben, um sicherere Entscheidungen im Arbeitsalltag treffen zu können. Zur Planung wurde eine Lernzielmatrix entwickelt, die unterschiedliche Kompetenzbereiche berücksichtigt und passende Methoden erarbeitet und getestet. Zusätzlich wurden die Schwerpunktsetzungen mittels Bedarfsanalyse pro Unternehmen individuell angepasst. Nach etwa einem Drittel der geplanten Entwicklungszeit stand die grundlegende Struktur und die zentralen Inhaltsblöcke fest, wobei der Fokus auf Passwörtern, Phishing, sicheren Geräten und sicherer Kommunikation liegt, während andere Themen wie allgemeines Datenschutzwissen für die KMUs lt. der Analysen eine geringere Priorität ergeben haben.

Arbeitspaket 4 - <Abhalten von Test Workshops mit KMUs und Feedback Erhebung, Auswertung>

Als besonders wertvoll erwiesen sich die Test-Workshops in Unternehmen aus unterschiedlichen Branchen. Die Teilnehmer:innen gaben wertvolle Einblicke in ihren Arbeitsalltag, dass dem Team die Anpassung der E-Learning Inhalte sehr erleichterten. Der kompakte Wissenstransfer war dabei ein zentrales Anliegen der Mitarbeiter:innen, aber auch die Erkenntnis, dass jedes Unternehmen seinen eigene Kommunikationsstrategie gemeinsam erarbeiten muss.

Dazu ergänzten wir das Workshop-Design mit einer Analyse des Schulungsbedarfs im Vorfeld, damit können wir Schulungsmaßnahmen modular und zielgerichtet auf den Arbeitsalltag der jeweiligen Unternehmen anpassen.Diese Bedarfsanalyse wird mit den Verantwortlichen des Unternehmens (Geschäftsführung, IT Abteilung, Büroleitung, u.a.) durchgeführt und wir entfernen und adaptieren basierend darauf Schulungsmaßnahmen um einen maximalen Wissenstransfer zu gewährleisten.

Arbeitspaket 5 - <Erstellung der finalen Versionen des E-Learnings und des Workshops>

Die Ein- und Umarbeitung der finalen Version des E-Learnings und des Workshop-Designs war ein laufender Prozess im letzten Jahr. Nach den Testworkshops konnten auch bereits einige Workshops in weiteren Unternehmen und NGOs abgehalten werden. Um die Anfragen für Workshops leichter zu managen wurde, auf Rückmeldung der Testunternehmen, auch Online-Buchungssystem etabliert. Die Recherche zu einem „datenfreundlichen“ Tool stellte sich als sehr schwierigen Prozess dar. Denn die Ansprüche, die wir als Datenschutzverein in Buchungstools haben, war nicht leicht erfüllbar. Wir haben rd. 30 Tools mit dem Entwickler getestet und leider hatten nur zwei unser Anforderungen erfüllt. Schlussendlich haben wir uns für das Tool von Appointmind entschieden, das auch mittlerweile umfänglich für die Terminvergabe der Schulworkshops und Organisationen verwendet wird.

Das Evaluierungstool, das gemeinsam mit einer externen Evaluatorin erarbeitet wurde, erweist sich als hilfreiches Analyse-Instrument für uns und ebenso für die Geschäftsleitung und den IT-Verantwortlichen in den jeweiligen Unternehmen. Es unterstützt uns bei der Qualitätssicherung und zeigt auf, welche Schwerpunkte vielleicht von den Mitarbeiter:innen noch vertieft werden müssen bzw. welche Schwachstellen die Teilnehmenden in ihren Kommunikationsabläufen sehen.

Arbeitspaket 6 - *<Dokumentation und Formales am Projektende>*

Die Dokumentation und Zusammenfassung wurde in den letzten Monaten laufend bearbeitet. Als Herausforderung erwies sich die vielen Workshop-Einsätze der epicenter.academy GmbH, sowie auch die berufliche Veränderung einiger Mitarbeitenden im Laufe des Jahres. Obwohl das E-Learning für KMUs bereits seit längerem fertig ist und auch die Workshops immer mehr von KMUs und NGOs gebucht werden, verzögerte sich die Erstellung des Endberichtes.

Umsetzung Förderauflagen

Dieses Kapitel ist nur relevant, wenn in der Fördervereinbarung spezielle Förderauflagen festgelegt wurden. In diesem Fall soll in diesem Kapitel dargestellt werden, wie diese berücksichtigt werden.

Keine speziellen Förderauflagen vereinbart

Liste Projektendergebnisse

Kurzbeschreibung der erreichten Projektendergebnisse jeweils mit Open Source Lizenz und Webadresse (netidee Vorgaben beachten!)

1	*Projektzwischenbericht*	*CC BY 4.0*	*https://www.netidee.at/kmu-digi-sicher*
2	*Projektendbericht*	*CC BY 4.0*	*https://www.netidee.at/kmu-digi-sicher*
3	*Entwickler_innen-DOKUMENTATION des Projektergebnisses für andere Entwickler_innen ("Dritte"), die das Projektergebnis nach Projektende nutzen/weiterentwickeln wollen* *Für Entwickler_innen (Systemkonzept, ggf. Grobspezifikationen):* *a. WAS IST ES* *b. FÜR WEN IST ES /WEM HILFT ES WODURCH* *c. WIE FUNKTIONIERT ES (für Entwickler_innen: Übersicht und detailliertes Systemkonzept, SW-Struktur)*	*CC BY 4.0*	*https://www.netidee.at/kmu-digi-sicher*
4	*Anwender_innen-DOKUMENTATION des Projektergebnisses für Anwender_innen, die das Projektergebnis nach Projektende nutzen wollen* *Für Anwender_innen ("Bedienungsanleitung") :* *a. WAS IST ES* *b. FÜR WEN IST ES /WEM HILFT ES WODURCH* *c. WIE FUNKTIONIERT ES*	*CC BY 4.0*	*https://epicenter.academy/unternehmen/anleitung*
5	*Veröffentlichungsfähiger*	*CC BY 4.0*	*https://*

	Einseiter / Zusammenfassung ** Kurzfassung WAS | FÜR WEN | WIE* ** Liste Projektergebnisse - also diese Liste, ggf. kompromiert* ** mit Angabe Open Source Lizenz/Webadresse* ** wo finden Dritte die Projektergebnisse (inkl. Dokumentation Anwender_innen bzw. Entwickler_innen)* ** mögliche Weiterentwicklungen/ weitere Einsatz-/ Nutzungsmöglichkeiten*		*www.netidee.at/kmu-digi-sicher*
6	*Dokumentation Externkommunikation zur Erreichung Sichtbarkeit /Nachhaltigkeit (separates Dokument oder als Teil des Endberichtes)* ** Welche Maßnahmen wurden in welchem Umfang gesetzt* ** Jeweils Bewertung Aufwand / Nutzen* ** Lessons Learned / Empfehlungen für andere Projekte*	*CC BY 4.0*	*Siehe in diesem Endbericht*
7	*Freies E-Learning - Open Educational Ressources Eine interaktive, multimediale OER zu Datenschutz und IT-Sicherheit steht für alle offen zugänglich als E-Learning auf https://epicenter.academy/e-learning/unternehmen zur Verfügung. Anpassung bestehender Inhalte an die Zielgruppe KMUs und der Entwicklung zusätzlicher für die Zielgruppe relevanter Kapitel zu digitaler Kriminalität, Phishing und Sicheres endgültiges*	*CC BY 4.0*	*https://epicenter.academy/e-learning/unternehmen*

	Löschen sind umgesetzt.		

Verwertung der Projektergebnisse in der Praxis

Angaben zur Verwertung der Projektergebnisse in der Praxis

KMU – E-Learning und die Workshops sind mittlerweile fixer Bestandteil des Leistungsangebotes der epicenter.academy GmbH. Das E-Learning wird laufend aktualisiert und dient weiterhin Unternehmen als freie Wissensplattform rund um IT-Sicherheit und Datenschutz.

Öffentlichkeitsarbeit/ Vernetzung

Beschreibung der im Rahmen Ihres netidee-Projektes bereits erfolgten bzw. noch geplanten Öffentlichkeitsarbeit oder Vernetzung

Es gab schon mehrere Aussendungen über den E-Mail Newsletter des Vereins epicenter.works, der Wiener Wirtschaftskammer, der Ärztekammer Niederösterreich sowie der Arbeiterkammer zu unserem Workshopangebot und dem offenen E-Learning für Untennehmen.
Gezielte Ansprache unserer Kolleg:innen von Dachverbänden sowie unsere Social-Media-Arbeit informiert laufend über das offene E-Learning für Unternehmen und Organisationen.

Eigene Projektwebsite

https://epicenter.academy/e-learning/unternehmen

Geplante Aktivitäten nach netidee-Projektende

Sind weiterführende Aktivitäten nach dem netidee-Projektende geplant?

Das E-Learning wird weiter inhaltlich aktuell gehalten und kann für die Zielgruppe weiter ausgebaut werden. Die Webseite wird gewartet (Sicherheitsupdates, PHP Versionen etc.) um auch weiterhin als eine funktionierende und sichere Ressource zur Verfügung zu stehen.

Anregungen für Weiterentwicklungen durch Dritte

Welche Nutzungs- und Weiterentwicklungsmöglichkeiten für Dritte ergeben sich durch Ihr netidee-Projekt bzw. empfehlen Sie?

Die E-Learninginhalte können von allen Unternehmen als Weiterbildungsressource genutzt werden. Auch ohne einen vorhergehenden Workshop von uns kann das E-Learning zb. von IT Abteilungen als Lernressource für die Weiterbildung der Mitarbeiter:innen angeboten werden. Die interaktiven Elemente und Inhalte können auf unsere Webseite genutzt oder in alle gängigen Lernplattformen integriert werden.