Interdisziplinäres Cyber-Schulungsprojekt. Einheit-2 für Manager

In der ersten Phase der Vermögensverwaltung wäre es sinnvoll, zunächst zu ermitteln und aufzulisten, welche Vermögenswerte wir haben. Was eine Institution besitzt oder nicht besitzt, sollte zuerst bekannt sein. 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.

Zweck: Identifizierung der Vermögenswerte der Organisation und Festlegung angemessener Schutzverantwortlichkeiten.

Inventarisierung der Vermögenswerte. Vermögenswerte im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen sollten identifiziert werden, und es sollte ein Inventar dieser Vermögenswerte erstellt und gepflegt werden.

Anwendungsleitfaden: Eine Organisation sollte relevante Vermögenswerte im Informationslebenszyklus 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.

Das 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.

Eigentum an Vermögenswerten. Für alle inventarisierten Vermögenswerte muss eine Eigentümerzuordnung vorgenommen werden.

Anwendungsleitfaden: Einzelpersonen und andere Stellen mit genehmigter Verwaltungsverantwortung für den Lebenszyklus des Vermögenswerts können als Eigentümer des Vermögenswerts benannt werden.

Um sicherzustellen, dass die Eigentumsverhältnisse 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 Vermögenswerts:

a) Sicherstellen, dass das Inventar des Vermögenswerts aufgezeichnet wird,

b) Sicherstellen, dass die Vermögenswerte ordnungsgemäß klassifiziert und geschützt sind,

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

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

Zulässige Nutzung von Vermögenswerten. 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 Informations- und Informationsverarbeitungseinrichtungen und -ressourcen aufgeklärt werden. Diese Benutzer sollten für die Nutzung aller Informationsverarbeitungsressourcen und für jede Nutzung, die unter ihrer eigenen Verantwortung erfolgt, verantwortlich sein.

Rückgabe von Vermögenswerten. Alle Mitarbeiter und Nutzer externer Parteien müssen bei Beendigung des Arbeitsverhältnisses, des Vertrages oder der Vereinbarung alle in ihrem Besitz befindlichen Unternehmensressourcen 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 Nutzer die Geräte der Organisation erwirbt oder nutzt, sind Verfahren einzuhalten, die sicherstellen, dass alle relevanten Informationen an die Organisation übertragen und sicher von den Geräten gelöscht werden.

Verfügt ein Mitarbeiter oder externer Benutzer über Informationen, die für den laufenden Betrieb wichtig sind, müssen diese dokumentiert und an die Organisation übertragen werden.

Bewertung und Management von Bedrohungen und Schwachstellen. Fast jede Organisation verfügt über sensible und wertvolle Güter, die geschützt werden müssen. Doch nicht jedes Unternehmen verfügt über eine umfassende und gut durchdachte Strategie zum Schutz dieser Werte. Im Bereich der Cybersicherheit bilden Strategien zum 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 identifiziert, bewertet und so schnell wie möglich behoben.

Was ist eine Schwachstellenanalyse? Unter Schwachstellenbewertung versteht man den Prozess der Ermittlung, Identifizierung, Klassifizierung und Priorisierung von Schwachstellen in Computersystemen, Anwendungen und Netzinfrastrukturen.

Ein Schwachstellenbewertungsprozess zielt darauf ab, Bedrohungen und die von ihnen ausgehenden Risiken zu identifizieren. Häufig werden dazu automatische Testwerkzeuge wie Netzwerksicherheitsscanner eingesetzt, deren Ergebnisse in einem Schwachstellenbewertungsbericht aufgeführt werden.

Die Bedeutung von Schwachstellenanalysen. Um die Bedeutung der Schwachstellenanalyse zu verdeutlichen, betrachten wir sie aus der Sicht eines Immobilienbesitzers. Wenn Sie ein wertvolles Gebäude besitzen, ergreifen Sie wahrscheinlich eine Reihe von Maßnahmen, um es zu schützen.

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 Anlagen, Sicherheitslücken und des Gesamtrisikos, wodurch die Wahrscheinlichkeit verringert wird, dass ein Cyberkrimineller in die Systeme eindringt und das Unternehmen unvorbereitet trifft.

Arten der Schwachstellenbewertung.

- Netzwerkbasierter Scan
- Host-basierter Scan
- Drahtloser Netzwerk-Scan
- Web-Test-Scan
- Datenbank-Scan

Cyber Continuity of Operations. 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 Arbeitsplatz ausreichen, bieten sie weitaus weniger Möglichkeiten, wenn die Mitarbeiter keinen Zugang zu den Systemen und Daten haben, die sie für die Erfüllung ihrer wichtigen Aufgaben benötigen.

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.

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 Konfigurationsdatensätze sind in den Datenbanken des Konfigurationsmanagementsystems enthalten. iguration Management Database: Die Konfigurationsmanagement-Datenbank wird mit CMDB abgekürzt. CMDB ist eine Datenbank, die zur Speicherung von Konfigurationsdatensätzen während ihres gesamten Lebenszyklus verwendet wird.

Bewertung von Sicherheitsrisiken. Das Risiko ist definiert als die Kombination der Wahrscheinlichkeiten eines Ereignisses und seiner Folgen. Die Risikobewertung, ein Schritt des Risikomanagements, ist ein Prozess, in dem Risiken definiert und die Auswirkungen und Prioritäten dieser identifizierten Risiken bestimmt werden. Das Risikomanagement besteht darin, ein akzeptables Risikoniveau zu bestimmen, das aktuelle Risiko zu bewerten, die notwendigen Schritte zu unternehmen, um dieses Risiko auf ein akzeptables Niveau zu reduzieren, und dieses Risikoniveau zu halten.

Ideale Konfiguration der Informationssicherheit. Erstens, Vorbeugung.

- Regelmäßige Überprüfung der Service Packs und Aktualisierungen des Betriebssystems und der Software,
- Beschränkung der Benutzerrechte auf ein Minimum,
- Einsatz von Schwachstellenscannern,
- E-Signatur verwenden,

- Verwendung eines passwortgeschützten Bildschirmschoners auf dem Computer.

Zweitens: Entschlossenheit. Sicherheit ist nicht nur eine Frage der Prävention. Die Tatsache, dass ein Museum gut geschützt ist, dass das Museum von Zäunen umgeben ist, dass die Türen geschlossen und verriegelt sind, macht es zum Beispiel nicht erforderlich, dass in diesem Museum nachts Wachen eingesetzt werden. In gleicher 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).

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, Intrusion Detection Systeme, Netzwerk-Traffic-Monitore, Port-Scanner, Honeypot-Nutzung, Echtzeitschutz-Viren- und Spyware-Tools, Datei-Prüfsummen-Kontrollprogramme und Netzwerk-Sniffer-Sensoren sind einige der gängigsten Methoden, die im Erkennungsprozess eingesetzt werden.

Die letzte Rückantwort. Die schnelle Reaktion erweist sich als wesentliches Element, das das Sicherheitssystem zur Abwehr dieser Angriffe ergänzt. Reaktion kann definiert werden als die Ausführung von Aktionen, die sofort oder so schnell wie möglich auf Angriffsversuche reagieren, die durch den Präventionsprozess nicht bewältigt werden können und durch Erkennungsprozesse ermittelt werden. Systeme zur Erkennung von Eindringlingen können sinnvoll sein, wenn es jemanden oder ein System gibt, das auf diese Erkennung reagiert. Andernfalls geht diese Situation nicht über den Nutzen einer Autoalarmanlage hinaus, die niemand hört und um die sich niemand kümmert.