CyberGuide

Anforderungen von KMU zur Cybersicherheit

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, CS F&EDienstleistungen (FED CS_2022)	**Status**	abgeschlossen
Projektstart	01.09.2023	**Projektende**	31.10.2024
Zeitraum	2023 - 2024	**Projektlaufzeit**	14 Monate
Keywords	Cybersicherheit, KMU, Cyber-Bewusstsein, Cyber-Resilienz, Cyber-Hygiene, Supply Chain Security, Guideline, Handlungsempfehlungen		

Projektbeschreibung

Ein erhebliches Risiko geht von Cyberangriffen auf KMUs aus, das weitreichende Folgen für sie und ihre Partner in der Lieferkette haben kann. Die Umsetzung wirksamer Cybersicherheitsmaßnahmen sind für KMU von entscheidender Bedeutung, um sich und ihre Kunden vor erheblichen finanziellen Schäden, Geschäftstätigkeitsausfällen, und Rufschädigung zu schützen. Es gibt bereits Studien, Initiativen, Strategien und Leitfäden, die sich mit dem Thema Cybersicherheit, Cyber-Resilienz und Cyber-Hygiene in Unternehmen befassen. Es fehlt jedoch ein Cybersecurity-Leitfaden, der auf die speziellen Bedürfnisse von österreichischen KMUs zugeschnitten ist.

Ausgehend von vorhandenem Wissen aus der Literatur, den Ergebnissen der Online-Umfrage und geführten Interviews wird ein Leitfaden für KMUs zur Verbesserung der Cybersicherheit, Cyber-Hygiene und Cyber-Resilienz entwickelt. Die besondere Neuheit durch CyberGuide liegt in der erhöhten Verständlichkeit des Leitfadens, sodass auch Personen, die keine Experten auf dem Gebiet der Cybersecurity sind, diesen umsetzen können. Darüber hinaus werden für bestehende Richtlinien, wie z.B. NIS2, die für KMU relevanten Inhalte identifiziert und klar herausgearbeitet. Basierend auf den erhobenen Bedürfnissen, Anforderungen und Fähigkeiten der österreichischen KMUs werden Handlungsfelder und Empfehlungen für die öffentliche Hand entwickelt.

Das Konsortium aus Brimatech und Silicon Austria Labs bildet eine optimale Kombination für eine erfolgreiche Bedarfsanalyse zum Thema Cybersecurity österreichischer KMUs, da die technische Expertise im Bereich Cybersecurity seitens SAL mit der Erfahrung in strategisch-politischen Fragestellungen und Marktforschungskompetenz von Brimatech gekoppelt wird.

Das Projekt CyberGuide fördert eine starke und widerstandsfähige KMU-Wirtschaft, die sowohl für Wachstum und Beschäftigung sorgt und letztlich auch den Wirtschaftsstandort Österreich attraktiver macht.

Abstract

A significant risk is posed by cyber-attacks on SMEs, which can have far-reaching consequences for them and their supply

chain partners. Implementing effective cybersecurity measures is critical for SMEs to protect themselves and their customers from significant financial damage, unintended business downtime, and reputational harm. Some studies, initiatives, strategies, and guides already exist to address cybersecurity, cyber resilience, and cyber hygiene in businesses. However, a cybersecurity guideline tailored to the specific needs of Austrian SMEs is missing.

Drawing on existing knowledge from the literature, our online survey results, and conducted interviews, a guideline for SMEs to improve cybersecurity, cyber hygiene, and cyber resilience is developed. The special novelty of CyberGuide lies in the increased comprehensibility of the guideline so that even people who are not experts in the field of cybersecurity can easily implement it. Furthermore, for existing regulations, such as NIS2, the content relevant to SMEs is identified and clearly elaborated. Based on the surveyed needs, requirements, and capabilities of Austrian SMEs, fields of action and recommendations for the public authorities will be developed.

The consortium of Brimatech and Silicon Austria Labs forms an optimal combination for a successful needs analysis on the topic of cybersecurity of Austrian SMEs, as the technical expertise in the field of cybersecurity by SAL is coupled with the experience in strategic-political matters and market research competence of Brimatech. The CyberGuide project promotes a strong and resilient SME economy, which provides both growth and employment and ultimately makes Austria more attractive as a business location.

Endberichtkurzfassung

Cybersicherheit zielt darauf ab, Netz- und Informationssysteme, die Nutzerinnen und Nutzer solcher Systeme und andere von Cyberbedrohungen betroffenen Personen zu schützen. Diese umfassende Perspektive reicht von der Absicherung einzelner Geräte und Netzwerke bis zur Etablierung einer gefestigten Sicherheitskultur durch Mitarbeiterschulungen und Awareness-Trainings. Ein gut strukturiertes Risikomanagement stärkt die Abwehr gegen potenzielle Cyberangriffe und -vorfälle.

Die gegenständliche Studie CyberGuide wurde im Rahmen des österreichischen Förderprogramms für Sicherheitsforschung, KIRAS, als F&E Dienstleistung „Anforderungen von KMU zur Cybersicherheit“ ausgeschrieben. Ziel ist es, die gegenwärtige Situation in österreichischen KMU zu analysieren, einen Leitfaden zu entwickeln, Handlungsfelder darzustellen und Handlungsempfehlungen für eine erhöhte Cybersicherheit abzuleiten.

Dabei werden Fragen beantwortet wie: Welche Fähigkeiten zur Cybersicherheit sind bei österreichischen KMU vorhanden? Welche Standards bestehen, sind für KMU relevant und den KMU bekannt? Mit welchen Herausforderungen sind KMU konfrontiert? Welche Bedürfnisse hinsichtlich Cybersicherheit haben KMU?

Die Fähigkeiten österreichischer KMU variieren deutlich nach Unternehmensgröße. Sei es in Bezug auf die Häufigkeit von Risikobewertungen, der unterschiedlich implementierten Sicherheitsmaßnahmen oder der Investitionen in Cybersicherheit. Während mittlere Unternehmen tendenziell häufiger Risikobewertungen durchführen, sind Kleinst- und kleine Unternehmen hier zurückhaltender. Die am weitesten verbreitete Cybersicherheitsmaßnahme sind regelmäßige Sicherheitsupdates, gefolgt von der Sicherung des Netzwerks vor unberechtigtem Zugriff von außen und der Verwendung sicherer Passwörter. Vorreiter sind mittlere Unternehmen im Bereich der klaren Zuständigkeiten und des Zugriffsmanagements nach Berechtigungskonzepten. Weniger verbreitet in KMU sind hingegen Maßnahmen wie regelmäßige Mitarbeiterschulungen und

das Erstellen von Notfallplänen. Zusätzlich ergreifen die meisten KMU entweder keine oder nur wenige Maßnahmen zur Risiko-minimierung bei Drittanbietern. Bezüglich der Investitionen in die Cybersicherheit, gibt ein Fünftel der KMU an, dass sie keine gezielten Investitionen tätigen. Bei Unternehmen mit gezielten Investitionen werden großteils 6-10 % des IT-Budgets für Cybersicherheit verwendet.

Es bestehen zahlreiche Cybersecurity-Standards , die für KMU in Österreich relevant sein könnten, abhängig von ihrer Branche und den gesetzlichen Vorgaben. Internationale und nationale Organisationen wie ISO, IEC, NIST und BSI bieten verschiedene Normen an, die eine Orientierung in der IT-Sicherheit geben, beispielsweise die ISO/IEC 27001 für Informationssicherheitsmanagement. Dennoch zeigt sich, dass viele KMU nur eine begrenzte Kenntnis über diese Standards und Richtlinien haben. Bekannte Verordnungen wie die Datenschutzgrundverordnung sind den meisten KMU geläufig, während neuere oder spezialisierte Regelungen wie der Digital Operational Resilience Act kaum bekannt sind. Für KMU sind weniger aufwändige Grundschutz-Varianten (wie die des BSI oder der WKO) oft praktikabler und sollten als Mindeststandard etabliert sein

Die Herausforderungen für KMU sind vielfältig und reichen von begrenzten finanziellen Ressourcen über fehlendes Bewusstsein für die Bedeutung von Cybersicherheit bis hin zu einem Mangel an Fachkräften. Zusätzlich steigen Compliance-Anforderungen und Cyberkriminelle entwickeln zunehmend raffiniertere Angriffsstrategien. Viele Angriffe, wie Phishing oder Social Engineering, nutzen gezielt menschliche Schwächen aus. Hinzu kommt, dass die Komplexität des Themas und das Fehlen maßgeschneiderter, kostengünstiger Lösungen, die den Bedürfnissen KMU gerecht werden, den Einstieg zusätzlich erschweren.

Der Wunsch nach praxisnaher Unterstützung und passgenauen Cybersicherheitslösungen prägt die Bedürfnisse österreichischer KMU. Viele Unternehmen möchten ihre Sicherheitsrichtlinien und -technologien modernisieren sowie gezielt IT-Expertise aufbauen, stoßen jedoch auf finanzielle und technische Hürden. Daher wünschen sie sich vor allem finanzielle Förderungen, kostengünstige Beratung und Schulungen, die speziell auf die Bedürfnisse kleinerer Betriebe zugeschnitten sind. Zusätzlich streben sie nach einfacheren und erschwinglichen Cybersecurity-Lösungen, die weniger komplex und schneller implementierbar sind. Der Wunsch nach einem niederschwelligen Zugang zu europäischer IT-Sicherheit und einer Notfall-Hotline für akute Probleme verdeutlicht, dass KMU einen flexiblen, bedarfsgerechten Ansatz zur Verbesserung ihrer Cybersicherheit bevorzugen.

Zur Stärkung der Cybersicherheit in österreichischen KMU wurden vier zentrale Handlungsfelder identifiziert. Zunächst ist es entscheidend, Cybersicherheit fest im Unternehmen zu verankern. Dies geschieht aufgrund von klaren Verantwortlichkeiten, regelmäßigen Trainings und einer offenen Fehler- und Kommunikationskultur. Darauf aufbauend hilft ein strukturiertes Risikomanagement, Bedrohungen frühzeitig zu erkennen und gezielt Maßnahmen zu priorisieren. Ergänzend hierzu sind technologische Schutzmaßnahmen wie Netzwerksicherheit und Endgeräteschutz unerlässlich, um gegen Cyberangriffe gewappnet zu sein. Schließlich spielt die Einhaltung gesetzlicher Vorgaben eine wesentliche Rolle, um rechtliche Risiken zu minimieren und Sicherheitsstandards nachhaltig zu sichern. Daraus resultieren Handlungsempfehlungen für die öffentliche Hand: Bewusstsein bilden, Mitarbeiterschulungen subventionieren, Cybersecurity Tool und Services Datenbank aufbauen, Open Source Paket und KMU-Ratgeber bereitstellen.

Der CyberGuide für KMU - Praxisleitfaden für Cybersicherheit ist ein Leitfaden, der speziell auf die Bedürfnisse von KMU

zugeschnitten ist. Die enthaltenen 19 Maßnahmen sind leicht-verständlich formuliert, schrittweise aufgebaut und erfordern keine umfassenden IT-Vorkenntnisse. Der Leitfaden bietet grundlegende Sicherheitsmaßnahmen, die jedes KMU umsetzen sollte. Die Maßnahmen sind in fünf Abschnitte unterteilt, die auf unterschiedliche Aspekte der Cybersicherheit abzielen: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

Die Politik steht in der Verantwortung, in den kommenden Jahren klare Leitlinien, verbindliche Vorgaben und wirkungsvolle Anreizsysteme zur Förderung der Cybersicherheit in KMU zu formulieren. Die Studie CyberGuide kann eine Basis für weitere strategiepolitische Maßnahmen seitens der öffentlichen Hand sein.

Projektkoordinator

- BRIMATECH Services GmbH

Projektpartner

- Silicon Austria Labs GmbH