Oktober 2023

CyberSicherheit für Berufsbildung und KMU

EUROPÄISCHES CURRICULUM FÜR CYBERSICHERHEIT

ENTWICKELT VON META4 INNOVATIONS E. U.

ARBEITSPAKET 3 - EUROPÄISCHES CURRICULUM FÜR CYBERSICHERHEIT

Kofinanziert von der Europäischen Union

Finanziert von der Europäischen Union. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die des Autors/der Autoren und spiegeln nicht unbedingt die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können für diese verantwortlich gemacht werden. KA220-VET-C9588303

INHALT

ÜBER DAS PROJEKT

SecureFuture - CyberSecurity for VET and SMEs - ist ein Erasmus+ Projekt, das zwischen Dezember 2022 und Dezember 2024 durchgeführt wird. Das Projekt wird von einem Konsortium aus sechs Partnern aus fünf Ländern durchgeführt, die alle über einschlägiges Fachwissen im Bereich der beruflichen Aus- und Weiterbildung (VET) und der Cybersicherheit verfügen.

LAND	ORGANISATION
Türkiye	Istanbul Ticaret Universitesi (Koordinator)
Türkiye	Istanbul Valiligi
Portugal	Mindshift Talent Advisory
Spanien	Media Creativa 2020
Italien	Pragma Engineering
Österreich	Meta4 Innovations

Das SecureFuture-Konsortium hat festgestellt, dass die derzeitige Ausbildung an den Berufsschulen in der Europäischen Union (EU) den Anforderungen des Arbeitsmarktes nicht gerecht wird und dass es Länder gibt, in denen es keine Ausbildung im Bereich der Cybersicherheit auf diesem Niveau gibt. Außerdem verfügen viele kleine und mittlere Unternehmen (KMU) nicht über qualifizierte MitarbeiterInnen, um ihre Unternehmen vor Cyber-Bedrohungen zu schützen, und die Suche nach externer Unterstützung im Bereich der Cybersicherheit ist sehr kostspielig.

Unter Berücksichtigung dieser Aspekte entwickelt das Projekt einen europäischen Rahmen, einen Curriculum und Schulungsinhalte zur Cybersicherheit, um Berufsbildungssysteme und KMUs zu leiten, die ihre SchülerInnen und Angestellten mit Cybersicherheitskompetenzen ausstatten wollen. Dieses Dokument bezieht sich auf den Europäischen Curriculum für Cybersicherheit.

SYNOPSE

Das vorgeschlagene europäische Cybersicherheits-Curriculum ist das Endergebnis des Arbeitspakets 3 des Projekts: AP3 - Europäisches Cybersicherheits-Curriculum.

Der Leiter von AP3 - Meta4 Innovations e. U. - erstellte einen Arbeitsplan, Richtlinien und Vorlagen für alle Partner, um die Gestaltung und Entwicklung eines vorgeschlagenen europäischen Cybersicherheits-Curriculums zu erleichtern. Als ein miteinander verbundener Entwicklungsprozess wird dieses europäische Cybersicherheits-Curriculum durch den Vergleich der aktuellen nationalen Kompetenzen im Bereich der Cybersicherheit, die von allen Partnern gemeinsam entwickelt wurden, durch den Rahmen gestaltet.

Im Juli 2023 wurde in allen Partnerländern - Österreich, Italien, Portugal, Spanien und der Türkei - eine europaweite Umfrage durchgeführt, bei der 66 ExpertInnen ihre Beiträge lieferten, um einen Überblick über die jeweiligen nationalen Bedürfnisse in Bezug auf den Curriculum für das Projekt zu erhalten. Diese Beiträge wurden von Meta4 zusammengefasst und mit den Partnern geteilt, um die Lerneinheiten dieses europäischen Cybersicherheits-Curriculums zu vereinbaren.

1. CURRICULUM

ÜBERBLICK

In Anbetracht des heterogenen Einsatzes von ECVET in den Partnerländern, der durchschnittlichen ECVET-Punkte pro Ausbildungsstunde, einigte sich die Partnerschaft des SecureFuture-Projekts wie folgt:

20 Stunden Ausbildung = 1 ECVET-Punkt

Das Europäische Cybersecurity Curriculum umfasst 10 Module mit einem Umfang von 120 Stunden, was 6 ECVET-Punkten entspricht.

Einheit 1: Einführung in die Cybersicherheitsverteidigung

Einführung

Das Modul "Einführung in die Cybersicherheitsverteidigung" ist ein grundlegender Einblick in die Cybersicherheit für KMU. Es vermittelt ein umfassendes Verständnis der zentralen Konzepte und Grundsätze, die für den Schutz digitaler Systeme und Daten angesichts der sich ständig ändernden Bedrohungen entscheidend sind. Dieses Modul stattet die Lernenden mit den wesentlichen Kenntnissen und Fähigkeiten aus, die sie benötigen, um sich gegen Cybersecurity-Bedrohungen zu verteidigen und kritische Informationsbestände in der heutigen dynamischen Landschaft zu schützen.

Zielsetzung

Ziel ist es, den TeilnehmerInnen ein solides Verständnis der wichtigsten Cybersicherheitskonzepte und -prinzipien zu vermitteln, damit sie Cyber-Bedrohungen wirksam erkennen, eindämmen und auf sie reagieren können.

LERNERGEBNISSE

Wissen	W1. Die Grundprinzipien der Cybersicherheit und des Datenschutzes zu verstehen. W2. Gemeinsame Cyber-Bedrohungen und Schwachstellen zu erkennen. W3. Die rechtlichen und ethischen Aspekte der Cybersicherheit zu verstehen.	**Fertigkeiten**	F1. Nachweis der Fähigkeit, den Netzverkehr auf verdächtige Aktivitäten zu analysieren. F2. Fähigkeit, Firewalls gegen Bedrohungen und Schwachstellen zu konfigurieren. F3. Befähigung zur Durchführung von Sicherheitstests und -bewertungen.	**Verantwortung und Autonomie**	VA1. Bewertung und Priorisierung von Sicherheitsrisiken zur Entwicklung eines maßgeschneiderten Aktionsplans für Cybersicherheit. VA2. Wirksame Reaktion auf gängige Cyber-Bedrohungen wie Malware oder Phishing. VA3. Arbeitet Verfahren aus, um die Auswirkungen von Sicherheitsvorfällen zu minimieren.

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 2: Datenschutz und Privatsphäre

Einführung

Dieses Modul vermittelt den Lernenden die wesentlichen Kompetenzen für den Datenschutz im digitalen Zeitalter. Es deckt Schlüsselaspekte des Datenschutzes ab, darunter Datenklassifizierung, verantwortungsvoller Umgang mit sensiblen Informationen, Datenschutz, geistiges Eigentum und die Komplexität der Cyber-Kriegsführung. GDPR und andere Datenschutzbestimmungen werden ebenso hervorgehoben wie effektive Datenverschlüsselung, sichere Speicherpraktiken und die Reaktion auf Datenschutzverletzungen. Das Modul fördert Einstellungen, die dem Datenschutz, der Ethik und der Anpassungsfähigkeit im Bereich der Cybersicherheit Vorrang einräumen, und befähigt die Lernenden, aktiv zur digitalen Verteidigung beizutragen und wachsame Daten- und Datenschutzbeauftragte zu werden.

Zielsetzung

Die Lernenden sollen mit dem Wissen, den Fähigkeiten und der Einstellung ausgestattet werden, die erforderlich sind, um Daten effektiv zu schützen und zu verwalten, die Einhaltung der Datenschutzbestimmungen zu gewährleisten und die Privatsphäre in der Cybersicherheit zu schützen.

LERNERGEBNISSE

Wissen	W1. Definition von datenbezogenen Konzepten, einschließlich sensibler Informationen, geistigem Eigentum und Cyber-Kriegsführung W2. Datenschutzbestimmungen in Bezug auf personenbezogene Daten, digitale Daten und die allgemeine Datenschutzverordnung (GDPR) zu unterscheiden W3. Erklärung, wie wichtig es ist, eine Mentalität zu fördern, die den verantwortungsvollen Umgang mit Daten in den Vordergrund stellt	**Fertigkeiten**	F1. Geeignete Verschlüsselungstechniken für verschiedene Datentypen zuzuordnen F2. Anwendung bewährter Verfahren zur sicheren Datenspeicherung, einschließlich Verschlüsselung, Zugriffskontrolle und regelmäßiger Backups F3. Erstellung von Plänen zum Umgang mit Datenschutzverletzungen unter Berücksichtigung der Schwere der Verstöße	**Verantwortung und Autonomie**	VA1. Sensibilisierung für den Schutz von Daten und die Achtung der Rechte des Einzelnen auf Privatsphäre VA2. Einen ethischen Ansatz im Umgang mit Daten und geistigem Eigentum verfolgen VA3. Entwicklung einer widerstandsfähigen und anpassungsfähigen Haltung gegenüber den sich ständig weiterentwickelnden Bedrohungen und Vorschriften für die Cybersicherheit

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 3: Risikomanagement und Einhaltung der Vorschriften

Einführung

Dieses Modul vermittelt wesentliche Kompetenzen für das Management von Cybersicherheitsrisiken und die Sicherstellung der Compliance. Es integriert das Cyber-Risikomanagement in unternehmensweite Risikomanagementpraktiken und erkennt an, dass eine vollständige Beseitigung von Risiken unerreichbar ist. Stattdessen konzentriert es sich darauf, die Auswirkungen von Bedrohungen durch effektive Cyber-Risikomanagement-Programme zu reduzieren. Das Modul führt die Lernenden in international anerkannte Standards ein, insbesondere in das Informationssicherheitsmanagementsystem (ISMS), und zeigt die wichtigsten Schritte und Checklisten für die Einhaltung der Standards auf. Zusätzlich zu den Kenntnissen und Fertigkeiten unterstreicht das Modul die Entwicklung von Einstellungen im Zusammenhang mit der Anwendung von ISMS-Konformitätsschemata und Empfehlungen zur Risikoanalyse, -erkennung und -minderung, wodurch die Lernenden in die Lage versetzt werden, sich proaktiv mit Bedrohungen der Cybersicherheit auseinanderzusetzen und diese zu bewältigen, indem sie einen systemischen Ansatz für die Informationssicherheit verfolgen.

Zielsetzung

Die Lernenden sollen mit dem Wissen, den Fähigkeiten und der Einstellung ausgestattet werden, die erforderlich sind, um Risikomanagement-Methoden, die sich auch auf internationale Compliance-Regeln für Cybersicherheit beziehen, effektiv anzuwenden.

LERNERGEBNISSE

Wissen	W1. Komponenten und Anforderungen eines Informationssicherheitsmanagementsystems zu definieren W2. Identifizierung des Informationsrisikomanagements als Funktion des Informationssicherheitsmanagementsystems W3. Beschreibung des Ansatzes für die Einhaltung der Cybersicherheitsvorschriften	**Fertigkeiten**	F1. Identifizierung der Hauptkomponenten des Informationssicherheitsmanagementsystems F2. Design-Risikomanagement-Systeme für KMU F3. Prüfung der Anforderungen an die Einhaltung der Cybersicherheitsvorschriften	**Verantwortung und Autonomie**	VA1: Zusammenarbeit bei der Definition des Informationssicherheitsmanagementsystems von KMU VA2. Einhalten des Risikomanagementprozesses VA3. Umgang mit der Verabschiedung von Regeln zur Einhaltung der Cybersicherheit

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 4: Social Engineering und Phishing-Bewusstsein

Einführung

Diese Lerneinheit konzentriert sich auf Social Engineering und Phishing, die in unserer digital vernetzten Welt lebenswichtig sind. Diese Themen sind ebenso wichtig wie die transformativen Auswirkungen von Cloud-Systemen auf Unternehmen. Am Ende der Einheit werden die Lernenden Social Engineering definieren, die Beweggründe (wie finanzieller Gewinn und Datendiebstahl) verstehen und verschiedene Phishing-Techniken und Angriffsvektoren erkennen, die von Cyberkriminellen verwendet werden. Dies verbessert ihre Fähigkeiten zur Erkennung von und Reaktion auf Bedrohungen. Die Lernenden werden auch die rechtlichen und ethischen Auswirkungen von Social-Engineering-Angriffen verstehen und verantwortungsvolle Praktiken im Bereich der Cybersicherheit fördern. Die Einheit schärft das ethische Bewusstsein, fördert die Zusammenarbeit bei der Reaktion auf Vorfälle und betont die Einhaltung gesetzlicher Vorschriften. Sie befähigt IT-Fachleute, GeschäftsinhaberInnen, BerufsschülerInnen und alle, die ihr Wissen über Cybersicherheit für eine sichere digitale Zukunft mit Vertrauen und Integrität erweitern möchten.

Zielsetzung

Diese Lerneinheit zielt darauf ab, die TeilnehmerInnen mit dem Wissen, den Fähigkeiten und der ethischen Einstellung auszustatten, um Social Engineering zu definieren, Phishing-Techniken zu identifizieren und ihre rechtlichen und ethischen Implikationen effektiv zu verstehen.

LERNERGEBNISSE

Wissen	W1. Social Engineering und seine Beweggründe im Kontext von KMU zu definieren W2. Identifizierung von Phishing-Techniken und Angriffsvektoren, die KMU verwundbar machen W3. Auflistung von rechtlichen und ethischen Implikationen von Social Engineering im Kontext von KMU	**Fertigkeiten**	F1. Beschreiben Sie die Hauptmotivationen für Social-Engineering-Angriffe F2. Erkennen von Methoden wie Spear-Phishing, Vishing (Voice-Phishing) und Pretexting F3. Die möglichen Folgen für Täter und Opfer verstehen	**Verantwortung und Autonomie**	VA1. Förderung des ethischen Bewusstseins bei der Festlegung von Motiven des Social Engineering für eine verantwortungsvolle, prinzipienfeste Nutzung von Wissen. VA2. Zusammenarbeit mit Teams zur Entschärfung von Phishing-Bedrohungen bei der Ermittlung von Angriffstechniken. VA3. Selbstständige Einhaltung von Gesetzen und Gewährleistung der Rechtmäßigkeit von Social-Engineering-Aktionen und -Praktiken.

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 5: Cloud-Sicherheit für KMU

Einführung

Dieses Referat befasst sich mit den besonderen Sicherheitsherausforderungen, die Cloud-Systeme für KMU darstellen, die aus Gründen der Flexibilität, Skalierbarkeit und Kosteneffizienz zunehmend auf diese Systeme angewiesen sind. Sie soll KMU das Wissen und die Fähigkeiten vermitteln, die für ein effektives Cloud-Sicherheitsmanagement erforderlich sind. Die Einheit ist auf die spezifischen Bedürfnisse und Einschränkungen von KMUs zugeschnitten und bietet praktische Einblicke und umsetzbare Strategien, um Risiken zu minimieren, sensible Informationen zu schützen und die Einhaltung von Branchenvorschriften zu gewährleisten. Die Teilnehmer lernen die Grundprinzipien der Cloud-Sicherheit und modernste Technologien kennen und sammeln praktische Erfahrungen bei der Umsetzung von Sicherheitsmaßnahmen. Ob GeschäftsinhaberInnen, IT-Fachleute, Auszubildende oder jemand, der sein Wissen über Cloud-Sicherheit erweitern möchte, dieser Curriculum stattet die Lernenden mit den Werkzeugen aus, die sie benötigen, um die digitale Zukunft ihres KMUs effektiv zu sichern.

Zielsetzung

Ziel dieser Einheit ist es, den Lernenden einen Einblick in die Vorteile, möglichen Risiken und Anleitungen zur Maximierung der Auswirkungen der Nutzung von Cloud-Systemen für ein KMU zu geben.

LERNERGEBNISSE

Wissen	W1. die Vorteile der Nutzung von Cloud-Systemen für ein KMU zu ermitteln W2. die möglichen Risiken bei der Nutzung von Cloud-Systemen zu beschreiben und abzuschwächen. W3. Skizziert die präventiven Schritte, die für die Sicherheit von KMU beim Cloud Computing in Betracht gezogen werden könnten.	**Fertigkeiten**	F1. Analyse, unter welchem Aspekt und wie Cloud Computing von KMU genutzt werden kann F2. Darstellung sicherheitsrelevanter Fragen im Kontext des Risikomanagements und Erarbeitung von Lösungsvorschlägen. F3. Veranschaulichung verschiedener Arten von rechtlichen Anforderungen, die sich auf die Nutzung von Cloud-Systemen auswirken könnten	**Verantwortung und Autonomie**	VA1. Gewährleistung einer Cloud-Sicherheit in Übereinstimmung mit Personenbezogene Daten in der EU und nationale Datenschutzvorschriften VA2. Arbeiten Sie mit KollegInnen zusammen, um ein Beispielszenario für ein Cloud-System zu erstellen VA3. Leitung eines Teams zur Bewertung von Sicherheitsmöglichkeiten in einem Beschaffungsverfahren

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 6: Grundlagen der Netzwerksicherheit

Einführung

Die Netzsicherheit ist für KMU, die sich gegen Cyber-Bedrohungen schützen wollen, ein wichtiges Anliegen. Es handelt sich um einen ganzheitlichen Ansatz, der physische und softwarebasierte Schutzmaßnahmen umfasst und ein unternehmensweites Verständnis erfordert. Die Lernenden erlangen vertiefte Kenntnisse über Vorsichtsmaßnahmen, die sowohl ein konzeptionelles Verständnis als auch zwischenmenschliche Fähigkeiten umfassen. Sie lernen die Maßnahmen kennen, die KMUs zur Verwaltung der Netzwerksicherheit zur Verfügung stehen, einschließlich der Bildung spezieller Teams, die in der Lage sind, Schutzmaßnahmen durchzuführen. Diese Einheit befähigt die Teilnehmer, sich auf dem komplexen Gebiet der Netzwerksicherheit zurechtzufinden, damit sie ihr Unternehmen und ihren Betrieb wirksam vor der sich ständig weiterentwickelnden Landschaft der Cyber-Bedrohungen schützen können.

Zielsetzung

Diese Lerneinheit zielt darauf ab, den Lernenden ein grundlegendes Verständnis der Netzwerksicherheit für KMU zu vermitteln und ihnen zu zeigen, wie sie ihr Unternehmen in Richtung KMU-Sicherheit lenken können.

LERNERGEBNISSE

Wissen	W1. Erläutert die grundlegenden Begriffe und Konzepte der Netzsicherheit W2. erinnert sich an die grundlegenden Topologien und Strategien, die in der Netzkommunikation verwendet werden W3. Identifiziert physische Netzwerkverbindungselemente und physische Sicherheitsverfahren	**Fertigkeiten**	F1. Erörtert, warum Netzwerksicherheit für ein KMU wichtig ist F2. Veranschaulichung möglicher Risiken und möglicher Lösungen im Bereich der Netzsicherheit F3. Umreißt potenzielle Netzbedrohungen und wie ein KMU darauf reagieren und sie verhindern sollte.	**Verantwortung und Autonomie**	VA1. Leitet ein gebildetes Team für Netzsicherheit VA2. Gibt Empfehlungen, wie ein Unternehmen die Netzwerksicherheit in seinen Geschäftsplan integrieren kann VA3. Überprüfung und Überwachung der Umsetzung von Netzsicherheitsverfahren

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 7: Sichere Softwareentwicklung

Einführung

Angesichts der zunehmenden Cyber-Bedrohungen ist eine sichere Softwareentwicklung von größter Bedeutung. Sie erfordert die Einbettung von Sicherheitspraktiken in den gesamten Softwareentwicklungszyklus, vom Entwurf und der Kodierung bis hin zu Tests, Bereitstellung und Wartung. Ziel ist es, Daten zu schützen, die Privatsphäre der Benutzer zu wahren und die Integrität und Verfügbarkeit von Softwaresystemen zu gewährleisten. Zu den wichtigsten Grundsätzen gehören die "Defense in Depth" mit mehreren Sicherheitsebenen, "Least Privilege" für minimalen Zugriff und "Secure-by-Design" von Beginn des Projekts an. Regelmäßige Tests, einschließlich Penetrationstests und Codeüberprüfungen, sind unerlässlich. Sichere Bereitstellung, Wartung und Reaktion auf Zwischenfälle sind entscheidend für die laufende Sicherheit. Schulung und Sensibilisierung sowie unterstützende Ressourcen erhöhen die organisatorische Sicherheit weiter. Sichere Softwareentwicklung ist in der heutigen Bedrohungslandschaft unverzichtbar, um Risiken zu mindern und das Vertrauen der Benutzer zu erhalten.

Zielsetzung

Lernen Sie, sichere Softwareentwicklungspraktiken zu implementieren, um Systeme, sensible Daten und die Privatsphäre der Benutzer zu schützen und gleichzeitig die Risiken von Sicherheitsverletzungen und Cyberangriffen zu minimieren sowie Wartung, Tests und Schulungen zu gewährleisten.

LERNERGEBNISSE

Wissen	W1. Sichere Kodierungspraktiken, häufige Sicherheitsbedrohungen sowie Sicherheitsstandards und -rahmen zu definieren W2. Lernen von sicheren Entwicklungslebenszyklus und das Konfigurations-management, die sichere Bereitstellung und Wartung W3. Schwachstellenbewertung und Penetrationstests, Verschlüsselung und Kryptografie, sichere APIs und Integrationen bestimmen	**Fertigkeiten**	F1. Experimentieren Sie mit sicherer Kodierung, Schwachstellenbewertung, Sicherheitstests, Verschlüsselung und Kryptografie F2. Aufbau einer sicheren Konfigurationsverwaltung, Bereitstellung und Wartung, sicheres API-Design F3. Verbesserung der Compliance und der Datenschutzbestimmungen, kontinuierliches Lernen	**Verantwortung und Autonomie**	VA1. Beachten Sie, dass Entwickler die Verantwortung haben, der Sicherheit in ihren Programmierpraktiken Vorrang einzuräumen. VA2. Trifft Entscheidungen zu sicherheitsrelevanten Fragen während des Softwareentwicklungsprozesses. VA3. Zusammenarbeit mit Sicherheitsexperten während des Entwicklungsprozesses, um sicherzustellen, dass die Sicherheitsanforderungen ordnungsgemäß erfüllt werden.

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 8: Sicherer Endpunktschutz

Einführung

In der vernetzten Welt von heute ist der Schutz von Endgeräten wie Laptops, Desktops, mobilen Geräten und Servern vor Cyberangriffen unerlässlich. Sicherer Endpunktschutz bedeutet die Implementierung einer mehrschichtigen Verteidigungsstrategie, um diese Geräte vor Malware, Ransomware, Phishing und unberechtigtem Zugriff zu schützen. Dazu gehört der Einsatz robuster Antiviren- und Anti-Malware-Software, die Nutzung fortschrittlicher Mechanismen zur Erkennung und Abwehr von Bedrohungen, die Durchsetzung strenger Zugangskontrollen und Authentifizierungsmaßnahmen sowie die regelmäßige Aktualisierung von Software und Betriebssystemen. Ein sicherer Endgeräteschutz ist für Unternehmen aller Größen und Branchen von entscheidender Bedeutung, da er Datenschutzverletzungen verhindert, den unbefugten Zugriff auf sensible Daten unterbindet und die Geschäftskontinuität sicherstellt. Durch die Verstärkung der Endpunkte können Unternehmen das Risiko von Cyberangriffen verringern, Branchenvorschriften einhalten und ihren Ruf und das Vertrauen ihrer Kunden schützen.

Zielsetzung

Lernen Sie, wie Sie Laptops, Desktops, mobile Geräte und Server vor Malware, Ransomware, Phishing und unbefugtem Zugriff schützen, um Datenschutzverletzungen und Betriebsunterbrechungen zu vermeiden und gleichzeitig die Einhaltung von Vorschriften zu gewährleisten und das Vertrauen zu erhalten.

LERNERGEBNISSE

Wissen	W1. Verständnis der Endpunktsicherheit und einen Überblick über sichere Endpunktschutzmaßnahmen W2. Definiert die Schlüsselkomponenten des sicheren Endpunktschutzes, Antivirus, Firewall und Verschlüsselung W3. Best Practices für die Implementierung von sicherem Endpunktschutz, Patch-Verwaltung, Bedrohungserkennung und Benutzerschulung zu ermitteln	**Fertigkeiten**	F1. In der Lage sein, Malware, Ransomware und Phishing-Bedrohungen zu analysieren und darauf zu reagieren, um sie wirksam zu bekämpfen. F2. Verwaltung und Konfiguration von Sicherheitstools für Endgeräte (Antivirus, Firewalls, Verschlüsselung) für eine effektive Bereitstellung und einen effektiven Betrieb. F3. Fähigkeit zur Patch-Verwaltung, Zugriffskontrolle, Datenverschlüsselung, Benutzerbewusstsein für Endpunktsicherheit.	**Verantwortung und Autonomie**	VA1: Sicherung der Endgeräte mit Virenschutz, Firewalls und Verschlüsselung, um Bedrohungen und Schwachstellen wirksam zu bekämpfen. VA2. Verantwortung für die Endpunktsicherheit, Identifizierung und Abschwächung von Risiken, Durchführung von Bewertungen und Aufrechterhaltung der Sicherheit. VA3. Rasche Reaktion auf Sicherheitsvorfälle, Durchführung forensischer Untersuchungen, Umsetzung von Abhilfemaßnahmen, Verhinderung von Wiederholungen.

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 9: Management und Reaktion auf Zwischenfälle

Einführung

Das Management von und die Reaktion auf Vorfälle ist für die Eindämmung eines breiten Spektrums von Störungen und Bedrohungen unerlässlich. Sie dienen der effizienten Identifizierung, Analyse und Reaktion auf Vorfälle, die den Betrieb stören oder die Vermögenswerte, den Ruf und die Interessengruppen einer Organisation schädigen können. Zu diesen Vorfällen gehören Cyberangriffe, Datenschutzverletzungen, Naturkatastrophen, Unfälle und Notfälle im Bereich der öffentlichen Gesundheit. Das Hauptziel besteht darin, die Auswirkungen zu minimieren, den Betrieb wiederherzustellen und zukünftige Vorfälle zu verhindern, indem ein strukturierter Rahmen eingehalten wird. Ein erfolgreiches Vorfallmanagement erfordert auch eine klare Kommunikation und Zusammenarbeit zwischen Teams und Beteiligten. Eine solide Strategie ermöglicht es Unternehmen, Risiken proaktiv anzugehen, die Widerstandsfähigkeit zu verbessern, Ausfallzeiten zu reduzieren, Daten zu schützen, Vorschriften einzuhalten und ihren Ruf zu wahren.

Zielsetzung

Lernen Sie, effektiv zu reagieren, um die Auswirkungen von Zwischenfällen zu minimieren, einschließlich der sofortigen Erkennung, der Mobilisierung von Ressourcen, der koordinierten Reaktion und der schnellen Wiederherstellung des normalen Betriebs für die allgemeine Stabilität und Sicherheit.

LERNERGEBNISSE

Wissen	W1. Bereitschaft zur Erkennung und Meldung von Vorfällen, Bewertung und Analyse von Vorfällen W2. Planung und Bereitschaft zur Reaktion auf Zwischenfälle, Eindämmung und Abschwächung von Zwischenfällen W3. Organisation der Kommunikation und Koordinierung von Zwischenfällen, der Wiederherstellung von Zwischenfällen und des Sammelns von Erkenntnissen.	**Fertigkeiten**	F1. Analyse von Vorfällen, Ermittlung der Ursachen und Auswahl geeigneter Reaktionsstrategien unter Einsatz ausgeprägter Problemlösungsfähigkeiten. F2. Effektive Kommunikation für das Management von und die Reaktion auf Vorfälle. F3. Anwendung von technischem Wissen zur Erkennung von Vorfällen im Rahmen eines effektiven Vorfallsmanagements und der Reaktion darauf.	**Verantwortung und Autonomie**	VA1. Vorbereitet auf die unverzügliche Identifizierung und Behandlung von Vorfällen, die innerhalb einer Organisation auftreten. VA2. Übernahme der Verantwortung für die Koordinierung und Durchführung der Reaktion auf Zwischenfälle. VA3. Übernahme der Verantwortung für die Dokumentation und Meldung von Vorfällen

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

Einheit 10: Kontinuität und Wiederherstellung im Katastrophenfall

Einführung

Geschäftskontinuität und Notfallwiederherstellung (Business Continuity and Disaster Recovery, BCDR) sind integraler Bestandteil der Risikomanagementstrategie eines Unternehmens, da sie die Kontinuität kritischer Geschäftsabläufe und die Wiederherstellung von Systemen und Daten in Zeiten der Unterbrechung gewährleisten. Business Continuity umfasst die proaktive Planung, die Identifizierung wichtiger Prozesse, die Bewertung von Risiken und die Entwicklung von Strategien zur Aufrechterhaltung des Geschäftsbetriebs während und nach einer Unterbrechung. Disaster Recovery konzentriert sich auf technische Aspekte und umfasst Sicherungs- und Wiederherstellungspläne, widerstandsfähige IT-Systeme und Verfahren zur schnellen Wiederherstellung des normalen Betriebs. Beide BCDR-Elemente erfordern ein gründliches Verständnis der Vermögenswerte, Abhängigkeiten und Risiken eines Unternehmens. Abteilungsübergreifende Zusammenarbeit und Koordination, klare Rollenverteilung, Kommunikation, Schulung und Tests sind von entscheidender Bedeutung. Wirksame BCDR-Pläne minimieren die Auswirkungen von Unterbrechungen, erhalten das Vertrauen und sorgen für langfristige betriebliche Stabilität.

Zielsetzung

Lernen Sie, kritische Geschäftsabläufe zu sichern, die Auswirkungen von Unterbrechungen zu minimieren, Risiken zu erkennen, Pläne zu entwickeln und zu testen, um die Widerstandsfähigkeit des Unternehmens zu verbessern und die langfristige Lebensfähigkeit zu gewährleisten.

LERNERGEBNISSE

Wissen	W1. Risikobewertung und Analyse der Auswirkungen auf das Geschäft, Planung der Geschäftskontinuität definieren W2. die Schlüsselelemente der IT-Disaster-Recovery-Planung und des Krisenmanagements zu identifizieren W3. Bewusstsein für Sicherungs- und Wiederherstellungsstrategien, die für die Kontinuität des Geschäftsbetriebs relevant sind.	**Fertigkeiten**	F1. Fähigkeit zur Durchführung von Risikobewertungen und -analysen, um potenzielle Bedrohungen und Schwachstellen für kritische Geschäftsabläufe zu ermitteln. F2. Erstellung umfassender Geschäftskontinuitäts- und Notfallwiederherstellungspläne. F3. Auflistung der Verfahren und Ressourcen, die erforderlich sind, um die Kontinuität kritischer Vorgänge und die rechtzeitige Wiederherstellung von Systemen und Daten zu gewährleisten.	**Verantwortung und Autonomie**	VA1. Verantwortung für die Bewertung potenzieller Risiken und Schwachstellen für kritische Geschäfts-abläufe und IT-Systeme. VA2. Vorbereitung auf die Umsetzung umfassender Pläne für Geschäftskontinuität und Notfallwiederherstellung. VA3. Regelmäßige Überwachung und Erprobung von Plänen zur Aufrechterhaltung des Betriebs und zur Notfallwiederherstellung, um ihre Wirksamkeit zu gewährleisten

Dauer

Kontaktstunden	Praktische Stunden	Stunden für das Selbststudium	Bewertungsstunden	GESAMT
0,5	2	9	0,5	12

2. SCHLUSSBEMERKUNGEN

Das im Rahmen des Erasmus+-Projekts SecureFuture entwickelte europäische Cybersicherheits-Curriculum wurde mit den Beiträgen der Projektpartner im Anschluss an die nationalen Konsultationen mit 66 Fachleuten aus dem Bereich der Cybersicherheit in den jeweiligen Ländern ausgearbeitet.

Dabei werden die folgenden Parameter berücksichtigt:

- Eine modulare Aufteilung der Ausbildungsinhalte in zehn Bereiche als Kompetenzeinheiten und zugehörige Inhalte;
- Eine Reihe von Kenntnissen, Fähigkeiten, Verantwortung und Autonomie, die in einer Tabelle für jede der zehn Lerneinheiten zusammengestellt sind;
- Zuweisung von 6,0 ECVET-Punkten für die 10 Einheiten, die 120 Ausbildungsstunden entsprechen.

Dieses Curriculum soll als Grundlage für die Entwicklung der europäischen Cybersicherheitsschulungsinhalte dienen, wie sie im WP4 - SecureFuture Schulungsinhalte definiert sind.

Zusammen bilden der Europäische Qualifikationsrahmen, das Ausbildungscurriculum und die Ausbildungsinhalte ein innovatives Angebot mit großem Potenzial, um die Bedürfnisse der europäischen Länder in Bezug auf die Ausbildung im Bereich der Cybersicherheit für Berufsbildungsstudenten und Mitarbeiter von KMU - den Hauptzielgruppen des Projekts - zu erfüllen und somit gut ausgebildete Cybersicherheitsexperten vorzubereiten, die europäische KMU vor Cyberbedrohungen schützen können.