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

InCyT Trainingsmodul

Informationssicherheit für Führungskräfte Einheit (Modul) 4, Woche 7 und 8 Name der Einheit (des Moduls): Cyber-Risiko und Resilienz	
Lern Aktivitäten	❑ **Webinar** ❑ **Übungen** ❑ **Workshop** ❑ **Präsentation** ❑ **anderes**
Verantwortlich	• Simon Tjoa • Peter Kieseberg
Ziele der Lernaktivitäten	1. Die Teilnehmer kennen die Grundlagen des Risiko- und Resilienzmanagements 2. Die Teilnehmer sind in der Lage, Business Impact Analysen und Risikoanalysen durchzuführen 3. Die Teilnehmer können aus den Ergebnissen von Analysen Gegenmaßnahmen und Sicherheitsentscheidungen ableiten
Zu erwerbende Fertigkeiten	• IS 1, IS 3 • MS 1
Dauer der Lernaktivität	2 Wochen • Woche 7 (2 Stunden) • Woche 8 (2 Stunden)
Voraussetzungen	***Was wird vorausgesetzt?***
	• Grundlegende Managementfähigkeiten • Grundlegende IT-Kenntnisse • Grundlegende Sicherheitskenntnisse

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

Kurze Informationen über das Modul

Beschreibung
Perfekte Sicherheit ist nicht möglich. Deshalb ist es wichtig, fundierte Entscheidungen darüber zu treffen, wie man Geld für die richtigen Sicherheitsmaßnahmen ausgibt. Cyber-Risiko- und Resilienzmanagement bietet eine Reihe wichtiger Instrumente und Techniken, um den aktuellen Sicherheitsstatus einer Organisation zu bewerten und Kontrollen zu planen, um das Informationssicherheitsrisiko auf einem akzeptablen Niveau zu halten.

Inhalt des Lernmaterials

Ohne das Eingehen von Risiken ist es unmöglich, ein Unternehmen zu führen. Daher bieten das Risikomanagement und die entsprechenden Instrumente und Techniken einen systematischen Weg zur Bewältigung von Risiken. Fragen danach, wie viel Sicherheit genug ist oder welche Gegenmaßnahme zuerst umgesetzt werden sollte, werden durch das Risikomanagement beantwortet. Daher ist das Risikomanagement eine wichtige Tätigkeit, die fundierte Entscheidungen ermöglicht. Wichtige Normen und bewährte Verfahren, die sich mit diesem wichtigen Thema befassen, sind ISO 27005, ISO 31000 oder BSI 200-3.

Bevor wir uns näher mit dem Risikomanagementprozess befassen, ist es wichtig, die wichtigsten Begriffe zu definieren:

- **Schwachstelle:** Eine Schwäche in einem Informationssystem, in Systemsicherheits-verfahren, internen Kontrollen oder in der Implementierung, die von einer Bedrohungsquelle ausgenutzt oder ausgelöst werden könnte.[1]
- **Kontrolle:** Eine Schutzmaßnahme oder Gegenmaßnahme, die für ein Informationssystem oder eine Organisation vorgeschrieben ist, um die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Informationen zu schützen und eine Reihe von definierten Sicherheitsanforderungen zu erfüllen.[2]

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control

- **Bedrohung:** Jeder Umstand oder jedes Ereignis, der/das das Potenzial hat, den Betrieb der Organisation (einschließlich der Mission, der Funktionen, des Images oder des Rufs), das Vermögen der Organisation, Einzelpersonen, andere Organisationen oder die Nation über ein Informationssystem durch unbefugten Zugriff, Zerstörung, Offenlegung, Modifizierung von Informationen und/oder Dienstverweigerung nachteilig zu beeinflussen.[3]
- **Risiko:** Ein Maß für das Ausmaß, in dem eine Organisation durch einen potenziellen Umstand oder ein potenzielles Ereignis bedroht ist, und ist typischerweise eine Funktion von: (i) den nachteiligen Auswirkungen oder dem Ausmaß des Schadens, der entstehen würde, wenn der Umstand oder das Ereignis eintritt, und (ii) der Wahrscheinlichkeit des Eintretens.[4]
  Auswirkung der Unsicherheit auf die Ziele[5]

Aus der Definition der ISO 31000 ("Auswirkung der Unsicherheit") können wir ableiten, dass Risiken positive und negative Auswirkungen haben können. Wenn Risiken positive Auswirkungen haben, werden sie oft als Chancen bezeichnet.

Der allgemeine Risikomanagementprozess beginnt mit dem Umfang, dem Kontext und den Kriterien. Da nicht alle Risiken für alle Aktivitäten analysiert werden können, ist es wichtig, Prioritäten zu setzen und zu entscheiden, welche Dienstleistungen, Prozesse und Organisationseinheiten in die Bewertung einbezogen werden sollen. Ein angemessener Umfang ist entscheidend, um einerseits valide Ergebnisse und andererseits einen angemessenen Aufwand zu gewährleisten. Der Kontext ist das interne und externe Umfeld. Die Festlegung von Risikokriterien ist wichtig, um einen wiederholbaren Prozess zu gewährleisten, der zu vergleichbaren Ergebnissen führt. Die Kriterien sollten so definiert werden, dass verschiedene Personen in der Lage sind, Risiken in einer gemeinsamen Weise zu bewerten.

Beispiele für Kriterien sind Auswirkungskriterien (z. B. niedrig, mittel, hoch) für verschiedene Dimensionen wie Finanzen, Ruf oder Gesundheit.

Im Folgenden wird ein Beispiel für OCTAVE Allegro hinsichtlich der Auswirkungen auf den Ruf und die Kunden vorgestellt:

[3] https://csrc.nist.gov/glossary/term/threat
[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Abbildung 1: Messkriterien für Reputation[6]

Nach der Festlegung der Risikokriterien und des Umfangs besteht der erste Schritt darin, die Risiken zu ermitteln. Die Risikoidentifizierung ist von entscheidender Bedeutung, da nur die Risiken bewertet werden können, die identifiziert wurden. Daher ist es sinnvoll, die identifizierten Risiken mit den Risikolisten von ISO 27005, MEHARI oder anderen Best Practices oder Standards zu vergleichen.

Es gibt verschiedene Techniken zur Ermittlung von Risiken, wie z. B. Brainstorming, Delphi-Technik, Fehlermöglichkeits- und Einflussanalyse (FMEA) oder Gefahren- und Betriebsfähigkeitsstudien (Hazard and Operability studies, HAZOP).

Im nächsten Schritt, der Risikoanalyse, wird ein besseres Verständnis der identifizierten Risiken gewonnen. Dazu werden Eintrittswahrscheinlichkeit/Häufigkeit und Auswirkungen/Folgen bestimmt. Um die Folgen zu bestimmen, ist es wichtig, eine systematische Methode zur Bewertung der Auswirkungen festzulegen. Oft ist ein qualitatives Maß (z. B. gering, mittel, hoch) einfacher zu verwenden als quantitative Maße.

Risiken werden häufig in einer so genannten Risikomatrix visualisiert, die das Risiko anhand der Wahrscheinlichkeit und der Auswirkung als Achsen hervorhebt.

[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Abbildung 2: Risiko Matrix [Quelle: Wikipedia][7]

Im nächsten Schritt werden die Risiken bewertet. Das bedeutet, dass die Ergebnisse des vorherigen Schritts berücksichtigt werden, um zu entscheiden, ob Maßnahmen ergriffen werden sollten. Außerdem wird eine Priorisierung der Risiken vorgenommen.

Anschließend wird eine der vier Hauptstrategien zur Bewältigung der Risiken festgelegt:

- Risikoakzeptanz: Dokumentieren und Überwachen des Risikos, wenn das Risiko im Rahmen der Risikobereitschaft der Organisation liegt
- Risikotransfer: Risiken teilen (z. B. Versicherung, Joint Venture)
- Risikovermeidung: Beseitigung der Risikoquelle (z. B. Air Gap)
- Risikominderung: Verringerung der Auswirkungen oder der Eintrittswahrscheinlichkeit (z. B. Zugangskontrolle)

Nach der Festlegung von Maßnahmen wird bewertet, ob das Restrisiko akzeptabel ist oder weitere Maßnahmen ergriffen werden müssen.

Als unterstützende Aktivitäten neben dem Hauptprozess der Risikobewertung finden Risikokommunikation (d.h. Kommunikation mit den relevanten Interessenvertretern), Risikoüberwachung und Risikoberichterstattung statt.

Da nicht alle Risiken berücksichtigt werden können, konzentriert sich Business Continuity & Resilience im Gegensatz zum Risikomanagement auf kritische Aktivitäten und nicht auf einzelne Risiken. Auf diese Weise ist es möglich, sich auf unbekannte und unwahrscheinliche Risiken mit hoher Auswirkung vorzubereiten.

[7] https://en.wikipedia.org/wiki/Risk_matrix

Um ein wirksames Programm zur Gewährleistung der Geschäftskontinuität zu gewährleisten, ist die Unterstützung der obersten Führungsebene unerlässlich. Ein wichtiges Artefakt, das die Bedeutung des Geschäftskontinuitätsmanagements unterstreicht, ist die Geschäftskontinuitätspolitik. In diesem Dokument wird die Zustimmung des Managements formell zum Ausdruck gebracht. Darüber hinaus werden in dem Dokument der Umfang und die Ziele der Business-Continuity-Aktivitäten, wichtige Rollen und Zuständigkeiten (z. B. der Business-Continuity-Manager) sowie der für die Durchführung des Programms verwendete operative Rahmen festgelegt. Es sollte betont werden, dass der Umfang nicht zu groß sein sollte, um sicherzustellen, dass die Komplexität der Analyse und der Aufwand nicht zu hoch werden.

Um die Auswirkungen von Serviceunterbrechungen auf das Geschäft zu verstehen und eine gute Grundlage für die Planung von Wiederherstellungsmaßnahmen zu haben, werden Business Impact Analysen durchgeführt. Das ist das zentrale Instrument innerhalb des Business Continuity Prozesses und erfasst die Relevanz/Signifikanz von Produkten/Dienstleistungen. Neben der Kritikalität von Produkten/Dienstleistungen werden auch deren Abhängigkeiten ermittelt und bewertet.

Wichtige Kennzahlen, die bei der Durchführung einer Business-Impact-Analyse verwendet werden, sind u.a:

- **MAO (maximum acceptable outage; maximal akzeptabler Ausfall):** Zeit, die erforderlich ist, damit nachteilige Auswirkungen [...], die durch die Nichtbereitstellung eines Produkts/einer Dienstleistung oder die Nichtdurchführung einer Tätigkeit [...] entstehen können, unannehmbar werden[8]
- **RTO (recovery time objective, angestrebte Wiederherstellungszeit):** Zeitspanne nach einem Vorfall [...], innerhalb derer ein Produkt und ein Dienst [...] oder eine Aktivität [...] wiederaufgenommen oder Ressourcen [...] wiederhergestellt werden[9]
- **RPO (recovery point objective, angestrebter Wiederherstellungspunkt):** Punkt, bis zu dem Informationen [...], die von einer Tätigkeit [...] verwendet werden, wiederhergestellt sind, damit die Tätigkeit bei Wiederaufnahme funktionieren kann[10]

In einem ersten Schritt werden die kritischsten oder wichtigsten Produkte und Dienstleistungen ermittelt. Nach der Identifizierung wird bewertet, welcher Schaden im Laufe der Zeit entstehen würde, wenn ein bestimmtes Produkt oder eine bestimmte Dienstleistung gestört oder unterbrochen wird.

[8] MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[9] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Die folgende Abbildung zeigt, wie die Auswirkungen im Zeitverlauf in einer Tabelle erfasst werden könnten.

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Darüber hinaus erhebt die Business Impact Analyse, von welchen Prozessen, Aktivitäten und Ressourcen relevante Dienste abhängig sind. Auf diese Weise lassen sich wichtige Kennzahlen wie das Wiederherstellungszeitziel, das Wiederherstellungspunktziel und der maximal akzeptable Ausfall ermitteln.

Nachdem die Kritikalität von Prozessen, Diensten und Ressourcen bekannt ist, werden Business-Continuity-Strategien ausgearbeitet. Zu den Strategien gehören u. a. Diversifizierung (z. B. Aktivitäten an geografisch getrennten Orten), Replikation (z. B. Kopieren von Daten zur Wiederherstellung an einem anderen Standort) oder Vergabe von Unteraufträgen (z. B. Inanspruchnahme von Diensten Dritter).

Auf der Grundlage dieser Strategien werden Business-Continuity-Pläne erstellt, die Organisationen dabei unterstützen, nach einem Vorfall effizient zu reagieren. Um in Situationen mit hohem Druck einsetzbar zu sein, ist es wichtig, dass die Pläne entsprechend verfasst werden. Das bedeutet, dass die Pläne nur die Informationen enthalten sollten, die für die Bewältigung eines Vorfalls relevant sind. Außerdem sollten die Informationen schnell erfassbar sein. Daher sollten klare und handlungsorientierte Checklisten verwendet werden.

Typische Business-Continuity-Pläne enthalten Informationen über Zweck, Umfang, Struktur des Notfallmanagements, Rollen und Zuständigkeiten, Aktivierung des Plans, Wiederherstellungs-vorkehrungen und Kontaktangaben.

Um die Angemessenheit der Pläne zu proben und zu überprüfen, werden verschiedene Arten von Übungen eingesetzt. Dabei kann es sich entweder um diskussionsbasierte Übungen wie Desk

Checks oder Tabletop-Übungen handeln oder um technische Übungen, bei denen beispielsweise die Wiederherstellung bestimmter Systeme getestet wird.

Fragen:

Siehe Word Dokumente

Anhänge:

Siehe PowerPoint und Videodateien

Referenzen:

- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22317:2021, Security and resilience — Business continuity management systems — Guidelines for business impact analysis
- ISO/TS 22331:2018, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy
- ISO/TS 22332:2021, Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures
- ISO 31000:2018, Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risk management — Risk assessment techniques