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

InCyT-Trainingsmodule

Informationssicherheit für Manager Einheit 1 Woche 2 Bezeichnung der Einheit: Einführung in die Informationssicherheit, interne Kontrollsysteme	
Lernaktivitäten	**❑ Webinar❑ Übungen❑ Workshop❑ Präsentation❑ Sonstiges**
Lehrverantwortliche	• Gabriel Vladut • Valentin Istratie
Ziele der Lernaktivitäten	1. Einführung in das Erasmus+ InCyT-Projekt 2. Cybersicherheit 3. Konzepte, Definitionen und Begriffe 4. Interne Kontrolle Standard 5. Ausarbeitung von Kontrollen der Cybersicherheit
Zu erwerbende Fertigkeiten	• TS3 Netzwerksicherheit • TS4 Penetrationstests (ausnutzbare Schwachstellen) • SS3 Kognitions- und Verhaltensanalyse
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	***Was wird benötigt?***
	• Gewinnen Sie ein Bewusstsein für Cybersicherheit und lernen Sie, was ein Cybersicherheitsangriff ist • Erlernen von Methoden zur Verhinderung von Datenschutzverletzungen, die von Angreifern genutzt werden, um auf sensible Daten zuzugreifen und Schwachstellen in Unternehmen auszunutzen • Erfahren Sie, wie Sie im Falle eines Angriffs auf die Cybersicherheit vorgehen sollten

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

Kurze Informationen zum Modul

Beschreibung
Informationssicherheit, interne Kontrollsysteme sind wichtig und sehr oft eine Bedrohung für die Cybersicherheit Der Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff oder unbefugter Veränderung von Informationen, sei es bei der Speicherung, Verarbeitung oder Übertragung, und vor der Verweigerung von Diensten für autorisierte Benutzer. Die Informationssicherheit umfasst die Maßnahmen, die notwendig sind, um solche Bedrohungen zu erkennen, zu dokumentieren und zu bekämpfen. Die Informationssicherheit setzt sich aus der Computersicherheit und der Kommunikationssicherheit zusammen. Auch INFOSEC genannt. Siehe auch Kommunikationssicherheit; Computersicherheit; Informationssicherheit; Informationssystem. Interne Kontrollen werden von Management, IT-Sicherheit, Finanz-, Buchhaltungs- und Betriebsteams eingesetzt, um die folgenden Ziele zu erreichen: 1. Gewährleistung der Zuverlässigkeit und Genauigkeit von Finanzinformationen - Interne Kontrollen stellen sicher, dass genaue, aktuelle und vollständige Informationen in den Buchhaltungssystemen und Finanzberichten wiedergegeben werden. Die Lernenden können sich über diese Aspekte informieren, indem sie den entsprechenden Text lesen, sich Streaming-Webinare ansehen und Übungen im eigenen Tempo lösen. Alle diese Dokumente befinden sich auf der digitalen interaktiven Projektplattform. Die Lernenden können ihre Antworten in den Selbsteinschätzungsübungen testen. Die Antworten auf die anderen 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.

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

Inhalt des Lernmaterials

Informationssicherheit

Die Informationssicherheit befasst sich mit dem Schutz von Informationen und Computersystemen vor unbefugtem Zugriff, unbefugter Nutzung, Offenlegung, Unterbrechung, Änderung oder Zerstörung.

ISO/IEC27002/2013 befasst sich mit der Informationssicherheit durch ihre drei Hauptkomponenten: Vertraulichkeit, Integrität und Verfügbarkeit. Die Vertraulichkeit wird durch die Verschlüsselung der Informationen gewährleistet. Die Integrität wird durch Streuungsmechanismen und Algorithmen erreicht.

Die Verfügbarkeit wird durch die Verstärkung der Sicherheit des Netzes oder der Netze des Computersystems und durch die Bereitstellung von Backups gewährleistet. Informationssicherheit ist eine Reihe von Praktiken, die dem Schutz von Daten dienen.

Die Informationssicherheit ist nicht auf Computersysteme oder Informationen in digitaler oder elektronischer Form beschränkt. Sie bezieht sich vielmehr auf alle Fragen im Zusammenhang mit der Sicherheit und dem Schutz von Daten und Informationen, unabhängig von ihrer Form.

Informationssicherheit kann nicht als Synonym für Computersicherheit, System- und Netzsicherheit, Sicherheit der Informationstechnologie, Informationssysteme oder Informations- und Kommunikationstechnologie definiert werden. Jeder dieser Ausdrücke bezieht sich auf ein anderes Thema, auch wenn sich der gemeinsame Punkt auf die Informationssicherheit in einigen ihrer Formen bezieht (hier sprechen wir über ihre elektronische Version): daher sind sie alle Teilbereiche der Informationssicherheit.

Im 21. Jahrhundert haben die meisten Unternehmen ein Computersystem, das mit dem Internet verbunden ist und über das sie Informationen austauschen. Informationen können durch eine Verbindung von Netzwerken weitergeleitet werden. Infolgedessen ist diese Verbindung umso mehr dem Risiko von Malware ausgesetzt, die von innen (Kopieren von Informationen, Verwendung von bösartigem Code) oder von außen in den Besitz sensibler Informationen gelangen will.

Um diesen Risiken entgegenzuwirken, erfordert die Informationssicherheit die Entwicklung von

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

Konzepten wie Data Tagging, Public Key Encryption (PKI) und Multi-Level Security (MLS). Zusätzlich zu den Problemen bei der Verbindung von Netzen ist es immer einfacher, große Mengen an Informationen zu transportieren (und dies auf eine Weise, die im Falle eines Hackerangriffs relativ schwer zu erkennen ist), aber auch physisch über USB-Sticks oder Speicherkarten.

Daher werden Computersysteme, die sensible Informationen enthalten, zunehmend als System-High-Mode-Umgebung konzipiert, in vielen Fällen in Form von separaten Netzen ohne Verbindung zu anderen Netzen und ohne USB-Anschlüsse. Drei Kriterien für die Sensibilität von Informationen sind allgemein anerkannt: Verfügbarkeit, Integrität und Vertraulichkeit. Ein viertes wird ebenfalls häufig verwendet (unter verschiedenen Bezeichnungen): Rückverfolgbarkeit, Rechenschaftspflicht, Überprüfbarkeit (in Bezug auf Computer-Audits) oder Beweisbarkeit. Ein fünftes Kriterium wird ebenfalls verwendet: Nichtabstreitbarkeit, die den Austausch von Nachrichten zwischen Absender und Empfänger gewährleistet.

Cyberangriffe und der Kompetenzrahmen

Ein Kompetenzrahmen wird von Unternehmen regelmäßig verwendet, um ihre Qualifikationsanforderungen, erforderlichen Kompetenzen, Mitarbeiterfähigkeiten und Lücken zu verstehen.

Wenn ein Kompetenzrahmen unter Berücksichtigung des Unternehmensprofils und der Mitarbeiterinteressen entwickelt wird, kann er die Leistung verbessern, Klarheit für jede einzelne Rollenanforderung schaffen und Talente am Arbeitsplatz entwickeln. In den letzten Jahren wurden aufgrund zahlreicher Cyberangriffe Cybersicherheitsrahmen hauptsächlich von großen Organisationen (Unternehmen, NROs und anderen Einrichtungen) oder von staatlichen Akteuren eingeführt.

Ein erfolgreicher Cyberangriff kann dem Geschäft eines Unternehmens großen Schaden zufügen. Er kann sich sowohl auf den Gewinn als auch auf den Geschäftsstatus des Unternehmens und das Vertrauen der Verbraucher auswirken. Die Auswirkungen einer Sicherheitsverletzung lassen sich in drei Kategorien einteilen: finanziell, rufschädigend und rechtlich.

Cyber-Angriffe

Cyberangriffe führen oft zu erheblichen finanziellen Verlusten durch den Diebstahl von Unternehmensdaten, Finanzinformationen (z. B. Bank- oder Zahlungskartendaten), Geld, Unterbrechungen von Transaktionen (z. B. die Unfähigkeit, Online-Transaktionen durchzuführen), den Verlust von Geschäften oder des Vertrags. Unternehmen, die von einem Cyberangriff betroffen sind, geben in der Regel Geld für die Reparatur der betroffenen Systeme, Netzwerke und Geräte aus.

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

Cyberangriffe können den Ruf eines Unternehmens und das Vertrauen der Kunden in das Unternehmen schädigen. Dies kann zu Kundenverlusten, Umsatzeinbußen und Gewinneinbußen führen. Die Auswirkungen der Rufschädigung können sich sogar auf die Lieferanten des Unternehmens auswirken oder die Beziehungen zu Partnern, Investoren und anderen Dritten, die an den Geschäften des Unternehmens beteiligt sind, beeinträchtigen.

Die Gesetze zum Datenschutz und zum Schutz der Privatsphäre verlangen daher ein Sicherheitsmanagement für alle personenbezogenen Daten, über die das Unternehmen (von seinen eigenen Mitarbeitern oder Kunden) verfügt. Wenn diese Daten versehentlich oder absichtlich kompromittiert werden und das Unternehmen keine angemessenen Sicherheitsmaßnahmen ergreift, kann es mit rechtlichen Sanktionen rechnen.

Risiken im Unternehmen

Es ist wichtig, dass Sie Ihre Risiken entsprechend verwalten. Nach einem Angriff kann ein wirksames Cybersicherheitstool oder ein Plan zur Reaktion auf einen Vorfall, z. B. durch einen Cyberberater, helfen:

- die Auswirkungen des Angriffs zu verringern
- Meldung des Vorfalls an die zuständige Behörde
- die betroffenen Systeme zu bereinigen
- Ihr Unternehmen in kürzester Zeit wieder zum Laufen zu bringen.

Es ist notwendig, in die Schulung und Ausbildung von Nutzern im Bereich der Cybersicherheit zu investieren, um Angriffe zu vermeiden und ein kontinuierliches Bewusstsein für eine Cyberstrategie in der eigenen Organisation zu entwickeln.

Rahmen für Cybersicherheit

Ein Cybersicherheitsrahmen ist eine Reihe von bewährten Verfahren und dokumentierten Prozessen, die zur Entwicklung von IT-Sicherheitsrichtlinien innerhalb einer Organisation verwendet werden. Im Gegensatz zu herkömmlichen, rein auf den rechtlichen Bereich bezogenen Richtlinien sollte ein Cybersicherheitsrahmen jedoch auch dokumentierte Beispiele für Probleme enthalten, die durch diese Richtlinien vermieden werden sollen, sowie für die geeigneten Verfahren und Wege zur Umsetzung der im Rahmen beschriebenen Sicherheitsrichtlinien.

Er ist sowohl ein Leitfaden für Mitarbeiter und Nutzer als auch ein überzeugendes Kompendium bewährter Sicherheitspraktiken, das von autorisierten externen Parteien (z. B. Behörden) konsultiert werden kann. Ein Rahmen für Cybersicherheitskompetenzen kann auch dazu beitragen, die zur Vermeidung von Angriffen erforderlichen Kompetenzen, Lücken und

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

Abhilfemaßnahmen besser zu bewerten.

Cyber-Sicherheit

Trotz des gestiegenen Bewusstseins und der mutigen Bemühungen ist bekannt, dass in der Europäischen Union ein erheblicher und zunehmender Mangel an Fachkräften für Cybersicherheit und an Kenntnissen und Fähigkeiten der Beschäftigten zur Vermeidung von Cyberangriffen weltweit besteht, und dieser Mangel stellt den öffentlichen und privaten Sektor weiterhin vor große Probleme.

Die Studie 2019 CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) schätzt, dass es weltweit 2,8 Millionen Fachkräfte für Cybersicherheit gibt, während die Lücke tatsächlich 4,07 Millionen beträgt.

Die Studie stellt fest, dass die Lücke in Europa derzeit 291.000 beträgt, und diese Zahl hat sich gegenüber den Vorjahren verdoppelt. Viele Länder mit hochentwickeltem Fachwissen ziehen es vor, ihre eigenen Vorschriften und Dokumente zu erstellen, aber viele Länder und kleine und mittlere Unternehmen (KMU) benötigen in diesem Zusammenhang Hilfe.

Social Engineering

- Es geht darum, Menschen zu manipulieren (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.
- könnte gefährliche Auswirkungen haben, z. B. Datenschutzverletzungen, mehr als jede andere Art von Angriffen.
- die Angriffe haben ein finanzielles Ziel, und die Unternehmen haben dadurch beträchtliche Geldbeträge verloren.
- Er ist besonders gefährlich, weil er 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.
- oft eine alte Reaktion auf einen Vorfall auslösen müssen.

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

- sollte Sicherheitssoftware zur Verfügung stellen, um zukünftige Angriffe zu verhindern.
- Sie müssten ihre Mitarbeiter häufig umschulen, um auf Angriffe vorbereitet zu sein.

Social Engineering; Schulung (Cyber-Bewusstsein)

- von Mitarbeitern und Führungskräften, für die es wichtig ist, Social-Engineering-Angriffe zu erkennen, weil das Risiko, Opfer zu werden, hoch ist.
- können in Sicherheitsprogramme für Gemeinden, Einzelpersonen und Bürger aufgenommen werden und den Einzelnen und seine Organisation schützen.
- Daher sollten sie dabei unterstützt werden, Schulungen zur Sensibilisierung für den Umgang mit dem Internet ernst zu nehmen und ihren Mitarbeitern die Möglichkeit zu geben, an solchen Schulungen teilzunehmen.

Ausbildung und Betreuung

Unternehmer, auch künftige, 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 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 einzelne Fächer.

Unternehmerische Fähigkeiten und Mentoring

Die Bewertung der Leistungen der Lernenden bei der Entwicklung unternehmerischer Fähigkeiten kann eine ganzheitliche Sichtweise einnehmen, die auch das Lernumfeld und die Lernergebnisse berücksichtigt und interaktives, effektives und aktives Lernen erleichtert.

Mentoring ist eine erfahrene Methode zur Unterstützung des individuellen Lernens und zum Erwerb persönlicher und beruflicher Fähigkeiten für neue Berufe. Es gibt Untersuchungen zu den Ergebnissen von Mentoring im Allgemeinen, aber es gibt nur wenige Untersuchungen zum Mentoring.

Mentoring bietet eine Reihe von Vorteilen für Arbeitnehmer, die in Unternehmen ausgebildet werden. Interdisziplinäres Team-Mentoring hat in den letzten Jahren an Bedeutung gewonnen

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

und spiegelt die Notwendigkeit einer veränderten Ausrichtung des Mentorings wider, da verschiedene unternehmerische Entwicklungen und Bereiche zunehmend multidisziplinär sind.

Interdisziplinäres Mentoring und Mentorennetzwerke können Synergieeffekte in Gruppen erzeugen, innovative Ideen und komplexe Lösungen für Herausforderungen hervorbringen und Möglichkeiten für Zusammenarbeit und Arbeit schaffen.

Konzepte, Definitionen und Begriffe

Der Begriff "**Cyberspace**" wurde 1982 von William Gibson geprägt. Der Begriff wurde in den 1990er Jahren mit dem Aufkommen des World Wide Web alltäglich

Cyber-Infrastrukturen - Informations- und Kommunikationstechnologie-Infrastrukturen, bestehend aus IT-Systemen, zugehörigen Anwendungen, Netzen und elektronischen Kommunikationsdiensten;

Cyberspace - die virtuelle Umgebung, die durch Cyberinfrastrukturen geschaffen wird, einschließlich der verarbeiteten, gespeicherten oder übertragenen Informationsinhalte sowie der von den Nutzern durchgeführten Aktionen;

Cybersicherheit - der Zustand der Normalität, der sich aus der Anwendung einer Reihe proaktiver und reaktiver Maßnahmen ergibt, die die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Nichtabstreitbarkeit von Informationen in elektronischem Format, von öffentlichen oder privaten Ressourcen und Diensten im Cyberspace gewährleisten.

Zu den proaktiven und reaktiven Maßnahmen können Sicherheitsstrategien, -konzepte, -standards und -leitlinien, Risikomanagement, Schulungs- und Sensibilisierungsmaßnahmen, die Umsetzung technischer Lösungen zum Schutz von Cyber-Infrastrukturen, Identitätsmanagement und Folgenmanagement gehören;

Cyberverteidigung - Maßnahmen im Cyberspace zum Schutz, zur Überwachung, zur Analyse, zur Aufdeckung, zur Abwehr von Angriffen und zur Gewährleistung einer rechtzeitigen Reaktion auf Bedrohungen der Cyberinfrastruktur, die speziell die nationale Verteidigung betreffen;

Operationen in Computernetzen - der komplexe Prozess der Planung, Koordinierung, Synchronisierung, Harmonisierung und Durchführung von Aktionen im Cyberspace zum Schutz, zur Kontrolle und zur Nutzung von Computernetzen, um eine Informationsüberlegenheit zu erlangen und gleichzeitig die Fähigkeiten des Gegners zu neutralisieren;

Cyber-Bedrohung - Umstand oder Ereignis, das eine potenzielle Gefahr für die Cybersicherheit darstellt;

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

Cyberangriff - feindliche Handlung im Cyberspace, die die Cybersicherheit beeinträchtigen kann;

Cybervorfall - Ereignis im Cyberspace, dessen Folgen die Cybersicherheit beeinträchtigen;

Cyber-Terrorismus - von politisch, ideologisch oder religiös motivierten Einzelpersonen, Gruppen oder Organisationen im Cyberspace durchgeführte vorsätzliche Aktivitäten, die materielle Zerstörung oder Opfer verursachen können und geeignet sind, Panik oder Terror auszulösen;

Cyberspionage - Handlungen, die im Cyberspace mit dem Ziel durchgeführt werden, unbefugt vertrauliche Informationen im Interesse einer staatlichen oder nichtstaatlichen Einrichtung zu erlangen;

Computerkriminalität - alle im Strafrecht oder in anderen Sondergesetzen vorgesehenen Handlungen, die eine soziale Gefahr darstellen und schuldhaft über oder an Cyber-Infrastrukturen begangen werden;

Schwachstelle im Cyberspace - Schwäche in der Konzeption und Umsetzung von Cyberinfrastrukturen oder damit verbundenen Sicherheitsmaßnahmen, die von einer Bedrohung ausgenutzt werden kann;

Sicherheitsrisiko im Cyberspace - die Wahrscheinlichkeit, dass eine Bedrohung eintritt, die eine spezifische Schwachstelle von Cyberinfrastrukturen ausnutzt;

Risikomanagement - ein komplexer, kontinuierlicher und flexibler Prozess der Identifizierung, Bewertung und Bekämpfung von Cybersicherheitsrisiken, der auf dem Einsatz komplexer Techniken und Instrumente beruht, um Verluste jeglicher Art zu verhindern;

Identitätsmanagement - Methoden zur Validierung der Identität von Personen beim Zugang zu bestimmten Cyber-Infrastrukturen;

Die Komponenten der internen Kontrolle

Gemäß der INTOSAI-Norm GOV 9100 "Leitlinien für Normen der internen Kontrolle". Im Jahr 2001 wurde auf dem Kongress der Internationalen Organisation der Obersten Rechnungskontrollbehörden (INCOSAI) beschlossen, die ursprünglich 1992 herausgegebenen INTOSAI-Leitlinien für Normen der internen Kontrolle im öffentlichen Sektor zu aktualisieren, indem alle Aspekte der jüngsten Entwicklungen im Bereich der internen Kontrolle in das Dokument aufgenommen und eine Reihe von Elementen des COSO-Modells (Internal Control - Integrated Framework) integriert wurden.

Durch die Integration in die Leitlinien - eine Tätigkeit, die von der operativen Gruppe des Normenausschusses für die interne Kontrolle der INTOSAI durchgeführt wurde - wurde versucht,

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

ein einheitliches Verständnis der Vertreter der Obersten Rechnungskontrollbehörden über die Funktionsweise des neuen internen Kontrollsystems zu erreichen.

Die "INTOSAI-Leitlinien für Normen der internen Kontrolle im öffentlichen Sektor" gehören zur INTOSAI-Kategorie GOV (Leitlinien für gute Regierungsführung) und gelten als äußerst nützlich sowohl für die Führungskräfte des öffentlichen Sektors, die das interne Kontrollsystem umsetzen müssen, als auch für die externen öffentlichen Rechnungsprüfer, die dieses System kennen und bewerten müssen.

Interne Kontrollnormen

Nach den Leitlinien der INTOSAI GOV 9100) besteht die interne Kontrolle aus fünf voneinander abhängigen Komponenten (die mit denen des COSO-Modells identisch sind):

- Kontrolle der Umgebung
- Risikobewertung
- Kontrolltätigkeiten
- Information und Kommunikation
- Überwachung

Die interne Kontrolle soll eine hinreichende Gewähr dafür bieten, dass die Gesamtziele der Einrichtung erreicht werden. Von den Leitern der Einrichtung klar festgelegte Ziele und eine angemessene Haushaltsplanung sind eine zwingende Voraussetzung für eine wirksame interne Kontrolle.

Kontrollumfeld

Das Kontrollumfeld umfasst die allgemeine Einstellung, das Bewusstsein und die Maßnahmen des Managements und der mit der Leitung betrauten Personen in Bezug auf das interne Kontrollsystem und dessen Bedeutung innerhalb der Organisation. Das Kontrollumfeld gibt den Ton in der Organisation an und beeinflusst das Kontrollbewusstsein der Mitarbeiter.

Es stellt die Grundlage für alle anderen Komponenten der internen Kontrolle dar und sorgt für eine einzuhaltende Disziplin innerhalb der Organisation und eine Struktur der Einheit, damit das interne Kontrollsystem wirksam angewendet werden kann. Das interne Kontrollumfeld ist ein wirksames Instrument zur Verhinderung von Korruption und Betrug.

Die Elemente, die das Kontrollumfeld definieren, sind:

- persönliche und berufliche Integrität, die von der Leitung für das gesamte Personal aufgestellten ethischen Werte, einschließlich einer ständigen unterstützenden Haltung

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

gegenüber der internen Kontrolle;
- ein ständiges Bemühen des Managements um die Kompetenz des Personals;
- "der von oben vorgegebene Ton" (die Philosophie und der Handlungsstil des Managements);
- die Organisationsstruktur des Unternehmens;
- Personalpolitik und -praxis.

Arten von Cyber-Sicherheitskontrollen

Cybersicherheitskontrollen sind Mechanismen zur Verhinderung, Erkennung und Abschwächung von Cyberbedrohungen und -angriffen. Die Mechanismen reichen von physischen Kontrollen wie Sicherheitspersonal und Überwachungskameras bis hin zu technischen Kontrollen wie Firewalls und Multi-Faktor-Authentifizierung.

Ein einseitiger Ansatz für die Cybersicherheit ist einfach überholt und ineffektiv. Und da es in der heutigen Bedrohungslandschaft unmöglich ist, alle Angriffe zu verhindern, sollten Unternehmen ihre Anlagen auf der Grundlage ihrer Bedeutung für das Unternehmen bewerten und entsprechende Kontrollen einrichten.

Erschwerend kommt hinzu, dass es unwahrscheinlich ist, dass sich die Mitarbeiter an die Compliance-Regeln halten, wenn strenge Kontrollen für alle Unternehmensressourcen eingeführt werden. Der Schweregrad einer Kontrolle sollte direkt die Vermögenswerte und die Bedrohungslage widerspiegeln.

Die Folgen eines Hackers, der Tausende von persönlichen Kundendaten über eine Cloud-Datenbank preisgibt, können weitaus größer sein, als wenn der Laptop eines Mitarbeiters kompromittiert wird.

Kontrollen der Cybersicherheit

"Es gibt viele verschiedene Möglichkeiten, Kontrollen anzuwenden, je nachdem, was man zu schützen versucht", sagt Joseph MacMillan, Autor von Infosec Strategies and Best Practices und Cybersecurity Global Black Belt bei Microsoft.

"Was ist die Art der Bedrohung, vor der Sie sich schützen wollen?

Handelt es sich um einen böswilligen Akteur?

Oder ist es ein verheerender Angriff?"

Sicherung von Informationsbeständen

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

Sie bezieht sich auf die Umsetzung angemessener Informationssicherheitskontrollen für Vermögenswerte. Wir wollen sicherstellen, dass wir uns auf starke und wirksame Ideologien konzentrieren, um die geeigneten Kontrollen auszuwählen, was bedeutet, dass der Vermögenswert auf der Grundlage seiner Kritikalität und Klassifizierung als "sicher genug" angesehen wird. Es gibt verschiedene Klassen, die die Arten von Kontrollen unterteilen:

- Administrative/managerielle Kontrollen sind die Richtlinien und Verfahren des Unternehmens. Sie sind nicht so "cool" wie eine neue Softwarekontrolle, aber sie dienen dazu, Einzelpersonen und anderen Mitgliedern der Organisation Struktur und Anleitung zu geben und sicherzustellen, dass niemand eine Geldstrafe erhält oder einen Verstoß verursacht.
- Physische Kontrollen, die den Zugang zu Systemen physisch begrenzen.
- Technische/logische Kontrollen sind solche, die den Zugang auf der Grundlage von Hardware oder Software beschränken, wie z. B. Verschlüsselung, Fingerabdruckleser, Authentifizierung oder vertrauenswürdige Plattformmodule (TPM).

Sie beschränken nicht den Zugang zu physischen Systemen wie physische Kontrollen, sondern den Zugang zu Daten oder Inhalten. Operative Kontrollen sind solche, die Menschen betreffen, die tagtäglich Prozesse durchführen. Beispiele hierfür sind Sensibilisierungsschulungen, die Klassifizierung von Vermögenswerten und die Überprüfung von Protokolldateien.

Arten von Kontrollen

Zu den präventiven Kontrollen, die eine Aktion verhindern sollen, gehören Firewalls, Zäune und Zugangsberechtigungen.

Detektivbefehle werden nur während oder nach einem Ereignis ausgelöst, z. B. bei Videoüberwachungs- oder Einbruchmeldeanlagen. Abschreckungsmaßnahmen schrecken Bedrohungen davon ab, eine Schwachstelle auszunutzen, z. B. ein "Watchdog" oder ein Hundezeichen. Korrektursteuerungen sind in der Lage, von einem Zustand in einen anderen zu wechseln. Die Befehle "fail open" und "fail closed" werden hier behandelt.

Wiederherstellungsbefehle stellen etwas von einem Verlust wieder her, z. B. die Wiederherstellung einer Festplatte. Kompensierende Kontrollen sind solche, die versuchen, Mängel in anderen Kontrollen auszugleichen, z. B. die regelmäßige Überprüfung von Zugriffsprotokollen. Auch bei diesem Beispiel handelt es sich um eine detektivische Kontrolle, aber Kompensationskontrollen können von unterschiedlicher Art sein.

Reihenfolge der Kontrollen

Sie schreckt Akteure davon ab, auf etwas zuzugreifen, das sie nicht betreten sollten.

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

Verweigern/Verhindern des Zugriffs durch eine präventive Kontrolle wie Zugriffsberechtigungen oder Authentifizierung.

Erkennen Sie Risiken, indem Sie dafür sorgen, dass die Erkennung aufgezeichnet wird, z. B. mit Software zum Schutz von Endgeräten. Verzögern Sie die Wiederholung des Risikos, z. B. mit einer Funktion für "zu viele Versuche" bei der Eingabe eines Passworts.

Behebung der Situation durch Reaktion auf die Kompromittierung, z. B. mit einem Notfallplan. Wiederherstellung eines kompromittierten Zustands, z. B. durch einen Backup-Generator, der die Verfügbarkeit eines Servers wiederherstellt.

Darüber hinaus sollten wir im Rahmen der kontinuierlichen Verbesserung den Wert jedes einzelnen Vermögenswerts auf etwaige Veränderungen überwachen. Der Grund dafür ist, dass wir möglicherweise unsere Kontrollen zum Schutz dieser Vermögenswerte überdenken müssen, wenn sie im Laufe der Zeit oder bei bestimmten wichtigen Ereignissen in Ihrer Organisation mehr oder weniger wertvoll werden.

Kontrollen und Wiederherstellung

Wenn wir uns mit Kontrollen befassen, sollten wir auch an die Wiederherstellung denken. Wir wollen in der Lage sein, uns von ungünstigen Situationen oder Veränderungen bei Vermögenswerten und deren Wert zu erholen. Als Beispiele seien hier nur Backups, Redundanz, Wiederherstellungsprozesse und Ähnliches genannt.

Besonders im Zeitalter von Cloud, SaaS, PaaS, IaaS, Lösungen von Drittanbietern und allen anderen Formen von "fremden Computern" muss sichergestellt werden, dass die Service Level Agreements (SLAs) klar definiert sind und Vereinbarungen über maximal zulässige Ausfallzeiten sowie Strafen für die Nichteinhaltung dieser Vereinbarungen enthalten. Dies ist ein Beispiel für eine kompensatorische Kontrolle.

Fragen:

Fragen Diskussionsforum, die mit einer kurzen Erklärung beantwortet werden müssen. Die Antworten werden mit dem Mentor während der Mentoring-Sitzungen besprochen

1. Wie groß sind die Risiken für Cyberangriffe im Unternehmen?
2. Nennen Sie einige Arten von Kontrollen der Cybersicherheit
3. Hexe sind interne Kontrollnormen
4. Kontrolle und Wiederherstellung von Informationen

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

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

- Risiken im Unternehmen für Cyberangriffe
- Interne Kontrollnormen und -regeln
- Kontrollumfeld

Anhänge

PowerPoint-Präsentation
Video-Filme

Referenzen:

- Cyber-Angriffe auf Unternehmen: Sind Sie gefährdet?
- Die zunehmenden strategischen Risiken von Cyberangriffen
- 10 häufige Cybersicherheitsrisiken für Unternehmen
- Interne Kontrollen und Datensicherheit: Wie Sie Kontrollen entwickeln, die Ihren IT-Sicherheitsbedürfnissen entsprechen
- Interne Kontrollen der Informationssysteme