Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Abschlussbericht Vorarbeiten ITSec4KMU

Inhalt

Autoren: René Hüsler, Ursula Sury, Nicole Wettstein, Pascal Engel, Cyrill Gössi
Verfasst: 18.12.2020, Rotkreuz

1. Management Summary

Förderung der Cyber-Resilienz von Schweizer KMU durch Information und Sensibilisierung

1.1. Ausgangslage

Mit mehr als drei Millionen Beschäftigten bilden KMU das Rückgrat der Schweizer Wirtschaft. Zahlreiche Befunde zeigen, dass KMU in Bezug auf Angriffe aus dem Cyberspace nur ungenügend geschützt sind und bereits ein einzelner Angriff z. B. mittels Ransomware, ein KMU in seiner Existenz bedrohen kann.

1.2. Leistungsangebot ITSec4KMU

ITSec4KMU – die zentrale Informations- und Anlaufstelle für KMU im Kontext der Cybersicherheit – hat das Ziel, die Resilienz von Schweizer KMU gegenüber Angriffen aus dem Cyberspace landesweit zu fördern und somit das Rückgrat der Schweizer Wirtschaft zu stärken. Das Angebot von ITSec4KMU setzt sich aus den drei Bereichen «Plattform», «Netzwerk» und «eigene Angebote» zusammen.

- Die **Plattform** dient als zentrales Präsentations-, Informations- und Kommunikationsmedium. Darauf werden verschiedene Inhalte präsentiert, wie etwa Best-Practice-Leitfäden und Hilfsmittel, Informationen zur KMU-Sicherheitslage und zu den Top-Sicherheitsrisiken, ein Veranstaltungskalender, eine Verlinkung zur Melde- und Analysestelle Informationssicherheit (Melani), ein Register von lokalen Sicherheitsdienstleistern, Informationen zum First-Level Support sowie ein fachliches Quiz zur spielerischen Auseinandersetzung mit dem Thema.
- Das **Netzwerk** setzt sich, neben den KMU selbst, aus verschiedenen Akteuren zusammen, die im Bereich Cybersicherheit für KMU in der Schweiz aktiv sind. Dies umfasst Verbände und Institutionen, den Bund und die Kantone, Fachhochschulen und Universitäten, sowie Service- und Sicherheitsdienstleister. Ziel des Netzwerks ist es, mittels auf Branchen und Gruppen abgestimmten Veranstaltungen der Netzwerkpartner, den Austausch und die Transparenz im Themenbereich zu fördern. Grundlage für ein funktionierendes Netzwerk stellt dabei der niederschwellige Zugang zu den Informationen dar.
- Der letzte Bereich des Leistungsangebotes besteht in **eigenen Angeboten**, welche als gezielte Ergänzungen zu bereits vorhandenen Hilfestellungen erstellt werden. Die eigenen Angebote beinhalten ausgewählte Awareness- und Präventionsveranstaltungen, ein Monitoring der Medienlandschaft und ein Awareness-Siegel für KMU als Anreiz dafür, sich mit dem Thema Cybersicherheit langfristig auseinander zu setzen.

1.3. Marktbeurteilung

Im Rahmen der Vorarbeitsphase haben diverse Gespräche mit den wichtigsten Akteuren stattgefunden, um im Sinne einer Marktanalyse die Möglichkeiten einer Zusammenarbeit auszuloten und Bedürfnisse an die Ausrichtung von ITSec4KMU abzuholen. Neben dem Nationalen Zentrum für Cybersicherheit (NCSC) und Melani beurteilen digitalswitzerland, die Zuger Wirtschaftskammer, der Gewerbeverband des Kantons Zug, Economiesuisse, asut, der Innovationspark Zentralschweiz, Swico und die Information Security Society Switzerland (ISSS) das Projekt als positiv und haben ihre Unterstützung in der weiteren Projektarbeit zugesichert. Interviews mit KMU aus verschiedenen Branchen haben gezeigt, dass ein grosses Bedürfnis für eine zentrale Informationsquelle für Sicherheitsthemen sowie für eine Community mit Möglichkeiten zum Austausch mit anderen KMU sowie Dienstleistungsanbietern besteht. Diese Bedürfnisse werden von den heutigen Akteuren noch nicht gesamtheitlich abgedeckt.

1.4. Rollout

ITSec4KMU soll phasenweise auf die ganze Schweiz ausgerollt werden. Bis im Juni 2021 ist eine Minimalversion der Plattform in Deutsch und Englisch verfügbar, ein Netzwerk in der Deutschschweiz aufgebaut und erste eigene Angebote nutzbar. Bis Ende 2021 erfolgt der Rollout in der französischsprechenden Schweiz und ab Juli 2022 kann ITSec4KMU mit der Abdeckung der italienisch sprechenden Schweiz in den Vollbetrieb übergehen.

1.5. Finanzierung

Für die Startphase von ITSec4KMU (Januar 2021 bis Juni 2022) wird Kapital im Umfang von total CHF 975’000 benötigt. Ab Juli 2022 rechnet ITSec4KMU mit einem jährlichen Umsatz von CHF 200'000 bei Betriebskosten von jährlich zwischen CHF 750'000 und CHF 1'000’000. Die Finanzierung der Startphase soll durch den Kanton Zug geleistet werden. Die Gelder für den Vollbetrieb beruhen auf einer gemischtwirtschaftlichen Finanzierung durch verschiedene Kantone, den Bund, Verbände und Institutionen sowie Erträgen aus eigenen Dienstleistungen. Die Ausarbeitung des genauen Verteilschlüssels der benötigten Finanzmittel ist Teil der Startphase.

2. Ausgangslage und Zielsetzung

Bedrohungen aus dem Cyberspace wie z.B. Ransomware und CEO-Fraud haben in letzter Zeit, und nicht zuletzt während der COVID-19 Pandemie, stark zugenommen und betreffen immer häufiger auch KMU. Wie eine Studie von Cisco zeigt, sind 43 Prozent aller Cyberangriffe gegen KMU gerichtet[1]. Zugleich kann das Informations- und Aufklärungsbedürfnis der KMU aktuell nicht gedeckt werden, wie u.a. eine repräsentative Umfrage von gfs-zürich zeigt[2]. Aus diesem Grund hat eine Arbeitsgruppe auf Initiative des Kantons Zug und unter der Leitung von Prof. René Hüsler (Direktor Departement Informatik der Hochschule Luzern) im Zeitraum vom November 2019 bis April 2020 eine erste Skizze eines Businessplans für die Ausgestaltung eines Awareness-Zentrums im Kontext von Cybersicherheit für KMU ausgearbeitet.

Das vorliegende Dokument ist der angereicherte Businessplan für dieses Awareness-Zentrum und beschreibt die organisatorische Ausgestaltung, die erbrachten Leistungen, die Marktanalyse, Marketing- und Kommunikationsaktivitäten sowie das Finanzierungsmodell des Zentrums. Der Businessplan wurde im Zeitraum vom 1.10.2020-18.12.2020 erarbeitet. Der vorliegende Businessplan soll als Entscheidungsgrundlage für den Regierungsrat des Kantons Zug dienen.

3. Organisation

Im nachfolgenden Kapitel wird erläutert, wie die organisatorische Ausrichtung von ITSec4KMU während der Startphase und während dem Vollbetrieb aussehen soll, wie die Finanzierung sichergestellt und welche Trägerschaft langfristig angestrebt wird.

3.1. Namensgebung, Rechtsform, Finanzierung und Trägerschaft

ITSec4KMU ist der Arbeitstitel, unter welchem das vom Kanton Zug unterstützte Projekt zur Ausarbeitung des Projekt-Plans für «Melani4KMU» gelaufen ist («Vorarbeitsphase»).

Die Abklärungen der Vorarbeitsphase haben gezeigt, dass ein Verein die geeignetste Rechtsform für ITSec4KMU darstellt. Die Verfolgung eines ideellen Zwecks, die Verwendung eines Gewinns im Sinne des Vereinszwecks, sowie die flexible Gestaltungsmöglichkeit der Mitgliederbeitragsstruktur vereinfacht die finanzielle Unterstützung durch den Bund und Kantone und erlaubt auch Verbänden und KMU die Aufnahme als Mitglied unter Entrichtung von Mitgliederbeiträgen. Zusätzlich zu den Erträgen durch Mitgliederbeiträge wird ITSec4KMU als Verein auch Einnahmen über eigene Angebote wie z.B. Awareness-Veranstaltungen erzeugen. Das konkrete Finanzierungsmodell für die Startphase und den darauffolgenden Vollbetrieb ist in Kapitel 7 dargelegt.

Aufgrund dieser Abklärungen wird für die Führung des in diesem Bericht dargelegten Gewerbes im ersten Quartal 2021 ein Verein mit Namen «Cybersicherheit KMU Schweiz» gegründet. Als ideeller Zweck des Vereins wird das im Management Summary präsentierte Leitbild gewählt. Das Präsidium des neu gegründeten Vereins wird durch einen Vertreter der Hochschule Luzern oder des Kantons Zug bekleidet.

[1] https://www.cisco.com/c/dam/global/de_ch/solutions/small-business/pdfs/securityessentialsPDF_DE.pdf
[2] https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/03_Cyber/Studie_Cyberrisiken_KMU.pdf

3.2. Projektorganisation

In einer ersten Amtshandlung wird der Vorstand des Vereins eine operative Kerngruppe zum Aufbau der in diesem Bericht dargelegten Leistungen ernennen. Die Führung dieser Kerngruppe wird auf Personen aus dem Umfeld der Hochschule Luzern, der SATW und weiterer Akteure verteilt. Begleitet wird der Verein von einem Executive Board bestehend aus Vertreterinnen und Vertretern der wichtigsten Netzwerkpartner, welche die Projektumsetzung aus fachlicher Sicht begleiten.

4. Leistungsangebot

Das Leistungsangebot der wirtschaftlichen Tätigkeit des Vereins besteht aus den drei Teilen Plattform, Netzwerk und eigene Angebote. Im folgenden Abschnitt werden die einzelnen Teile genauer erläutert.

4.1. Plattform: Alle für KMU relevanten Cybersicherheits-Informationen an einem Ort

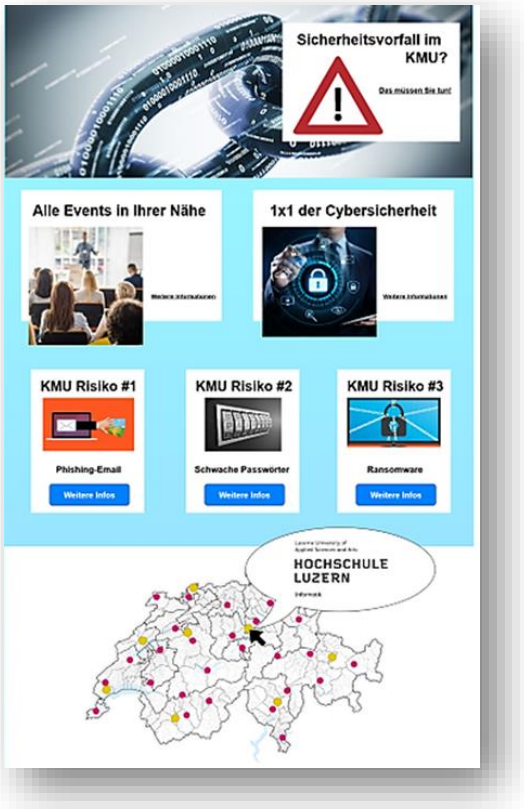


Abbildung 1: Mockup Plattform Landingpage

Die Plattform dient dem Verein als zentrales Präsentations- und Kommunikationsmedium, auf dem die folgenden Inhalte präsentiert werden:

- Sammlung von **Best-Practice Leitfäden**, **Hilfsmitteln** und **bestehenden Angeboten** (wie z.B. Merkblätter von Melani[3], existierende Schnelltests[4], usw.)
- Informationen zur **KMU-Sicherheitslage** (Melani-Halbjahresberichte) adaptiert auf die Zielgruppe der KMU, um jederzeit über die neusten Bedrohungen informiert zu sein.
- Informationen zu aktuellen **Top-Sicherheitsrisiken** (z.B. aktuelle Phishing-Wellen, die eine schnelle Reaktion seitens KMU erfordern).
- **Kalender** mit landesweiten Veranstaltungen z.B. in den Bereichen Awareness und Prävention, Weiterbildungen an Fachhochschulen, Universitäten und von Unternehmungen, sowie Anlässe zur Vernetzung und zum Austausch innerhalb der Cybersicherheit-Community oder zwischen verschiedensten Teilnehmern des Netzwerks.
- Verlinkung zu **Melani** mit seinem Meldeformular für Cybersicherheits-Vorfälle.
- **Register** von lokalen Sicherheitsdienstleistern: Mittels einer Stichwortsuche können KMU nach einem externen Dienstleister für ihr Cybersicherheits-Bedürfnis suchen. Die Aufnahme in das Register erfolgt über eine Selbstbeurteilung des Sicherheitsdienstleisters und ohne rechtliche Haftungsübernahme durch den Verein.
- Informationen zu **First-Level Support**: Da viele KMU nicht auf einen Cybervorfall vorbereitet sind und nicht wissen, wie sie im Notfall reagieren müssen, wird auf der Plattform ein spezieller Bereich diesem Thema gewidmet. KMU erhalten so unmittelbare Hilfe, welches die ersten Schritte im Falle eines Notfalls sind und an welche privaten Firmen in ihrer Umgebung sie sich für einen Notfallsupport wenden können («Cybersicherheits-Rega für KMU»).
- **Fachliches Quiz**: Den KMU auf spielerische Art und Weise einen Zugang zum Thema Cybersicherheit ermöglichen und die Awareness für das Thema erhöhen.

4.2. Netzwerk: Austausch und Transparenz fördern

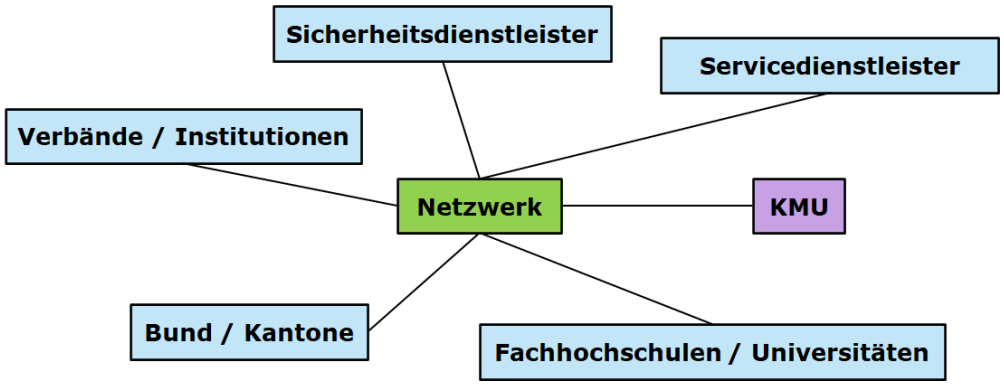


Abbildung 2: Das Netzwerk des Vereins

[3] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen.html
[4] https://ictswitzerland.ch/themen/cyber-security/check/

Der Verein unterhält ein Netzwerk bestehend aus verschiedenen Akteuren, welche in der Schweiz bereits unterschiedliche Rollen im Bereich Cybersicherheit einnehmen (vgl. Abb. 2):

- **KMU** als Hauptzielgruppe der Aktivitäten des Vereins und an welchen sich die wirtschaftlichen Tätigkeiten des Vereins orientieren.
- **Service- und Sicherheitsdienstleister** sind wichtige Partner für KMU. In der komplexen Welt der Informations- und Kommunikationstechnologie werden IT- oder Cybersicherheits-Dienstleistungen wie das Hosten von Rechenleistung oder das Überwachen von Netz-/Hardware mit Alarmierung bei Cyber-Angriffen häufig ausgelagert. Sowohl Service- als auch Sicherheitsdienstleister können das Netzwerk nutzen, um sich über aktuelle Cybersicherheits-Gefahren auszutauschen und sich im Sinne einer Frühwarnung gegenseitig zu informieren.
- **Verbände und weitere Institutionen** wie zum Beispiel ICTswitzerland (bzw. neu digitalswitzerland), Economiesuisse, SwissICT, asut und die Zuger Wirtschaftskammer. Diese Verbände und Institutionen haben einen hohen Grad an Vernetzung zu Schweizer KMU, weiteren Verbänden oder Sicherheitsdienstleistern und werden daher dem Verein bei seinen Bemühungen um Zugang zu KMU im Sinne eines Multiplikators dienen können. Ebenfalls haben einige dieser Verbände bereits beträchtliche Ressourcen in die Ausarbeitung von Awareness- und Sensibilisierungsunterlagen im Bereich der Cybersicherheit für KMU investiert, z.B. in Form des Cybersicherheits-Schnelltests von digitalswitzerland. Auf solche Ressourcen wird der Verein gerne zurückgreifen und diese auf der Plattform verlinken oder in eigene Angebote einbinden.
- **Bund und Kantone**, u.a. mit dem NCSC und Melani als zwei Bundesinstitutionen, welche über wertvolle Informationen über die Cybersicherheitslage der Schweiz und Hilfestellungen für KMU in Form von Merkblättern und Verhaltensempfehlungen verfügen. Den Kantonen kommt hauptsächlich die Rolle der finanziellen Unterstützung zu, sowie auch der Unterstützung bei der Bekanntmachung und allgemeinen Förderung des Vereins im Kanton. Zudem sind die Kantonspolizeien und das Netzwerk Nedik eine wichtige Quelle zusätzlicher Informationen zur Sensibilisierung.
- **Fachhochschulen und Universitäten** werden als Partner gesehen, die das Netzwerk dezentral über die Schweiz ausbreiten und so den KMU eine gute Erreichbarkeit des Vereins mit seinen Angeboten in z.B. allen Sprachregionen der Schweiz ermöglichen.

Das Netzwerk wird durch schweizweite Aktivitäten, abgestimmt auf KMU-Branchen und -Gruppen und in Zusammenarbeit mit den Netzwerkpartnern, aufgebaut und weiterentwickelt. Ein grosses Augenmerk legt der Verein dabei auf einen niederschwelligen Zugang zum Netzwerk: KMU werden in ihrer Sprache und bei ihren Bedürfnissen abgeholt, um so die Mitarbeit im Netzwerk sicherzustellen. Als Teil des Netzwerks ist zudem der Aufbau einer moderierten Community geplant, in der KMU sich mit Gleichgesinnten austauschen können und Antworten auf die drängendsten Fragen erhalten.

4.3. Eigene Angebote: Gezielte Ergänzungen zu bestehenden Angeboten

Im Bereich der eigenen Angebote führt der Verein gezielt und abgestimmt auf das Bedürfnis der Zielgruppen eigene Awareness- und Präventionsveranstaltungen durch. Der Fokus liegt dabei auf neuen Formaten, die interaktive Elemente enthalten und so eine grösstmögliche Attraktivität zur Teilnahme und einen grösstmöglichen Erfolg versprechen. Der Verein wird seinen Netzwerkmitgliedern zudem ein Monitoring der Schweizer Medienlandschaft mit Stellungnahmen anbieten. Dies ist ein Mehrwert, der einen weiteren wichtigen Beitrag zur Sensibilisierung für das Thema leistet. Als weiteres eigenes Angebot ist ein Awareness-Siegel angedacht, das als ein Anreiz-System für KMU dienen soll, um sich proaktiv und langfristig mit dem Thema Cybersicherheit auseinander zu setzen. KMU, die regelmässig Awareness-Veranstaltungen besuchen, erhalten vom Verein ein Gütesiegel, mit dem sie ihren Kunden zeigen können, dass für sie Cybersicherheit ein wichtiges Thema ist, das ernst genommen wird und mit dem sie sich von der Konkurrenz abheben.

5. Marktanalyse

Im Rahmen der Vorarbeitsphase fanden Gespräche mit verschiedenen Akteuren statt. Es ging dabei einerseits darum, die Bedürfnisse der KMU an ein Awareness-Zentrum abzuholen, andererseits konnten einige der wichtigsten Verbände, Institutionen und Bundesorganisationen über das Projekt informiert sowie Möglichkeiten der Zusammenarbeit besprochen und definiert werden.

5.1. KMU und Bedürfnisse

KMU bilden mit 3 Millionen Beschäftigten in 600'000 Unternehmen das Rückgrat der Schweizer Wirtschaft. Die Digitalisierung der Gesellschaft hat nicht nur bei KMU zu teilweise existenziellen Abhängigkeiten von IT-Systemen geführt, aber im Gegensatz zu grossen Unternehmen stehen KMU oft nicht die finanziellen Ressourcen zur Verfügung, um in gut ausgebaute und sichere IT-Systeme zu investieren. Dies macht KMU gegenüber Angriffen aus dem Cyberspace anfällig. Eine repräsentative Umfrage von gfs-zürich hat dann auch gezeigt, dass bereits 25% aller KMU durch einen Cyberangriff einen Schaden erlitten haben, dessen Behebung mit hohem Aufwand verbunden war[5].

Die zeitliche und wirtschaftliche Relevanz zur Abdeckung des Bedürfnisses von KMU nach Sicherheit gegenüber Angriffen aus dem Cyberspace ist aus den oben genannten Zahlen und Statistiken erkennbar. Um im Kontext von Cybersicherheit Kenntnis zu konkreten Bedürfnissen von KMU zu erhalten, wurden Interviews mit KMU aus verschiedenen Branchen (Treuhand, Immobilien, Holzbau, Stahlbau, IT, Consulting, Analytics/Softwareproduzenten) durchgeführt. Zusammengefasst, konnten aus diesen Interviews die folgenden Erkenntnisse gewonnen werden:

- Der Stellenwert von IT ist hoch.
- Das potenzielle Schadensausmass nach einem Cyberangriff ist hoch.
- Das Bedürfnis nach einer zentralen Informationsquelle für Sicherheitsthemen ist gross.
- Das Bedürfnis nach einer Community für den gegenseitigen Austausch ist gross.
- Die Bereitschaft, für eine Plattform oder eine Awareness-Veranstaltung zu bezahlen ist teilweise vorhanden.

Die Erkenntnisse aus den Interviews zeigen, dass das Leistungsangebot des Vereins (Plattform, Netzwerk, eigene Angebote) bei KMU auf Interesse stösst.

5.2. Marktbeurteilung und Alleinstellungsmerkmale des Vereins

Die wirtschaftliche Bedeutung der Resilienz von KMU gegenüber Angriffen aus dem Cyberspace ist, wie im vorangegangenen Kapitel dargelegt, gross. Dies wurde auch von öffentlichen Institutionen (z.B. dem Nationalen Zentrum für Cybersicherheit (NCSC)[6]), aber auch diversen Verbänden (z.B. digitalswitzerland[7]) und privaten Sicherheitsdienstleistern (z.B. secnovum[8], SMESEC[9]) erkannt. Das Resultat daraus ist, dass heute eine Vielzahl an Initiativen existiert, welche die Cybersicherheit von KMU in der Schweiz erhöhen möchten.

Keine der betrachteten Initiativen von Seiten der Verbände und privaten Sicherheitsdienstleistern erreicht jedoch die physische Reichweite oder den hohen Vernetzungsgrad zwischen den relevanten Akteuren, wie dies der neu zugründende Verein mit seinem dezentralen Netzwerk anstrebt. Auf Seite der

[5] *Digitalisierung und Cyberrisk in Schweizer KMU, gfs-zürich, Oktober 2020; https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/03_Cyber/Studie_Cyberrisiken_KMU.pdf
[6] https://www.melani.admin.ch/melani/de/home.html
[7] https://ictswitzerland.ch/themen/cyber-security/
[8] https://www.secnovum.ch/
[9] https://www.fhnw.ch/de/internationales/forschung/smesec

Institutionen hat das NCSC nach eigenen Angaben (mehr dazu in Abschnitt 5.3.1) nicht die Kapazität, sich in gleichem Ausmass der Cybersicherheit von KMU anzunehmen, wie dies dem zu gründenden Verein mit seinem spezialisierten Leistungsangebot möglich ist. Das dezentrale Netzwerk, die Koordination und Führung durch Fachhochschulen und Verbände, sowie eine überwiegend öffentliche Trägerschaft verschaffen dem Verein eine einmalige Marktstellung: Mit dem Netzwerk erreicht der Verein physische Nähe zu KMU im ganzen Land, dank der Koordination und Führung durch Fachhochschulen und Verbände verfügt der Verein über eine grösstmögliche fachliche Kompetenz, und die überwiegend öffentliche Trägerschaft ermöglicht Transparenz bezüglich wirtschaftlicher Interessen.

Der Verein stellt keine Konkurrenz zu bestehenden Initiativen dar, sondern versteht sich als Koordinations- und Anlaufstelle für sämtliche Aktivitäten im Bereich der Cybersicherheit für KMU in der Schweiz.

5.3. Angestrebte Zusammenarbeiten

Der neu zugründende Verein möchte sich im Kontext der Cybersicherheit als zentrale Informations- und Anlaufstelle für KMU etablieren. Um dies zu erreichen ist es notwendig, mit den wichtigsten bereits existierenden Akteuren im Markt eine Zusammenarbeit anzustreben, gegenseitig die Interessen abzugleichen und von Synergien und Multiplikator-Effekten zu profitieren. Im Rahmen der Vorarbeitsphase wurden Akteure identifiziert, die den Verein entweder als Finanzgeber unterstützen oder ihn mit Sachinformation sowie Kontakten zu KMU und Sicherheitsdienstleistern beliefern können. Nachfolgend ist eine Zusammenfassung der Gespräche ersichtlich, welche mit den wichtigsten Akteuren im Rahmen der Vorarbeitsphase geführt wurden.

5.3.1. NCSC und Melani

Das NCSC[10] beurteilt das Projekt grundsätzlich positiv und sieht darin eine Ergänzung zu den eigenen Zielen der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Dem NCSC selbst fehlen die Ressourcen für den Aufbau einer KMU-Plattform und der Fokus im Bereich Sensibilisierung liegt auf der Bevölkerung. Damit sich das NCSC auf den Verein abstützten kann, bedarf es einer konkreten und langfristigen Finanzierung, einer Definition der benötigten, personellen Ressourcen, sowie klar definierte Zuständigkeiten und Ansprechpersonen. Zudem sollten alle Aktivitäten des Vereins laufend mit den Aktivitäten des NCSC abgestimmt werden. Unter diesen Bedingungen ist das NCSC bereit, das Projekt während der Startphase und dem anschliessenden Vollbetrieb inhaltlich sowie finanziell zu unterstützen. Eine offizielle Zusage wird das NCSC jedoch erst aufgrund des Abschlussberichts geben können.

Melani[11] ist dem Projekt gegenüber positiv eingestellt und schätzt es sehr, frühzeitig in die Arbeiten und Aktivitäten involviert zu sein. Melani, als offizielle Bundesstelle zur Meldung von Cybervorfällen, könnte sich eine Zusammenarbeit mit dem Verein vorstellen. Konkret könnte Melani, im Rahmen seiner Antworten auf Meldungen im Meldeformular, auf den Verein als Informationsquelle und Netzwerkpartner verweisen.

5.3.2. digitalswitzerland (Zusammenschluss ICTswitzerland und digitalswitzerland)

digitalswitzerland, eine Standortinitiative mit 220 Mitgliedern aus Wirtschaft, öffentlicher Hand, Nicht-Regierungsorganisationen und Verbänden sowie der Forschung und Lehre, beurteilt das Projekt positiv

[10] Das Gespräch fand am 13.11.2020 mit Manuel Suter (Geschäftsstelle NCSC) und Dominique Trachsel (Verantwortliche Sensibilisierung und Prävention) statt.
[11] Das Gespräch fand am 26.11.2020 mit Pascal Lamia (Stv. des Delegierten des Bundes für Cybersicherheit, Leiter Operative Cybersicherheit und Melani) statt.

und ist von dessen Bedeutung überzeugt[12]. Das Projekt passt zu den übrigen Aktivitäten des Cybersicherheits-Komitees im Bereich Stärkung der Cyber-Resilienz von KMU. Die Unterstützung und Eingliederung des Vereins in die laufenden Cybersicherheits-Aktivitäten von digitalswitzerland ist eines der Ziele des nächsten Jahres 2021, das vom Executive Board von digitalswitzerland verabschiedet wurde. Die Möglichkeiten zur finanziellen Unterstützung werden im Rahmen der Startphase des Vereins mit digitalswitzerland abgeklärt.

5.3.3. Zuger Wirtschaftskammer

Die Zuger Wirtschaftskammer[13] beurteilt das Projekt als hochinteressant und grundsätzlich besteht die Bereitschaft an einer Kooperation im Bereich Vermarktung und Kommunikation. Zum Zeitpunkt des Gesprächs (03.12.2020) war für die Zuger Wirtschaftskammer das Leistungsangebot und der USP des Projektes noch zu wenig geschärft. Die Inputs der Zuger Wirtschaftskammer zur Ausrichtung des Vereins sind in diesen Schlussbericht eingeflossen und werden den verantwortlichen Personen bei einem positiven Entscheid des Regierungsrates des Kantons Zug erneut präsentiert. Im Rahmen dieses Nachfolgegesprächs könnten auch Möglichkeiten der Finanzierung diskutiert werden.

5.3.4. Gewerbeverband Kanton Zug

Der Gewerbeverband Zug[14] beurteilt das Projekt positiv und schätzt das Vorhaben als relevant für den Verband ein. Der Gewerbeverband ist bereit, den Verein über Newsletter und Soziale Meiden seinen Mitgliedern bekannt zu machen. Zudem hat der Verband die gemeinsame Umsetzung eines Pilotprojektes zugesichert, bei der interessierte KMU die Dienstleistungen der Plattform (insbesondere die Zusammenarbeit mit Service- und Sicherheitsdienstleistern) nutzen und auf diese Weise eine Vorzeigefunktion für die anderen KMU im Verband wahrnehmen können. Eine enge Zusammenarbeit im Rahmen des Pilotprojektes zwischen dem Gewerbeverband und dem Verein ist geplant.

5.3.5. Economiesuisse

Economiesuisse[15] beurteilt das Projekt positiv und zeigt viel Interesse am Vorhaben. Kommunikative Unterstützung, z.B. in Form eines Newsletter-Beitrages, wurde zugesichert. Economiesuisse als Verband der Verbände ermöglicht dem Verein den Zugang zu weiteren, relevanten Verbänden in der Schweiz. Die genaue Form der Zusammenarbeit zwischen dem Verein und Economiesuisse muss in einem weiteren Gespräch definiert werden.

5.3.6. asut: Schweizerischer Verband der Telekommunikation

asut[16] beurteilt das Projekt positiv und sieht darin eine wichtige Initiative, die gerade für ein KMU-Land wie die Schweiz einen grossen Mehrwert bedeuten kann. asut spricht grundsätzlich keine finanziellen Mittel für die Zusammenarbeit mit Partnern, hat jedoch seine ideelle Unterstützung zugesichert, und sieht im Rahmen von Gegenleistungen die Möglichkeit, den Verein zu unterstützen. An einer Mitarbeit in einem allfälligen Lenkungsausschuss des Vereins, wäre asut grundsätzlich interessiert.

[12] Das Projekt wurde im Rahmen der Sitzung der Kommission Cybersecurity von ICTswitzerland vom 10.11.2020 präsentiert.
[13] Das Gespräch fand am 3.12.2020 mit Dirk Hoffmann (Vorsitzender Ausschuss Industrie und Technologie der Zuger Wirtschaftskammer) und Andreas Umbach (Präsident Zuger Wirtschaftskammer) statt.
[14] Das Gespräch fand am 7.12.2020 mit Flavio Niederhäuser (Vorstandsmitglied und Ressortverantwortlicher Digitalisierung & Marketing) statt.
[15] Das Gespräch fand am 8.12.2020 mit Erich Herzog (Mitglied der Geschäftsleitung, Leiter Wettbewerb & Regulatorisches) statt.
[16] Das Gespräch fand am 20.11.2020 mit Christian Grasser (Geschäftsführer asut) statt.

5.3.7. Innovationspark Zentralschweiz

Der Innovationspark Zentralschweiz[17] beurteilt das Projekt positiv und möchte einen aktiven Teil innerhalb der Plattform und des Netzwerks wahrnehmen. Das Thema Cybersicherheit ist für den Innovationspark mit seinem Fokus auf "gebaute Umwelt" sehr relevant. Die Möglichkeiten der Zusammenarbeit mit dem Innovationspark Zentralschweiz sind vielfältig und reichen von kommunikativer Unterstützung, der Organisation von gemeinsamen Events, der Nutzung des Parks als physische Plattform für den Austausch bis hin zu gemeinsamen Projekten im Bereich "Building". Konkrete Aktivitäten werden im Rahmen der Startphase mit dem Innovationspark Zentralschweiz definiert.

5.3.8. Swico: Der Wirtschaftsverband für die digitale Schweiz

Swico[18] beurteilt das Projekt positiv und hat zugesichert, das Projekt mittels eines dedizierten Newsletters bei seinen rund 800 Mitgliedern (ICT-Unternehmen jeglicher Grössen und aller Wertschöpfungsstufen) bekannt zu machen. Bezüglich einer finanziellen Unterstützung oder weiteren Formen der Zusammenarbeit wurden noch keine Entscheide getroffen.

5.3.9. Information Security Society Switzerland (ISSS)

Die ISSS[19] beurteilt das Projekt sehr positiv und unterstützt das Vorhaben mit der Begründung, dass insbesondere der Netzwerk- und Sensibilisierungsgedanke des Vereins ein grosses Bedürfnis der KMU abdeckt. Die ISSS ist sehr an einer Mitarbeit in einem allfälligen Lenkungsausschuss des Vereins interessiert, und möchte insbesondere ihre guten Kontakte zu KMU einbringen. Eine allfällige finanzielle Unterstützung des Vereins wird innerhalb des Vorstands der ISSS abgeklärt.

5.3.10. SwissICT: Fachverband der Schweizerischen ICT

SwissICT[20] beurteilt das Projekt positiv. Insbesondere der Ansatz, die bestehenden Angebote zu bündeln und eine Plattform mit allen Playern zu lancieren, wird als sinnvoll eingeschätzt. SwissICT hat Unterstützung im Bereich Kommunikation zugesichert und fungiert als Multiplikator mit starker Medienpräsenz, um insbesondere die Sicherheitsdienstleister für ein Engagement im Netzwerk und als Partner zu gewinnen.

5.3.11. Projektteam Businessplan 1.0

Die Mitglieder des ursprünglichen Projektteams (HSLU, BFH, ZHAW, SUPSI, SATW, InfoGuard) sind in die Projektarbeit miteinbezogen und unterstützen das Projekt weiterhin. Dies ist insbesondere aufgrund der guten Kontakte zu den KMU und aufgrund des Leistungsangebotes der Fachhochschulen ein grosser Mehrwert für das Projekt.

[17] Das Gespräch fand am 10.12.2020 mit Sem Mattli (Geschäftsleiter Innovationspark Zentralschweiz) statt.
[18] Das Gespräch fand am 3.12.2020 mit Dario Perfettibile (Vertreter Swico in der Kommission Cybersecurity von ICTswitzerland) statt.
[19] Das Gespräch fand am 20.11.2020 mit Arié Malz (Co-Präsident ISSS) und Dario Walder (Vizepräsident ISSS) statt.
[20] Das Gespräch fand am 11.12.2020 mit Christian Hunziker (Geschäftsführer SwissICT) statt.

6. Marketing und Kommunikation

Der Hauptfokus im Bereich Marketing und Kommunikation liegt in einer direkten Ansprache der Wirtschafts- und Branchenverbänden, die Empfehlungen für ihre Mitglieder (KMU und/oder Sicherheitsdienstleister) aussprechen können sowie in der Kommunikation mit Entscheidungstragenden von KMU. Die Wirtschafts- und Branchenverbände sollen dabei als Netzwerkpartner gewonnen werden, ihre Ansprache erfolgt über persönliche Treffen im Rahmen der Arbeiten zum Netzwerkaufbau. Idealerweise beinhalten die Partnerschaften kostenlose Kommunikationsmöglichkeiten zur Bekanntmachung des Vereins, z.B. in Form von Berichten in Fachzeitschriften, Newsletter, Blogs, etc. der Netzwerkpartner.

Für die direkte Ansprache der Entscheidungstragenden der KMU sind die folgenden Marketingmassnahmen vorgesehen:

- Suchmaschinenmarketing (Google Ads, sowie Banner-Werbung)
- Soziale Medien (LinkedIn, Facebook)
- Blogbeiträge und Newsletter
- Direktansprache z.B. via E-Mail

6.1. Netzwerksegmente

Der Verein unterhält ein dezentrales Netzwerk bestehend aus verschiedenen Segmenten, welche bereits in Kapitel 4.2 dargelegt wurden und in der nachfolgenden Tabelle noch einmal aufgelistet sind. Jedem dieser Segmente kommt bei der wirtschaftlichen Tätigkeit des Vereins eine bestimmte Rolle zu. Diese Rollen haben entscheidende Wirkung auf die Art des Informationsflusses zwischen dem Verein und dem Segment, was dann eine Ausprägung in verschiedenartigen Marketing- und Kommunikationsaktivitäten findet. Diese Aktivitäten, aufgeschlüsselt nach den einzelnen Segmenten, sind ebenfalls in der nachfolgenden Tabelle aufgezeigt.

Segment	Rollen	Kommunikationsaktivitäten
Schweizer KMU	• Zu schützende Subjekte gemäss Leitbild • Benutzer der Plattform • Besucher von Veranstaltungen	• Bekanntmachung der Plattform, Veranstaltungen und weiterer Angebote
NCSC mit Melani	• Politische Legitimatoren • Finanzielle Träger • Informationsquelle zu Vorfällen und Best Practices	• Kontinuierlicher Abgleich bezüglich Kampagnen und Strategien • Regelmässige Berichterstattung über Leistungsmetriken (durchgeführte Veranstaltungen, registrierte KMU, …) • Regelmässige Einforderung von Statistiken und Aufarbeitungen von Vorfällen
Kantone	• Finanzielle Träger • Politische Legitimatoren • Bindeglied zu Gemeinden • Awareness-Schaffung bei Kantonsverwaltung	• Regelmässige Berichterstattung über Leistungsmetriken (durchgeführte Veranstaltungen, registrierte KMU, …) • Unterstützung kantonale Verwaltungen mit Infomaterial, etc.
Fachhochschulen	• Lokale Kompetenzzentren • Austragungsorte von Veranstaltungen • Multiplikatoren für Zugang zu KMU	• Regelmässiges Einholen von eingegangenen Anfragen von KMU zu Statistikzwecken • Regelmässiges Aktualisieren des Veranstaltungskalenders

		• Regelmässige Planung und Durchführung von Veranstaltungen vor Ort
Verbände	• Multiplikatoren für Zugang zu Branchen- und Wirtschaftsverbänden, KMU und Sicherheitsdienstleistern • Informationsquelle für Best Practices Leitfäden und Informationen • Finanzielle Träger	• Regelmässige Belieferung mit Werbung für Plattform und Veranstaltungen (mit sowohl KMU wie auch Sicherheitsdienstleister als Ziel) • Kontinuierliche Abgleiche bezüglich Kampagnen und Strategien • Austausch von Inhalten für Kampagnen
Sicherheitsdienstleister	• Einträge in Register auf der Plattform • Umsetzer von Cybersicherheit bei KMU	• Bekanntmachung von Plattform, Veranstaltungen und weiteren Angeboten.

Ein passendes Marketing- und Kommunikationsmedium muss vom Verein (E-Mail, Flyer, Fachartikel, Rapport, etc.) in Abhängigkeit des angesprochenen Netzwerksegmentes und dessen eingenommener Rolle gewählt werden.

7. Kosten und Finanzierung

In der nachfolgenden Tabelle sind für die Startphase (Januar 2021 bis Juni 2022) und den Vollbetrieb des Vereins (ab Juli 2022) die anfallenden Kosten und die jeweils über eigene Angebote selbst erwirtschafteten Erträge ersichtlich. Alle gezeigten Beträge sind in CHF.

	Phase	
	Start (Jan. 2021 – Jun. 2022)	**Vollbetrieb (ab Juli 2022, jährlich)**
Kosten	975’000	750'000 – 1’000'000
Erträge aus eigenen Angeboten	0	200’000
Saldo	**975’000**	**550'000 - 800’000**

Aus der obigen Tabelle ist ersichtlich, dass in der Startphase ein Kosten-Saldo entsteht, der mit den Erträgen aus den eigenen Angeboten nicht ausgeglichen werden kann.

Wie diese verbleibenden Kosten in den einzelnen Phasen auf die öffentliche Hand (Bund und Kantone) sowie auf Institutionen und Verbände verteilt werden, ist in der nachfolgenden Tabelle ersichtlich.

	Phase			
	Start		**Vollbetrieb**	
	Anteil [%]	Nominal	Anteil [%]	Nominal
Öffentliche Hand	100	975’000	70	385'000 - 560’000
Institutionen & Verbände	0	0	30	165'000 - 240’000
Total	**100**	**975’000**	**100**	**550'000 - 800’000**

Wie für die Vollbetriebsphase die Kosten-Saldi innerhalb z.B. der öffentlichen Hand verteilt werden ist noch nicht festgelegt und wird mit grosser Wahrscheinlichkeit jährlich neu festgelegt.

Die Kosten (in CHF) für die Startphase setzen sich wie folgt zusammen:

Kategorie	Kosten	Details
Weitere Personalkosten	120’000	Koordination Projektleitung, Administration
Plattform	305’020	Siehe Anhang A
Netzwerk	348’000	Siehe Anhang B
Eigene Angebote	125’000	Siehe Anhang C
Marketing	45’000	Siehe Anhang D
Sonstiger Aufwand	30’000	Spesen, Allg. Unkosten, Material, Beratung
Total Gerundet	**975’000**	

Die detaillierte Zusammenstellung der Kosten einzelner Kategorien kann den Detailbudgets in den Anhängen A, B, C und D entnommen werden.

8. Planung Startphase

Die Starphase selbst besteht aus drei Teilphasen.

- In der ersten Phase wird die Plattform aufgebaut und die Netzwerkpartner aus der deutschsprachigen Schweiz werden angegangen. Ziel ist, die Plattform bis am 31. Juni 2021 live zu stellen. Dies stellt denn auch den eigentlichen Startschuss für den Betrieb des Vereins dar.
- In der zweiten Teilphase wird die französischsprechende Schweiz angegangen. Dazu gehört auch der Ausbau der Plattform betreffend sprachlichen Anpassungen. Diese Teilphase soll bis zum 31. Dezember 2021 abgeschlossen sein.
- In der letzten Teilphase wird die Plattform weiter ausgebaut und das Netzwerk auf die italienische Schweiz ausgeweitet. Nach Beendigung dieser Phase ist die gesamte Schweiz abgedeckt, so dass der Verein am 1. Juli 2022 in den Vollbetrieb übergehen kann.

Für die Startphase wurden die folgenden Meilensteine definiert:

Meilensteine	Datum
Interner Kickoff Startphase	KW 01, 2021
Start Aufbau Netzwerk (mit NCSC und Melani)	KW 04, 2021
Start Entwicklung Plattform	KW 06, 2021
Aufschalten Plattform (MVP, unter itsec4kmu.ch/itsec4sme.ch)	KW 27, 2021
Erweiterung Plattform (Französisch, unter itsec4pme.ch)	KW 52, 2021
Erweiterung Plattform (Italienisch, unter itsec4pmi.ch)	KW 27, 2022
Start Vollbetrieb	KW 28, 2022

Eine detaillierte Projektplanung kann in Anhang E gefunden werden.

Anhang A

Plattform

Inhalt

Autoren: René Hüsler, Ursula Sury, Nicole Wettstein, Pascal Engel, Cyrill Gössi
Verfasst: 18.12.2020, Rotkreuz

1. Phasen der Entwicklung

Die Entwicklung der Plattform wird in zwei Phasen verlaufen. In Phase 1 wird eine minimale Plattform erstellt, welche als reines Präsentationsmedium die Leistungsangebote des Vereins präsentiert. Darauf aufbauend wird in einer Phase 2 die Plattform um einen interaktiven Teil zur Realisierung des Awareness-Siegel erweitert.

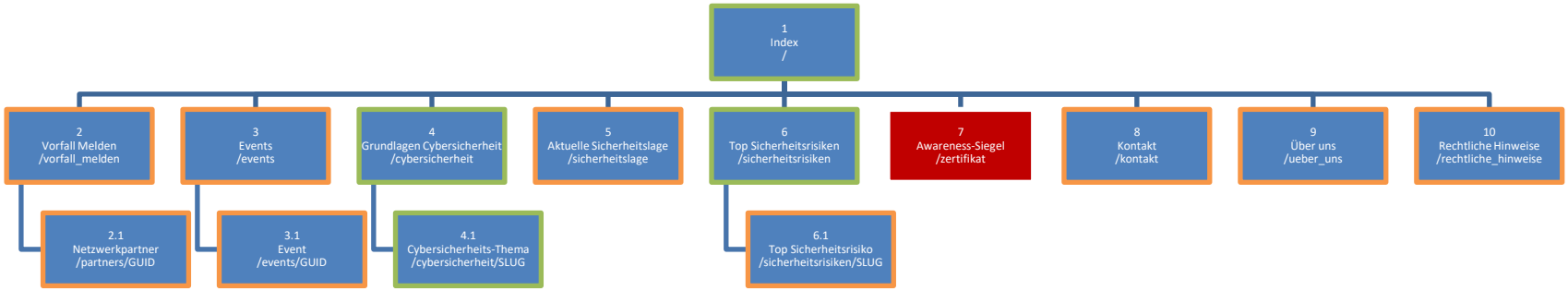
Funktionsumfang und Inhalt nach Phase 1:

- Auswahl der Sprache (DE und EN)
- Anleitung für Vorgehen bei Vorfall
- Veranstaltungskalender mit Anmeldemöglichkeit für eigene Veranstaltungen
- Grundlagen der Cybersicherheit
- Aktuelle Sicherheitslage und Top Sicherheitsrisiken
- Abonnieren eines Newsletters

Zusätzlicher Funktionsumfang nach Phase 2:

- Interaktive Mini-Spiele zur Erlangung des Awareness-Siegels
- Zusätzliche Sprachen (FR, IT)

2. Struktur



Für jede Ressource ist der Pfad relativ zum Host angegeben. Die Ressourcen 1 bis 6 und 8 bis 10 sind Teil der Minimal-Version der Plattform und werden in Phase 1 der Entwicklung erstellt. Ressourcen vom Typ 2.1, 3.1 und 6.1 werden mehrfach erstellt. Die Ressource 7 ist Teil der Erweiterung für die Unterstützung von Awareness-Siegel, welche in Phase 2 erstellt wird. Alle Ressourcen haben das gleiche Grundlayout (Header, Body, Footer). Darauf aufbauend haben die Ressourcen 1, 4, und 6 ein Layout mit der Möglichkeit zur Darstellung verschiedener Kacheln, und die restlichen Ressourcen haben ein auf dem Grundlayout aufbauendes Layout, welches ein einfaches 2-Spalten Layout ist. Mehr zum angedachten Design kann in den Mockups im Anhang dieses Dokuments gefunden werden.

3. Arbeiten durch Interne und Externe

Bei der Entwicklung der Plattform werden die folgenden Arbeiten durch interne Mitarbeitende durchgeführt:

- Erarbeitung der Inhalte der Ressourcen (z.B. Top-Sicherheitsrisiken)
- Erstellung der effektiven Ressourcen nach Erhalten des Frameworks von Webagentur
- Übersetzung der Inhalte von DE nach EN
- Gegenlesen der Texte durch Marketing und Kommunikation
- Kauf der Domain
- Bestellung Webhosting
- Testing

Die folgenden Arbeiten werden durch externe Mitarbeitende durchgeführt:

- Design von Logo sowie Primär- und Sekundärfarben
- Design von Bildern und Icons
- Entwicklung des Frameworks durch Webagentur
    - Layout der Ressourcen gemäss Kapitel Struktur und den Mockups im Anhang
    - Primär- und Sekundärfarben gemäss Design-Vorgabe
    - Möglichkeit zur Anmeldung für einen Newsletter
    - Möglichkeit zur Anmeldung für eigene Events
    - Möglichkeit zur Wahl der Sprache (DE und EN für Phase 1)

4. Aufwand und Kosten

Die folgende Auflistung zeigt eine Abschätzung bezüglich der Anzahl Ressourcen, die in Phase 1 ungefähr erstellt werden müssen, und des Aufwands in Stunden für die effektive Erarbeitung des Inhalts der Ressourcen vom jeweiligen Typ (siehe Kapitel 2).

Ressource	Anzahl	Erarbeitung Inhalt [h]
1	1	16
2	1	16
2.1	25	50
3	1	24
3.1	4	8
4	1	8
4.1	8	64
5	1	24
6	1	8
6.1	8	64
8	1	8
9	1	8
10	1	16
Total:	54	314

Die Anzahl für Ressource 2.1 setzt sich aus einer Ressource pro Fachhochschule, Melani und Sicherheitsdienstleister zusammen. Die Anzahl für Ressource 3.1 setzt sich aus einer initialen Awareness-Veranstaltung, welche alle 3 Monate an der HSLU durchgeführt wird, zusammen. Die Anzahl für Ressource 4.1 und 6.1 ergibt sich aus den initial zu erarbeiteten Themen-Inhalten.

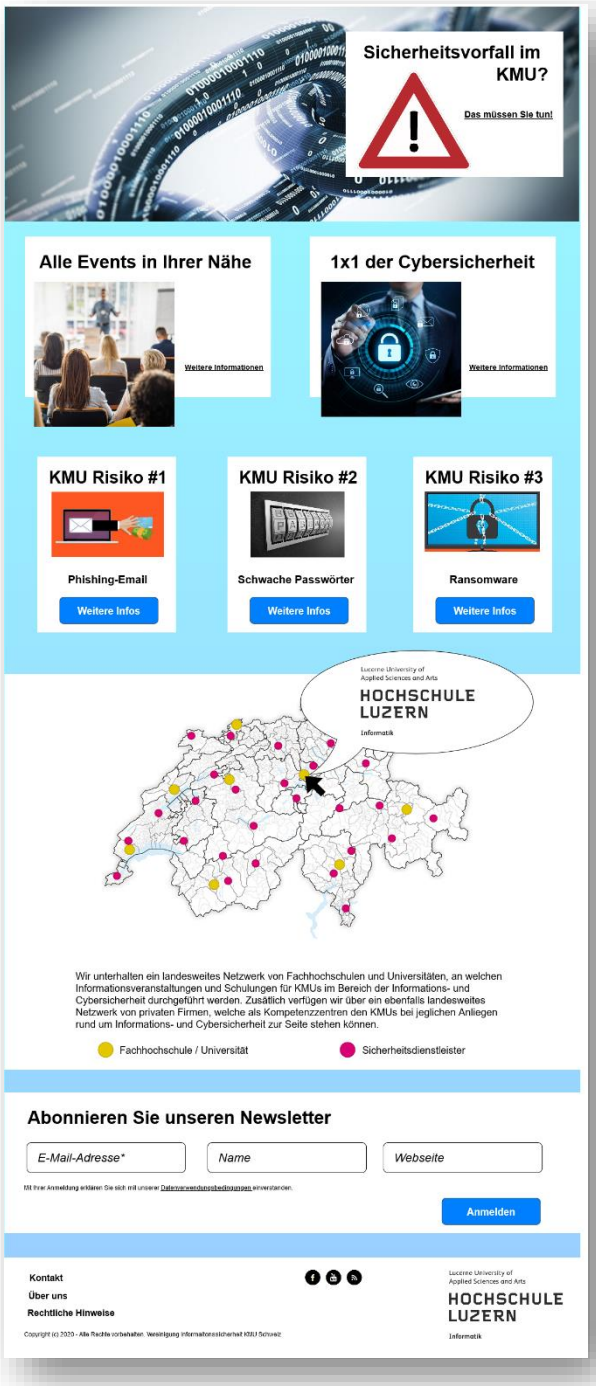
In Phase 2 findet die externe Übersetzung der Webseite sowie die Entwicklung der Interaktive Mini-Spiele zur Erlangung des Awareness-Siegels statt

Aufgrund dieser Abschätzung des Aufwands ergibt sich folgende Abschätzung der Kosten, welche für die Erstellung der Minimal-Version der Plattform anfallen werden.

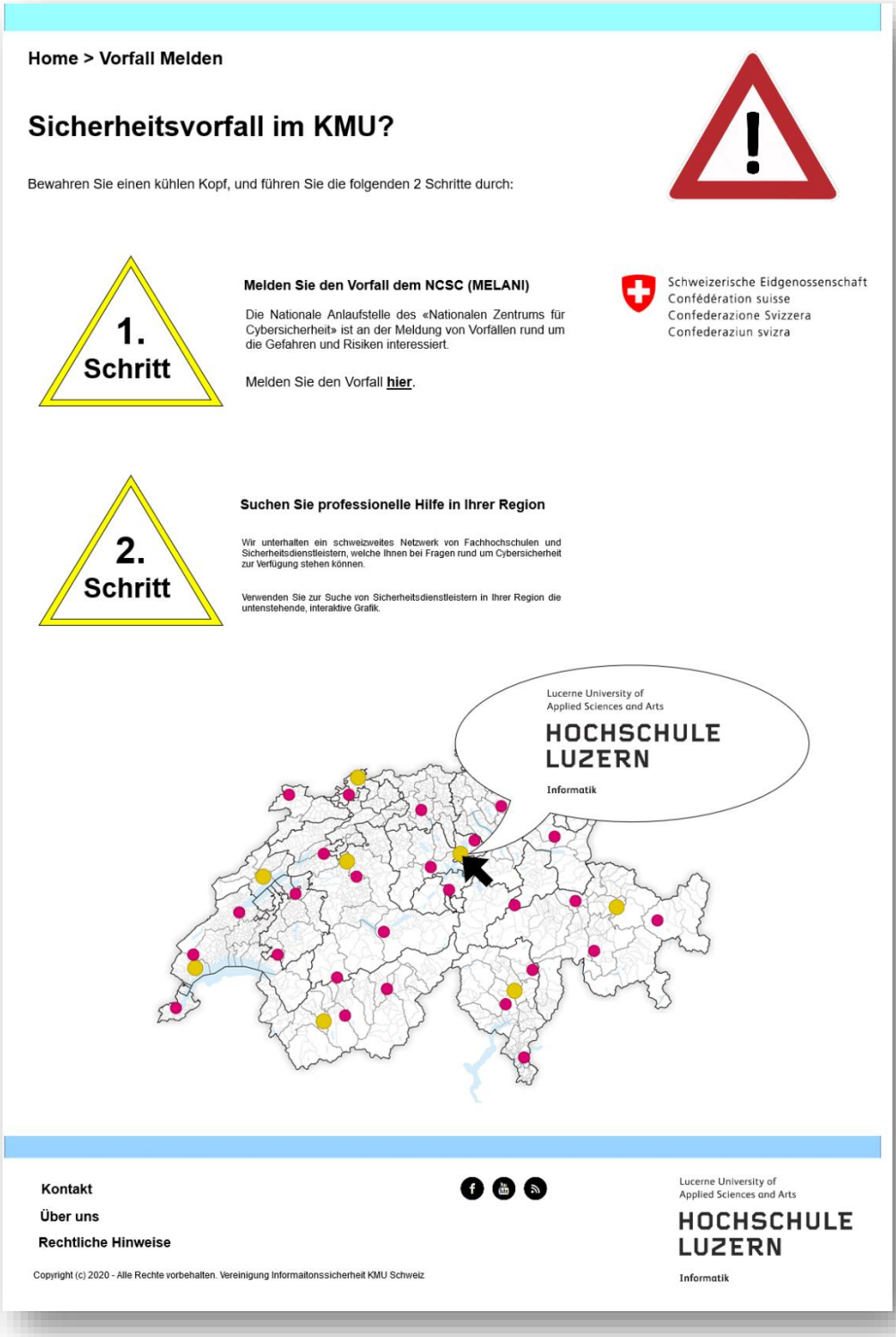
Kostenpunkt	Aufwand [h]	Ansatz [CHF / h]	Sub-Total [CHF]
Intern			
Erarbeitung Ressourcen-Inhalte Phase 1	314	85	26’690
Ausbau Webseite in Phase 2	150	85	12’750
Entwicklung Mini-Spiele Phase 2	240	85	20’400
Übersetzung nach EN	100	85	8’500
Marketing und Kommunikation	150	85	12’750
Kauf der Domain	4	85	340
Bestellung Webhosting	4	85	340
Zusammenarbeit mit Entwicklungs-Agentur	200	85	17’000
Testing	300	85	25’500
Extern			
Kaufpreis der Domains			250
Kaufpreis Webhosting			500
Übersetzung (EN) Kontrolle	50	150	7’500
Übersetzung (IT) Webseite und Dokumente	200	150	30’000
Übersetzung (FR) Webseite und Dokumente	200	150	30’000
Design Logo und Primärfarben			5’000
Design Bilder und Icons			20’000
Entwicklung von Framework und Recommender-System durch Agentur	500	175	87’500
Total:			**305’020**

5. Mockups

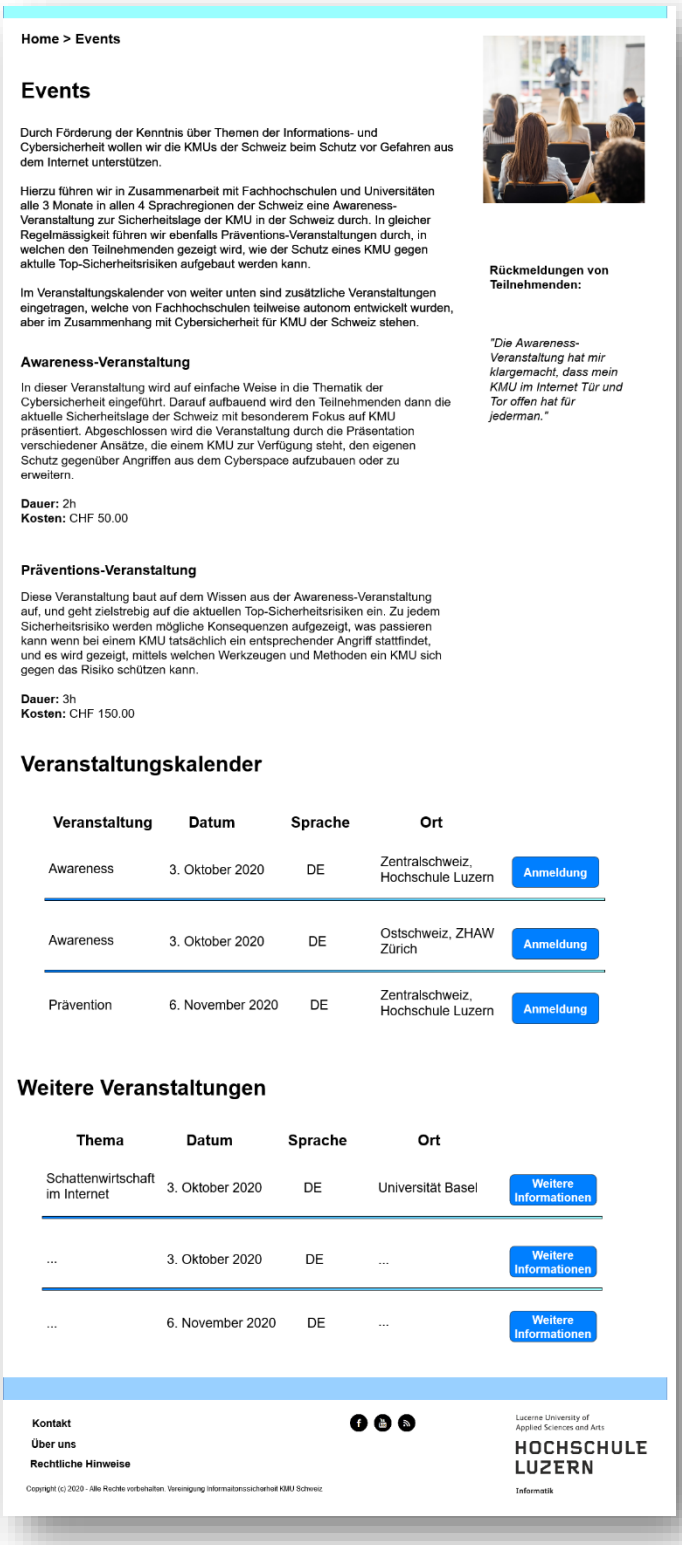
5.1. Index



5.2. Vorfall melden



5.3. Events



Home > Events

Events

Durch Förderung der Kenntnis über Themen der Informations- und Cybersicherheit wollen wir die KMUs der Schweiz beim Schutz vor Gefahren aus dem Internet unterstützen.

Hierzu führen wir in Zusammenarbeit mit Fachhochschulen und Universitäten alle 3 Monate in allen 4 Sprachregionen der Schweiz eine Awareness-Veranstaltung zur Sicherheitslage der KMU in der Schweiz durch. In gleicher Regelmässigkeit führen wir ebenfalls Präventions-Veranstaltungen durch, in welchen den Teilnehmenden gezeigt wird, wie der Schutz eines KMU gegen aktulle Top-Sicherheitsrisiken aufgebaut werden kann.

Im Veranstaltungskalender von weiter unten sind zusätzliche Veranstaltungen eingetragen, welche von Fachhochschulen teilweise autonom entwickelt wurden, aber im Zusammenhang mit Cybersicherheit für KMU der Schweiz stehen.

Awareness-Veranstaltung

In dieser Veranstaltung wird auf einfache Weise in die Thematik der Cybersicherheit eingeführt. Darauf aufbauend wird den Teilnehmenden dann die aktuelle Sicherheitslage der Schweiz mit besonderem Fokus auf KMU präsentiert. Abgeschlossen wird die Veranstaltung durch die Präsentation verschiedener Ansätze, die einem KMU zur Verfügung steht, den eigenen Schutz gegenüber Angriffen aus dem Cyberspace aufzubauen oder zu erweitern.

Dauer: 2h
Kosten: CHF 50.00

Präventions-Veranstaltung

Diese Veranstaltung baut auf dem Wissen aus der Awareness-Veranstaltung auf, und geht zielstrebig auf die aktuellen Top-Sicherheitsrisiken ein. Zu jedem Sicherheitsrisiko werden mögliche Konsequenzen aufgezeigt, was passieren kann wenn bei einem KMU tatsächlich ein entsprechender Angriff stattfindet, und es wird gezeigt, mittels welchen Werkzeugen und Methoden ein KMU sich gegen das Risiko schützen kann.

Dauer: 3h
Kosten: CHF 150.00

Rückmeldungen von Teilnehmenden:

"Die Awareness-Veranstaltung hat mir klargemacht, dass mein KMU im Internet Tür und Tor offen hat für jederman."

Veranstaltungskalender

Veranstaltung	Datum	Sprache	Ort	
Awareness	3. Oktober 2020	DE	Zentralschweiz, Hochschule Luzern	Anmeldung
Awareness	3. Oktober 2020	DE	Ostschweiz, ZHAW Zürich	Anmeldung
Prävention	6. November 2020	DE	Zentralschweiz, Hochschule Luzern	Anmeldung

Weitere Veranstaltungen

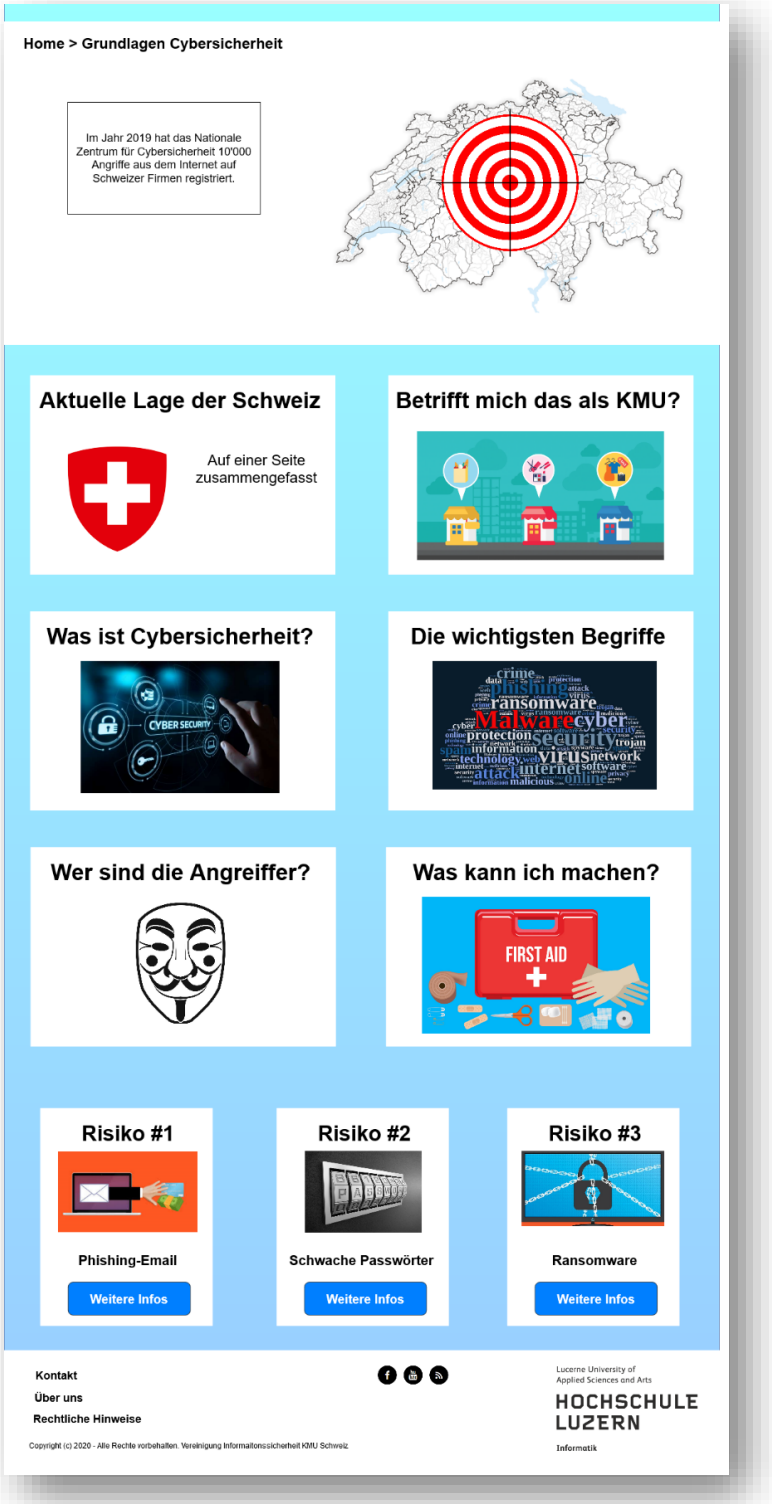
Thema	Datum	Sprache	Ort	
Schattenwirtschaft im Internet	3. Oktober 2020	DE	Universität Basel	Weitere Informationen
...	3. Oktober 2020	DE	...	Weitere Informationen
...	6. November 2020	DE	...	Weitere Informationen

Kontakt
Über uns
Rechtliche Hinweise

Copyright (c) 2020 - Alle Rechte vorbehalten. Vereinigung Informationssicherheit KMU Schweiz

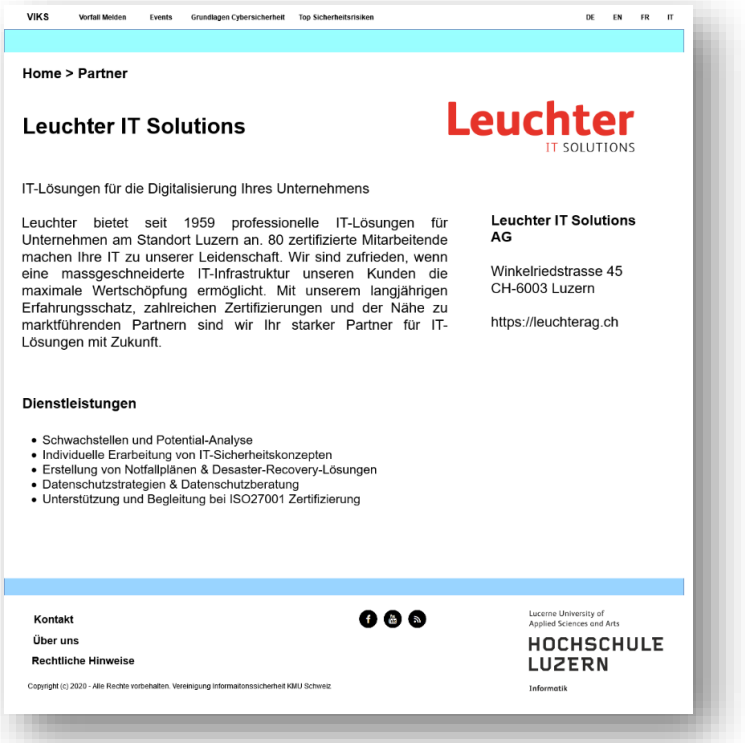
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
Informatik

5.4. Grundlagen Cybersicherheit

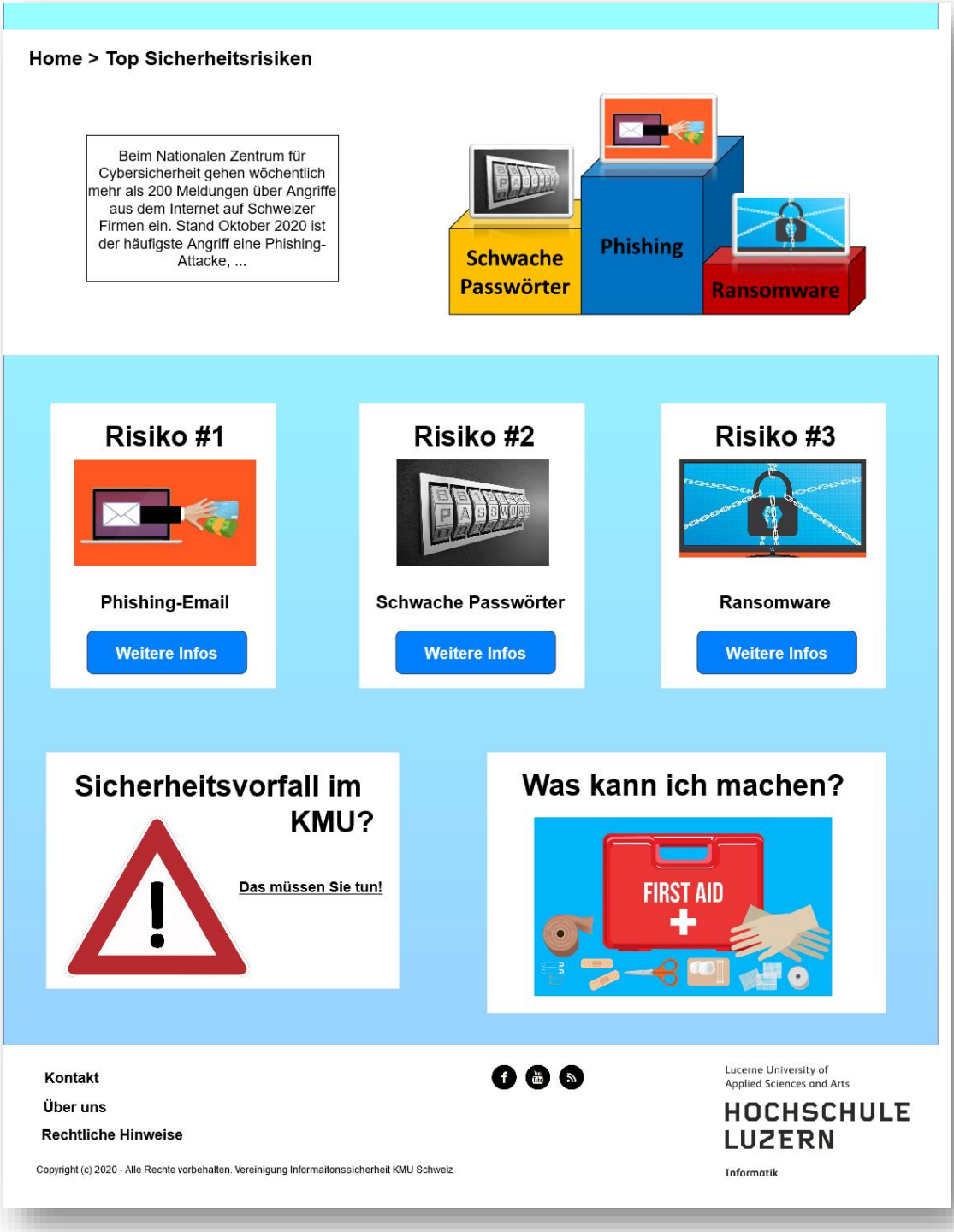


5.5. Partner

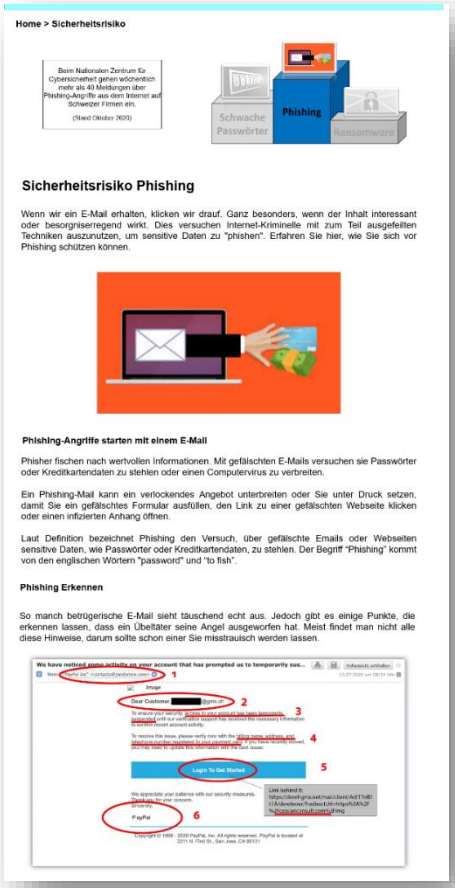

VIKS
Vorfall Melden
Events
Grundlagen Cybersicherheit
Top Sicherheitsrisiken
DE EN FR IT
Home > Partner
Hochschule Luzern
Das grösste Informatik-Bildungsangebot unter einem Dach.
Die Hochschule Luzern – Informatik bietet Bachelor- und Master-Studiengänge, anwendungsorientierte Forschung und Entwicklung sowie Weiterbildungsangebote der Informatik und Wirtschaftsinformatik auf einem Campus. Insbesondere die Aus- und Weiterbildungsangebote Bachelor in Information & Cyber Security und CAS-/MAS in Information & Cyber Security vermitteln das notwendige Fachwissen, um Unternehmen und Verwaltungen vor Hacker-Angriffen zu schützen und mit einer sicheren IT-Infrastruktur auszustatten.
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
Informatik
Hochschule Luzern – Informatik
Campus Zug-Rotkreuz
Suurstoffi 1
CH-6343 Rotkreuz
Aus- und Weiterbildungen
Bachelor in Information & Cyber-Security
CAS Information-Security Technology
CAS Information-Security Management
CAS Information-Security Advanced
CAS Cyber Security Defence & Response
CAS Cyber Investigations & Digital Forensics
CAS Data Privacy Officer
MAS Information & Cyber Security
MAS Information Security & Privacy
Kontakt
Über uns
Rechtliche Hinweise
Copyright (c) 2020 - Alle Rechte vorbehalten. Vereinigung Informaitonssicherheit KMU Schweiz
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
Informatik


VIKS
Vorfall Melden
Events
Grundlagen Cybersicherheit
Top Sicherheitsrisiken
DE EN FR IT
Home > Partner
Leuchter IT Solutions
Leuchter
IT SOLUTIONS
IT-Lösungen für die Digitalisierung Ihres Unternehmens
Leuchter bietet seit 1959 professionelle IT-Lösungen für Unternehmen am Standort Luzern an. 80 zertifizierte Mitarbeitende machen Ihre IT zu unserer Leidenschaft. Wir sind zufrieden, wenn eine massgeschneiderte IT-Infrastruktur unseren Kunden die maximale Wertschöpfung ermöglicht. Mit unserem langjährigen Erfahrungsschatz, zahlreichen Zertifizierungen und der Nähe zu marktführenden Partnern sind wir Ihr starker Partner für IT-Lösungen mit Zukunft.
Leuchter IT Solutions AG
Winkelriedstrasse 45
CH-6003 Luzern
https://leuchterag.ch
Dienstleistungen
Schwachstellen und Potential-Analyse
Individuelle Erarbeitung von IT-Sicherheitskonzepten
Erstellung von Notfallplänen & Desaster-Recovery-Lösungen
Datenschutzstrategien & Datenschutzberatung
Unterstützung und Begleitung bei ISO27001 Zertifizierung
Kontakt
Über uns
Rechtliche Hinweise
Copyright (c) 2020 - Alle Rechte vorbehalten. Vereinigung Informaitonssicherheit KMU Schweiz
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
Informatik

5.6. Top Sicherheitsrisiken



5.7. Sicherheitsrisiko



Home > Sicherheitsrisiko

Beim Nationalen Zentrum für Cybersicherheit gehen wöchentlich mehr als 40 Meldungen über Phishing-Angriffe aus dem Internet auf Schweizer Firmen ein.

(Stand Oktober 2020)

Sicherheitsrisiko Phishing

Wenn wir ein E-Mail erhalten, klicken wir drauf. Ganz besonders, wenn der Inhalt interessant oder besorgniserregend wirkt. Dies versuchen Internet-Kriminelle mit zum Teil ausgefeilten Techniken auszunutzen, um sensitive Daten zu "phishen". Erfahren Sie hier, wie Sie sich vor Phishing schützen können.

Phishing-Angriffe starten mit einem E-Mail

Phisher fischen nach wertvollen Informationen. Mit gefälschten E-Mails versuchen sie Passwörter oder Kreditkartendaten zu stehlen oder einen Computervirus zu verbreiten.

Ein Phishing-Mail kann ein verlockendes Angebot unterbreiten oder Sie unter Druck setzen, damit Sie ein gefälschtes Formular ausfüllen, den Link zu einer gefälschten Webseite klicken oder einen infizierten Anhang öffnen.

Laut Definition bezeichnet Phishing den Versuch, über gefälschte Emails oder Webseiten sensitive Daten, wie Passwörter oder Kreditkartendaten, zu stehlen. Der Begriff "Phishing" kommt von den englischen Wörtern "password" und "to fish".

Phishing Erkennen

So manch betrügerische E-Mail sieht täuschend echt aus. Jedoch gibt es einige Punkte, die erkennen lassen, dass ein Übeltäter seine Angel ausgeworfen hat. Meist findet man nicht alle diese Hinweise, darum sollte schon einer Sie misstrauisch werden lassen.

1 "PayPal Inc" contacto@jondemon.com - Nicht immer ist steckt hinter dem Absender das, was davor angeschrieben steht. Kontrollieren Sie darum die Absenderadresse genau.

2 Lieber Kunde... - Trauen Sie keiner E-Mail mit einer allgemeinen Anrede.

3 Ihr Zugang wurde zeitweilig aufgehoben - Seien Sie misstrauisch bei E-Mails, die "umgehendes Handeln" erfordern oder sonst versuchen, Sie unter Druck zu setzen.

4 Sende deine detaillierte Adresse und dein Passwort - Geben Sie nie Benutzername, Passwort oder detaillierte Adressangaben via E-Mail weiter.

5 Klick hier - Ein Link in einer E-Mail? Fahren Sie mit der Maus darüber und finden Sie heraus, wo der Link wirklich hinführt.

6 P ayPal - Seien Sie misstrauisch gegenüber E-Mails mit Rechtschreib- und Grammatikfehlern.

7 rechnung.zip - Öffnen Sie nur E-Mail-Anhänge von Absendern, denen Sie vertrauen und die Sie erwartet haben. Auch Mails mit Anhängen von Freunden oder Verwandten sollte man genauer prüfen - deren E-Mail-Konten könnten infiziert oder gehackt sein.

Testen Sie Ihr Phising-Wissen

Machen Sie das Quiz von «eBanking – aber sicher!».

Sind Sie auf ein Phishing-Mail hereingefallen?

Keine Panik – so etwas kann jedem passieren. Je nachdem, welche Informationen Sie preisgegeben haben, haben Sie verschiedene Möglichkeiten:

Nehmen Sie Kontakt zu Ihrer Bank auf und sperren Sie Ihre Kreditkarte und ggf. Ihr Konto.

Informieren Sie Unternehmen oder Institution, von denen die E-Mail vermeintlich versendet wurde.

Ändern Sie alle Passwörter, die gestohlen worden sein könnten. Wenn zum Beispiel Ihr E-Mail-Passwort „gephisht" wurde, überlegen Sie, ob der Phisher mit dem Zugriff auf Ihre E-Mails noch weitere Passwörter besitzen könnte.

Beobachten Sie all Ihre Online-Konten wie Amazon, Facebook etc. und melden Sie verdächtige Vorfälle. Es kann nicht schaden, die Passwörter zu ändern.

Stellen Sie sicher, dass Ihr Antivirenprogramm auf dem neusten Stand ist und starten Sie einen Virenscan auf Ihrem Computer.

Haben Sie ein Phishing-Mail entdeckt?

Helfen Sie mit, das Internet sicherer zu machen! Melden Sie die Phishing-Adresse.

Weitere Sicherheitsrisiken

Risiko #2

Schwache Passwörter

Weitere Infos

Risiko #3

Ransomware

Weitere Infos

Kontakt
Über uns
Rechtliche Hinweise

Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
Informatik

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Anhang B

Netzwerk

Inhalt

Autoren: René Hüsler, Ursula Sury, Nicole Wettstein, Pascal Engel, Cyrill Gössi
Verfasst: 18.12.2020, Rotkreuz

1. Phasen des Netzwerk Aufbaus

Der Aufbau des Netzwerks wird in verschiedenen Phasen verlaufen. In der ersten Phase werden, die aus der Sicht des Projektteams, wichtigsten Player abgeholt. In einer weiteren Phase folgen die Verbände und Gewerkschaften sowie Vertreter von Sicherheitsdienstleister. Das Projektteam führt eine Liste mit potenziellen Netzwerkpartner, welche Verlaufe der Starthase des Vereins angegangen werden sollen. Für die Startphasen sind dies primär Partner aus den folgenden Sektoren:

- Fachhochschulen
- Universitäten
- Bund und Kantone
- Gewerbe- und Wirtschaftsverbände
- Sicherheitsdienstleister

2. Arbeiten durch Interne

Beim Ausbau des Netzwerks werden die folgenden Arbeiten durch interne Mitarbeitende durchgeführt:

- Potenzielle Netzwerkpartner evaluieren
- Kontaktaufnahme mit den potentiellen Netzwerkpartnern
- Präsentationen und Workshops mit den potenziellen Netzwerkpartnern
- Ausbau und Pflege bestehender Zusammenarbeiten
    - Koordinationssitzungen
    - Bestehende Angebote der Netzwerkpartner abgleichen
    - Marketing Aktivitäten koordinieren
    - Austausch der Netzwerkpartner pflegen
- Besuch von Veranstaltungen der Netzwerkpartner

3. Aufwand und Kosten

Aufgrund der Abschätzung des Aufwands ergibt sich folgende Abschätzung der Kosten, welche für den Aufbau des Netzwerks anfallen werden:

Kostenpunkt	Aufwand [h]	Ansatz [CHF / h]	Sub-Total [CHF]
Evaluation potenzieller Netzwerk-partner	400	85	34’000
Kontaktaufnahme mit dem potenti-ellen Netzwerkpartner	400	85	34’000
Präsentationen und Workshops mit den potenziellen Netzwerkpartner	650	85	55’000
Ausbau und Pflege der bestehenden Netzwerkpartner • Koordinationssitzungen • Bestehende Angebote der Netzwerkpartner abglei-chen	1600	85	136’000

• Marketing Aktivitäten koordinieren • Austausch der Netzwerkpartner pflegen			
Besuch von Veranstaltungen der Netzwerkpartner	400	85	34’000
Weitere Auslagen			55’000
Total:			**348’000**

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Anhang C

Eigene Angebote

Inhalt

Autoren: René Hüsler, Ursula Sury, Nicole Wettstein, Pascal Engel, Cyrill Gössi
Verfasst: 18.12.2020, Rotkreuz

1. Eigene Angebote

Im Bereich der eigenen Angebote führt der Verein gezielt und abgestimmt auf das Bedürfnis der Zielgruppen eigene Awareness- und Präventionsveranstaltungen durch. Der Fokus liegt dabei auf neuen Formaten, die interaktive Elemente enthalten und so eine grösstmögliche Attraktivität zur Teilnahme und einen grösstmöglichen Erfolg versprechen. Der Verein wird seinen Netzwerkmitgliedern zudem ein Monitoring der Schweizer Medienlandschaft mit Stellungnahmen anbieten. Dies ist ein Mehrwert, der einen weiteren wichtigen Beitrag zur Sensibilisierung für das Thema leistet. Als weiteres eigenes Angebot ist ein Awareness-Siegel geplant, das als ein Anreiz-System für KMU dienen soll, um sich proaktiv und langfristig mit dem Thema Cybersicherheit auseinander zu setzen. KMU, die regelmässig Awareness-Veranstaltungen besuchen, erhalten vom Verein ein Gütesiegel, mit dem sie ihren Kunden zeigen können, dass für sie Cybersicherheit ein wichtiges Thema ist, das ernst genommen wird und mit dem sie sich von der Konkurrenz abheben.

2. Arbeiten durch Interne

Bei dem Aufbau und der Gestaltung der eigenen Angebote werden die folgenden Arbeiten durch interne Mitarbeitende durchgeführt:

- Entwicklung der Awareness- und Präventionsveranstaltungen
- Koordination von Awareness- und Präventionsveranstaltungen mit anderen Netzwerkpartner
- Erstellung der Schulungsunterlagen
- Erstellung von Workshops
- Entwicklung des Konzepts für Awareness-Siegel und Definition der Zusammenarbeit mit anderen Labels
- Aufbau und Betrieb eines Monitorings der Medienlandschaft

3. Aufwand und Kosten

Aufgrund der Abschätzung des Aufwands ergibt sich folgende Abschätzung der Kosten, welche für den Aufbau des Netzwerks anfallen werden:

Kostenpunkt	Aufwand [h]	Ansatz [CHF / h]	Sub-Total [CHF]
Intern			
Entwicklung von Awareness- und Präventionsveranstaltungen sowie Workshops	600	85	51’000
Koordination von Awareness- und Präventionsveranstaltungen mit anderen Netzwerkpartner	90	85	7’650
Koordination Awareness-Siegel	145	85	12’000
Konzept und Betrieb Medien-Monitoring	250	85	21’250
Extern			
Medien-Monitoring			33’000
Total:			**125’000**

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Anhang D

Marketing

Inhalt

Autoren: René Hüsler, Ursula Sury, Nicole Wettstein, Pascal Engel, Cyrill Gössi
Verfasst: 18.12.2020, Rotkreuz

1. Marketing

Der Hauptfokus im Bereich Marketing und Kommunikation liegt in einer direkten Ansprache der Wirtschafts- und Branchenverbänden, die Empfehlungen für ihre Mitglieder (KMU und/oder Sicherheitsdienstleister) aussprechen können sowie in der Kommunikation mit Entscheidungstragenden von KMU. Die Wirtschafts- und Branchenverbände sollen dabei als Netzwerkpartner gewonnen werden, ihre Ansprache erfolgt über persönliche Meetings im Rahmen der Arbeiten zum Netzwerkaufbau. Idealerweise beinhalten die Partnerschaften kostenlose Kommunikationsmöglichkeiten zur Bekanntmachung von ITSec4KMU, z.B. in Form von Berichten in Fachzeitschriften, Newsletter, Blogs, etc. der Netzwerkpartner.

2. Arbeiten

Für die direkte Ansprache der Entscheidungstragenden der KMU sind die folgenden Marketingmassnahmen vorgesehen:

- Suchmaschinenmarketing (Google Ads, sowie Banner-Werbung)
- Soziale Medien (LinkedIn, Facebook)
- Blogbeiträge und Newsletter
- Direktansprache z.B. via E-Mail

3. Aufwand und Kosten

Aufgrund der Abschätzung des Aufwands ergibt sich folgende Abschätzung der Kosten, welche für das Marketing anfallen werden:

Kostenpunkt	Aufwand [h]	Ansatz [CHF / h]	Sachkosten	Sub-Total [CHF]
Suchmaschinenmarketing (SEO)	40	85	10’000	13’400
Soziale Medien	100	85	8’000	16’500
Newsletter (4 Newsletter à 5h), Blog und Webseite (10 Blogs à 10h)	120	85		10’200
Flyer gestalten und drucken	10	85	4’150	5’000
Total:				**45’000**

Projektplan

Plattform ITSec4KMU

Stand	1

Geplant | Ist | Meilenste

AKTIVITÄT

ZEITRÄUME = KW

2021 | 2022

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

Interner Kickoff Startphase

Plattform

Offertenphase Plattform
Kickoff Plattform
Entwicklung Plattform (extern)
Content Entwicklung Plattform MVP (Sicherheitslage, Best-Practice-Leitfäden etc.)
Übersetzung nach Englisch
Testing
Aufschalten Plattform MVP unter itsec4kmu.ch/itsec4sme.ch
Feedback verarbeiten
Ausbau/Weiterentwicklung Plattform
Entwicklung Fachquiz
Testing Fachquiz
Übersetzung nach Französisch
Testing
Aufschalten Plattform Französisch unter itsec4pme.ch
Übersetzung nach Italienisch
Testing
Aufschalten Plattform Italienisch unter itsec4pmi.ch
Moderation Community

Netzwerk

Bestehende Netzwerkparnter informieren
Kickoff NCSC, Melani
Koordinationstreffen NCSC, Melani
Netzwerkpartner identifizieren/angehen/managen (Fokus DE)
Plattform Launch-Event (MVP)
Netzwerkpartner identifizieren/angehen/managen (Fokus FR)
Plattform Launch-Event (FR)
Netzwerkpartner identifizieren/angehen/managen (Fokus IT)
Plattform Launch-Event (IT)
Koordination gemeinsame / bestehende Angebote

Eigene Angebote

Awareness- und Präventionsveranstaltungen planen und
Awareness-Siegel koordinieren und planen
Konzipierung Medien-Monitoring
Betrieb Medien-Monitoring

Marketing

Detailiertes Marketingkonzept ausarbeiten
Textbeiträge verfssen (Blog, Newsletter etc)
Marketingmassnahmen umsetzen

Kickoff Vollbetrieb