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

uli di formazione InCyT

Sicurezza delle informazioni per manager Unità 1 Settimana 2 Nome dell'unità: Introduzione alla sicurezza delle informazioni e ai sistemi di controllo interno.	
Attività di apprendimento	❑ **Webinar**❑ **Esercitazioni**❑ **Workshop**❑ **Presentazione**❑ **Altro**
Apprendimento responsabile	• Gabriel Vladut • Valentin Istratie
Obiettivi dell'attività di apprendimento	1. Introduzione al progetto Erasmus+ InCyT 2. Sicurezza informatica 3. Concetti, definizioni e termini 4. Standard di controllo interno 5. Elaborazione dei controlli di sicurezza informatica
Competenze da acquisire	• Sicurezza di rete TS3 • TS4 Test di penetrazione (vulnerabilità sfruttabili) • SS3 Analisi cognitiva e comportamentale
Durata dell'attività di apprendimento	2 settimane
Apprendimento requisiti	***Cosa serve?*** • Acquisire la consapevolezza della sicurezza informatica e imparare cosa sono gli attacchi di sicurezza informatica. • Imparare i metodi per prevenire le violazioni dei dati utilizzati dagli aggressori per accedere ai dati sensibili e sfruttare le vulnerabilità organizzative • Imparare come procedere in caso di attacco alla sicurezza informatica

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

Brevi informazioni sul modulo

Descrizione
Sicurezza delle informazioni, i sistemi di controllo interno sono importanti e spesso minacciati dalla sicurezza informatica. La protezione delle informazioni e dei sistemi informativi contro l'accesso non autorizzato o la modifica delle informazioni, sia in fase di archiviazione, che di elaborazione o di transito, e contro la negazione del servizio agli utenti autorizzati. La sicurezza delle informazioni comprende le misure necessarie per individuare, documentare e contrastare tali minacce. La sicurezza delle informazioni è composta da sicurezza informatica e sicurezza delle comunicazioni. Chiamata anche INFOSEC. I controlli interni sono utilizzati dai team di gestione, sicurezza informatica, finanziari, contabili e operativi per raggiungere i seguenti obiettivi: 1. Garantire l'affidabilità e l'accuratezza delle informazioni finanziarie - I controlli interni assicurano che i sistemi contabili e i rapporti finanziari riportino informazioni accurate, aggiornate e complete. I discenti possono essere informati su questi aspetti leggendo il testo corrispondente, guardando i webinar in streaming e risolvendo gli esercizi al proprio ritmo. Tutti questi documenti sono presenti sulla piattaforma digitale interattiva del progetto. I discenti possono verificare le loro risposte negli esercizi di autovalutazione. Le risposte agli altri esercizi devono essere salvate sul forum di discussione corrispondente e discusse con il tutor durante l'incontro comune organizzato una volta alla settimana. Gli studenti possono lavorare in modo cooperativo con gli altri e con il tutor, in particolare durante gli incontri. Saranno aiutati a sviluppare un e-portfolio importante per la riflessione e la valutazione della formazione.

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

Contenuto del materiale didattico

Sicurezza delle informazioni

La sicurezza delle informazioni si occupa di proteggere le informazioni e i sistemi informatici da accesso, uso, divulgazione, interruzione, modifica o distruzione non autorizzati.

La norma ISO/IEC27002/2013 tratta la sicurezza delle informazioni attraverso le sue tre componenti principali: riservatezza, integrità e disponibilità. La riservatezza è garantita dalla crittografia delle informazioni. L'integrità è ottenuta attraverso meccanismi e algoritmi di dispersione.

La disponibilità è garantita dal rafforzamento della sicurezza della rete o delle reti del sistema informatico e dalla fornitura di backup. La sicurezza delle informazioni è un insieme di pratiche volte a proteggere i dati.

La sicurezza delle informazioni non si limita ai sistemi informatici o alle informazioni in forma digitale o elettronica. Si applica piuttosto a tutte le questioni relative alla sicurezza e alla protezione dei dati o delle informazioni, indipendentemente dalla loro forma.

La sicurezza informatica non può essere definita come semplice sinonimo di sicurezza degli elaboratori, sicurezza dei sistemi e delle reti, sicurezza dell'Information Technology, dei sistemi informativi o tecnologia dell'informazione e della comunicazione. Ognuna di queste espressioni si riferisce a un argomento diverso, anche se il punto in comune è la sicurezza dell'informazione in alcune delle sue forme (qui nella sua versione elettronica): pertanto, sono tutti sottocampi della sicurezza delle informazioni.

Nel XXI secolo, la maggior parte delle organizzazioni ha un sistema informatico collegato a Internet e scambia informazioni attraverso di esso. Le informazioni possono passare attraverso un'interconnessione di reti. Di conseguenza, questa interconnessione è ancora più esposta ai rischi di malware da parte di chi vuole impossessarsi di informazioni sensibili, agendo dall'interno (copiando informazioni, utilizzando codice maligno) o dall'esterno.

Per contrastare questi rischi, la sicurezza delle informazioni richiede lo sviluppo di concetti quali l'etichettatura dei dati, la crittografia a chiave pubblica (PKC) e la sicurezza multilivello (MLS). Oltre ai problemi di connessione delle reti, è sempre più facile spostare grandi quantità di informazioni (in modo relativamente difficile da individuare in caso di hacking), ma anche trasportarle fisicamente tramite chiavette USB o schede di memoria.

Pertanto, i sistemi informatici contenenti informazioni sensibili sono sempre più spesso progettati come ambiente System high mode, in molti casi sotto forma di reti separate senza connessione ad

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

altre reti e senza porte USB. I criteri di sensibilità delle informazioni comunemente accettati sono tre: *Disponibilità*, *Integrità* e *Riservatezza*. Anche un quarto criterio è utilizzato abbastanza frequentemente (con nomi diversi): *Tracciabilità*, *Responsabilità*, "Audibilità" (con riferimento alle verifiche informatiche dette audit) o *Evidenza*. Viene utilizzato anche un quinto criterio: il *Non ripudio*, questo garantisce lo scambio di messaggi tra il mittente e il destinatario.

Attacchi informatici e quadro delle competenze

Un quadro di riferimento per le competenze viene regolarmente utilizzato dalle aziende per comprendere i propri requisiti basati sulle competenze, le abilità richieste, le capacità dei dipendenti e le lacune.

Quando un quadro di competenze viene sviluppato tenendo conto del profilo dell'azienda e degli interessi dei dipendenti, può migliorare le prestazioni e fornire chiarezza per ogni singolo requisito di ruolo e sviluppare il talento sul posto di lavoro. Negli ultimi anni, a causa dei numerosi attacchi informatici, i framework di sicurezza informatica sono stati adottati principalmente da grandi organizzazioni (aziende, ONG e altre entità) o da attori statali.

Un attacco informatico riuscito può causare gravi danni all'attività di un'azienda. Può influire sul risultato economico, sullo status commerciale dell'azienda e sulla fiducia dei consumatori. L'impatto di una violazione della sicurezza può essere suddiviso in tre categorie: finanziario, reputazionale e legale.

Attacchi informatici

Gli attacchi informatici spesso comportano ingenti perdite finanziarie derivanti dal furto di informazioni aziendali, informazioni finanziarie (ad esempio, dati bancari o di carte di pagamento), denaro, interruzioni delle transazioni (ad esempio, impossibilità di effettuare transazioni online), perdita dell'attività o del contratto. Le aziende che hanno subito una violazione informatica generalmente spendono denaro per riparare i sistemi, le reti e i dispositivi colpiti.

Gli attacchi informatici possono danneggiare la reputazione di un'azienda e la fiducia che i clienti ripongono in essa. Ciò può comportare la perdita di clienti, di vendite e di profitti. L'effetto del danno alla reputazione può persino ripercuotersi sui fornitori dell'azienda o sui rapporti con partner, investitori e altre terze parti coinvolte nell'attività dell'azienda.

Pertanto, le leggi sulla protezione dei dati e sulla privacy richiedono la gestione della sicurezza di tutti i dati personali in possesso dell'azienda (del proprio personale o dei clienti). Se questi dati vengono accidentalmente o deliberatamente compromessi e l'azienda non implementa misure di sicurezza adeguate, può incorrere in sanzioni normative.

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

Rischi in azienda

È importante gestire i rischi di conseguenza. Dopo un attacco, uno strumento di sicurezza informatica efficace o un piano di risposta agli incidenti, ad esempio ricorrendo a un consulente informatico, possono aiutare a:

- ridurre l'impatto dell'attacco
- segnalare l'incidente alle autorità competenti
- ripulire i sistemi interessati
- Rendere di nuovo operativa la vostra azienda nel più breve tempo possibile.

È necessario investire nella formazione e nell'educazione degli utenti nel campo della sicurezza informatica per evitare attacchi e sviluppare costantemente la consapevolezza di una strategia informatica nella propria organizzazione.

Quadro di sicurezza informatica

Un framework di cybersecurity è un insieme di best practice e processi documentati che vengono utilizzati per sviluppare politiche di sicurezza informatica all'interno di un'organizzazione. Tuttavia, a differenza delle politiche tradizionali strettamente legate all'ambito legale, un framework di cybersecurity dovrebbe includere anche esempi documentati dei problemi che devono essere evitati da tali politiche e dei processi e dei modi appropriati per implementare le politiche di sicurezza descritte nel framework.

Si tratta sia di una guida per i dipendenti e gli utenti, sia di un compendio convincente di best practice di sicurezza che può essere consultato da soggetti esterni autorizzati (come le autorità). Un quadro di competenze di cybersecurity può anche aiutare a valutare meglio le competenze necessarie per evitare gli attacchi, le lacune e le misure di rimedio.

Sicurezza informatica

Nonostante la maggiore consapevolezza e gli sforzi coraggiosi, è nota la carenza altamente significativa e crescente di professionisti della sicurezza informatica nell'Unione europea e di conoscenze e competenze dei dipendenti per evitare gli attacchi informatici in tutto il mondo, e queste carenze continuano a presentare problemi importanti per il settore pubblico e privato.

Lo studio CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) stima che a livello globale ci siano 2,8 milioni di professionisti della cybersecurity, mentre il gap è in realtà di 4,07 milioni.

Lo studio rileva che il divario attuale in Europa è di 291.000 unità, un numero raddoppiato rispetto

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

agli anni precedenti. Molti Paesi con competenze altamente sviluppate preferiscono creare una propria serie di regolamenti e documenti, ma molti Paesi e piccole e medie imprese (PMI) hanno bisogno di aiuto in questo contesto.

Ingegneria sociale

- Significa manipolare gli esseri umani (spesso utilizzando metodi psicologici) per ottenere l'accesso a dati, documenti e informazioni di interesse per l'attaccante.
- È oggi una delle principali minacce alla sicurezza informatica e rappresenta una forma efficace di criminalità informatica.
- Potrebbero avere pericolose ripercussioni, ad esempio la violazione dei dati, più di qualsiasi altro tipo di attacco.
- Gli attacchi hanno uno scopo finanziario e quindi le organizzazioni hanno perso notevoli somme di denaro.
- È particolarmente pericoloso perché si basa più sull'errore umano che sulle vulnerabilità del software e dei sistemi operativi.

Le aziende:

- potrebbero subire una perdita di produttività, un calo del morale dei dipendenti e difficoltà di recupero;
- hanno un danno di reputazione perché i clienti non sono convinti che l'organizzazione sia in grado di proteggersi;
- spesso è necessario che utilizzino una risposta agli incidenti già utilizzata in precedenza;
- dovrebbero essere fornite di un software di sicurezza che aiuti a prevenire attacchi futuri;
- spesso devono riqualificare i dipendenti per essere pronti agli attacchi.

Ingegneria sociale; formazione (consapevolezza informatica)

Riguarda i dipendenti e i manager per i quali è importante riconoscere gli attacchi di social engineering perché il rischio di diventarne vittima è elevato.

Questi potrebbero essere inclusi in programmi di sensibilizzazione alla sicurezza della comunità, dei singoli e dei cittadini e proteggere gli individui e la loro organizzazione.

È particolarmente carente nelle PMI che dispongono di minori risorse, per cui dovrebbero essere aiutate a prendere sul serio la formazione sulla consapevolezza informatica e a offrire ai dipendenti l'opportunità di seguirla.ione sulla consapevolezza informatica e a offrire ai dipendenti l'opportunità di seguirla.

Formazione e tutoraggio

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

La valutazione delle prestazioni dei discenti nello sviluppo delle competenze imprenditoriali può avere una visione olistica che include uno sguardo all'ambiente di apprendimento e ai risultati dell'apprendimento, per facilitare un apprendimento interattivo, efficace e attivo.

Il mentoring è un metodo per sostenere un apprendimento più individuale e per acquisire competenze personali e di carriera per nuove professioni. Offre una serie di vantaggi ai dipendenti che si formano in azienda.

Esistono (poche) ricerche sui risultati del mentoring in generale.

Il mentoring di gruppo interdisciplinare ha acquisito importanza negli ultimi anni, riflettendo la necessità di un cambiamento nell'orientamento del mentoring, dato che i vari sviluppi e campi imprenditoriali sono sempre più multidisciplinari.

Competenze imprenditoriali e mentoring

La valutazione delle prestazioni dei discenti nello sviluppo delle competenze imprenditoriali può avere una visione olistica, che include uno sguardo all'ambiente di apprendimento e ai risultati dell'apprendimento, e facilitare un apprendimento interattivo, efficace e attivo.

Il mentoring è un metodo sperimentato per sostenere un apprendimento più individuale e per acquisire competenze personali e di carriera per le nuove professioni. Esistono ricerche sui risultati del mentoring in generale, ma ci sono poche ricerche sul mentoring.

Il mentoring offre una serie di vantaggi ai dipendenti che si formano nelle aziende. Il mentoring di gruppo interdisciplinare ha acquisito importanza negli ultimi anni, riflettendo la necessità di un cambiamento nell'orientamento del mentoring, dato che i vari sviluppi e campi imprenditoriali sono sempre più multidisciplinari.

Il mentoring interdisciplinare e le reti di mentori possono produrre sinergie nei gruppi, generare idee innovative e soluzioni complesse alle sfide e creare opportunità di collaborazione e lavoro.

Concetti, definizioni e termini

infrastrutture informatiche - infrastrutture di tecnologia dell'informazione e della comunicazione, costituite da sistemi informatici, applicazioni correlate, reti e servizi di comunicazione elettronica;

cyberspazio - l'ambiente virtuale generato dalle infrastrutture informatiche, compresi i contenuti informativi elaborati, memorizzati o trasmessi, nonché le azioni compiute dagli utenti al suo interno; il termine è stato coniato nel 1982 da William Gibson ed è entrato nella vita quotidiana negli anni '90 con l'avvento del World Wide Web.

sicurezza informatica - lo stato di normalità risultante dall'applicazione di un insieme di misure

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

proattive e reattive che garantiscono la riservatezza, l'integrità, la disponibilità, l'autenticità e la non ripudiabilità delle informazioni in formato elettronico, delle risorse e dei servizi pubblici o privati, nello spazio cibernetico.

Le misure proattive e reattive possono includere politiche di sicurezza, concetti, standard e linee guida, gestione del rischio, attività di formazione e sensibilizzazione, implementazione di soluzioni tecniche per proteggere le infrastrutture informatiche, gestione delle identità, gestione delle conseguenze;

difesa cibernetica - azioni svolte nello spazio cibernetico allo scopo di proteggere, monitorare, analizzare, rilevare, contrastare le aggressioni e garantire una risposta tempestiva contro le minacce alle infrastrutture cibernetiche specifiche della difesa nazionale;

operazioni nelle reti informatiche - il complesso processo di pianificazione, coordinamento, sincronizzazione, armonizzazione e realizzazione di azioni nel cyberspazio per la protezione, il controllo e l'uso delle reti informatiche al fine di ottenere la superiorità informativa, contemporaneamente alla neutralizzazione delle capacità dell'avversario;

minaccia informatica - circostanza o evento che costituisce un potenziale pericolo per la sicurezza informatica;

attacco informatico - azione ostile condotta nello spazio cibernetico in grado di compromettere la sicurezza informatica;

incidente informatico - evento che si verifica nello spazio cibernetico e le cui conseguenze si ripercuotono sulla sicurezza informatica;

terrorismo informatico - attività premeditate svolte nel cyberspazio da individui, gruppi o organizzazioni con motivazioni politiche, ideologiche o religiose che possono causare distruzione materiale o vittime, in grado di provocare panico o terrore;

spionaggio informatico - azioni condotte nello spazio cibernetico, con l'obiettivo di ottenere informazioni riservate non autorizzate nell'interesse di un'entità statale o non statale;

crimine informatico - tutti gli atti previsti dal diritto penale o da altre leggi speciali che presentano un pericolo sociale e sono commessi con colpa, attraverso o su infrastrutture informatiche;

vulnerabilità nello spazio cibernetico - debolezza nella progettazione e nell'implementazione delle infrastrutture cibernetiche o delle relative misure di sicurezza che può essere sfruttata da una minaccia;

rischio di sicurezza nel cyber-spazio - la probabilità che una minaccia si concretizzi, sfruttando una specifica vulnerabilità propria delle infrastrutture informatiche;

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

gestione del rischio - un processo complesso, continuo e flessibile di identificazione, valutazione e contrasto dei rischi di sicurezza informatica, basato sull'utilizzo di tecniche e strumenti complessi, per prevenire perdite di qualsiasi tipo;

gestione dell'identità - metodi di convalida dell'identità delle persone quando accedono a determinate infrastrutture informatiche.

Le componenti del controllo interno

Secondo lo standard INTOSAI GOV 9100 "Linee guida per gli standard di controllo interno"originariamente pubblicate nel 1992, nel 2001, in occasione del Congresso dell'Organizzazione Internazionale delle Istituzioni Superiori di Controllo (INCOSAI), è stato deciso di aggiornarle nel settore pubblico, introducendo nel documento tutti gli aspetti dei recenti sviluppi nel campo del controllo interno e integrando una serie di elementi del modello COSO (Internal Control - Integrated Framework).

Integrandolo nelle Linee guida - attività svolta dal gruppo operativo del Comitato per gli standard di controllo interno dell'INTOSAI - si è cercato di ottenere una comprensione unitaria del funzionamento del nuovo sistema di controllo interno da parte dei rappresentanti delle Istituzioni superiori di controllo.

Le "Linee guida INTOSAI per gli standard di controllo interno nel settore pubblico" fanno parte della categoria INTOSAI GOV (good governance guidance) e sono considerate estremamente utili sia per i dirigenti del settore pubblico che devono realizzare il sistema di controllo interno, sia per i revisori pubblici esterni che devono conoscere questo sistema e valutarlo.

Standard di controllo interno

Secondo le Linee guida INTOSAI GOV 9100), il controllo interno è costituito da cinque componenti interdipendenti (identiche a quelle del modello COSO):

- Ambiente di controllo
- Valutazione del rischio
- Attività di controllo
- Informazione e comunicazione
- Monitoraggio

Il controllo interno è progettato per fornire una ragionevole garanzia sul raggiungimento degli obiettivi generali dell'ente. Gli obiettivi chiaramente stabiliti dai responsabili dell'ente e l'adeguata pianificazione del bilancio sono una condizione obbligatoria per un controllo interno efficace.

Ambiente di controllo

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

L'ambiente di controllo comprende l'atteggiamento generale, la consapevolezza e le azioni intraprese dalla direzione e dai responsabili della governance in merito al sistema di controllo interno e alla sua importanza all'interno dell'entità. L'ambiente di controllo stabilisce il tono dell'organizzazione, influenzando la consapevolezza del controllo a livello di personale.

Rappresenta la base di tutte le altre componenti del controllo interno, garantendo una disciplina all'interno dell'organizzazione che deve essere rispettata e una struttura dell'entità, in modo che il sistema di controllo interno possa essere applicato efficacemente. L'ambiente di controllo interno è uno strumento efficace per prevenire corruzione e frodi.

Gli elementi che definiscono l'ambiente di controllo sono:

- l'integrità personale e professionale, i valori etici stabiliti dalla direzione per tutto il personale, compreso un atteggiamento di sostegno permanente nei confronti del controllo interno;
- una costante preoccupazione del management per la competenza del personale;
- la filosofia e il modo di porsi della direzione;
- la struttura organizzativa dell'ente;
- la politica e le pratiche in merito alle Human Resources.

Tipi di controlli di sicurezza informatica

I controlli di cybersecurity sono meccanismi utilizzati per prevenire, rilevare e mitigare le minacce e gli attacchi informatici. I meccanismi vanno dai controlli fisici, come le guardie di sicurezza e le telecamere di sorveglianza, ai controlli tecnici, come i firewall e l'autenticazione a più fattori.

Un approccio unilaterale alla sicurezza informatica è semplicemente obsoleto e inefficace. Poiché nel panorama odierno delle minacce è impossibile prevenire tutti gli attacchi, le organizzazioni devono valutare le proprie risorse in base alla loro importanza per l'azienda e stabilire i controlli di conseguenza.

A ciò si aggiunge il fatto che è improbabile che i dipendenti seguano le regole di conformità se vengono implementati controlli rigorosi su tutte le risorse aziendali. La severità di un controllo dovrebbe riflettere direttamente il panorama delle risorse e delle minacce.

Le conseguenze di un hacker che espone migliaia di dati personali dei clienti attraverso un database in cloud, ad esempio, possono essere molto più gravi rispetto alla compromissione del computer portatile di un dipendente.

Controlli di sicurezza informatica

"Ci sono molti modi diversi di applicare i controlli in base alla natura di ciò che si sta cercando di proteggere", ha dichiarato Joseph MacMillan, autore di Infosec Strategies and Best Practices e

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

cintura nera globale di cybersecurity presso Microsoft.

"Qual è la natura della minaccia da cui state cercando di proteggervi?

Si tratta di un soggetto malintenzionato?

O è un attacco devastante?".

Protezione del patrimonio informativo

Si riferisce all'implementazione di controlli appropriati sulla sicurezza delle informazioni per gli asset. Vogliamo assicurarci di concentrarci su ideologie forti ed efficaci per capire di selezionare i controlli appropriati, il che significa che l'asset è considerato "abbastanza sicuro" in base alla sua criticità e classificazione. Esistono diverse classi che suddividono i tipi di controlli:

- I controlli amministrativi/gestionali sono le politiche e le procedure dello studio. Non sono così "cool" come un nuovo controllo software, ma esistono per fornire una struttura e una guida ai singoli e agli altri membri dell'organizzazione, assicurando che nessuno venga multato o provochi una violazione.
- Controlli fisici che limitano l'accesso ai sistemi in modo fisico.
- I controlli tecnici/logici sono quelli che limitano l'accesso in base all'hardware o al software, come la crittografia, i lettori di impronte digitali, l'autenticazione o i moduli di piattaforma fidata (TPM).

Non limitano l'accesso ai sistemi fisici come i controlli fisici, ma piuttosto l'accesso ai dati o ai contenuti. I controlli operativi sono quelli che coinvolgono le persone che eseguono i processi su base giornaliera. Tra gli esempi si possono citare la formazione di sensibilizzazione, la classificazione delle risorse e la revisione dei file di log.

Tipi di controlli

I controlli preventivi esistono per impedire un'azione e comprendono firewall, recinzioni e permessi di accesso.

I sistemi di rilevamento vengono attivati solo durante o dopo un evento, come i sistemi di videosorveglianza o di rilevamento delle intrusioni. I deterrenti scoraggiano le minacce dal tentare di sfruttare una vulnerabilità, come un "Watchdog". I controlli correttivi sono in grado di passare da uno stato all'altro.

I sistemi di recupero permettono di recuperare qualcosa da una perdita, come ad esempio il recupero di un disco rigido. I controlli compensativi sono quelli che cercano di compensare le carenze di altri controlli, come la revisione regolare dei registri di accesso. Anche questo esempio è un controllo investigativo, ma i controlli di compensazione possono essere di diverso tipo.

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

Ordine dei controlli

Scoraggia gli attori dal tentare di accedere a qualcosa che non dovrebbero. Negare/impedire l'accesso attraverso un controllo preventivo come i permessi di accesso o l'autenticazione.

Rilevare il rischio assicurandosi di registrare il rilevamento, ad esempio con il software di protezione degli endpoint. Impedire al processo di ripetere il rischio, ad esempio con una funzione di "troppi tentativi" per l'inserimento di una password.

Correggere la situazione rispondendo alla compromissione, ad esempio con un piano di risposta agli incidenti. Recuperare da uno stato compromesso, come ad esempio un generatore di backup che ripristina la disponibilità di un server.

Inoltre, in un'ottica di miglioramento continuo, è necessario monitorare il valore di ogni asset per verificarne eventuali variazioni. Il motivo è che potrebbe essere necessario ripensare i controlli per la protezione di questi asset, se diventano più o meno preziosi nel tempo o in occasione di alcuni eventi importanti dell'organizzazione.

Controlli e recupero

Quando consideriamo i controlli dobbiamo pensare anche al recupero, vogliamo essere in grado di recuperare da qualsiasi situazione avversa o da cambiamenti nelle attività e nel loro valore. A titolo di esempio, parliamo di backup, ridondanza, processi di ripristino e simili.

È importare assicurarsi (soprattutto in merito all'attualità del cloud, del SaaS, del PaaS, dell'IaaS, delle soluzioni di terze parti e di tutte le altre forme di remote computing) che gli accordi sul livello di servizio (SLA) siano chiaramente definiti e che prevedano il massimo tempo di inattività consentito, nonché sanzioni per il mancato rispetto di tali accordi. Questo è un esempio di controllo compensativo.

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

1. Quali sono i rischi in azienda per gli attacchi informatici?
2. Chiamare alcuni tipi di controlli di sicurezza informatica
3. Le streghe sono standard di controllo interno
4. Come controllare e recuperare le informazioni

Domande di autovalutazione.

- Rischi in azienda per attacchi informatici
- Standard di controllo interno e roulette
- Ambiente di controllo

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

Allegati

Presentazione di PowerPoint

Filmati

Riferimenti:

- Attacchi informatici alle aziende: Siete a rischio?
- I crescenti rischi strategici dei cyberattacchi
- 10 rischi comuni di sicurezza informatica per le aziende
- Controlli interni e sicurezza dei dati: come sviluppare controlli che soddisfino le vostre esigenze di sicurezza IT
- Controlli interni sui sistemi informativi

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.