Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Training Module

Informationssicherheit für Mitarbeiter Einheit 1 Woche 1 Name der Einheit: Einführungswebinar	
Lernaktivitäten	❑ **Webinar** ❑ **Aufgaben** ❑ **Workshop** ❑ **Präsentation** ❑ **Sonstige**
Lehrverantwortliche	• Gabriel Vladut • Valentin Istratie
Lernziele	1. Über das Erasmus+ InCyT Projekt 2. Ziele 3. Ergebnisse und Produkte 4. Wie man sich vor Cyberangriffen schützen kann 5. Schulung und Betreuung 6. Social Engineering 7. Soziale Netzwerke (Social Media)
Zu erwerbende Kompetenzen	• TS3 Netzwerksicherheit • TS4 Penetrationstests (ausnutzbare Schwachstellen) • SS3 Kognitive und Verhaltensanalyse
Dauer der Lernaktivitäten	2 Wochen
Lernanforderungen	***Was wird benötigt***
	• Informationen über das Erasmus+ InCyT-Projekt / Ziele / Ergebnisse und Produkte • Wie Sie sich vor Cyberangriffen schützen können • Schulung und Betreuung • Social Engineering / Soziales Netzwerk (Soziale Medien)

Co-funded by the
Erasmus+ Programme
of the European Union

Kurze Information zum Modul

Co-funded by the
Erasmus+ Programme
of the European Union

Beschreibung
InCyT ist ein Erasmus+ Projekt, das darauf abzielt, einen Rahmen und eine Methodik für die Ausbildung zu schaffen, die ein Verfahren für die Berufsbildung und die Unternehmen bietet, um die Kompetenzen und Fähigkeiten zu beschreiben, die im Bereich der Cybersicherheit für Fachleute und Nicht-Fachleute erforderlich sind, um Cyberangriffe sowie digitale Lücken etc. zu vermeiden. Die Nationale Initiative für Cybersicherheitsausbildung (NICE) des NIST unterstreicht, dass dies ein entscheidender Schritt zur Behebung des Mangels an "Menschen mit den Kenntnissen, Fähigkeiten und Fertigkeiten, die für die Arbeit im Bereich der Cybersicherheit erforderlich sind", sein sollte. Eine solche Belegschaft wird "technische und nicht-technische Rollen umfassen, die mit sachkundigen und erfahrenen Personen besetzt sind." Das Projekt möchte in diesem Zusammenhang einige Lösungen umsetzen. Es zielt zunächst auf die Entwicklung eines Rahmenwerks ab, das ein Verfahren für die Berufsbildung und die Unternehmen bereitstellt, um die digitalen Lücken und andere notwendige Maßnahmen im Bereich der Cybersicherheit für Fachleute und Nichtfachleute zu beschreiben, um Cyberangriffe zu vermeiden und ihnen zu helfen, diese Situation zu verbessern. Unter Berücksichtigung der Vorteile von interdisziplinären Ausbildungs- und Mentoring-Programmen, insbesondere im Bereich der Cybersicherheit, wird das Projekt digitale interdisziplinäre Ausbildungsprogramme, unterstützt durch E-Mentoring, für KMU entwickeln und testen und für die Berufsbildung anpassen. Zusammenarbeit und Kommunikation zwischen Pädagogen, Forschern und Menschen, die IT-Systeme nutzen, sind notwendig. Ein Problem besteht darin, dass Unternehmen, insbesondere KMU mit wenig Ressourcen, Hilfe benötigen, um die Kompetenzen und Qualifikationslücken ihrer Mitarbeiter zu erkennen, Methoden zur Bewertung der bestehenden Situation zu entwickeln und Schulungsmöglichkeiten zur Umschulung ihrer Mitarbeiter zu nutzen. Die Lernenden können sich über diese Aspekte informieren, indem sie den entsprechenden Text lesen, Webinare ansehen und Übungen im eigenen Tempo lösen. Alle diese Dokumente befinden sich auf der digitalen interaktiven Projektplattform. Die Lernenden können ihre Antworten in Selbsteinschätzungsübungen testen. Die Antworten auf andere Übungen sollten im entsprechenden Diskussionsforum gespeichert und mit dem Mentor bei dem wöchentlich stattfindenden gemeinsamen Treffen besprochen werden. Die Lernenden können vor allem während der Treffen mit anderen und dem Mentor kooperativ zusammenarbeiten. Sie werden dabei unterstützt, ein E-Portfolio zu erstellen, das für die Reflexion und Bewertung der Ausbildung wichtig ist.

Content of the Learning Material

Kompetenzrahmen

Im Rahmen unseres Projekts werden 3 transnationale Treffen stattfinden. Sie waren für den 3., 13. und 20. Monat des Projekts geplant. Es werden einige zusätzliche Projekttreffen stattfinden, da wir der Meinung sind, dass 3 Treffen nicht ausreichen, um ein 24-monatiges Projekt durchzuführen. Diese Treffen sind online und finden regelmäßig jeden Monat statt. Das Projektleitungsteam wird diese Projekte organisieren. Die Projekte werden von dem Projektkoordinator, dem WP-Leiter, geleitet. In unserem Projekt wird es 7 Multiplikatorenveranstaltungen geben. Jede Partnerinstitution wird diese Aktivitäten organisieren, um die Projektidee in ihrem Land bekannt zu machen und die entwickelten Produkte zu präsentieren. Jede Partnerinstitution wird die interdisziplinäre Schulung für KMU-Mitarbeiter und Lehrer im Bereich der Cybersicherheit in ihrem Land durchführen.

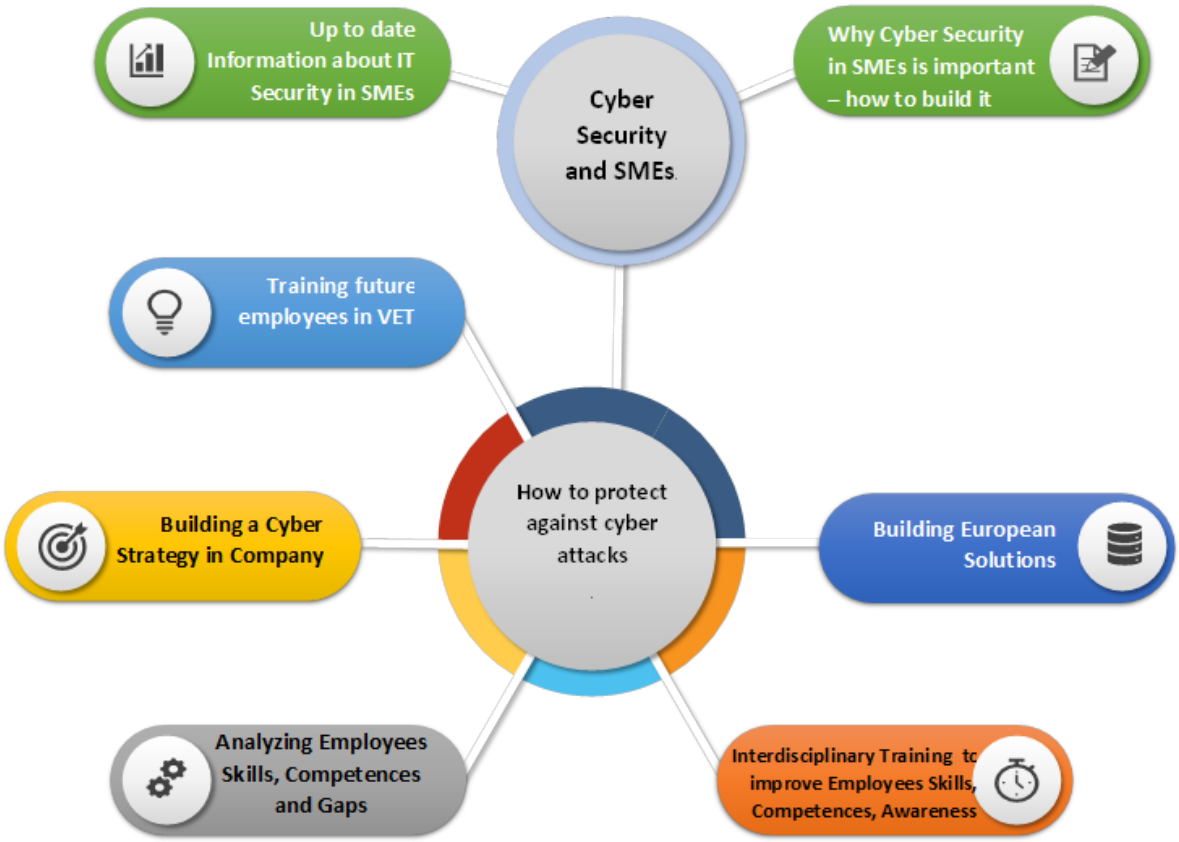

Abbildung 1: Aktivitäten des InCyT-Projektes

Ziele

Das InCyT-Projekt möchte einige Lösungen umsetzen:

- Die Entwicklung eines Rahmenwerks, das einen Mechanismus für die Berufsbildung und Unternehmen bietet, um die Kompetenzen und Fähigkeiten zu beschreiben, die im Bereich der Cybersicherheit für Fachleute und Nicht-Fachleute erforderlich sind, um Cyber-Angriffe sowie digitale Lücken und andere zu vermeiden.
- Unter Berücksichtigung der Vorteile von interdisziplinären Trainings- und Mentoring-Programmen, insbesondere im Bereich der Cybersicherheit, wird das Projekt digitale interdisziplinäre Trainingsprogramme und eine kollaborative e-Learning-Plattform für KMU entwickeln und testen.
- diese für die Berufsbildung anpassen.
- Entwicklung eines europäischen Übertragbarkeitsmodells
- Unter Berücksichtigung der Vorteile von interdisziplinären Trainings- und Mentoring-Programmen, insbesondere im Bereich der Cyber-Sicherheit, wird das Projekt digitale interdisziplinäre Trainingsprogramme, unterstützt durch E-Mentoring, für KMUs entwickeln, testen und für die Berufsbildung anpassen.

Ergebnisse des Projekts werden sein:

- Methodischer Rahmen für die Implementierung
- Vorhandene und durchgeführte Schulungen (Kurse)
- Möglichkeiten zur Verbesserung dieser durch die Nutzung von Interdisziplinarität und Mentoring.
- Lern- und Mentoring-Methodik

Outcomes of the project will be:

- Methodological Framework for Implementation
- Existing and followed training (courses)
- Opportunities for improvements of these by using interdisciplinarity and mentoring.
- Learning and mentoring methodology

Produkte:

1. Rahmenwerk

2. Ein digitales interdisziplinäres Cybersicherheits-Trainingsmaterial für KMU, unterstützt durch Mentoring und eine angepasste Methodik für einen speziellen Berufsbildungskurs.

3. Eine digitale Plattform zur Unterstützung der Ausbildung

4. Bericht, wie interdisziplinäre Fähigkeiten Vorteile für KMU und die Mehrwertsteuer bieten.

5. Europäisches Übertragbarkeitsmodell für das erprobte interdisziplinäre Training und Mentoring

Partner aus: Deutschland (Koordinator), Türkei, Polen, Italien, Österreich, Dänemark, Rumänien.

Aktivitäten

- Methodischer Rahmen für Cybersicherheit - Führende Organisationen: IAT, Deutschland, Italien
- Ein digitales interdisziplinäres Ausbildungsmaterial für Cybersicherheit - Leitende Organisation: Fachhochschule St. Pölten, Österreich
- IKT-Plattform für Cybersicherheit - federführende Organisation: IPA, Rumänien
- Methodisches Modell für Cybersicherheit - federführende Organisation: Politechnik Universität, Polen
- Übertragbarkeitsmodell - federführende Organisation: Europäisches Ausbildungszentrum Kopenhagen, Dänemark
- Multiplikator-Veranstaltungen - federführende Organisation: Türkei

Wie Sie sich vor Cyberangriffen schützen können

Die digitale Wirtschaft basiert in erster Linie auf Daten. Im Zeitalter von Industrie 4.0, cyber-physischen Systemen und dem Internet der Dinge werden immer mehr Produkte und Prozesse digitalisiert. Cybersecurity, also der Schutz dieser Daten und der zugehörigen Informationsverarbeitungssysteme, ist heute so relevant wie nie zuvor in der Wirtschaftsgeschichte.

Geschäftsprozesse können erheblich gestört, verlangsamt oder sogar komplett blockiert werden, wenn beispielsweise Datensätze falsch, unvollständig oder gar nicht vorhanden sind, der Datenabgleich zwischen Systemen gestört ist, IT-Systeme fehlerhaft arbeiten oder komplett ausfallen.

Vor allem KMU sind Zielscheibe krimineller Handlungen im Zusammenhang mit diesen Problemen. Im Gegensatz zu großen Unternehmen sind ihre Ressourcen begrenzt - und die Hacker wissen das! KMU sind das Rückgrat der Wirtschaft in Europa, d. h. über 99 % der Unternehmen in Deutschland sind KMU.

Mehr als die Hälfte der Erwerbstätigen ist in KMU beschäftigt. Es ist daher notwendig, KMU dabei zu helfen, Cyberangriffe zu vermeiden.

Die Bildungsinitiative für Cybersicherheit weist darauf hin, dass ein entscheidender Schritt unternommen werden sollte, um den Mangel an "Personen mit dem Wissen, den Fertigkeiten und den Fähigkeiten, die für die Arbeit im Bereich der Cybersicherheit erforderlich sind" zu beheben.

Eine solche Gruppe umfasst "technische und nicht-technische Funktionen, die von Mitarbeitern mit Wissen und Erfahrung ausgefüllt werden".

Es ist jedoch schwierig, Arbeitskräfte mit den erforderlichen interdisziplinären Fähigkeiten zu schaffen und das Problem der Kommunikation zwischen Ausbildern, Forschern und Personen, die Informationstechnologien nutzen, zu lösen.

Die Zusammenarbeit und Kommunikation zwischen diesen Gruppen ist notwendig.

Ein Problem besteht darin, dass Unternehmen, insbesondere KMU mit weniger Ressourcen, Hilfe benötigen, um die Fähigkeiten und Lücken ihrer Mitarbeiter zu bewerten, digitale Methoden zu nutzen, um die bestehende Situation zu verbessern, und Ausbildungsmöglichkeiten zu organisieren, um ihre Mitarbeiter neu zu qualifizieren.

Training and Mentoring

Unternehmer, auch zukünftige, brauchen komplexe Denkweisen und die Fähigkeit, Wissen aus verschiedenen Bereichen zu verstehen und zu integrieren, was interdisziplinäres Lernen erfordert.

Komplexe technische Probleme erfordern die Schaffung einer interdisziplinären Situation auf fast natürliche Art und Weise.

Bei einem interdisziplinären Ansatz sollten die Lernenden Informationen aus verschiedenen Disziplinen und Bereichen integrieren.

Sie entwickeln ein interdisziplinäres Verständnis und lernen, Fachgebiete und disziplinspezifische Denkweisen zu integrieren.

Dadurch werden die kognitiven Fähigkeiten und das kritische Denken stärker gefördert als durch den Einsatz einzelner Disziplinen.

Social Engineering

- ist die Manipulation von Menschen (oft mit psychologischen Methoden), um Zugang zu Daten, Dokumenten und Informationen zu erhalten, die für den Angreifer von Interesse sind.
- ist heute eine der größten Bedrohungen für die Informationssicherheit und eine wirksame Form der Internetkriminalität.

- mehr als jede andere Art von Angriffen gefährliche Auswirkungen haben kann, z. B. Datenverletzungen.
- Die Angriffe haben ein finanzielles Ziel, so dass Organisationen erhebliche Geldbeträge verloren haben.
- Sie ist besonders gefährlich, weil sie mehr auf menschliches Versagen als auf Schwachstellen in Software und Betriebssystemen beruht.

Die Unternehmen:

- Sie könnten Produktivitätseinbußen, einen Rückgang der Arbeitsmoral und Schwierigkeiten bei der Wiederherstellung erleiden.
- Sie haben einen Imageschaden, weil die Kunden nicht davon überzeugt sind, dass das Unternehmen sich selbst schützen kann.
- müssen oft eine Reaktion auf einen Vorfall auslösen.
- Sicherheitssoftware bereitstellen sollten, um zukünftige Angriffe zu verhindern.
- sie müssten oft Mitarbeiter umschulen, um auf Angriffe vorbereitet zu sein.

Social Engineering Training (cyber awareness)

- von Mitarbeitern und Führungskräften, für die es wichtig ist, Social-Engineering-Angriffe zu erkennen, weil das Risiko, Opfer zu werden, hoch ist.
- könnte in Programme zur Sensibilisierung von Gemeinden, Einzelpersonen und Bürgern für die Sicherheit aufgenommen werden und den Einzelnen und seine Organisation schützen.
- vor allem in KMU, die über weniger Ressourcen verfügen, fehlt, weshalb sie dabei unterstützt werden sollten, Schulungen zum Cyber-Bewusstsein ernst zu nehmen und ihren Mitarbeitern die Möglichkeit zu geben, diese zu absolvieren.

Der Lebenszyklus einer Social Engineering Attacke

Angreifer:

- zunächst das anvisierte Opfer untersuchen, um die für den Angriff erforderlichen grundlegenden Informationen zu sammeln, wie z. B. Eintrittspunkte und schwache Sicherheitsprotokolle.
- Dann versuchen sie, das Vertrauen des Opfers zu gewinnen und Anreize für Handlungen zu schaffen, die normalerweise nicht zu den Sicherheitspraktiken gehören, z. B. die Preisgabe sensibler Informationen oder die Gewährung des Zugangs zu wichtigen Ressourcen

Abbildung 2 erklärt den Zyklus einer Attacke

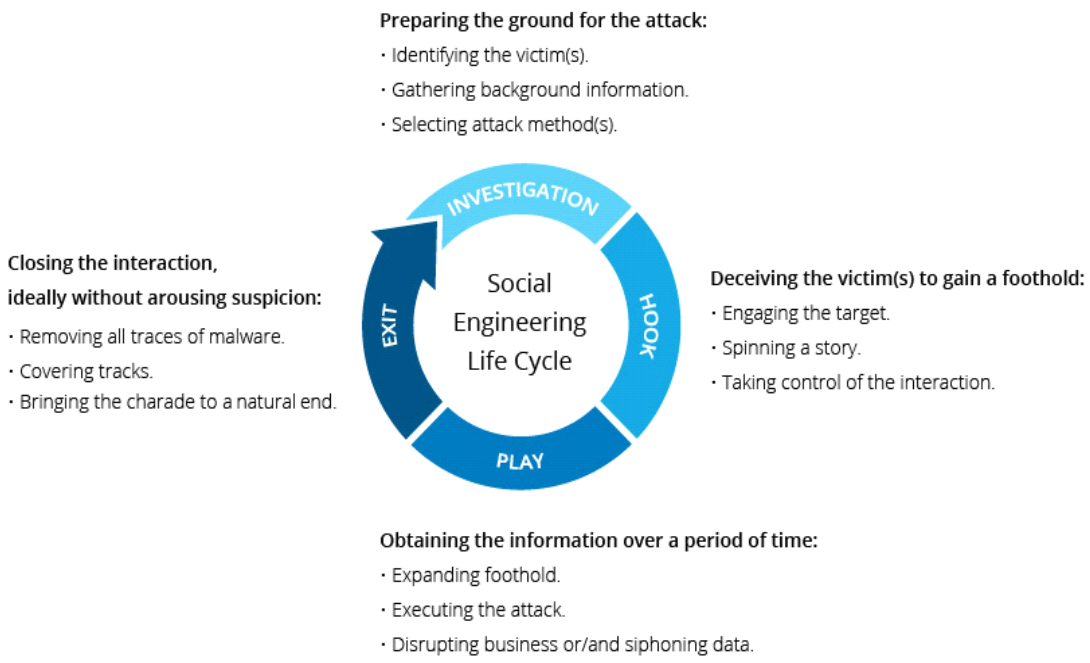

Abbildung 2: Zyklus eines Angriffes

Soziale Netzwerke

- Sind in den letzten Jahren sehr populär geworden und biete den Nutzern eine Plattform zur Kommunikation mit ihrer Familie, ihren Freunden und Kollegen.
- Social Networking bezieht sich auf die Nutzung von internetbasierten Social-Networking-Sites, um mit Freunden, Familie, Kollegen, Kunden oder Klienten in Kontakt zu treten und zu kommunizieren.
- Soziale Netzwerke haben ihre Server in Datenzentren, die mit den wichtigsten Netzzugangspunkten des Internets verbunden sind.

Rolle der sozialen Medien (Abbildung 3) zeigt einige Bereiche, in denen soziale Medien eine Rolle spielen

- Entertainment
- building business opportunities
- to make a career
- improving social skills

- developing relationships with other individuals

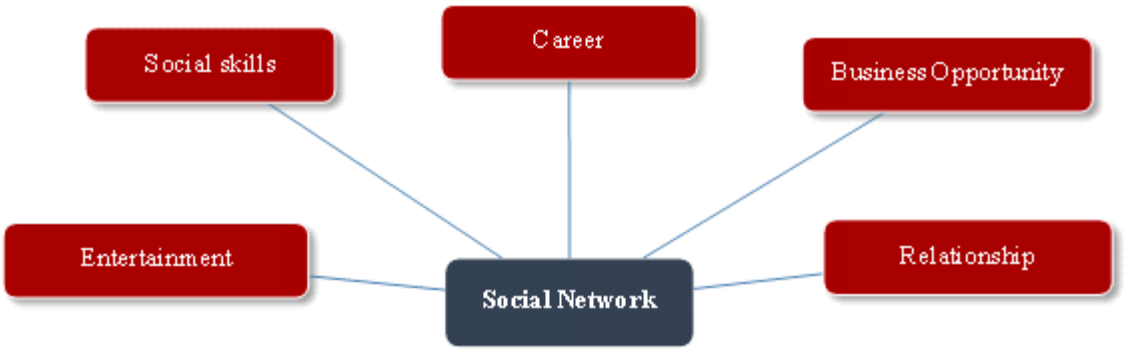

Abbildung 3: Rolle von sozialen Netzwerken

Soziale Netzwerke:

- Sind eine Grundlage für Vermarkter, die auf der Suche nach Kunden sind, um den Wiedererkennungswert der Marke zu erhöhen, die Markentreue zu fördern, die Konversionsraten zu verbessern, den Zugang zu und das Engagement mit neuen, aktuellen und alten Kunden zu ermöglichen.
- Durch das Teilen von Blogeinträgen, Bildern, Videos oder Kommentaren in sozialen Netzwerken mehr Menschen dazu bringen, die Website des Unternehmens zu besuchen und Kunden zu werden.
- Es ist schwierig, mit den Veränderungen Schritt zu halten, und wirkt sich auch auf den Marketingerfolg eines Unternehmens aus.

Die beliebtesten Websites für soziale Netzwerke (soziale Medien) in den Vereinigten Staaten und Europa sind:

- Facebook
- Instagram
- Twitter
- YouTube
- WhatsApp
- LinkedIn

Soziale Netzwerke basieren auf dem Aufbau und der Pflege persönlicher und geschäftlicher Beziehungen mithilfe von Technologie und Social-Networking-Websites (Social Media), die es Menschen und Unternehmen ermöglichen, miteinander in Kontakt zu treten, Beziehungen aufzubauen und Informationen, Ideen und Nachrichten auszutauschen.

Familienmitglieder können über persönliche soziale Netzwerke wie Facebook in Verbindung bleiben, Fotos austauschen und andere Nachrichten über ihr Leben schicken.

Menschen können auch mit anderen (Fremden) in Kontakt treten, die dieselben Interessen haben.

Soziale Medien haben aber auch Nachteile, wie die Verbreitung von Fehlinformationen und die hohen Kosten für die Nutzung und Pflege von Social-Media-Profilen.

Die Funktionen sozialer Plattformen lassen sich wie folgt einteilen:

- Netzwerkfunktionen dienen der Förderung sozialer Beziehungen zwischen Nutzern innerhalb virtueller Plattformen und bieten Funktionen zum Aufbau und zur Pflege des sozialen Netzwerkgraphen.
- Datenfunktionen sind für die Verwaltung der von den Nutzern bereitgestellten Inhalte und die Kommunikation zwischen den Nutzern zuständig und tragen dazu bei, die Interaktion zwischen den Nutzern zu verbessern (zu erweitern) und die Attraktivität der Plattform zu erhöhen
- Zugangskontrollfunktionen zielen darauf ab, benutzerdefinierte Maßnahmen zum Schutz der Privatsphäre umzusetzen und den unbefugten Zugang zu den von den Nutzern bereitgestellten Daten und Informationen zu beschränken.

Vor- und Nachteile von Sozialen Netzwerken

Vorteile

- Mit neuen und bestehenden Kunden in Kontakt zu treten.
- Markenbekanntheit zu schaffen, zu fördern und zu steigern.
- sich auf Bewertungen und Kommentare ihrer Kunden zu stützen, die wichtig sind, um den Absatz der Marke und die Platzierung in Suchmaschinen zu erhöhen.
- in der Lage sein, eine neue Marke zu etablieren. ein hohes Serviceniveau für seine Kunden demonstrieren.
- die Produkte und die Beziehungen zu den Verbrauchern verbessern zu können.

Nachteile

- sie können zur Verbreitung von Fehlinformationen beitragen.
- kann sich negativ auf Unternehmen auswirken, da sich Kritik an einer Marke in den sozialen Medien sehr schnell verbreitet hat.
- erfordert jede Woche Arbeitsstunden und Kosten für den Aufbau und die Pflege eines Unternehmensprofils.

Sicherheit und Datenschutz in sozialen Netzwerken

- Informationen, die in sozialen Netzwerken und Medien geteilt werden, verbreiten sich sehr schnell, was es für Angreifer attraktiv macht, sie zu erlangen.
- Fragen der Sicherheit und des Datenschutzes im Zusammenhang mit vom Nutzer freigegebenen Informationen, wenn ein Nutzer persönliche Inhalte wie Fotos, Videos und Audiodateien hochlädt, sollten beachtet werden, da ein Angreifer die freigegebenen Informationen böswillig für unrechtmäßige Zwecke nutzen kann.
- Ein mangelndes Bewusstsein der Nutzer für Sicherheit und Datenschutz kann zu verschiedenen Cyberangriffen über soziale Medien führen.

Die Bedrohungen lassen sich in drei Kategorien einteilen:

- Zu den konventionellen Bedrohungen gehören solche, denen die Nutzer seit den Anfängen des sozialen Netzwerks ausgesetzt sind.
- Moderne Bedrohungen sind Angriffe, die fortgeschrittene Techniken verwenden, um Benutzerkonten zu kompromittieren.
- Gezielte Angriffe sind Angriffe, die auf einen bestimmten Nutzer abzielen, die aber von jedem Nutzer aus verschiedenen persönlichen Gründen begangen werden können.

Lösungen für Betreiber sozialer Netzwerke

- Es wurden Authentifizierungsverfahren wie CAPTCHA, Multi-Faktor-Authentifizierung und Fotoidentifizierung von Freunden vorgeschlagen.
- Sicherheits- und Privatsphäre-Einstellungen, die es dem Kunden ermöglichen, persönliche Informationen vor unerwünschtem Zugriff durch Außenstehende oder Anwendungen zu schützen.

Nutzermeldungen über jegliche Form von Missbrauch oder Richtlinienverstößen durch Nutzer in ihrem Netzwerk. Das heißt, wenn Facebook eine Nutzermeldung erhält, wird diese geprüft und gemäß den Gemeinschaftsstandards von Facebook entfernt.

Fragen:

Die Antworten werden mit dem Mentor während der Sitzungen besprochen

1. Welche Erwartungen haben Sie an das InCyT-Projekt
2. Wie können Sie sich vor Cyber-Attacken schützen
3. Was ist Social Engineering
4. Was sind Soziale Netzwerke (Social Media)

Fragen zur Selbsteinschätzung. Nachder Beantwortung kann der Lernende die Ergebnisse sehen und sie mit den auf der Plattform gespeicherten Ergebnissen vergleichen

- Wie Sie sich vor Cyberangriffen schützen können
- Was ist Social Engineering
- Soziale Netzwerke (Social Media)

Literatur:

- InCyT – Interdisciplinary Cyber Training
- Cyber Incident Recovery
- Minimize Cyber Attacks - Cyber Resiliency Strategy
- How to Prevent Cyberattacks: Top Ways to Protect Yourself
- Social Media Security: How Safe is Your Information?
- Internal Controls Over Information Systems
- Social Media Adoption Brings New Risks
- Social Media Security – 5 Security Tips
- 19 Social Media Security Best Practices