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

InCyT-Trainingsmodule

Informationssicherheit für Manager Einheit 2 Woche 4 Name der Einheit (des Moduls): Management der Informationssicherheit -2	
Lernaktivitäten	❑ **Webinar** ❑ **Übungen** ❑ **Workshop** ❑ **Präsentation** ❑ **Sonstiges** Streaming Webinar, Text, Übungen zur Selbsteinschätzung, Übungen mit Antworten in Diskussionsforen und Diskussion mit Trainer/Mentor
Lehrverantwortliche	• Fatma Gökdemir • Ali Gökdemir
Ziele der Lernaktivitäten	1. Bewertung von Bedrohungen und Schwachstellen 2. Management von Bedrohungen und Schwachstellen 3. Arten der Schwachstellenbewertung 4. Cyber Continuity of Operations 5. Cyber-Vermögen 6. Bewertung der Wirksamkeit von Cybersicherheitsmaßnahmen
Zu erwerbende Fertigkeiten	• IS 1 • IS 3 • MS 5
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	***Was wird benötigt?*** • Mittlere Computerkenntnisse

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Kurze Informationen über das Modul

Beschreibung
Die Verwaltung von Vermögenswerten nimmt einen wichtigen Platz im Rahmen des ISO 27001 Information Security Management System ein. In der Tat ist die Identifizierung und Klassifizierung von Informationswerten einer der ersten Schritte bei der Einrichtung der Informationssicherheit. Die Identifizierung und Wertzuweisung von Vermögenswerten in einer Organisation ist ein grundlegender Schritt im Prozess der Risikoanalyse. Um den Werten einen Wert zuzuweisen, wird ein Inventar der Vermögenswerte erstellt. Vor der Bestandsaufnahme der Vermögenswerte sollte eine Sondierungsstudie durchgeführt werden, die alle Mitarbeiter erfasst. Mit dieser Studie wird das Anlageninventar der Abteilung erkundet und mit möglichen Risiken und dem Grad der Vertraulichkeit aufgelistet. Die Anlageninventur sollte nach und nach auf der Grundlage der erfassten Prozesse durchgeführt werden. Bei der Erstellung des Bestandsverzeichnisses werden die Anlagengruppe, die Umgebung, in der sich die betreffende Anlage befindet, der Klassifizierungscode ermittelt und der Wert der Anlage (Vertraulichkeit, Integrität, Zugänglichkeit) berechnet. Anhand des Berechnungsergebnisses wird der Prioritätsstatus bestimmt, und es werden Aktionsentscheidungen getroffen. Nach Abschluss der Inventarisierungsarbeiten wird eine detaillierte Inventarliste für die ermittelten Software- und Hardwarebestände erstellt. Die Bedingungen/Kontrollen bezüglich der Vermögensverwaltung in der ISO27001-Norm sind in Anhang A.8 zusammengefasst. In diesem Modul werden wir die in A.8.1 definierten Begriffe für die Haftung von Vermögenswerten untersuchen.

Inhalt des Lernmaterials

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

1. Bewertung des Managements der Informationssicherheit

In der ersten Phase der Vermögensverwaltung wäre es sinnvoll, zunächst einmal festzustellen und aufzulisten, welche Vermögenswerte wir haben. Zunächst sollte bekannt sein, was eine Institution besitzt oder nicht besitzt. Dann müssen die Eigentumsverhältnisse definiert werden. Kein Geschäft und keine Transaktion sollte unbeaufsichtigt bleiben. Dann sollten die Regeln für die Verwendung dieser Vermögenswerte festgelegt werden.

Die Einzelheiten zu diesem Thema sind in der Norm ISO27002 zu finden. Die Erwartungen bezüglich der Vermögensverwaltung in ISO27002 sind im 8. Artikel der Norm enthalten:

Vermögensverwaltung und Haftung für Vermögenswerte

Zweck: Ermittlung der Vermögenswerte der Organisation und Festlegung der entsprechenden Schutzverantwortlichkeiten.

1. Bestandsaufnahme der Vermögenswerte

Kontrolle: Die Vermögenswerte im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen sollten ermittelt werden, und es sollte ein Inventar dieser Vermögenswerte erstellt und gepflegt werden.

Anwendungsleitfaden: Eine Organisation sollte die für den Lebenszyklus von Informationen relevanten Werte identifizieren und ihre Bedeutung dokumentieren. Der Lebenszyklus von Informationen sollte die Erstellung, Verarbeitung, Speicherung, Übertragung, Löschung und Vernichtung umfassen. Die Dokumentation sollte in Übereinstimmung mit bestehenden Inventaren oder spezifisch gepflegt werden.

Bestandsverzeichnis; muss aktuell, konsistent, genau und mit anderen Verzeichnissen kompatibel sein.

Das Eigentum an den Vermögenswerten sollte für jeden identifizierten Vermögenswert zugewiesen werden (siehe Artikel 2) und seine Klasse sollte bestimmt werden.

Sonstige Informationen: Die Inventarisierung von Vermögenswerten trägt zu einem wirksamen Schutz bei und kann auch aus anderen Gründen wie Gesundheit und Sicherheit, Versicherung oder Finanzen (Vermögensverwaltung) erforderlich sein.

Die Norm ISO/IEC 27005[11] enthält Beispiele für Vermögenswerte, die von der Organisation bei der Identifizierung von Vermögenswerten berücksichtigt werden müssen. Der Prozess der Erstellung eines Anlageninventars ist eine wichtige Voraussetzung für das Risikomanagement (siehe ISO/IEC 27000 und ISO/IEC 27005[11]).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2. Eigentum an Vermögenswerten

Kontrolle: Für alle im Bestand befindlichen Vermögensgegenstände müssen Eigentümerzuordnungen vorgenommen werden.

Leitfaden für die Anwendung: Einzelpersonen und andere Stellen mit genehmigter Managementverantwortung für den Lebenszyklus von Vermögenswerten können als Eigentümer von Vermögenswerten benannt werden.

Um sicherzustellen, dass die Eigentumsverhältnisse an den Vermögenswerten rechtzeitig geklärt werden, wird häufig ein Verfahren eingesetzt. Die Eigentumsverhältnisse müssen festgelegt werden, wenn Vermögenswerte geschaffen oder an die Organisation übertragen werden. Der Eigentümer des Vermögenswerts sollte für die ordnungsgemäße Verwaltung des Vermögenswerts während des gesamten Lebenszyklus des Vermögenswerts verantwortlich sein.

Eigentümer des Vermögens:

a) Sicherstellen, dass das Inventar der Vermögenswerte erfasst wird,

b) Sicherstellung, dass die Vermögenswerte ordnungsgemäß klassifiziert und geschützt werden,

c) Festlegung und regelmäßige Überprüfung von Zugangsbeschränkungen zu wichtigen Vermögenswerten und deren Klassifizierung unter Berücksichtigung der geltenden Zugangskontrollpolitik,

d) Sicherstellung, dass bei der Löschung oder Vernichtung von Vermögenswerten angemessene Maßnahmen ergriffen werden.

Andere Informationen: Es kann sich um eine natürliche oder juristische Person handeln, die über die Genehmigung verfügt, die Verantwortung für die Verwaltung eines Vermögenswerts während seines gesamten Lebenszyklus zu übernehmen. Der identifizierte Eigentümer hat kein Eigentumsrecht an dem Vermögenswert.

Routineaufgaben können delegiert werden (z. B. an einen Verwalter, der sich täglich um einen Vermögenswert kümmert), aber die Verantwortung liegt beim Eigentümer des Vermögenswerts.

Die Identifizierung von Gruppen von Assets innerhalb komplexer Informationssysteme kann für die gemeinsame Bereitstellung von Funktionen nützlich sein. In diesem Fall ist dieser Diensteigentümer für die Erbringung des Dienstes, einschließlich des Betriebs der Assets,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

verantwortlich.

3. Zulässige Verwendung von Vermögenswerten

Kontrolle: Es sollten ***Regeln*** für die zulässige Nutzung von Informationen und Vermögenswerten im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen festgelegt, dokumentiert und umgesetzt werden.

Anwendungsleitfaden: Mitarbeiter und externe Benutzer, die die Vermögenswerte der Organisation nutzen oder Zugang zu ihnen haben, sollten über die Anforderungen an die Informationssicherheit der Vermögenswerte der Organisation im Zusammenhang mit den Einrichtungen und Ressourcen zur Informationsverarbeitung aufgeklärt werden. Diese Benutzer sollten für die Nutzung aller Informationsverarbeitungsressourcen und für jede Nutzung, die unter ihrer eigenen Verantwortung erfolgt, verantwortlich sein.

4. Rückgabe von Vermögenswerten

Kontrolle: Alle Mitarbeiter und Nutzer externer Parteien müssen bei Beendigung des Arbeitsverhältnisses, des Vertrags oder der Vereinbarung alle in ihrem Besitz befindlichen Vermögenswerte des Unternehmens zurückgeben.

Anwendungsleitfaden: Der Beendigungsprozess sollte so formuliert werden, dass er die Rückgabe des Eigentums an allen zuvor gewährten physischen und elektronischen Vermögenswerten oder Treuhandkonten der Organisation beinhaltet.

Wenn ein Mitarbeiter oder ein externer Benutzer Geräte der Organisation erwirbt oder benutzt, werden Verfahren befolgt, die sicherstellen, dass alle relevanten Informationen an die Organisation übertragen und sicher von den Geräten gelöscht werden.

Wenn ein Mitarbeiter oder ein externer Benutzer über Informationen verfügt, die für den laufenden Betrieb wichtig sind, müssen diese Informationen dokumentiert und an das Unternehmen weitergegeben werden.

Während der Kündigungsfrist muss die Organisation das unerlaubte Kopieren von Informationen, wie z. B. geistiges Eigentum, durch entlassene Mitarbeiter und Auftragnehmer kontrollieren.

2. Bewertung und Management von Bedrohungen und Schwachstellen

Fast jedes Unternehmen verfügt über sensible und wertvolle Vermögenswerte, die geschützt

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

werden müssen. Doch nicht jedes Unternehmen verfügt über eine umfassende und gut durchdachte Strategie zum Schutz dieser Vermögenswerte. Im Bereich der Cybersicherheit sind Strategien für das Schwachstellenmanagement die Grundlage für eine starke Verteidigung. In der Regel sind Strategien für das Schwachstellenmanagement darauf ausgerichtet, die Systeme, Netzwerke, Anwendungen usw. eines Unternehmens zu schützen. Sie verfolgen einen ganzheitlichen und kontinuierlichen Ansatz zur Verwaltung von Sicherheitsschwachstellen. Diese Schwachstellen werden dann ermittelt, bewertet und so schnell wie möglich behoben.

Sicherheitsbedrohungen und -trends entwickeln sich ständig weiter und erfordern wirksame, präventive Maßnahmen zum Umgang mit Bedrohungen und Schwachstellen, die Ihre Daten gefährden könnten. Um alle potenziellen Ziele einer Sicherheitsverletzung oder eines Angriffs zu identifizieren, muss das Risiko zunächst durch eine Bestandsaufnahme der Anlagen gemindert werden. Die Ziele müssen dann klassifiziert und kontinuierlich auf neue potenzielle Schwachstellen überwacht werden. Anschließend sollte ein Bedrohungsmodell entwickelt und getestet werden, das die wertvollsten und am stärksten gefährdeten Vermögenswerte des Unternehmens identifiziert. Der Hauptzweck des Prozesses der Bedrohungs- und Schwachstellenprüfung (Bewertung) besteht darin, die Kritikalität von Vermögenswerten und die Schwachstellen dieser Vermögenswerte bestmöglich zu verstehen und die notwendigen Maßnahmen zum wirksamen Schutz dieser Vermögenswerte zu reduzieren.

2.1. Was ist eine Schwachstellenanalyse?

Unter Schwachstellenbewertung versteht man den Prozess der Identifizierung, Klassifizierung und Priorisierung von Schwachstellen in Computersystemen, Anwendungen und Netzinfrastrukturen.

Schwachstellenbewertungen verschaffen einer Organisation auch das Wissen, das Bewusstsein und den Risikohintergrund, die notwendig sind, um Bedrohungen für ihre Umgebung zu verstehen und auf sie zu reagieren. Ein Schwachstellenbewertungsprozess zielt darauf ab, Bedrohungen und die von ihnen ausgehenden Risiken zu ermitteln. Häufig werden dazu automatische Testwerkzeuge wie Netzwerksicherheitsscanner eingesetzt, deren Ergebnisse in einem Schwachstellenbewertungsbericht aufgeführt werden.

Organisationen jeder Größe und sogar Einzelpersonen, die einem erhöhten Risiko von Cyberangriffen ausgesetzt sind, können in irgendeiner Form von einer Schwachstellenanalyse profitieren, aber große Organisationen und andere Arten von Organisationen, die ständigen Angriffen ausgesetzt sind, werden am meisten von einer Schwachstellenanalyse profitieren.

Da sich Hacker über Schwachstellen Zugang zu IT-Systemen und -Anwendungen verschaffen

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

können, ist es für Unternehmen entscheidend, Schwachstellen zu erkennen und zu beheben, bevor sie ausgenutzt werden. Eine umfassende Schwachstellenbewertung in Verbindung mit einem Verwaltungsprogramm kann Unternehmen dabei helfen, die Sicherheit ihrer Systeme zu verbessern.

2.2. Die Bedeutung von Schwachstellenanalysen

Um die Bedeutung der Schwachstellenbewertung zu verdeutlichen, betrachten wir sie mit den Augen eines Immobilienbesitzers. Wenn Sie ein wertvolles Gebäude besitzen, ergreifen Sie wahrscheinlich eine Reihe von Maßnahmen, um es zu schützen: Sie halten es instand, versichern es und sorgen dafür, dass die Türen und Fenster verschlossen und die Alarmanlagen aktiviert sind. All diese Schritte können als Risikomanagement für die Immobilie und ihren Inhalt bezeichnet werden.

Was wäre, wenn Sie jemanden anstellen könnten, der Ihre Alarme und externen Verteidigungsmaßnahmen testet und darüber berichtet? Schwachstellen in der Cybersicherheit werden auf ähnliche Weise angegangen. Schwachstellenmanagement ist eine übergreifende und fortlaufende Strategie, während Schwachstellenbewertungen ein spezifisches Instrument sind, das im Rahmen dieser breiteren Managementstrategie eingesetzt wird.

Eine Schwachstellenbewertung liefert einer Organisation detaillierte Informationen über etwaige Sicherheitslücken in ihrer Umgebung. Sie gibt auch Hinweise darauf, wie die mit diesen Schwachstellen verbundenen Risiken bewertet werden können. Dieser Prozess verschafft dem Unternehmen ein besseres Verständnis seiner Vermögenswerte, Sicherheitsmängel und des Gesamtrisikos, wodurch die Wahrscheinlichkeit verringert wird, dass ein Cyberkrimineller in die Systeme eindringt und das Unternehmen unvorbereitet trifft.

2.3. Arten der Schwachstellenbewertung

Schwachstellenbewertungen decken verschiedene System- oder Netzschwachstellen auf. Das bedeutet, dass der Bewertungsprozess die Verwendung einer Vielzahl von Tools, Scannern und Methoden umfasst, um Schwachstellen, Bedrohungen und Risiken zu ermitteln.

Einige der verschiedenen Arten von Schwachstellen-Scans sind (Abbildung 1):

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

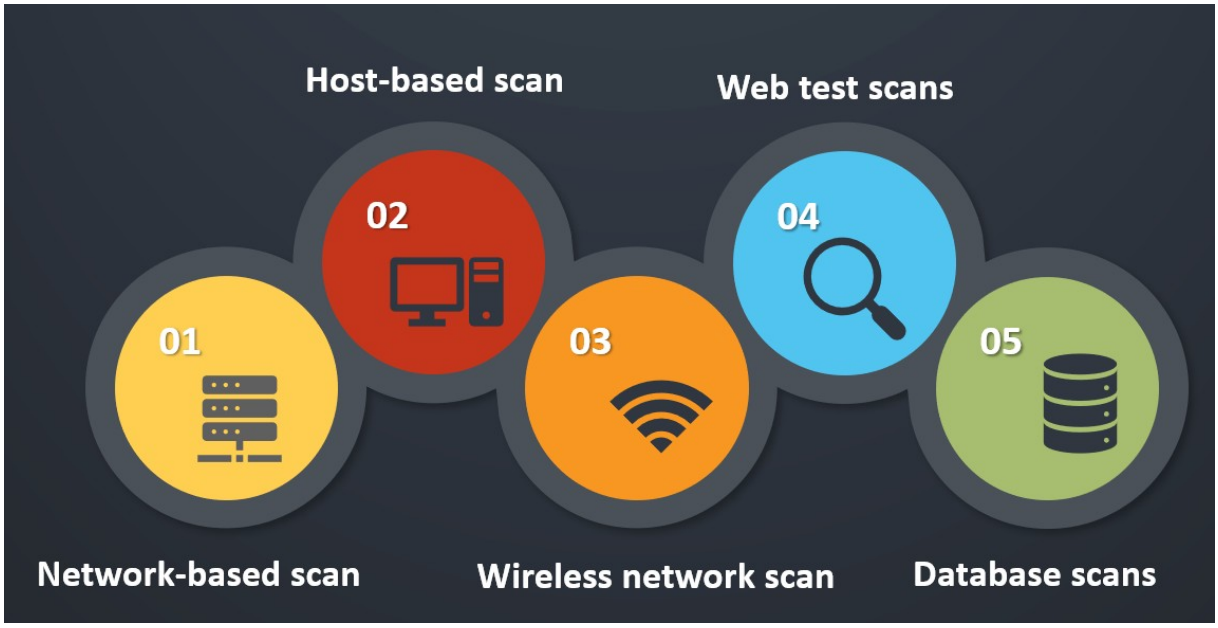

Abbildung 1. Arten der Schwachstellenbewertung

- **Netzwerkbasierte Scans** werden eingesetzt, um potenzielle Angriffe auf die Netzwerksicherheit zu erkennen. Diese Art von Scan kann auch anfällige Systeme in kabelgebundenen oder drahtlosen Netzwerken aufspüren.
- **Host-basierte Scans** werden verwendet, um Schwachstellen in Servern, Workstations oder anderen Netzwerk-Hosts zu finden und zu identifizieren. Bei dieser Art von Scans werden in der Regel Ports und Dienste untersucht, die auch bei netzwerkbasierten Scans zu sehen sind. Sie bietet jedoch einen besseren Einblick in die Konfigurationseinstellungen und die Patch-Historie der gescannten Systeme, einschließlich älterer Systeme.
- **Scans** der Wi-Fi-Netzwerke eines Unternehmens konzentrieren sich häufig auf Angriffspunkte in der drahtlosen Netzwerkinfrastruktur. Durch das Scannen von Drahtlosnetzwerken können nicht nur böswillige Zugangspunkte identifiziert werden, sondern es kann auch überprüft werden, ob das Netzwerk eines Unternehmens sicher konfiguriert ist.
- Web-Scan-Testseiten, um bekannte Software-Schwachstellen und Fehlkonfigurationen in Anwendungen, Netzwerken oder Web-Applikationen zu erkennen.
- **Datenbank-Scans** können Schwachstellen in einer Datenbank identifizieren, um bösartige Angriffe zu verhindern.

2.4. Schwachstellenanalysen und Penetrationstests

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Eine Schwachstellenbewertung umfasst häufig auch eine Komponente für Penetrationstests, um Schwachstellen im Personal, in den Verfahren oder Prozessen eines Unternehmens zu ermitteln. Schwachstellenbewertungen weisen viele der gleichen Merkmale auf wie Penetrationstests, da beide es Organisationen ermöglichen, ihre Verteidigungsmaßnahmen gründlich zu untersuchen. Diese Schwachstellen werden normalerweise nicht durch Netzwerk- oder Systemscans aufgedeckt. Der Prozess wird manchmal auch als Schwachstellenbewertung/Penetrationstest oder **VAPT** bezeichnet.

Penetrationstests reichen jedoch nicht aus, um eine vollständige Schwachstellenanalyse durchzuführen, sondern sind ein separater Prozess. Eine Schwachstellenbewertung zielt darauf ab, Schwachstellen in einem Netz aufzudecken und geeignete Abhilfemaßnahmen vorzuschlagen, um die Risiken zu mindern oder zu beseitigen.

Bei einer Schwachstellenbewertung werden automatisierte Tools zum Scannen der Netzwerksicherheit eingesetzt. Die Ergebnisse werden im Schwachstellenbewertungsbericht aufgeführt, der sich darauf konzentriert, Unternehmen eine Liste von Schwachstellen zu liefern, die behoben werden müssen. Dies geschieht jedoch ohne Bewertung spezifischer Angriffsziele oder Szenarien.

Unternehmen sollten regelmäßig Schwachstellentests durchführen, um die Sicherheit ihrer Netze zu gewährleisten, insbesondere wenn Änderungen vorgenommen werden. Zum Beispiel sollten Tests durchgeführt werden, wenn Dienste hinzugefügt, neue Geräte installiert oder Ports geöffnet werden.

Im Gegensatz dazu geht es bei Penetrationstests darum, Schwachstellen in einem Netz zu ermitteln und zu versuchen, sie für einen Angriff auf das System zu nutzen. Obwohl sie manchmal in Verbindung mit Schwachstellenbewertungen durchgeführt werden, besteht der Hauptzweck von Penetrationstests darin, zu prüfen, ob eine Schwachstelle tatsächlich existiert. Darüber hinaus wird bei Penetrationstests versucht zu beweisen, dass die Ausnutzung einer Schwachstelle der Anwendung oder dem Netzwerk schaden kann.

Während eine Schwachstellenbewertung in der Regel automatisiert erfolgt, um eine Vielzahl ungepatchter Schwachstellen zu erfassen, werden bei Penetrationstests häufig automatisierte und manuelle Techniken kombiniert, damit die Tester die Schwachstellen weiter untersuchen und sie nutzen können, um sich in einer kontrollierten Umgebung Zugang zum Netzwerk zu verschaffen.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

2.5. Schwachstellenmanagement und Risikomanagement

Während das Schwachstellenmanagement ein fortlaufender Prozess zur Verwaltung von Schwachstellen ist, betrachtet das Risikomanagement alles, was eine Bedrohung für ein Unternehmen darstellen kann, aus einem breiteren Blickwinkel. Eine solide Risikomanagementstrategie ermöglicht es, Risiken zu identifizieren, zu analysieren und wirksam zu mindern. Dieser Ansatz hilft Organisationen, nicht nur die vorhandenen Schwachstellen zu verstehen, sondern auch das Ausmaß des Schadens, der entstehen kann, wenn sie missbraucht werden. Eine Risiko- und Schwachstellenbewertung, die im Rahmen des Risikomanagements durchgeführt wird, kann einen besonders umfassenden Überblick über die Stärke der Sicherheitsvorkehrungen eines Unternehmens geben.

3. Cyber Continuity of Operations

Die Erhöhung der Widerstandsfähigkeit gegen die Bedrohung durch destruktive Malware erfordert einen Einblick in die aktuelle Sicherheitslage, die Planung und Koordinierung wichtiger Abwehrmaßnahmen und die richtige Ausrichtung der wichtigsten Abwehrressourcen.

Cybervorfälle haben die grundlegende Kontinuitätsplanung ebenfalls in Frage gestellt. Zwar verfügen viele Behörden über Ausrüstung und Strategien zur Erkennung, Aufdeckung und zum Schutz vor Cyberangriffen, aber weit weniger haben sich mit der harten Realität der Kontinuität ihrer Abläufe bei einem tatsächlichen Angriff auseinandergesetzt. Wenn es zu einem Cyberangriff kommt, stellen viele betroffene Behörden fest, dass ihre grundlegenden COOP-Pläne nicht ausreichen. Während die Pläne für den Übergang zu einem alternativen Arbeitsort ausreichen, haben sie weit weniger zu bieten, wenn es darum geht, ohne Zugang zu den Systemen und Daten zu arbeiten, die die Mitarbeiter für die Erfüllung ihrer wesentlichen Aufgaben benötigen. Den bestehenden Plänen mangelt es auch an der notwendigen Spezifität, um die Reaktion zu steuern, und wichtige Interessengruppen wie die IT-Mitarbeiter sind oft nicht in die Reaktionsstrukturen integriert. Und die Pläne werden nicht anhand einer Übung oder eines realen Vorfalls getestet.

Herkömmliche COOP-Pläne sind für die Kontinuität bei Cybervorfällen in mehrfacher Hinsicht unzureichend (Abbildung 2):

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

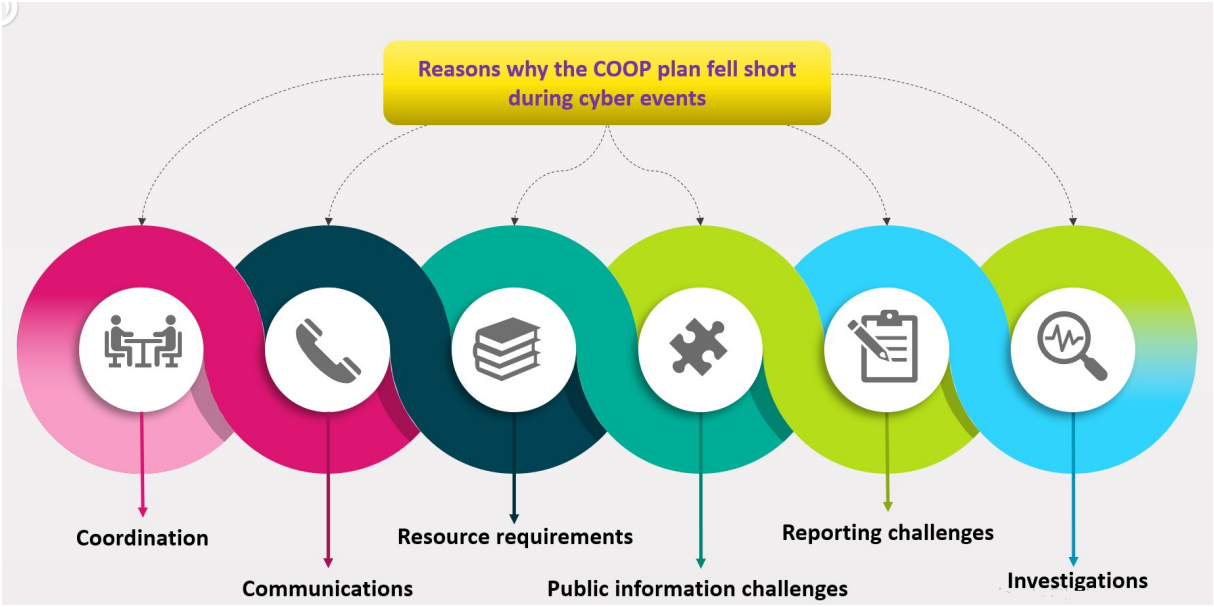

Abbildung 2. Gründe, warum COOP-Pläne für die Kontinuität bei Cyber-Ereignissen unzureichend sind

Koordination: Dazu gehört, wer an der Entscheidungsfindung in Bezug auf Ransomware, Entscheidungen über das Abschalten von Systemen und Entscheidungen über die Aktivierung des Notfallzentrums der jeweiligen Behörde beteiligt ist. Darüber hinaus verfügen die meisten Kommunalverwaltungen weder über klare Eskalationsstufen für einen Angriff noch über die damit verbundenen Aktionspunkte für jede Stufe. Auch die Führung und die personelle Besetzung der Einsatzkräfte kann unklar sein. Die Arten von Fachwissen, die benötigt werden, um eine Gemeinde durch einen Cybervorfall zu führen, unterscheiden sich von denen, die für extreme Wetterbedingungen benötigt werden.

Kommunikation: Dazu gehört auch die Frage, wie die lokalen Manager das Personal schnell informieren, wenn ein Cyberangriff die Kommunikation stark beeinträchtigt hat. Dazu gehören sowohl unmittelbare Mitteilungen, die erklären, was zu tun ist, wenn der Angriff beginnt, als auch laufende Mitteilungen, z. B. darüber, wie die Gehälter bis zum Zahltag ausgezahlt werden. Beides ist für die Reaktion von entscheidender Bedeutung, muss aber unter Umständen ohne die üblichen Notfallkommunikationssysteme übermittelt werden.

Ressourcenbedarf: Diese können sich stark von denen für eine herkömmliche Antwort unterscheiden. So benötigen die Mitarbeiter möglicherweise saubere Computer, saubere Server, lokale Drucker und sogar Faxgeräte und Papier. Wichtig ist, dass der Personalbedarf bei der Wiederherstellung sogar noch stärker ansteigen kann als bei der Reaktion, da die Abteilungen und Behörden versuchen, fehlende oder verdächtige Daten zu replizieren.

Herausforderungen bei der Information der Öffentlichkeit: Dazu gehören Beamte, die für die Information der Öffentlichkeit zuständig sind und wenig bis gar keine Ausbildung oder Erfahrung

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

im Bereich Cybersicherheit haben, ein Mangel an vorgefertigten Nachrichten und Uneinigkeit darüber, wann Informationen über den Angriff veröffentlicht werden sollten. Die Information der Öffentlichkeit ist von entscheidender Bedeutung, denn die Bürger sorgen sich um ihre Daten und die Vertrauenswürdigkeit wichtiger demokratischer Systeme wie Wahlen und Justiz.

Probleme bei der Berichterstattung: Dies kann die Reaktion verzögern, da Ausfälle nicht einheitlich gemeldet werden, so dass die IT-Abteilungen nicht über das notwendige gemeinsame Betriebsbild verfügen, um einen Angriff schnell zu erkennen. Darüber hinaus sind die Berichtswege oft unklar, und nur wenige Personen außerhalb der IT-Abteilung wissen, welche Systeme innerhalb und außerhalb des Zuständigkeitsbereichs miteinander verbunden sind.

Nachforschungen: Dies ist für viele Kommunen eine Blackbox. Die Beteiligung einer oder mehrerer Bundesorganisationen und die Grenzen, die Untersuchungen den Sanierungsbemühungen setzen, sind nicht gut bekannt oder geplant. Dies macht die Kontinuitätsplanung extrem schwierig, da nicht klar ist, wie und wann die Sanierung überhaupt beginnen kann.

3.1. Prioritäten für sofortige Maßnahmen mit koordinierter Verteidigung

- Entwickeln Sie eine "Cyber-Tasche" mit den wichtigsten Verfahren und Informationen.
    - o Zusammenstellung mobiler Cybersicherheits-Toolkits, die Verfahren zur Einrichtung, Umsetzung, Aufrechterhaltung und Ermöglichung der Aufrechterhaltung cyberresistenter TTPs innerhalb einer als COOP bezeichneten Einrichtung enthalten
- Entwicklung, Test und Validierung von Playbooks, Rollen, Verantwortlichkeiten und Tools.
    - o Benennung spezifischer Cyber-Rollen, zugehöriger Verantwortlichkeiten und der Cyber-Werkzeuge, die eingesetzt werden können, um die Umsetzung der Cyber-COOP zu gewährleisten.
    - o Definition von Standard-COOP-Spielen für Einzelpersonen oder Cyber-Teams unter Verwendung von "Go Bag"-Tools und elastischen TTPs.
    - o Durchführung verschiedener Arten von Cyber-Übungen (z. B. Mini-Tischübungen) unter Verwendung des Cyber-"Go Bag" und des Spielbuchs.
- Definition von Prozessen für die Zusammenarbeit und Anschaffung von Tools für Cyberverteidiger und Notfallhelfer.
    - o Sicherstellen, dass sowohl mobile als auch stationäre Cyber-COOP-Prozesse eine Verzahnung von Kommunikation und Koordination beinhalten, um ein angemessenes Management der Cyber-Verteidigung, Synergieeffekte zwischen allen Reaktionsaktivitäten und die Verringerung von Sicherheitslücken während der Wiederherstellungsaktivitäten zu fördern.

Zwar haben die grundlegenden COOP-Pläne die lokale Bereitschaft für viele der Bedrohungen, mit denen die Gerichtsbarkeiten konfrontiert sind, gefördert, doch greifen sie in Situationen, die eine ganz andere Umgebung als die Norm schaffen, zu kurz. Während die IT-Abteilungen im

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

ganzen Land weiterhin versuchen, ihre Systeme und Daten so sicher wie möglich zu machen, ist es an den Notfallmanagern, ihre Vorstellungskraft zu erweitern und für Cyberangriffe zu planen, die kritische Systeme und Daten ernsthaft beeinträchtigen.

3.2. Prioritäten für sofortige Maßnahmen bei der Neuausrichtung

- Ermittlung der Abhängigkeiten von Cyber-Ressourcen in Bezug auf den Auftrag und die Geschäftsfunktionen.

o Bestimmung der Einsatzzwecke von Ressourcen, damit Verwendungen, die das Risiko erhöhen, ohne einen entsprechenden Nutzen für den Einsatz zu haben, ermittelt und beseitigt werden können.

✓ Identifizieren und Entfernen oder Ersetzen von Dateneinspeisungen und -verbindungen, bei denen die Risiken die Vorteile überwiegen.

o Berücksichtigung der Interdependenzen zwischen und unter den Geschäftsfunktionen und Organisationen, die bei der Bereitstellung der NEF-Fähigkeiten eine entscheidende Rolle spielen.

✓ Neuzuweisung von Ressourcen oder Neuzuweisung von Verwaltungs- und Managementverantwortung auf der Grundlage des Risikos für den Auftrag und die Geschäftsfunktion.

- Identifizierung von Abhängigkeiten von Cyber-Ressourcen, die nicht zu den Aufgaben und Geschäftsfunktionen gehören, oder von deren Nutzung.

o Einsatz von Missionsablaufanalysen, Missionsabhängigkeitsanalysen, Tabletop-Übungen und Red Teaming zur Aufdeckung nicht dokumentierter Missionsabhängigkeiten.

o Überprüfung und Korrelation der Aufgaben- und Geschäftsfunktionen mit den Aktivitäten und Ergebnissen der Abbildung des Abhängigkeitsmodells und der Wirkungsanalyse.

o Ermittlung von Systemen, Anwendungen und Prozessen für nicht unternehmenskritische Funktionen und der sie unterstützenden Ressourcen.

✓ Bewertung dieser Funktionen anhand einer fließenden Cyber-COOP-Implementierungsstrategie, um vorrangige Operationen und eine bessere Nutzung oder Beseitigung von Abhängigkeiten zu ermöglichen.

4. Verwaltung von Cyber-Assets, Änderungen und Konfigurationen

✓ **Vermögenswert:** Beginnen wir mit der Definition des Begriffs "Vermögenswert". Nach der Definition des Wörterbuchs ist ein Vermögenswert eine **nützliche oder**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

wertvolle Sache oder Person. In ähnlicher Weise sind die Assets eines IT-Dienstleisters seine Tools, Anwendungen, Konfigurationsobjekte und alle anderen wertvollen Objekte, die dazu beitragen, Dienstleistungen für Kunden oder Unternehmen zu erbringen. Assets sind ein Teil des Service Asset und Configuration Management.

- ✓ **Konfigurationselement:** Configuration Item wird mit CI abgekürzt und ein Configuration Item ist **jede Komponente, die verwaltet werden muss, um einen IT-Service zu erbringen.** Beispiele für Configuration Items sind IT-Services, Hardware, Software, Gebäude, Mitarbeiter und formale Dokumentation. Kurz gesagt, jede Komponente oder jeder Gegenstand, der dazu beiträgt, dem Kunden einen IT-Service zu liefern, wird als Configuration Item klassifiziert. Informationen über jedes Configuration Item werden in einem Configuration Record innerhalb des Configuration Management Systems aufgezeichnet, und diese Informationen werden während des gesamten Lebenszyklus vom Configuration Management gepflegt.
- ✓ **Konfigurationsmanagement-Datenbank:** Die Konfigurationsmanagement-Datenbank wird als CMDB abgekürzt. CMDB ist eine **Datenbank, in der Konfigurationsdatensätze während ihres gesamten Lebenszyklus gespeichert werden. Die CMDB** speichert Informationen über Ihre CIs, die sich jeweils durch eine eindeutige Kennung unterscheiden, einschließlich identifizierende Informationen wie Seriennummer, MAC-Adresse oder IP-Adresse, die aktuelle Version, den Standort sowie Informationen über den Hersteller und Lieferanten.
- ✓ **Konfigurationsmanagement-System: Das** Configuration Management System, abgekürzt CMS, ist **eine Reihe von Tools und Datenbanken, die zur Verwaltung der Konfigurationsdaten eines IT-Dienstleisters verwendet werden.** Daten über Konfigurationselemente werden in Konfigurationsdatensätzen gespeichert, und die Konfigurationsdatensätze sind in den Datenbanken des Konfigurationsmanagementsystems enthalten. Die CMDBs eines IT-Dienstleisters zur Verwaltung der Konfigurationsdaten sind in den Prozess des Service Asset- und Konfigurationsmanagements eingebunden. Das Configuration Management System enthält auch Informationen über Vorfälle, Probleme, bekannte Fehler, Änderungen und Freigaben, Mitarbeiter, Lieferanten, Standorte, Geschäftsbereiche, Kunden und Benutzer. Zusammenfassend lässt sich sagen, dass alle notwendigen Informationen über Konfigurationselemente und IT-Assets im Konfigurationsmanagementsystem enthalten sind. Bei Bedarf werden diese Informationen aus dem CMS abgerufen und entsprechend genutzt**.**

Das Konfigurationsmanagement, das im Wesentlichen als Prozess der Identifizierung, Kontrolle,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Überwachung und Prüfung von Änderungen definiert ist, ist ein wichtiger Bestandteil eines starken Sicherheitsprogramms. Das Änderungs- und Konfigurationsmanagement in einem Unternehmen ist eng mit den Audit-Anforderungen in fast allen Sicherheitsrahmen und -vorschriften verknüpft.

Das Konfigurationsmanagement basiert auf der Kontrolle und Freigabe verschiedener Produktversionen. Die Standardkonfigurationen für Betriebssysteme und Anwendungen sind im Allgemeinen auf eine einfache Bereitstellung und Nutzung ausgerichtet und nicht auf bewährte Verfahren für die Cybersicherheit. Heutzutage ist das Konfigurationsmanagement eine gefragte Disziplin mit erheblichen Auswirkungen auf die Cybersicherheit, insbesondere da Unternehmen von Standardkonfigurationen zu sichereren Anwendungs- und Hardwarekonfigurationen übergehen.

Heutzutage hat der Begriff Konfigurationsmanagement für verschiedene Menschen unterschiedliche Bedeutungen. Bei einigen Implementierungen bezieht es sich auf die Art und Weise, wie Netzwerkgeräte konfiguriert werden. In anderen Fällen geht es um die Version einer Anwendung, die ein Team ausführt. Manchmal wird in der Branche das IT-Asset-Management mit dem Änderungs- und Konfigurationsmanagement verwechselt. Sie sind zwar ähnlich und für das Unternehmen gleichermaßen wichtig, aber sie sind nicht dasselbe. IT-Management-Lösungen überwachen, optimieren und verwalten Assets über den gesamten Asset-Lifecycle. CM hingegen sammelt, speichert, verwaltet, aktualisiert und analysiert alle Konfigurationselemente.

Obwohl viele Unternehmen über unausgereifte CM-Programme verfügen, sind sie für die moderne Cybersicherheitslandschaft von entscheidender Bedeutung und werden mit der Weiterentwicklung der Bedrohungslandschaft nur noch an Bedeutung gewinnen.

4.1. Konfigurationsmanagement und Disaster Recovery

Wenn es um moderne Notfallwiederherstellung geht, ist das Konfigurationsmanagement unerlässlich. Im Falle einer Cybersecurity-Katastrophe (immerhin haben 76 % der Unternehmen einen IoT-Cybersecurity-Vorfall erlebt) kann es unmöglich sein, die letzte Konfiguration wiederherzustellen, wenn es keine Dokumentation dieser Konfiguration gibt.

Das Gleiche gilt für die Cybersicherheit: Ohne eine standardisierte Methode zur Konfiguration, Änderung und Dokumentation der digitalen Umgebung können die Teams nicht erkennen, ob etwas nicht in Ordnung ist.

4.2. Änderungsmanagement

Das Änderungsmanagement läuft parallel zum Konfigurationsmanagement, obwohl die beiden Dinge *nicht dasselbe* sind. Die Leute verwechseln sie immer wieder.
Während das Konfigurationsmanagement den Prozess der Identifizierung und Dokumentation von

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Hardware-Komponenten und Software sowie der zugehörigen Einstellungen umfasst, ist das Änderungsmanagement eine grundlegende Funktion des umfassenderen Konfigurationsmanagementprozesses. Das Änderungsmanagement bezieht sich auf die damit verbundenen Prozesse und dient dazu, Stabilität innerhalb eines Systems zu schaffen und unkontrollierte oder zufällige Änderungen zu verhindern oder Änderungsprozesse zu dokumentieren, wenn es innerhalb der Organisation zu einem Wechsel kommt. Mit anderen Worten: Es ermöglicht den Unternehmen, Veränderungen zu planen, anstatt nur auf sie zu reagieren.

4.2.1. Der Änderungsmanagementprozess

Ein gut strukturierter Veränderungsmanagementprozess umfasst heute Folgendes:

- Einreichung von Änderungsanträgen
- Risiko- und Folgenabschätzungen
- Funktionen zum Genehmigen/Ablehnen von Änderungen
- Prüfung
- Funktionen für Terminplanung/Benutzerbenachrichtigung/Schulung
- Umsetzung
- Validierung
- Dokumentation

Das Änderungsmanagement kommt unter anderem dann zum Tragen, wenn Entscheidungen in Notfällen getroffen werden und Änderungen vorgenommen werden müssen. Sobald die Änderung umgesetzt wurde, sollte sie in den Änderungsmanagementprozess zurückgeführt werden, wo sie dann von den bereits etablierten Validierungs- und Dokumentationsprotokollen profitieren kann.

4.3. Cybersecurity Asset Management

Bei der Verwaltung von Cybersecurity-Assets handelt es sich um den Prozess der Erfassung von Asset-Daten (Geräte, Cloud-Instanzen und Benutzer) zur Stärkung zentraler Sicherheitsfunktionen, einschließlich:

- **Erkennung und Reaktion:** Sicherstellen, dass die Erkennungs- und Reaktionsfähigkeiten das gesamte Unternehmen abdecken
- **Schwachstellen-Management:** Verstehen, welche Anlagen für Angriffe anfällig sind, und sicherstellen, dass alle Anlagen auf Schwachstellen geprüft werden
- **Cloud-Sicherheit:** Sicherstellen, dass Cloud-Instanzen sicher und so konfiguriert sind, dass sie keine allzu freizügigen Zugriffsrechte haben, selbst wenn sie schnell in Betrieb genommen und außer Betrieb genommen werden
- **Reaktion auf Zwischenfälle:** Verwendung angereicherter, korrelierter Daten über

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Anlagen zur Beschleunigung von Untersuchungen und Abhilfemaßnahmen bei Zwischenfällen

- **Kontinuierliche Überwachung der Kontrollen:** Erkennen, wann Sicherheitskontrollen fehlen und angewendet werden müssen

5. Bewertung der Wirksamkeit von Cybersicherheitsmaßnahmen

Die Entwicklung eines Informationssystems durchläuft mehrere verschiedene Phasen, von der Problemanalyse bis zur Implementierung des Systems. Während dieses Prozesses wird jeder Schritt durch eine Reihe von Ergebnissen dokumentiert, die von einer Durchführbarkeitsstudie bis hin zu Schulungshandbüchern und Systemdokumentation reichen. Bei der Entwicklung einer Sicherheitspolitik findet dieser Prozess der Selbstdokumentation im Allgemeinen nicht statt.

Viele der derzeit entwickelten Strategien versuchen, alles in die Sicherheitspolitik zu packen: die Begründung der Wichtigkeit und spezifische Systemanweisungen und -beschreibungen. Sicherlich ist das Sicherheitskonzept selbst schon langatmig genug, ohne dass Einzelheiten darüber vorliegen, wie das Dokument erstellt wurde, wer bei seiner Ausarbeitung konsultiert wurde oder wie die Formulierung des Konzepts erreicht wurde. Es wird auch nicht dokumentiert, welche politischen Probleme bei der Umsetzung der Politik aufgetreten sind oder wie die Mitarbeiter über die Politik geschult wurden. Durch den Einsatz von Dokumentationstechniken während der Entwicklung der Politik könnte eine Sicherheitspolitik jedoch wieder zu einem Grundsatzdokument werden. Andere Fragen, die sich nicht mit den Grundsätzen der Sicherheitspolitik befassen, würden an anderer Stelle zusammen mit der Begründung für die Politik dokumentiert werden.

Die wichtigste Information, die oft fehlt oder nur unzureichend ist, wenn wir versuchen, eine Sicherheitspolitik in einer Organisation zu bewerten, ist die Dokumentation der Anforderungen. Ohne ein klares Verständnis der Anforderungen ist die Bewertung der Qualität einer Sicherheitspolitik fast unmöglich. Eine Analyse der Risiken/Bedrohungen, denen die Organisation ausgesetzt ist, ist nur ein Teil der Anforderungen, die für die Entwicklung einer Sicherheitspolitik erforderlich sind. Genauso wichtig sind die Ziele der Organisation und andere politische Aspekte, die die Entwicklung, Umsetzung und Akzeptanz der Sicherheitspolitik beeinflussen. Die Verfügbarkeit einer umfassenden Dokumentation, die auch die Ergebnisse einer ausführlichen Anforderungsanalyse enthält, ermöglicht eine tiefergehende Bewertung der Sicherheitspolitik, anstatt das Endprodukt nur oberflächlich zu bewerten. Anstatt sich beispielsweise nur darauf zu konzentrieren, ob die Politik in einem bestimmten Bereich umgesetzt wurde, kann die Bewertung nun auch berücksichtigen, wie dieser Bereich im Rahmen der Politik entwickelt wurde. Anhand von Belegen ließe sich feststellen, ob die Politik alle im Rahmen der Entwicklung ermittelten Themen angemessen abdeckt, ohne eines davon zu verwässern. Sicherheitsrichtlinien sind jedoch je nach dem Kontext der Organisation sehr

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

unterschiedlich, und es ist zu erwarten, dass auch ihre Entwicklung unterschiedlich ist. Es gibt einige Gemeinsamkeiten zwischen den Richtlinien, auch wenn die Zielbereiche voneinander abweichen. Anders als bei der Produktevaluierung sind jedoch viele Kriterien bei der Bewertung der Sicherheitspolitik subjektiver Natur. Dies liegt an der subjektiven Natur der Entwicklung einer Politik und an der Umgebung, in der die Politik umgesetzt wird.

5.1. Aufrechterhaltung der Effektivität von IT-Sicherheitsrichtlinien

Die Informationstechnologie (IT) ist wohl die Technologie des Jahrhunderts schlechthin. Sie hat die Welt wirklich verändert. Mit all den Vorteilen der IT sind jedoch auch viele Sicherheitsrisiken in unser Leben eingedrungen. Unternehmen müssen wirksame Richtlinien für die Informationssicherheit entwickeln, um sicherzustellen, dass ihre Geschäftsabläufe vor böswilligen Eindringlingen und Datendieben geschützt sind. Ironischerweise besteht eine hervorragende Möglichkeit, die Wirksamkeit der Sicherheitsrichtlinien angesichts der sich verändernden IT-Risikolandschaft zu erhalten, darin, mehr IT einzusetzen.

Im Folgenden sind einige Möglichkeiten aufgeführt, wie die IT-Abteilung die Wirksamkeit von Sicherheitsrichtlinien aufrechterhalten kann:

- **Bessere Risikobewertung:** Die Bewertung des Sicherheitsrisikos ist ein wesentlicher erster Schritt bei der Ausarbeitung jeder Informationssicherheitspolitik. Um den Bedrohungen zu begegnen, die sich aus dem sich schnell entwickelnden IT-Sektor ergeben, ist die IT das einzige Gegenmittel. Da sich die Risiken ständig ändern, ist die IT ein Muss, um die neuen Bedrohungen unter Kontrolle zu halten. Sie ermöglicht es Ihnen, neue Risiken auf der Grundlage Ihrer bisherigen Compliance-Aufzeichnungen leicht zu entdecken, die Risikofaktoren einzustufen und zu klassifizieren und die Schäden zu bewerten, die sie verursachen können. Daher ist es wichtig, aus den neuen Entwicklungen in der IT zu lernen - ob sie nun gut oder schlecht sind. So können Sie Ihre Risikobewertung verbessern und sind besser auf eine drohende Gefahr vorbereitet.
- **Bessere Einhaltung der Vorschriften**: IT hilft Ihnen dabei, zu überwachen, wie gut die Mitarbeiter und Leiter Ihrer Organisation die Vorschriften der Aufsichtsbehörden sowie Ihre organisationsspezifischen Sicherheitsrichtlinien einhalten. Mit einer einzigen Software können Sie Zugriffsberechtigungen, unsicheren Datenaustausch, unsicheres Surfen im Internet, unzureichende Datenverschlüsselung und zahllose andere Faktoren, die Ihre Sicherheit ernsthaft beeinträchtigen können, im Auge behalten.
- **Ständige Aktualisierung ist ein Muss**: Da sich die IT-Welt mit jedem Atemzug verändert, müssen Sie ständig nach neuen Änderungen Ausschau halten, die Ihr System gefährden könnten. Verfolgen Sie die Entwicklungen in der Welt der Cyber-Risiken, der Cyber-Kriminalität und der Cyber-Security. Aktualisieren Sie Ihre Informationssicherheitsrichtlinien und Ihre Sicherheitssoftware häufig und regelmäßig,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

da sie sehr schnell veraltet sein können. Auf diese Weise können Sie die Wirksamkeit Ihrer Sicherheitsrichtlinien aufrechterhalten.

- **Schnelle Abhilfe**: Wenn Ihr Unternehmen mit einer drohenden Sicherheitsbedrohung konfrontiert wird, die zu einem möglichen Datenverlust oder -diebstahl führen kann, müssen Sie einen Plan zur Schadensbegrenzung oder -behebung parat haben. IT hilft Ihnen dabei, Abhilfemaßnahmen auf einfache und effiziente Weise zu planen. Mithilfe von IT können Sie bei der Ausarbeitung Ihrer Sicherheitsrichtlinien den verschiedenen potenziellen Risiken Schritte zur Risikominderung zuordnen und mit ihnen verknüpfen. Auf diese Weise können Sie die Abhilfemaßnahmen zeitnah und effizienter durchführen und die Wirksamkeit Ihrer Sicherheitsrichtlinien aufrechterhalten.
- **Verbesserte Rechenschaftspflicht**: Keine Informationspolitik kann wirksam bleiben, wenn die Menschen nicht für die Risiken, die Einhaltung der Vorschriften und die Schadensbegrenzung verantwortlich und rechenschaftspflichtig sind. Die IT macht es einfacher, die Verantwortlichkeit für Abhilfemaßnahmen zu gewährleisten. Sie kann die Sichtbarkeit von Risiken und Reifegradbewertungen, die Einhaltung von Vorschriften und die Abhilfemaßnahmen, die Ihr Unternehmen ergreift, erheblich verbessern. Dies bedeutet, dass Ihre Mitarbeiter die in Ihren Informationssicherheitsrichtlinien aufgeführten Schritte schneller und verantwortungsbewusster durchführen.

5.2. Bewertung der Sicherheitsrisiken

Risikobewertung: Nachdem festgelegt wurde, welche Informationsgüter geschützt werden sollen, wird die Risikobewertungsmethode ausgewählt und die Risiken werden definiert. Entsprechend der gewählten Risikobewertungsmethode werden die Informationsgüter auf der in der Abbildung gezeigten Risikokarte positioniert. Nach der Bewertung umfasst die Risikobewertungskarte die Prozesse zur Verbesserung und Kontrolle der Risiken für Bedrohungen mit hohen Auswirkungen und hoher Wahrscheinlichkeit. Da sich die Lage der Informationswerte in der Risikokarte ändern kann, sollte die Risikokarte regelmäßig aktualisiert werden, und es sollten die erforderlichen Vorkehrungen getroffen werden.

Risiko ist definiert als die Kombination der Wahrscheinlichkeiten eines Ereignisses und seiner Folgen. Die Risikobewertung, die ein Schritt des Risikomanagements ist, ist ein Prozess, in dem Risiken definiert und die Auswirkungen und Prioritäten dieser identifizierten Risiken bestimmt werden. Das Risikomanagement besteht darin, ein annehmbares Risikoniveau zu bestimmen, das aktuelle Risiko zu bewerten, die notwendigen Schritte zu unternehmen, um dieses Risiko auf ein annehmbares Niveau zu reduzieren, und dieses Risikoniveau zu halten. Informationen und andere Werte, Bedrohungen für diese Werte, Schwachstellen im bestehenden System und Sicherheitssystemkontrollen sind die Komponenten, die das aktuelle Risiko bestimmen. Die Identifizierung von Informationen oder Vermögenswerten, die geschützt werden müssen; die

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Bestimmung, wie wertvoll diese Vermögenswerte für die Einrichtungen sind; die Feststellung, welche der bekannten und möglichen Bedrohungen für diese Vermögenswerte versucht werden, zu verhindern; die Untersuchung, wie mögliche Verluste auftreten könnten; die Ermittlung des Ausmaßes möglicher Bedrohungen für jeden Vermögenswert; die Prüfung, was in erster Linie getan werden kann, um das Ausmaß und die Wahrscheinlichkeit von Verlusten, die bei diesen Vermögenswerten auftreten können, zu verringern, und die Planung der Schritte, die unternommen werden müssen, um die vorausschauenden Bedrohungen auf einem Mindestniveau zu halten, sind bestimmte Phasen der Risikobewertung. Die Kosten des Sicherheitssystems, das als Ergebnis des Risikomanagements eingerichtet und umgesetzt werden soll, sind ein weiterer wichtiger Aspekt, der berücksichtigt werden muss. Die Kosten des Sicherheitssystems sollten durch den Wert der geschützten Informationen und das durch die Prüfung möglicher Bedrohungen ermittelte Risiko begrenzt werden. Neben dem Grundsatz, dass es keine 100%ige Sicherheit geben kann, wird die ideale Konfiguration der Informationssicherheit durch drei Prozesse realisiert. Diese Prozesse sind Vorbeugung, Erkennung und Reaktion (Response oder Reaction).

Vorbeugung: Dies ist der Prozess, auf den sich Sicherheitssysteme konzentrieren und der am meisten funktioniert. Es werden verschiedene Maßnahmen entwickelt, um das System gegen Bedrohungen und Angriffe auf Computersysteme abzuschirmen, wie z. B. Sicherheitsmaßnahmen im täglichen Leben, wie die Umzäunung des Gartens eines Hauses und die Verwendung einer Stahltür. In Bezug auf die Sicherheit von Personalcomputern sind die Installation von Virenscanprogrammen, die regelmäßige Durchführung dieser Programme und der Service Packs für das Betriebssystem sowie die Fehlerkorrektur und Aktualisierung in regelmäßigen Abständen, die Verwendung eines passwortgeschützten Bildschirmschoners auf dem Computer, das Verlassen des Systems nach längerer Abwesenheit vom Computer, die Schätzung der verwendeten Passwörter, die Geheimhaltung dieser Passwörter und ihre regelmäßige Änderung, die Vorsicht bei der gemeinsamen Nutzung von Datenträgern, die Beachtung von Dateien, die aus dem Internet heruntergeladen oder per E-Mail verschickt werden, der Schutz wichtiger Dokumente durch ein Passwort oder ihre Verschlüsselung, die Übermittlung vertraulicher oder wichtiger Informationen per E-Mail, Websites ohne Sicherheitszertifikate. Einige der Maßnahmen, die einfach erscheinen mögen, aber Leben retten, wie z. B. nicht über unsichere Wege zu versenden, den Internetzugang auszuschalten, wenn er nicht benutzt wird, regelmäßige Sicherungskopien von wichtigen Informationen und Dokumenten zu machen. Die Präventionsmaßnahmen, die im Rahmen der Computersicherheit in Unternehmen umgesetzt werden müssen, sind umfassender und komplexer. Einige der Maßnahmen, die in solchen Systemen, in denen Sicherheitsexperten arbeiten, zur Vorbeugung ergriffen werden:

- Regelmäßige Überprüfung der Service Packs und Updates des Betriebssystems und der Software,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Beschränkung der Benutzerrechte auf ein Minimum, keine Ausführung ungenutzter Protokolle, Dienste, Komponenten und Prozesse,
- Verschlüsselungstechniken bei der Datenübertragung, Schwachstellen-Scanner,
- Verwendung eines virtuellen privaten Netzwerks,
- Die Nutzung der Public Key Infrastructure und der elektronischen Signatur kann als Nutzung biometrischer Systeme aufgeführt werden.

Wenn der im Präventionsprozess ermittelte Fortschritt perfekt wäre, wären weitere Prozesse gar nicht nötig. Alle Angriffe wären im schlimmsten Fall verhindert worden. Aber kein Sicherheitsprodukt ist perfekt oder vollständig. Darüber hinaus werden fast täglich verschiedene Schwachstellen in Übertragungssystemen, Internetdiensten, Webtechnologien und Sicherheitsanwendungen entdeckt. Unter diesem Gesichtspunkt nimmt der Einsatz von Erkennungs- und Abgleichverfahren zu.

Entschlossenheit; Sicherheit ist nicht nur eine Frage der Prävention. Die Tatsache, dass beispielsweise ein Museum gut geschützt ist, dass das Museum von Zäunen umgeben ist, dass die Türen geschlossen und verriegelt sind, macht es nicht erforderlich, dass in diesem Museum nachts Wachen eingesetzt werden. Auf die gleiche Weise wird auch der Einsatz von Methoden zur Erkennung von Angriffsversuchen auf Computersysteme erhöht. Prävention bedeutet, eine Barriere zu errichten, die entweder Angriffe erschwert (aber nicht unmöglich macht) oder Angreifer abschreckt (aber nicht vernichtet). Vorbeugung ohne Erkennung und Reaktion kann nur begrenzten Nutzen haben. Wenn nur Prävention ausreichen würde, wären die meisten Angriffe nicht einmal bekannt. Mit Hilfe der Erkennung können bereits bekannte oder neu auftretende Angriffe gemeldet und entsprechende Maßnahmen ergriffen werden. Der erste und grundlegendste Schritt bei der Erkennung besteht darin, den gesamten Zustand und die Bewegungen des Systems zu überwachen und diese Informationen aufzuzeichnen. Auf diese Weise werden auch Daten und Beweise für die Analyse nach einem Angriff gesammelt. Firewalls, Systeme zur Erkennung von Eindringlingen, Überwachungssysteme für den Netzwerkverkehr, Port-Scanner, die Nutzung von Honigtöpfen, Echtzeitschutz-Tools für Viren und Spyware, Programme zur Kontrolle von Dateiprüfsummen und Netzwerk-Sniffer-Sensoren sind einige der am häufigsten verwendeten Methoden im Erkennungsprozess.

Antwort: Genauso wie ein Ort, der mit Wachen, Hunden, Sicherheitskameras und Sensoren ausgestattet ist, die Aufmerksamkeit von Dieben auf sich ziehen kann, sind Computersysteme mit Echtzeit-Erkennungssystemen auch für Hacker und Angreifer attraktiv. Die schnelle Reaktion ist ein wesentliches Element, das das Sicherheitssystem ergänzt, um diese Angriffe abzuwehren. Reaktion kann definiert werden als die Ausführung von Aktionen, die sofort oder so schnell wie möglich auf Angriffsversuche reagieren, die nicht durch den Präventionsprozess bewältigt und durch Erkennungsprozesse ermittelt werden können. Systeme zur Erkennung von Eindringlingen können sinnvoll sein, wenn es jemanden oder ein System gibt, das auf diese Erkennung reagiert.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Andernfalls geht diese Situation nicht über den Nutzen einer Autoalarmanlage hinaus, die niemand hört und um die sich niemand kümmert. In dieser Hinsicht ist die Reziprozität ein wichtiges Glied, das den Sicherheitsprozess vervollständigt. Selbst wenn der Angriff nicht vollständig verhindert wird, ermöglicht sie es dem System, in den Normalzustand zurückzukehren, die Ursachen des Angriffs zu ermitteln, den Angreifer gegebenenfalls zu fangen, die Schwachstellen des Sicherheitssystems zu ermitteln und die Vorbeugungs-, Erkennungs- und Reaktionsprozesse neu zu organisieren. Die Planung der Maßnahmen, die zu ergreifen sind, wenn ein Angriff entdeckt wird, im Voraus gewährleistet, dass dieser Prozess effektiv funktioniert und keine Zeit und kein Geld verschwendet wird. Die Wiederherstellung im Katastrophenfall steht an der Spitze der wichtigsten Pläne für den schlimmsten Fall, die in dieser Phase durchgeführt werden.

Fragen:

1. Welcher der folgenden Punkte gehört nicht zu den Phasen der Vermögensverwaltung.

A) Erstellung eines Inventars der Vermögenswerte

B) Feststellung des Eigentums an den Vermögenswerten

C) Bestimmung der Kostenrechnung

D) Festlegung von Regeln für die Nutzung von Vermögenswerten

2. Was ist der Hauptzweck des Bedrohungs- und Schwachstellenprüfungsprozesses?

A) Um die Sicherheitsschwachstellen der Vermögenswerte bestmöglich zu verstehen und die notwendigen Maßnahmen zu ergreifen, um diese Vermögenswerte wirksam zu schützen.

B) Verwaltung von Sicherheitsschwachstellen

C) Einholung von Vorabinformationen über das Anlageninventar

D) Schließen von Sicherheitslücken

3. Welche der folgenden Arten der Schwachstellenbewertung ist keine?

A) Netzwerkbasierte Scans

B) Host-basierte Scans

C) Datenbank-Scans

D) Serverbasierte Scans

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

4. Welcher der folgenden Punkte gehört nicht zum Prozess des Cybersecurity Asset Management?

A) Schwachstellenmanagement

B) Kostenmanagement

C) Kontinuierliche Überwachung der Kontrolle

D) Erkennung und Intervention

5. Welche der folgenden Möglichkeiten steht der IT-Abteilung nicht zur Verfügung, um die Wirksamkeit ihrer Sicherheitsrichtlinien zu gewährleisten?

A) Risikobewertung

B) Ständige Verbesserung

C) Schnelle Schadensbegrenzung

D) Sicherheitsrichtlinien

6. Welcher der folgenden Prozesse gehört nicht zu den drei Prozessen, die die ideale Konfiguration der Informationssicherheit darstellen?

A) Vorbereitung

B) Prävention

C) Bestimmung

D) Rückantwort

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

- **Was ist die Anfälligkeit von IT-Systemen?**
- **Erläutern Sie und geben Sie Beispiele für Schwachstellenmanagement und Risikomanagement**

Anhänge *(PowerPoint-Präsentation, Handouts, Ausdrucke, Links, Video...):*

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

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

Referenzen:

1. Bewertung der Entwicklung von IS-Sicherheitsrichtlinien S.B. Maynard1 & A.B. Ruighaver2 Abteilung für Informationssysteme Universität Melbourne Australien
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/
10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.