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

InCyT-Trainingsmodule

Informationssicherheit für Manager Einheit 3 -Woche 6 Name der Einheit (Module): Sicherheit von Drittanbietern	
Lernaktivitäten	❑ **Webinar**❑ **Übungen**❑ **Workshop**❑ **Präsentation**❑ **Sonstiges**
Lehrverantwortliche	• George Matache - und andere.
Ziele der Lernaktivitäten	1. Risiken in sozialen Netzwerken 2. Maßnahmen zur Gewährleistung von Sicherheit und Datenschutz in sozialen Netzwerken 3. Sicherheitstechniken 4. Anforderungen an die Auftragsvergabe
Zu erwerbende Fertigkeiten	• TS3 Netzwerksicherheit • TS4 Penetrationstests (ausnutzbare Schwachstellen) • SS3 Kognitions- und Verhaltensanalyse
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	***Was wird benötigt?***
	• Grundlegende Managementfähigkeiten • IT-Grundkenntnisse • Grundlegende Sicherheitskenntnisse

Kurzinformationen zum Modul

Beschreibung
Beschaffungsanforderungen beziehen sich auf die Waren und Dienstleistungen, die von Organisationen außerhalb der ausführenden Organisation erworben werden müssen. Aus verschiedenen Gründen sind ausführende Organisationen manchmal auf Lieferanten angewiesen, um die für die Durchführung eines Projekts erforderlichen Leistungen zu erbringen. Nehmen wir zum Beispiel einen Widgethersteller, der ein Projekt zur Automatisierung seines Bestandsverfolgungssystems in Angriff nimmt. Einige der Projektaktivitäten umfassen die Verlagerung von Lagerplätzen in ihrem Hauptlager. Einige der Arbeitsaktivitäten umfassen die Entwicklung von Individualsoftware. Was die Softwareentwicklung betrifft, so verfügt der Witwenhersteller nicht über Personal, das sich mit der Entwicklung der Softwareanwendung auskennt. Für die Softwareentwicklung muss der Widgethersteller diese Dienstleistungen einkaufen. Webbasierte soziale Netzwerke (WBSN) sind Online-Gemeinschaften, die es den Nutzern ermöglichen, Ressourcen (z. B. persönliche Daten, Anmerkungen, Blogs) zu veröffentlichen und Beziehungen zu knüpfen, möglicherweise zu unterschiedlichen Zwecken, z. B. in den Bereichen Geschäft, Unterhaltung, Religion, Partnersuche usw. In den letzten Jahren hat die Nutzung und Verbreitung von WBSNs zugenommen, wobei etwa 300 Websites die Informationen von mehr als 400 Millionen registrierten Benutzern sammeln. Infolgedessen wird das "Netzmodell" heute von Unternehmen und Organisationen immer häufiger für die Kommunikation, den Informationsaustausch, die Entscheidungsfindung und die Abwicklung von Geschäften genutzt. Es ist daher eine Herausforderung, Sicherheitsmechanismen für soziale Netzwerke zu entwickeln, die in der Lage sind, private Informationen zu schützen und den Zugang zu gemeinsamen Ressourcen zu regeln. In diesem Artikel geben wir nicht nur einen Überblick über die Merkmale der WBSN-Umgebung und ihre Schutzanforderungen, sondern erläutern auch die aktuellen Ansätze und künftigen Trends im Bereich der Sicherheit sozialer Netzwerke, wobei wir den aufkommenden Technologien im Zusammenhang mit dem sogenannten Web 2.0 besondere Aufmerksamkeit schenken. 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.

Inhalt des Lernmaterials (🕓 ?? Minuten oder 10-12 Seiten)

Ein Drittanbieter ist eine Person oder ein Unternehmen, das Dienstleistungen für ein anderes Unternehmen (oder dessen Kunden) erbringt. Während Verkäufer als "Dritte" betrachtet werden, unterscheiden einige Branchen einen "Drittanbieter" speziell als einen Verkäufer mit schriftlichem Vertrag, aber nicht alle Verkäufer arbeiten im Rahmen eines Vertrags. Der Klarheit halber bezieht sich der Begriff "Drittanbieter" in diesem Artikel auf jede Person oder jedes Unternehmen, das einem anderen Unternehmen mit oder ohne Vertrag Dienstleistungen erbringt.

Zusammenarbeit ist der Schlüssel zum Erfolg. Die Zusammenarbeit mit Dritten hilft Unternehmen, ihre Produktivität und Effizienz zu steigern, bessere Produkte und Dienstleistungen zu produzieren, hochqualifizierte Experten zu beschäftigen und Kosten zu senken. Doch all diese Vorteile haben ihren Preis in Form von erhöhten Risiken für die Cybersicherheit. Kleinere Mängel in den Sicherheits- und Datenschutzroutinen Ihres Drittanbieters können sich zu Schwachstellen in der Cybersicherheit Ihres Unternehmens entwickeln. In diesem Artikel analysieren wir die besonderen Cybersicherheitsrisiken, die mit Drittanbietern verbunden sind, und zeigen Ihnen, wie Sie diese Risiken abmildern können.

Zu den Waren und Dienstleistungen, die von Drittanbietern bezogen werden, können unter anderem gehören:

- Cloud-Webhosting-Dienste. Ein Cloud-Hosting-Anbieter kann alles anbieten, von Speicherplatz und Bandbreite bis hin zu Verschlüsselung und Hightech-Sicherheitslösungen.
- Cloud-basierte Software-Lösungen. SaaS-Softwareanbieter bieten Zugang zu Softwareprogrammen entweder für Ihr Unternehmen oder für Ihre Kunden. Zum Beispiel Marketing-Automatisierungsplattformen, CRMs, Buchhaltungspakete usw.
- Wartung der Geräte. Das Unternehmen, das Ihren Kopierer repariert, und das Team, das Ihre Netzwerksicherheit verwaltet, sind Drittanbieter.

- HVAC-Wartung. Die lokale HLK-Firma, die Ihr Gerät wartet, erbringt Dienstleistungen von Drittanbietern.
- Auftragnehmer jeglicher Art. Jeder Auftragnehmer, ob kurz- oder langfristig, ist ein Drittanbieter.
- Callcenter-Anbieter. Wenn Sie Ihr Call Center bei einem anderen Unternehmen hosten, wird es als Drittanbieter betrachtet.
- Buchhaltung/Finanzprüfer. Jede Person oder jedes Unternehmen, das mit der Verwaltung Ihrer Finanzen, der Aufstellung eines Budgets oder der Prüfung Ihrer Finanzen beauftragt wird, ist ein Drittanbieter.
- Anwälte. Manchmal ist es notwendig, einen Anwalt zu konsultieren, bevor man Verträge unterschreibt oder größere Anschaffungen tätigt. Alle juristischen Dienstleistungen werden als Drittanbieter betrachtet.

Da sich Unternehmen bei der Bereitstellung wichtiger Dienstleistungen zunehmend auf Drittanbieter verlassen, werden sie auch anfälliger für anbieterbezogene Cybersicherheitsrisiken. Eine kürzlich durchgeführte Studie hat ergeben, dass fast 60 % der Unternehmen im vergangenen Jahr von einer Datenverletzung durch einen Drittanbieter betroffen waren. Doch was sind die häufigsten Cyberlücken bei Anbietern, die Unternehmen kennen sollten?

Was sind die Vorteile des Einsatzes von Drittanbietern für Dienstleister?

In der heutigen Welt lässt sich der Einsatz von Drittanbietern nicht mehr vermeiden. Egal, wie viele Abteilungen Ihr Unternehmen einrichtet, Sie werden nie alle Dienstleistungen abdecken können, die Sie jemals benötigen werden. Das sollten Sie auch nicht, denn Unternehmen müssen das richtige Gleichgewicht zwischen Fähigkeiten, die für das Unternehmen unerlässlich sind, und solchen, die ausgelagert werden können, finden. Hier sehen Sie, was passiert, wenn Sie das richtige Gleichgewicht finden:

Sie werden Zeit sparen. Niemand hat die Zeit, alle Fähigkeiten zu erlernen oder alle Mitarbeiter einzustellen, die für den Betrieb eines Unternehmens erforderlich sind. Drittanbieter sorgen für reibungslose Geschäftsabläufe, indem sie alle professionellen Dienstleistungen erbringen, die für den Betrieb und die Auftragsabwicklung für Ihre Kunden erforderlich sind.

Sie werden Geld sparen. Der vielleicht größte Vorteil sind die Kosteneinsparungen. Die Beauftragung eines Drittanbieters für Arbeiten nach Bedarf kann wesentlich günstiger sein als die ständige Beschäftigung von Fachleuten auf der Gehaltsliste des Unternehmens. So ist es beispielsweise weitaus kostengünstiger, einen Anwalt zu beauftragen, wenn Sie ihn brauchen, als einen Anwalt auf Vorrat zu haben.

Sie erhalten wertvolles Fachwissen. Ihr Unternehmen hat keine Zeit für den Aufbau eines neuen Expertenteams. Der Zeit- und Kostenaufwand dafür wäre enorm. Die Beauftragung eines Drittanbieters mit Fachwissen, das Sie nicht im Haus haben, wird wahrscheinlich zu besseren Ergebnissen führen.

Welche Risiken bestehen beim Einsatz von Drittanbietern?

Dritte nehmen die Sicherheit ihrer Netze möglicherweise nicht so ernst, wie Sie es wünschen. Aus diesem Grund greifen Hacker Ihr Unternehmen möglicherweise nicht direkt an. Stattdessen suchen sie sich vielleicht ein leichteres Ziel unter Ihren Drittanbietern. Ein kompromittierter Unterauftragnehmer kann leicht zu einem Einfallstor für Cyberkriminelle werden.

Wenn Ihre Lieferanten nicht liefern, werden auch Sie nicht liefern können. Jede Geschäftsbeziehung ist jedoch mit Risiken verbunden. Der Einsatz von Drittanbietern ist mit vielen Risiken verbunden, von denen die meisten gemildert werden können.

Das größte Risiko besteht darin, eine Beziehung zu einem Dritten zu wählen, die nicht mit Ihren Sicherheitsstandards übereinstimmt. So muss Ihr Netzwerksicherheitsteam beispielsweise Sicherheitsprotokolle befolgen, die Ihren spezifischen Standards entsprechen. Wenn Ihr Unternehmen an Vorschriften wie die der Krankenversicherung gebunden ist, können Sie es sich nicht leisten, ein Netzwerksicherheitsunternehmen einzustellen, das die Vorschriften der Krankenversicherung nicht einhält. Sie brauchen einen Anbieter, der sich mit den Vorschriften auskennt und bereit ist, sie zu erfüllen.

Wenn Sie an Datenschutzvorschriften gebunden sind, müssen Sie genau wissen, welche Sicherheitsstandards implementiert sind, und wenn Ihre Anbieter diese nicht erfüllen, müssen Sie versuchen, Abhilfe zu schaffen. Andernfalls setzen Sie Ihr Unternehmen Cybersicherheitsrisiken wie einer Datenpanne aus.

Datenschutzverletzungen sind extrem störend, vor allem wenn es um den Schutz persönlicher Daten geht. Leider sind Datenschutzverletzungen auf dem Vormarsch und treten häufiger auf als je zuvor. Datenschutzverletzungen können zu Betriebsunterbrechungen, verheerenden finanziellen Folgen, rechtlichen Schritten und einem beschädigten Ruf führen. Um dies zu vermeiden, dürfen Sie nicht nachlässig werden, wenn es um Ihre eigene Sicherheit oder die Ihrer Zulieferer geht.

Je nach Art der Kompromittierung von Drittanbietern kann ein Unternehmen unterschiedlichen Risiken ausgesetzt sein. Lassen Sie uns einen Blick auf die häufigsten Risikokategorien und die Bedrohungen werfen, auf die Sie vorbereitet sein müssen, um sie zu entschärfen. Ein kompromittierter Drittanbieter kann zu mehreren Risiken führen, die in vier Hauptkategorien unterteilt werden können: Abbildung 1

Cybersicherheitsrisiken - Unterauftragnehmer haben in der Regel legitimen Zugang zu verschiedenen Umgebungen, Systemen und Daten ihrer Kunden. Angreifer können einen Drittanbieter als Einstiegspunkt nutzen, um sich Zugriff auf Ihre wertvollen Vermögenswerte zu verschaffen.

Betriebliche Risiken - Cyberkriminelle können es auf Ihre internen Systeme und die von Ihnen genutzten Dienste abgesehen haben und nicht nur auf Ihre Daten. Dies kann zu einer teilweisen Unterbrechung Ihres Betriebs oder sogar zum völligen Stillstand führen.

Compliance-Risiken - Internationale, lokale und branchenspezifische Standards und Vorschriften legen strenge Kriterien für die Cybersicherheit fest, die Unternehmen erfüllen müssen. Darüber hinaus müssen auch Dritte, die mit diesen Organisationen zusammenarbeiten, diese Anforderungen einhalten. Die Nichteinhaltung führt in der Regel zu erheblichen Geldstrafen und Rufschädigung.

Reputationsrisiken - Wenn Ihre wertvollen Daten und Systeme kompromittiert werden, ist das ein Warnsignal für Ihre Partner und Kunden, sowohl für die derzeitigen als auch für die zukünftigen. Ihr Vertrauen zurückzugewinnen, wird viel Zeit und Mühe kosten. Und leider gibt es keine Garantie dafür, dass Sie Ihren Ruf nach einem schwerwiegenden Cybersicherheitsvorfall erfolgreich wiederherstellen können.

Anforderungen an die Auftragsvergabe

Aus einer Vielzahl von Gründen verlassen sich ausführende Organisationen manchmal auf Anbieter, die ihnen das liefern, was für die Durchführung eines Projekts benötigt wird. Insbesondere die

KMUs. Die Beschaffungsanforderungen sind daher von größter Bedeutung für die Sicherheit der Arbeit mit Drittanbietern.

Es stimmt zwar, dass die Beschaffung ein sehr individueller Prozess ist, aber es gibt auch einige grundlegende Schritte, die in der Regel überall angewendet werden.

Beschaffungsanforderungen beziehen sich auf die Waren und Dienstleistungen, die von Organisationen außerhalb der ausführenden Organisation erworben werden müssen. Aus verschiedenen Gründen sind ausführende Organisationen manchmal auf Lieferanten angewiesen, um die für die Durchführung eines Projekts erforderlichen Leistungen zu erbringen.

Die Etappen der Beschaffung
Stufe 1: Identifizierung eines Bedarfs an Produkten und/oder Dienstleistungen.
Schritt 2: Erstellen und Einreichen eines Kaufantrags.
Phase 3: Bewertung und Auswahl von Lieferanten/Anbietern.
Phase 4: Verhandlung der Vertragsbedingungen mit dem ausgewählten Anbieter.
Stufe 5: Schließen Sie eine Bestellung ab.

Der erste Schritt im Beschaffungsprozess besteht darin, den Bedarf zu ermitteln. Alle Beschaffungsanforderungen beginnen mit der Wahrnehmung eines Bedarfs. Die Notwendigkeit, ein Gewässer zu überqueren, könnte den Bau einer Brücke, einer Fähre oder eines anderen Verkehrssystems erforderlich machen.

Stufe 1: Ermittlung des Bedarfs an Produkten und/oder Dienstleistungen
Bevor der Beschaffungsprozess beginnen kann, muss ein bestimmter Bedarf festgestellt werden. So kann ein Unternehmen beispielsweise daran interessiert sein, neue Computermonitore zu kaufen, seinen monatlichen Vorrat an Papierprodukten neu zu bestellen oder aktualisierte Software zu erwerben. Je nach Unternehmensstruktur kann dieser Schritt von den Geschäftsinhabern, den Abteilungsleitern, dem Führungsteam, den Mitarbeitern und/oder den Beschaffungsmanagern durchgeführt werden. In dieser Phase wird ein Budget festgelegt, und häufig wird ein umfassender Überblick über die Ausgaben erstellt.

In dieser Phase muss der Bedarf klar definiert werden. Dies kann durch eine Studie geschehen, in der die beste Art der Überquerung des Gewässers (angesichts der gegenwärtigen Situation und des prognostizierten künftigen Bedarfs), die Art der zu bauenden Brücke oder eine vergleichende Kosten-Nutzen-Analyse zur Bestimmung der besten Lösung zwischen einer Brücke und anderen Alternativen ermittelt wird. Die Studie sollte auch Angaben darüber enthalten, ob der Bedarf intern gedeckt werden kann oder ob eine Auftragsvergabe möglich ist, sowie eine Quantifizierung des ursprünglichen Haushaltsvoranschlags und eine Vorstellung von der Vorlaufzeit für die Beschaffung.

Schritt 2: Erstellen und Einreichen eines Kaufantrags
Eine Beschaffungsanfrage (oder Bestellanforderung) ist eine formelle Anforderung von Waren oder Dienstleistungen und wird in der Regel mit einer speziellen Beschaffungssoftware eingereicht. Oftmals wird der Antrag von einem Mitarbeiter oder einer Führungskraft gestellt und dann vom Beschaffungsteam des Unternehmens geprüft.

Wenn ein Antrag genehmigt wird, wird er in eine Bestellung umgewandelt. Wird der Antrag jedoch abgelehnt, wird er in der Regel mit einer kurzen Erklärung an den Antragsteller zurückgeschickt. Eine abgelehnte Bestellung ist zwar nicht ideal, kann aber eine gute Gelegenheit zum Lernen sein.

Stufe 3: Bewertung und Auswahl von Lieferanten/Anbietern
Der nächste Schritt besteht darin, verschiedene Anbieter zu bewerten und dann einen auszuwählen, der die wichtigsten Anforderungen erfüllt. Einige Organisationen führen einen Katalog zugelassener Anbieter, in dem verschiedene Lieferanten aufgeführt sind, die sich bereits bewährt haben.

Die Suche nach Anbietern ist ein Prozess, der von einfach bis komplex reichen kann und dessen Umfang von den jeweiligen Anforderungen abhängt. In der Regel werden mehrere Anfragen an verschiedene Anbieter verschickt, damit das Unternehmen/Beschaffungsteam Preise und Optionen vergleichen kann.

Denken Sie daran, dass der Preis nicht das einzige Kriterium bei der Auswahl eines Anbieters sein sollte. Die besten Ergebnisse erzielen Sie, wenn Sie das "Gesamtbild" dessen betrachten, was ein Anbieter bieten kann, einschließlich:
-Einfache Kommunikation
-Unternehmensethik
-Rechenschaftspflicht
-Produktionsmöglichkeiten

Nachdem ein Lieferant ausgewählt wurde, ist es wichtig, Zeit und Energie in die Beziehung zu investieren. Eine gute Beziehung zu einem Lieferanten kann zu besseren Einsparungen und besserem Service führen und langfristig einen maximalen Nutzen bringen.

Phase 4: Verhandlung der Vertragsbedingungen mit dem ausgewählten Lieferanten
Sobald Sie den am besten geeigneten Anbieter ausgewählt haben, ist es an der Zeit, zu den Vertragsverhandlungen überzugehen. Im Hinblick auf eine erfolgreiche Beschaffung ist dies eine der bei weitem kritischsten Phasen. In dieser Phase legen Sie die Preise fest und vereinbaren Details wie Liefertermine, besondere Bedingungen und vieles mehr. Oft kann es sinnvoll sein, frühere

Verträge zu bewerten, um Verbesserungsmöglichkeiten zu ermitteln, damit Sie in Zukunft fundierter vorgehen können.

Stufe 5: Abschließen einer Bestellung

Nach der Genehmigung des endgültigen Vertrags ist der nächste Schritt die Bestellung (PO). Der Vertrag regelt in der Regel die gesamte Käufer-Lieferanten-Beziehung, während eine Bestellung auf einen bestimmten Kauf abzielt.

-Betrachten Sie dieses Dokument als einen weiteren förmlichen Vertrag, in dem die folgenden Punkte ausführlich beschrieben werden:

-Gesamtkosten/Preis

-Detaillierte Beschreibung der Waren und/oder Dienstleistungen

-Quantität

-sonstige besondere Bestimmungen und Bedingungen

Stufe 6: Auftragsverwaltung

Bei der Lieferung von Waren/Dienstleistungen sollte es eine verantwortliche Person geben, idealerweise der Endnutzer des Produkts oder der Dienstleistung, die überprüft, ob alle Standards eingehalten wurden (Lieferfristen, Produktmengen, Qualität usw.). Wenn es Probleme mit den Artikeln gibt (z. B. beschädigte Produkte), haben Sie die Möglichkeit, die Lieferung abzulehnen. Im Falle von Lieferproblemen ist eine klare Kommunikation mit dem Lieferanten wichtig.

Da Technologie und Kommunikation es Unternehmen ermöglichen, ihre Lieferketten zu erweitern, nimmt die Komplexität des Lieferantenrisikomanagements zu. Ihr Unternehmen arbeitet wahrscheinlich mit mehr Anbietern zusammen als je zuvor, und jeder dieser Anbieter stellt ein gewisses Risiko für Ihr Unternehmen dar.

Das Sicherheitsrisikomanagement für Lieferanten ist eine Strategie, die darauf abzielt, die Anzahl der Bedrohungen, Anfälligkeiten und Schwachstellen zu verringern, denen Ihr Unternehmen durch die Lieferanten in Ihrer Lieferkette ausgesetzt ist. Ein Lieferant ist in der Regel ein Drittunternehmen, das ein Produkt, eine Dienstleistung oder ein Gerät verkauft, das Ihr Unternehmen für den Betrieb benötigt.

Jeder Anbieter, der mit Ihrem Unternehmen in Verbindung steht, birgt ein gewisses Risiko für die Cybersicherheit. Wenn sie ihren Teil der Abmachung nicht einhalten oder Opfer eines Cyberangriffs werden, kann sich dies direkt auf Ihr Unternehmen auswirken. Eine effektive Risikobewertung als Teil eines umfassenderen Plans für das Risikomanagement von Anbietern zielt darauf ab, diese potenziellen Schwachstellen zu identifizieren, lange bevor sie zu einem Problem werden, und sie zu beheben.

Der Kreislauf des Risikomanagements für Lieferanten

Das Sicherheitsrisikomanagement für Lieferanten ist ein fortlaufender Prozess, den Sie mit jedem Lieferanten, den Sie in Ihre Lieferkette aufnehmen, durchführen müssen. In der Regel sieht der Prozess wie folgt aus:

Schritt 1: Analyse - Das Unternehmen ermittelt das inhärente Risiko der Beziehung und den Umfang der durchzuführenden Sorgfaltspflicht. Dementsprechend bewertet das Unternehmen die Sicherheitslage der dritten Partei und führt eine Lückenanalyse durch.
Schritt 2: Engagement - Das Unternehmen und die Drittpartei arbeiten gemeinsam an der Behebung der Lücken.
Schritt 3: Behebung - Die dritte Partei behebt die Cyber-Lücken.
Schritt 4: Genehmigung - Das Unternehmen genehmigt die Drittpartei oder lehnt sie je nach Risikotoleranz ab.
Schritt 5: Überwachung - Das Unternehmen überwacht die Drittpartei weiterhin, um etwaige Cyber-Lücken zu erkennen.

Soziale Netzwerke und Sicherheitsrisiken für Anbieter

Soziale Netzwerke sind in der heutigen Welt sehr beliebt. Normalerweise wird ein soziales Netzwerk als ein Netzwerk in einer kleinen Welt definiert, das aus einer Reihe von Individuen (Personen, Gruppen, Organisationen) besteht, die durch persönliche, berufliche oder vertrauensvolle Beziehungen verbunden sind. Soziale Netzwerke sind also ein recht weit gefasster und allgemeiner Begriff, der im Web-Kontext auf jede Art von virtueller Gemeinschaft angewendet werden kann. So können beispielsweise Benutzer, die bei einem Webdienst wie Webmail, Online-Zeitschriften oder Zeitungen, die ein Abonnement erfordern, registriert sind, als soziales Netzwerk betrachtet werden. Im Folgenden übernehmen wir die Definition, nach der die Website einer Online-Gemeinschaft nur dann als webbasiertes soziales Netzwerk betrachtet werden kann, wenn sie die folgenden Bedingungen erfüllt:

- Die Beziehungen werden von den Mitgliedern explizit angegeben und nicht aus bestehenden Interaktionen abgeleitet (z. B. kann eine Mailingliste verwendet werden, um implizite Beziehungen abzuleiten).
- Beziehungen werden mit Hilfe von Technologien wie Datenbankverwaltungssystemen gespeichert und verwaltet, die eine Analyse der Beziehungen ermöglichen und den Zugang und die Abfrage von Beziehungsdaten regeln.
- Die Mitglieder können zumindest teilweise auf Beziehungsinformationen zugreifen.

Schlüsselbegriffe

Beziehungsbasierte Zugangskontrolle: Ein Paradigma der Zugriffskontrolle, das speziell auf soziale Netzwerke zugeschnitten ist und bei dem die Mitglieder eines sozialen Netzwerks, die zum Zugriff

auf eine bestimmte Ressource berechtigt sind, anhand der Beziehungen, an denen sie teilnehmen müssen, um den Zugriff zu erhalten, bezeichnet werden.

Soziales Netzwerk: Ein Netzwerk in einer kleinen Welt, das aus einer Reihe von Individuen (Personen, Gruppen, Organisationen) besteht, die durch persönliche, berufliche oder vertrauensvolle Beziehungen miteinander verbunden sind. In der Regel wird es als Graph modelliert, wobei die Knoten den Mitgliedern des sozialen Netzwerks entsprechen und die Kanten die zwischen ihnen bestehenden Beziehungen bezeichnen.

Soziale Netzwerke. Die Kommunikation und der Austausch von Informationen mit den Menschen um uns herum ist ein Teil unseres Lebens und hat sich von einfachen Textnachrichten über E-Mails bis hin zu dem entwickelt, was wir heute soziale Medienplattformen nennen. Was nicht sehr bekannt oder bewusst ist, ist die Tatsache, dass unser Engagement in der Online-Umgebung mit einer Menge Risiken verbunden ist.

Soziale Medien und Social-Networking- oder Messaging-Anwendungen können sowohl für Unternehmen als auch für Einzelpersonen eine Reihe von Sicherheits- und Datenschutzrisiken mit sich bringen, wenn sie in unangemessener oder unsicherer Weise genutzt werden. Die beliebtesten und am weitesten verbreiteten Plattformen in sozialen Netzwerken:

-Facebook mit über 1.300.000.000 Mitgliedern;
-Flickr dient zum Speichern, Organisieren und Freigeben von Mediendateien;
-LinkedIn mit über 300 Millionen Nutzern;
-Instagram mit über 30 Millionen Nutzern;
-Twitter mit über einer Milliarde Mitgliedern;
-YouTube mit über einer Milliarde Nutzern;
-Tinder mit etwa 12 Millionen Nutzern;
-TikTok mit über 800 Millionen Nutzern.

Datenschutzbewusste Zugangskontrolle: Bezeichnet im Zusammenhang mit sozialen Netzwerken ein Zugangskontrollparadigma, bei dem die Zugangskontrollanforderungen von Mitgliedern sozialer Netzwerke durchgesetzt werden, ohne dass private Informationen über die Beziehungen, an denen sie beteiligt sind, offengelegt werden.

Webbasiertes soziales Netzwerk: Ein webbasiertes System, das es seinen registrierten Mitgliedern ermöglicht, Beziehungen zu anderen Mitgliedern aufzubauen und verschiedene Arten von Informationen auszutauschen (z. B. persönliche Daten, Kontakte, Multimedia-Ressourcen).

Analyse sozialer Netzwerke: Eine Disziplin, die darauf abzielt, statistische Daten aus der Analyse der Topologie sozialer Netzwerke zu sammeln.

Vertrauensniveau der Beziehung: Bezeichnet in einem sozialen Netzwerk den mit einer Vertrauensbeziehung verbundenen Wert, der ein Maß dafür ist, wie sehr ein bestimmtes Mitglied ein anderes Mitglied für vertrauenswürdig hält. Je nach dem Zweck, für den er verwendet wird, kann dieser Begriff unterschiedliche Bedeutungen haben. In einer kollaborativen Bewertungsumgebung gibt er beispielsweise an, wie sehr ein bestimmtes Mitglied den Meinungen eines anderen Mitglieds in Bezug auf ein bestimmtes Thema (thematisches Vertrauen) oder im Allgemeinen (absolutes Vertrauen) vertraut. In einem Zugangskontrollkontext hingegen hat er einige Ähnlichkeiten mit dem Begriff der Sicherheitsstufe, der in obligatorischen Zugangskontrollmodellen verwendet wird.

Störung der Kanten: Technik zur Anonymisierung von Graphen, die darauf abzielt, die tatsächlichen sozialen Netzwerkbeziehungen zu verbergen, indem eine Reihe von zufälligen Kantenlöschungen/-einfügungen im Netzwerkgraphen vorgenommen werden.

Beziehung zwischen sozialen Netzwerken: Eine Beziehung zwischen zwei Mitgliedern eines sozialen Netzwerks. In WBSNs können neben persönlichen/beruflichen Beziehungen (z. B. Freund/Kollege) auch Vertrauensbeziehungen unterstützt werden, die angeben, wie sehr ein Mitglied einem anderen vertraut. In der grafischen Darstellung eines sozialen Netzwerks werden Beziehungen in der Regel durch Kanten dargestellt, die mit einem Beziehungstyp und/oder einer Vertrauensstufe gekennzeichnet sind.

Anonymisierung von Graphen: Technik, die darauf abzielt, private Informationen über Mitglieder sozialer Netzwerke bei der Analyse sozialer Netzwerke zu verbergen. Knotenanonymisierung und Kantenstörung sind die beiden wichtigsten Techniken zur Anonymisierung von Graphen, die derzeit verwendet werden.

Anonymisierung von Knoten: Technik zur Anonymisierung von Graphen, die darauf abzielt, die Identität von Mitgliedern sozialer Netzwerke zu verbergen, indem die entsprechenden Knoten mit zufälligen Identifikatoren gekennzeichnet werden (naive Anonymisierung), oder, falls Knoten mit Attributen verknüpft sind, die zur Identifizierung des entsprechenden Nutzers verwendet werden können, unter Verwendung von Techniken, die auf k-Anonymität basieren (Sweeney, 2002).

Risiken

Geotagging

- Bezeichnet die Hinzufügung von geoidentifizierenden Daten zu Fotos, Videos, Websites und Textnachrichten durch Anwendungen, die Ihren Standort auslesen können oder dies in Ihren Einstellungen erlauben;

- Achten Sie darauf, Geotagging-Funktionen an sensiblen Orten zu deaktivieren, um zu vermeiden, dass Ihr genauer Standort, Ihr Arbeitsort oder Ihr Wohnort preisgegeben wird.

"Publikum"

- Es ist ein allgemeiner Begriff, der sich darauf bezieht, wer Ihre Beiträge sehen und/oder kommentieren kann;
- Ihre Freundesgruppe kann sich jederzeit ändern und in der Lage sein, einen Beitrag zu sehen, der Informationen über Sie enthält. Sie können absichtlich etwas mit Ihren "Freunden" teilen, aber was sie mit dem Beitrag machen, liegt außerhalb Ihrer persönlichen Kontrolle.

Identität

- Beschreibt die Bandbreite der Informationen, die sich speziell auf eine Person beziehen;
- Es sollte bedacht werden, dass es Personen gibt, die soziale Medien als Recherchemethode nutzen, um nach Identitätsinformationen zu suchen, möglicherweise in böswilliger Absicht, wie Identitätsdiebstahl, Betrug, Unterschlagung oder Einschüchterung.

Maßnahmen

Passwort

- Es wird empfohlen, für jedes Online-Konto ein anderes Passwort zu verwenden;
- Er sollte mindestens 10 Zeichen lang sein und Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten;
- Es darf niemandem mitgeteilt werden, egal wie nah oder vertrauenswürdig die Person ist, der wir es sagen wollen.
- Es wird empfohlen, bei der Erstellung eines Passworts keine persönlichen Daten zu verwenden (z. B. Name der Eltern, Geburtsdatum, Name des Haustiers usw.);
- Ändern Sie Ihr Passwort regelmäßig;
- Melden Sie sich von Ihrem Konto ab, wenn Sie ein Gerät verwenden, das nicht Ihnen gehört oder von einer anderen Person verwendet wird.

Führen Sie Ihre Sicherheitsaktualisierungen rechtzeitig durch!

- Soziale Medienplattformen führen regelmäßig neue Datenschutz- und Sicherheitseinstellungen ein. Diese sind in den Einstellungen Ihres Kontos zu finden, und es wird empfohlen, sie regelmäßig zu überprüfen;
- Verwenden Sie die Zwei-Faktor-Authentifizierungsoption (2FA), um sicherzustellen, dass niemand versucht, Ihr Konto zu hacken.

Nehmen Sie keine Freundschaftsanfragen von anderen an!

- Akzeptiere oder sende Freundschaftsanfragen nur von/an Personen, die du im wirklichen Leben triffst, oder an öffentliche Personen, an denen du interessiert bist, indem du darauf achtest, ihren offiziellen Profilen zu folgen;

- NICHT VERGESSEN! Wenn Sie sich mit bestimmten Konten verbunden fühlen, können Sie deren Zugang zu Ihren Beiträgen einschränken oder das Konto sperren. Sie haben auch die Möglichkeit, Konten oder Beiträge aus folgenden Gründen zu melden: gefälschtes Konto, falscher Name, Beiträge mit unangemessenem Inhalt, Anstiftung zur Gewalt, falsche Informationen usw.
- NICHT klicken!
- Viele Angreifer nutzen Social Engineering, um das Vertrauen einer Person zu gewinnen, um später Zugang zu Informationen zu erhalten;
- Öffnen Sie keine Links und Anhänge aus sozialen Medien, wenn Sie sich der Quelle nicht zu 100 % sicher sind (z. B. sind Websites, auf denen Preise angeboten werden, oft dazu gedacht, Informationen zu stehlen);
- Wenn sich ein Freund in den Chats anders zu verhalten scheint (viele Fragen stellt, sehr neugierig auf sein Privatleben ist, Geld verlangt), besteht die Möglichkeit, dass sein Konto gehackt wurde und ein Angreifer es für bösartige Zwecke nutzt.

Überlegen Sie es sich zweimal, bevor Sie etwas veröffentlichen!

- Soziale Medien bieten ebenso die Möglichkeit, einen positiven Online-Ruf zu schaffen wie einen negativen, und selbst wenn wir einen Beitrag "löschen", kann er, sobald er online erschienen ist, nicht mehr dauerhaft gelöscht werden;
- Geben Sie nicht zu viele persönliche Details in sozialen Medien preis! "Über mich"-Felder sind optional.
- Die Grenze zwischen Berufs- und Privatleben in der Online-Umgebung
- Geben Sie keine Informationen über Ihren Arbeitgeber online bekannt
- Stellen Sie keine Arbeitsfotos oder negative Nachrichten ein, die den Arbeitgeber in ein schlechtes Licht rücken.
- Denken Sie nach, bevor Sie einen Beitrag schreiben, und riskieren Sie nicht Ihren Job.

Schließen Sie alte Konten!

- Wenn Sie alte Konten auf sozialen Medienplattformen haben, die Sie nicht mehr nutzen, oder sogar alte Konten auf derselben Plattform, versuchen Sie, diese zu schließen. Auf diese Weise schaffen Sie so wenig Verknüpfungen wie möglich, und die aktuellen Konten sind besser vor möglichen Angreifern geschützt;
- Ältere Konten oder Plattformen sind möglicherweise nicht so sicher wie die heutigen.

Soziale Medien bergen große Risiken

- Soziale Netzwerke stellen ein hohes Sicherheits- und Datenschutzrisiko dar, da sie eine zentralisierte Architektur haben, einen riesigen Bestand an personenbezogenen Daten enthalten, die jeder Hacker gerne hätte, und die Bevölkerung im Allgemeinen nicht weiß, wie sie soziale Medien richtig nutzen kann.
- Ein weiteres sehr hohes Risiko, vor allem bei Jugendlichen, ist das Vertrauen in andere Menschen und in die Art der persönlichen Informationen, die online preisgegeben werden.

- Dies kann durch technische Mittel und die Durchsetzung von Sicherheitsmaßnahmen bekämpft werden.
- Wir sollten Informationen, die über soziale Medien übermittelt werden, als unsicher betrachten und daher keine sensiblen Informationen über soziale Medien übermitteln; die Hauptverantwortung für die Sicherheit liegt daher beim BENUTZER.

Schlechte Gewohnheiten in den sozialen Medien

- Soziale Netzwerke sind heute weit verbreitete Plattformen für Nutzer. Wir haben eine breite Palette von Möglichkeiten zur Verfügung.
- Einige sind eher auf das Hochladen von Fotos oder Videos ausgerichtet, andere auf unsere Meinung und in anderen Fällen einfach darauf, mit Freunden und Familie in Kontakt zu bleiben. In jedem Fall haben wir es mit Plattformen zu tun, die viele Nutzer auf der ganzen Welt haben.
- Dies führt auch dazu, dass Hacker hier ihr Ziel finden. Wir werden über diese Gewohnheiten sprechen, die in sozialen Netzwerken geändert werden sollten, wenn wir unsere Privatsphäre und Sicherheit bewahren wollen.
- Es gibt viele Arten von Plattformen, die wir im Netz finden können, die uns die Möglichkeit geben, Nachrichten an Freunde oder Familie zu senden, Fotos und Videos zu kommentieren ...
- Dies macht sie zu einer sehr beliebten Umgebung sowohl für private Nutzer als auch für Unternehmen.
- Dies birgt jedoch auch ein gewisses Risiko für unsere Sicherheit und Privatsphäre. Hacker können hier zusehen, wie sie ihre Angriffe durchführen. Sie können insbesondere schlechte Nutzergewohnheiten bei der Verwendung dieser Plattformen ausnutzen.

Gewohnheiten, die geändert werden müssen

- Datenschutz und Sicherheit sind sehr wichtige Faktoren für die Nutzer.
- Sie sind jedoch nicht immer vorhanden.
- Wir können Opfer vieler Arten von Angriffen werden, die diese beiden Faktoren gefährden.
- Wir können auch Fehler machen, wenn wir soziale Medien nutzen, und das wirkt sich auf uns aus.

Jede Art von Kontakt hinzufügen

- Ein sehr häufiger Fehler in sozialen Netzwerken ist das Hinzufügen von Kontakten jeglicher Art. Dies kann auf Plattformen wie Facebook passieren.
- Es ist möglich, dass es sich bei dem hinzugefügten Eintrag um einen Bot und nicht um einen echten Benutzer handelt.
- Sie müssen wissen, wie Sie sie unterscheiden können, und vermeiden, dass Sie jede Art von Kontakt hinzufügen, die Ihre Einladung erhält.
- Manchmal sind Bots nur dazu gedacht, Nutzerdaten zu sammeln. Dies kann unsere Privatsphäre gefährden. Wir müssen einen echten Filter für die Kontakte haben, die wir hinzufügen.
- Es ist wichtig, dass wir Menschen in unserem Freundeskreis haben, die kein Problem für unsere Sicherheit und Privatsphäre darstellen.

Verbinden Sie sich nicht von überall aus mit sozialen Netzwerken

- Oft meldet man sich über soziale Netzwerke auf einer beliebigen Website an. Das ist sehr bequem, aber nicht das Beste für die Privatsphäre.
- Sicherlich finden wir bei vielen Gelegenheiten die Möglichkeit, uns auf einer Seite zu registrieren oder über Facebook oder Twitter mit einer Plattform zu verbinden. Wir vermeiden es, uns auf dieser Seite zu registrieren und ein langes Formular auszufüllen. Das Problem ist, dass wir dieser Website über Facebook persönliche Daten zur Verfügung stellen. Diese Daten/Informationen, die wir weitergeben, können von Dritten zu Werbezwecken verwendet werden.

Geben Sie nicht mehr Informationen als nötig

- Es ist definitiv eine der schlimmsten Angewohnheiten, die viele Nutzer haben. Sie geben in sozialen Netzwerken viele persönliche Daten ein, Informationen, die eigentlich nicht notwendig sind.
- Zum Beispiel Daten wie unsere Telefonnummer, E-Mail-Adresse, Informationen darüber, wo wir wohnen ... All dies wirkt sich auf unsere Werbung aus und könnte für schlechte Zwecke verwendet werden.
- Geben Sie nicht mehr Informationen an, als wirklich notwendig sind. Auf diese Weise verbessern wir unsere Privatsphäre im Netz und können sogar bestimmte Sicherheitsprobleme vermeiden.

Verbreitung von Fake News

- Das Problem der Fake News ist auch heute noch präsent. Ich kann sie auf vielen Wegen erreichen, aber in den sozialen Netzwerken sind sie zweifellos mehr als nur präsent.
- Wie wir wissen, sind es gefälschte Nachrichten, die sie als Köder benutzen und manchmal sogar Malware verbreiten können.
- Es ist wichtig, dass wir diese Art von Fake News nicht weitergeben und auch nicht darauf zugreifen, wenn wir sie in den sozialen Medien sehen.
- Dies wird unsere Sicherheit verbessern.

Wir schützen unsere Privatsphäre nicht

- Ein letzter Fehler ist der mangelnde Schutz der Privatsphäre. Wir lassen zum Beispiel unsere Profile offen, so dass jeder sie betreten kann.
- Wir geben Informationen an jeden weiter, der sie sammeln könnte, um ein Profil für uns zu erstellen und sogar gezielte Werbung zu versenden oder verschiedene Angriffe durchzuführen, die unsere Sicherheit beeinträchtigen.

Social Engineering aus einer interdisziplinären Perspektive

-Aufgrund der von Hackern verwendeten Technik ist es notwendig, eine interdisziplinäre Perspektive wie Informationstechnologie, Psychologie, Wirtschaft und Ethik einzunehmen.

Die Disziplin der Informationstechnologie

- Social Engineering sollte im Zusammenhang mit aktuellen Informationssystemen und deren Verteidigung als eine Form der Risikominderung diskutiert werden.
- Die Multi-Faktor-Authentifizierung ist eine gängige und oft wirksame Methode für Unternehmen, um zu bestätigen, dass die Person, die auf Systeme zugreift, auch tatsächlich über diesen Zugriff verfügen sollte.
- Ein zusätzlicher Faktor könnte die Verwendung eines virtuellen privaten Netzes (VPN) sein, d.h. eine Authentifizierung zur weiteren Validierung des Benutzers.

Disziplin Psychologie

- Es ist notwendig, das Konzept zu verstehen und die Gedanken und Verhaltensweisen sowohl des Angreifers als auch des Opfers zu kennen.
- Diese Methoden sind für das Social Engineering wichtig, da sie dazu dienen, vorhandene Schutzmaßnahmen wie Firewalls und Systeme zur Identifizierung von Eindringlingen zu umgehen.
- Es hilft, die Handlungen der Mitarbeiter zu verstehen, die eine der Hauptursachen für Datenschutzverletzungen sind.

Geschäftliche Perspektive

- Es ist wichtig, weil Social Engineering viele Arten von Unternehmen betreffen kann und Auswirkungen darauf hat, wie Organisationen strukturiert und verwaltet werden.
- Sie hilft bei der Ermittlung der Faktoren, die Social-Engineering-Angriffe beeinflussen, und ist von Vorteil, wenn sie in Bezug auf die folgenden Unternehmensbereiche genauer betrachtet wird: Schulung und Entwicklung, dokumentierte Richtlinien, interne Prüfverfahren, Budgets und Organisationskultur.
- kann Mängel in allen Bereichen aufdecken, die zu Angriffen beitragen können.

Ethische Perspektive

- Sie ist im Zusammenhang mit Social Engineering und verwandter Forschung wichtig, weil die Idee, einen anderen Menschen zu manipulieren, gegen viele ethische Grundsätze verstößt.
- hilft im Falle eines Social Engineering-Ereignisses bei der Behandlung der Opfer.

Es ist wichtig, dies zu berücksichtigen:

- Jede Disziplin bietet Informationen zum Verständnis und zur Interpretation des Themas, zum Schutz vor verschiedenen Arten von Angriffen und zum Verständnis der Auswirkungen von Social Engineering sowohl aus menschlicher als auch aus organisatorischer Sicht.
- dass die Interpretation eines Themas durch die einzelnen Disziplinen nur dann sinnvoll ist, wenn sie im Zusammenhang mit den anderen Disziplinen betrachtet wird.

Sicherheitstechniken

- Inventar der Ausrüstung
- Bestandsaufnahme der Anwendungen und Betriebssysteme
- Drahtlose Gerätesteuerung
- Entwurf der Netzsicherheit
- Begrenzung und Kontrolle von Netzwerkanschlüssen, Kommunikationsprotokollen und Diensten
- Schutz der umliegenden Gebiete
- Physischer Zugang zu den Standorten
- Kontrollierte Nutzung von Verwaltungsrechten
- Überwachung und Kontrolle von Benutzerkonten
- Kompetenzbewertung und Sicherheitsschulung

VPN (Virtuelles Privates Netzwerk)

Ein virtuelles privates Netz ist eine sichere Verbindung über ein unsicheres Netz wie das Internet. Virtuell bedeutet das Vorhandensein eines einzigen Netzes, unabhängig von der Topologie, d. h. einer Gruppe von geografisch verteilten Computern, die miteinander kommunizieren und als ein einziges Netz verwaltet werden können.

Privat bedeutet ein virtuelles Netz mit Zugangskontrolle, das die Vertraulichkeit und Integrität von Nachrichten gewährleistet und die Authentizität zwischen den Benutzern und den an der Kommunikation beteiligten Computern sicherstellt.

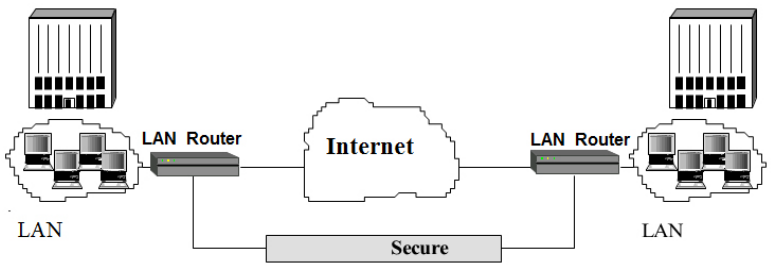

Abb. 2: VPN (Virtuelles Privates Netzwerk)

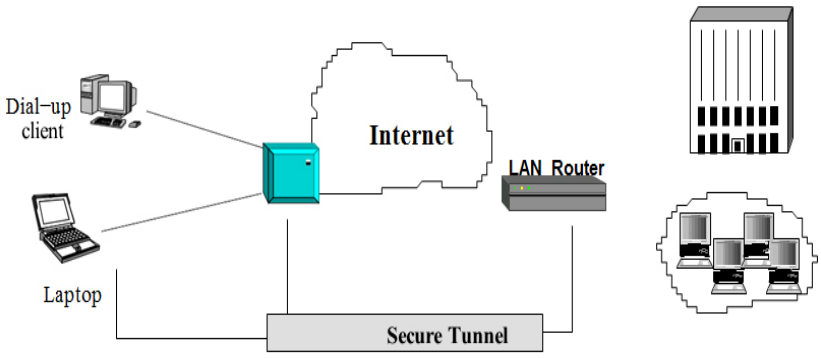

Abb. 3: VPN für Fernzugriff

Schaffung einer sicheren industriellen Infrastruktur

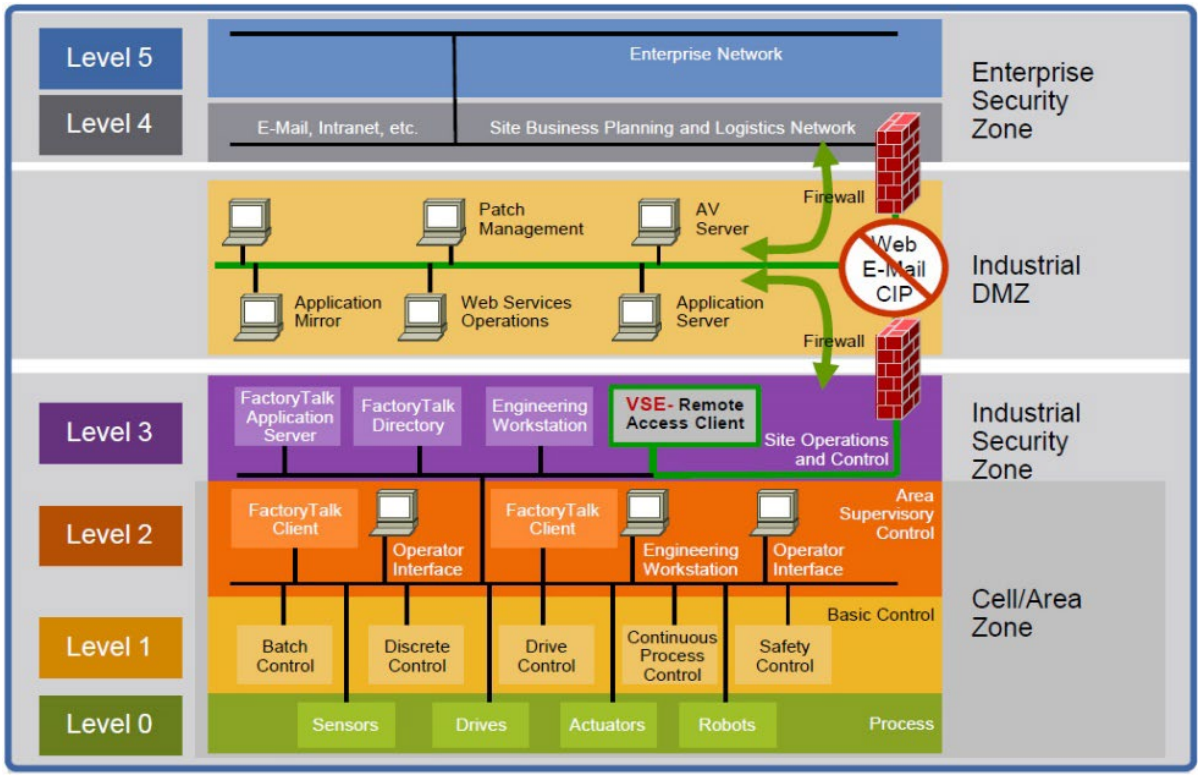

Abb. 4: ISA 95 Logikmodell - Industrielles Automatisierungs- und Steuerungssystem (IACS)

- Defense-in-Depth (DiD) unterstützt diesen Ansatz. Ausgehend von dem Gedanken, dass ein einzelner Schutzpunkt überwunden werden kann und wahrscheinlich auch wird, werden bei der

DiD-Sicherheit mehrere Schutzschichten durch eine Kombination aus physischen, elektronischen und verfahrenstechnischen Sicherheitsvorkehrungen eingerichtet.

- Eine Bank setzt mehrere Sicherheitsmaßnahmen ein, z. B. Videokameras, einen Wachmann und einen Tresorraum, um sicherzustellen, dass Bedrohungen mehr als eine Verteidigungslinie treffen.
- Ein Security-in-Depth-Ansatz umfasst sechs Hauptkomponenten:

1. Richtlinien und Verfahren
2. Physisch
3. Netzwerk
4. Computer
5. Anmeldung
6. Das Gerät

Schaffung einer sicheren industriellen Infrastruktur

- Die physische Sicherheit sollte den Zugang des Personals nicht nur auf bestimmte Bereiche einer Einrichtung beschränken, sondern auch auf Zugangspunkte zur physischen Netzinfrastruktur, wie z. B. Schalttafeln, Verkabelung und Geräte.
- Die Segmentierung von Anlagenbereichen in virtuelle lokale Netze (VLANs) ist eine netzweite bewährte Sicherheitsmethode.
- Kleinere VLANs sind einfacher zu verwalten und in der Echtzeitkommunikation zu pflegen.
- Sie können helfen, Geräte von denen zu isolieren, die kompromittiert wurden, wodurch die negativen Auswirkungen auf ein einzelnes VLAN beschränkt bleiben.
- Eine der diskutierten Technologien sollte eine industrielle entmilitarisierte Zone (IDMZ) sein, die eine kritische Schutzbarriere zwischen dem Unternehmen und den Industriegebieten schafft.
- Eine IDMZ verhindert, dass der Datenverkehr direkt zwischen den beiden Zonen fließt, und kann den Zugang besser verwalten, indem sie die Authentifizierung erzwingt oder den Datenverkehr auf bekannte Bedrohungen überwacht.

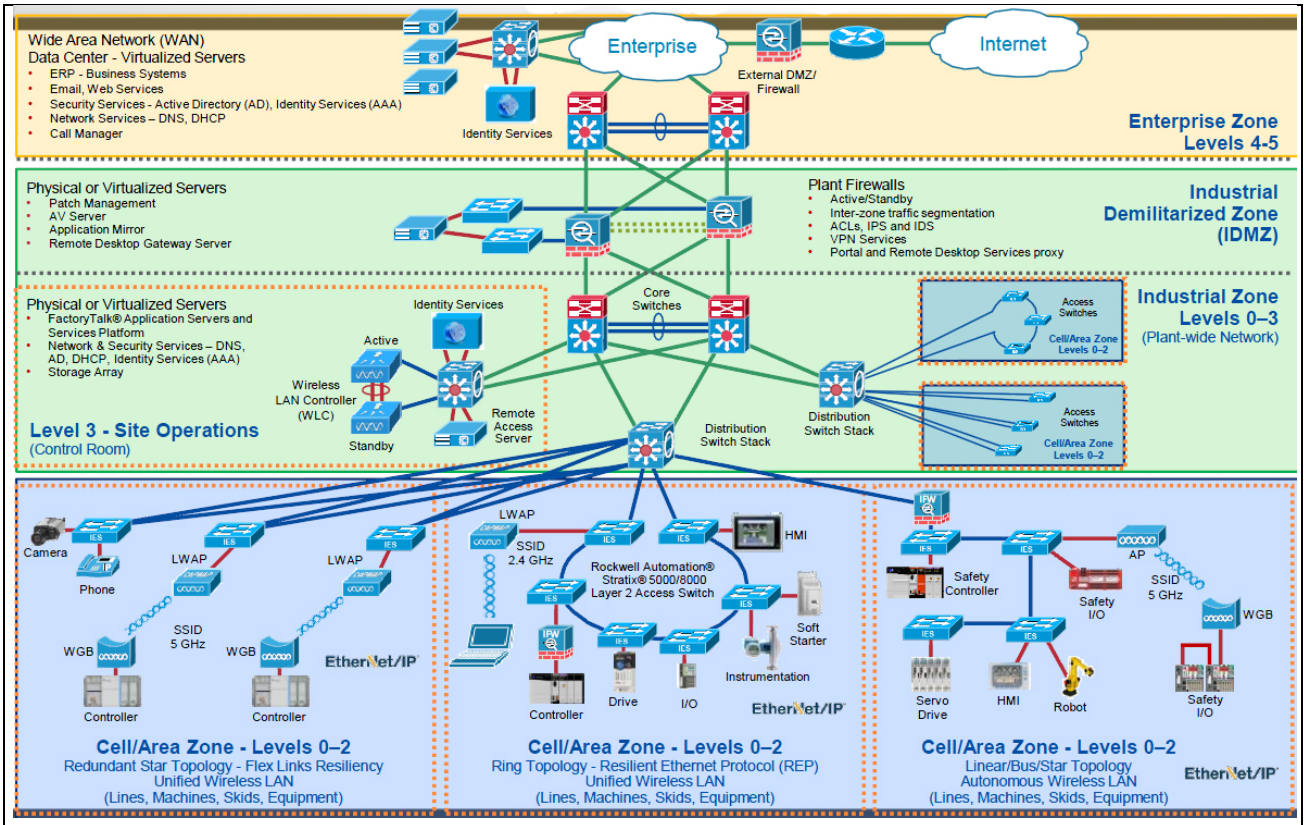

Abb. 5: IDMZ

Fragen:

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

1. welche Risiken es in sozialen Netzwerken gibt
2. Maßnahmen für Sicherheit und Datenschutz in sozialen Netzwerken
3. welche die wichtigsten Sicherheitstechniken in sozialen Netzwerken sind

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

- Risiken in sozialen Netzwerken
- Sicherheit und Datenschutz in sozialen Netzwerken
- Sicherheitstechniken

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

Siehe Anhang

Referenzen:

Beschaffungsanforderungen
URL: Beschaffungsanforderungen
URL: https://www.ekransystem.com/en/blog/third-party-providers
Ermittlung des Beschaffungsbedarfs
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Sicherheit und Datenschutz in sozialen Netzwerken
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Sicherheit und Datenschutz in sozialen Netzwerken
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Datenschutz und Sicherheit in sozialen Online-Medien
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Datensicherheitstechniken und Datenschutz
URL: https://www.educba.com/data-security-techniques/
Was sind Sicherheitstechniken?
URL: Sicherheits-Konzepte-Entwicklungen-und-Zukunfts-Trends
Die wirksamsten Sicherheitstechniken
URL: https://dzone.com/articles/most-effective-security-techniques-part-1
URL: https://panorays.com/blog/what-is-a-third-party-vendor/