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

InCyT træningsmoduler

Informationssikkerhed for ledere **Enhed 1 uge 2** **Enhedsnavn: Introduktion til informationssikkerhed, interne kontrolsystemer**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑**Andet**
Læringsansvarlig	• Gabriel Vladut • Valentin Istratie
Læringsaktivitetsmål	1. Introduktion til Erasmus+ InCyT- projekt 2. Cyber-sikkerhed 3. Begreber, definitioner og udtryk 4. Intern kontrolstandard 5. Udarbejdelse af cybersikkerhedskontrol
Færdigheder, der skal opnås	• TS3 netværkssikkerhed • TS4 Penetration (udnyttelige sårbarheder) test • SS3 Kognitiv og adfærdsanalyse
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?***
	• Få bevidsthed om cybersikkerhed og lær, hvad et cybersikkerhedsangreb er • Lær metoder til at forhindre databrud, der bruges af angribere til at få adgang til følsomme data og udnytte organisatoriske sårbarheder • Lær, hvordan du fortsætter i tilfælde af et cybersikkerhedsangreb

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

Kort information om modulet

Beskrivelse
Informationssikkerhed, interne kontrolsystemer er vigtige og truer meget ofte cybersikkerhed Beskyttelse af informations- og informationssystemer mod uautoriseret adgang eller ændring af information, uanset om det er i opbevaring, behandling eller transit, og mod denial of service til autoriserede brugere. Informationssikkerhed omfatter de foranstaltninger, der er nødvendige for at opdage, dokumentere og imødegå sådanne trusler. Informationssikkerhed er sammensat af computersikkerhed og kommunikationssikkerhed. Også kaldet INFOSEC. Se også kommunikationssikkerhed; computersikkerhed; informationssikkerhed; informationssystem. Interne kontroller bruges af ledelses-, it-sikkerheds-, økonomi-, regnskabs- og driftsteams for at nå følgende mål: 1. Sikre pålideligheden og nøjagtigheden af finansielle oplysninger – Interne kontroller sikrer, at nøjagtige, opdaterede og fuldstændige oplysninger afspejles i regnskabet. systemer og økonomiske rapporter. Eleverne kunne blive informeret om sådanne aspekter ved at læse den tilsvarende tekst, se streaming webinarer og løse øvelser i eget tempo. Alle disse dokumenter er på den digitale interaktive projektplatform. Eleverne kan teste deres svar på selvevalueringsøvelser. Svarene på andre øvelser skal gemmes på det tilsvarende diskussionsforum og diskuteres med mentoren på det fælles tilrettelagte møde en gang om ugen. Eleven kan arbejde sammen med andre og vejlede især under møderne. De vil blive støttet til at udvikle e-portfolio, der er vigtig for refleksion og evaluering af træningen.

Lærematerialets indhold

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

Informationssikkerhed

Informationssikkerhed handler om at beskytte information og computersystemer mod uautoriseret adgang, brug, offentliggørelse, afbrydelse, ændring eller ødelæggelse.

ISO/IEC27002/2013 beskæftiger sig med informationssikkerhed gennem sine tre hovedkomponenter: fortrolighed, integritet og tilgængelighed. Fortrolighed sikres ved at kryptere oplysningerne. Integritet opnås gennem spredningsmekanismer og algoritmer.

Tilgængeligheden sikres ved at styrke sikkerheden på computersystemets netværk eller netværk og sørge for backup. Informationssikkerhed er et sæt praksisser designet til at beskytte data.

Informationssikkerhed er ikke begrænset til computersystemer eller information i dens digitale eller elektroniske form. Det gælder derimod for alle forhold relateret til sikkerhed, sikkerhed og beskyttelse af data eller information, uanset deres form.

Informationssikkerhed kan ikke defineres som synonymt med computersikkerhed, system- og netværkssikkerhed, informationsteknologisikkerhed, informationssystemer eller informations- og kommunikationsteknologi. Hvert af disse udtryk refererer til et andet emne, selvom det fælles punkt refererer til informationssikkerhed i nogle af dets former (her taler vi om dens elektroniske version): derfor er de alle underområder af informationssikkerhed.

I det 21. århundrede har de fleste organisationer et computersystem forbundet til internettet og udveksler information gennem det. Information kan bringes til at passere gennem en sammenkobling af netværk. Som følge heraf er denne sammenkobling så meget desto mere udsat for malware-risici fra dem, der ønsker at få fat i følsom information, der handler indefra (kopierer information, bruger ondsindet kode) eller udefra.

For at imødegå disse risici kræver informationssikkerhed udvikling af koncepter som datatagging, offentlig nøglekryptering (PKI) og multi-level security (MLS). Udover problemerne med at forbinde netværk, er det i stigende grad nemt at flytte store mængder information (og dette på en måde, der er relativt svær at opdage i tilfælde af hacking), men også at transportere den fysisk via USB-sticks eller hukommelseskort.

Derfor er computersystemer, der indeholder følsomme oplysninger, i stigende grad designet som et System high mode-miljø, i mange tilfælde i form af separate netværk uden forbindelse til andre netværk og uden USB-porte. Tre informationsfølsomhedskriterier er almindeligt accepterede: Tilgængelighed, Integritet og Fortrolighed. En fjerde bruges også ret hyppigt (under forskellige navne): Sporbarhed, Ansvarlighed, Audibility (med reference til computerrevisioner) eller Evidens. Et femte kriterium anvendes også: Ikke-afvisning , som sikrer udveksling af beskeder mellem

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

afsender og modtager.

Cyberangreb og kompetencerammen

En kompetenceramme bruges regelmæssigt af virksomheder til at forstå deres færdighedsbaserede krav, nødvendige kompetencer, medarbejdernes færdigheder og huller.

Når en kompetenceramme udvikles under hensyntagen til virksomhedens profil og medarbejderinteresser, kan den forbedre præstationer og skabe klarhed for hvert enkelt rollekrav og udvikle talenter på arbejdspladsen. I de senere år, på grund af mange cyberangreb , er cybersikkerhedsrammer primært vedtaget af store organisationer (virksomheder, ngo'er og andre enheder) eller af statslige aktører.

Et vellykket cyberangreb kan forårsage stor skade på en virksomheds forretning. Det kan påvirke dens bundlinje såvel som virksomhedens forretningsstatus og forbrugertillid. Virkningen af et sikkerhedsbrud kan opdeles i tre kategorier: økonomisk, omdømme og juridisk.

Cyberangreb

Cyberangreb resulterer ofte i betydelige økonomiske tab som følge af tyveri af virksomhedsoplysninger, finansielle oplysninger (f.eks . bankoplysninger eller betalingskortoplysninger), penge, transaktionsforstyrrelser (f.eks . manglende evne til at handle online), tab af forretning eller af kontrakten. Virksomheder, der har været udsat for et cyberbrud, vil generelt bruge penge på at reparere berørte systemer, netværk og enheder.

Cyberangreb kan skade en virksomheds omdømme og den tillid, kunderne har til virksomheden. Dette kan føre til mistede kunder, tabt salg og reduceret fortjeneste. Effekten af omdømmeskader kan endda påvirke virksomhedens leverandører eller påvirke forholdet til partnere, investorer og andre tredjeparter, der er involveret i virksomhedens forretning.

Så databeskyttelses- og privatlivslovgivningen kræver sikkerhedsstyring af alle personlige data, som virksomheden opbevarer (om dets egne medarbejdere eller kunder). Hvis disse data ved et uheld eller bevidst kompromitteres, og virksomheden ikke implementerer tilstrækkelige sikkerhedsforanstaltninger, kan den blive udsat for lovmæssige sanktioner.

Risici i virksomheden

Det er vigtigt at styre dine risici derefter. Efter et angreb har fundet sted, kan et effektivt cybersikkerhedsværktøj eller hændelsesresponsplan, dvs. brug af en cyberkonsulent, hjælpe med at:

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

- reducere virkningen af angrebet
- rapportere hændelsen til den relevante myndighed
- rense de berørte systemer
- få din virksomhed op at køre på kortest mulig tid.

Det er nødvendigt at investere i at træne og uddanne brugere inden for cybersikkerhed for at undgå angreb og løbende udvikle bevidstheden om en cyberstrategi i ens organisation.

Cybersikkerhedsramme

En cybersikkerhedsramme er et sæt af bedste praksis og dokumenterede processer, der bruges til at udvikle it-sikkerhedspolitikker i en organisation. Men i modsætning til traditionel politik, der er strengt relateret til det juridiske domæne, bør en cybersikkerhedsramme også indeholde dokumenterede eksempler på problemer, der skal undgås med disse politikker, og på passende processer og måder at implementere sikkerhedspolitikkerne beskrevet i rammen.

Det er både en guide til medarbejdere og brugere samt et overbevisende kompendium af bedste sikkerhedspraksis, som kan konsulteres af autoriserede eksterne parter (såsom myndigheder). En kompetenceramme for cybersikkerhed kan også hjælpe med bedre at vurdere de nødvendige kompetencer for at undgå angreb, huller og afhjælpningsforanstaltninger.

Cybersikkerhed

På trods af øget bevidsthed og dristige indsats er den meget betydelige og voksende mangel på cybersikkerhedsprofessionelle i Den Europæiske Union og medarbejderes viden og færdigheder til at undgå cyberangreb verden over kendt, og denne mangel udgør fortsat store problemer for den offentlige og private sektor .

2019 CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) undersøgelse anslår, at der er 2,8 millioner cybersikkerhedsprofessionelle globalt, mens forskellen faktisk er 4,07 millioner.

Undersøgelsen bemærker, at den nuværende forskel i Europa er 291.000, og dette antal er fordoblet i forhold til tidligere år. Mange lande med højt udviklet ekspertise foretrækker at skabe deres eget sæt af regler og dokumenter, men mange lande og små og mellemstore virksomheder (SMV'er) har brug for hjælp i denne sammenhæng.

Social ingeniørkunst

- det betyder at manipulere mennesker (ofte ved hjælp af psykologiske metoder) for at få

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

adgang til data, dokumenter og information af interesse for angriberen.

- er en af de vigtigste trusler mod informationssikkerheden i dag og er en effektiv form for cyberkriminalitet.
- kunne have farlige konsekvenser, for eksempel databrud, mere end nogen anden form for angreb.
- angrebene har et økonomisk formål, og dermed har organisationer tabt betydelige pengebeløb.
- det er særligt farligt, fordi det er mere afhængigt af menneskelige fejl end på sårbarheder i software og operativsystemer.

Virksomhederne:

- de kunne lide tabt produktivitet, et fald i medarbejdernes moral og vanskeligheder med at komme sig.
- de har skade på omdømmet, fordi kunderne ikke er overbeviste om, at organisationen kan beskytte sig selv.
- ofte nødt til at udløse en gammel hændelsesreaktion.
- skal levere sikkerhedssoftware til at forhindre fremtidige angreb.
- de ville ofte skulle omskole medarbejdere for at være klar til angreb.

S **ocial ingeniørvirksomhed; Træning (cyberbevidsthed)**

- af medarbejdere og ledere, for hvem det er vigtigt at anerkende socialtekniske angreb, fordi risikoen for at blive offer er høj.
- kunne inkluderes i fællesskabs-, individ- og borgersikkerhedsbevidsthedsprogrammer og beskytte enkeltpersoner og deres organisation.
- er især mangelfuld i SMV'er, der har færre ressourcer, så de bør hjælpes til at tage cyberbevidsthedstræning seriøst og give medarbejderne mulighed for at tage den.

Træning og vejledning

Iværksættere, herunder fremtidige, har brug for komplekse måder at tænke på og evnen til at forstå og integrere viden fra forskellige sektorer, hvilket kræver tværfaglig læring. Komplekse tekniske problemer kræver at skabe en tværfaglig situation på en næsten naturlig måde.

I en tværfaglig tilgang bør eleverne integrere information fra forskellige discipliner og områder. De udvikler en tværfaglig forståelse, lærer at integrere ekspertiseområder og disciplinspecifikke måder at tænke på.

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

Dette øger kognitive færdigheder og kritisk tænkning mere end gennem enkelt disciplinære midler.

Iværksætterkompetencer og vejledning

Vurdering af elevers præstationer med hensyn til at udvikle entreprenørielle færdigheder kan tage et holistisk syn, herunder et kig på læringsmiljøet og læringsresultater, og lette interaktiv, effektiv og aktiv læring.

Mentoring er en erfaren metode til at understøtte mere individuel læring og til at opnå personlige og karrieremæssige kompetencer til nye erhverv. Der er forskning i resultaterne af mentoring generelt, men der er lidt forskning i mentoring.

Mentoring giver en række fordele for medarbejdere, der uddanner sig i virksomheder. Tværfaglig teammentoring har fået betydning i de senere år, hvilket afspejler behovet for en ændring i orienteringen af mentoring, da forskellige iværksætterudviklinger og -områder i stigende grad er tværfaglige.

Tværfaglig vejledning og netværk af mentorer kan skabe synergi i grupper, skabe innovative ideer og komplekse løsninger på udfordringer og skabe muligheder for samarbejde og arbejde.

Begreber, definitioner og udtryk

Udtrykket " **cyberspace** " blev opfundet i 1982 af William Gibson. Udtrykket trådte ind i hverdagen i 1990'erne med fremkomsten af World Wide Web

cyberinfrastrukturer - informations- og kommunikationsteknologiske infrastrukturer, bestående af it-systemer, relaterede applikationer, netværk og elektroniske kommunikationstjenester;

cyberspace - det virtuelle miljø, genereret af cyberinfrastrukturer, herunder det informationsindhold, der behandles, lagres eller transmitteres, samt de handlinger, der udføres af brugerne i det;

cybersikkerhed - normaliteten som følge af anvendelsen af et sæt proaktive og reaktive foranstaltninger, der sikrer fortroligheden, integriteten, tilgængeligheden, ægtheden og ikke-afvisningen af information i elektronisk format, af offentlige eller private ressourcer og tjenester i cyberspace .

Proaktive og reaktive foranstaltninger kan omfatte sikkerhedspolitikker, koncepter, standarder og retningslinjer, risikostyring, trænings- og bevidstgørelsesaktiviteter, implementering af tekniske løsninger til beskyttelse af cyberinfrastrukturer, identitetsstyring, konsekvensstyring;

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

cyberforsvar - handlinger udført i cyberrummet med det formål at beskytte, overvåge, analysere, opdage, imødegå aggressioner og sikre en rettidig reaktion mod trusler mod cyberinfrastruktur, der er specifik for nationalt forsvar;

operationer i computernetværk - den komplekse proces med planlægning, koordinering, synkronisering, harmonisering og udførelse af handlinger i cyberspace til beskyttelse, kontrol og brug af computernetværk for at opnå informationsoverlegenhed, samtidig med neutralisering af modstanderens kapaciteter;

cybertrussel - omstændighed eller begivenhed, der udgør en potentiel fare for cybersikkerhed;

cyberangreb - fjendtlig handling udført i cyberrummet, der sandsynligvis vil påvirke cybersikkerheden;

cyberhændelse - begivenhed, der finder sted i cyberspace, hvis konsekvenser påvirker cybersikkerheden;

cyberterrorisme - overlagte aktiviteter udført i cyberspace af politisk, ideologisk eller religiøst motiverede individer, grupper eller organisationer, der kan forårsage materiel ødelæggelse eller ofre, som sandsynligvis vil forårsage panik eller terror;

cyberspionage - handlinger udført i cyberrummet med det formål at indhente uautoriseret fortrolig information i en statslig eller ikke-statslig enheds interesse;

computerkriminalitet - alle de handlinger, der er fastsat i straffeloven eller andre særlige love, der udgør en social fare og begås med skyld, gennem eller på cyberinfrastrukturer;

sårbarhed i cyberspace - svaghed i design og implementering af cyberinfrastruktur eller relaterede sikkerhedsforanstaltninger, der kan udnyttes af en trussel;

sikkerhedsrisiko i cyberspace - sandsynligheden for, at en trussel vil materialisere sig, udnyttelse af en specifik sårbarhed, der er specifik for cyberinfrastrukturer;

risikostyring - en kompleks, kontinuerlig og fleksibel proces til at identificere, evaluere og imødegå cybersikkerhedsrisici, baseret på brugen af komplekse teknikker og værktøjer, for at forhindre tab af enhver art;

identitetsstyring - metoder til at validere personers identitet, når de får adgang til visse cyberinfrastrukturer;

Komponenterne i intern kontrol

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

I henhold til INTOSAI GOV 9100 Standard "Guidelines for Internal Control Standards". I 2001 blev det på kongressen for International Organisation of Supreme Audit Institutions (INCOSAI) besluttet at opdatere INTOSAI-retningslinjerne for interne kontrolstandarder i den offentlige sektor, der oprindeligt blev udgivet i 1992, ved at indføre alle aspekter af den seneste udvikling i dokumentet. inden for området intern kontrol og at integrere en række elementer i COSO-modellen (Internal Control – Integrated Framework).

Ved at integrere det i retningslinjerne - en aktivitet udført af den operative gruppe af INTOSAI's interne kontrolstandarder - blev et forsøg på at opnå en samlet forståelse af, hvordan det nye interne kontrolsystem fungerer, af repræsentanterne for de øverste revisionsinstitutioner. .

"INTOSAI Guidelines for Internal Control Standards in the Public Sector" er en del af INTOSAI GOV-kategorien (good governance guidance) og anses for yderst nyttige både for ledere i den offentlige sektor, der skal implementere det interne kontrolsystem og eksterne offentlige revisorer, som skal kende dette system og evaluere det.

Interne kontrolstandarder

I henhold til INTOSAI GOV 9100-retningslinjerne består intern kontrol af fem indbyrdes afhængige komponenter (identisk med COSO-modellen):

- Kontrolmiljø
- Risikovurdering
- Kontrolaktiviteter
- Information og kommunikation
- Overvågning

Intern kontrol er designet til at give rimelig sikkerhed for opnåelsen af institutionens overordnede mål. Mål, der er klart fastsat af enhedens ledere, og passende planlægning af budgettet er en obligatorisk betingelse for en effektiv intern kontrol.

Kontrolmiljø

Kontrolmiljøet omfatter den generelle holdning, bevidsthed og handlinger truffet af ledelsen og de personer, der har til opgave at styre det interne kontrolsystem og dets betydning i virksomheden. Kontrolmiljøet sætter tonen i organisationen og påvirker kontrolbevidstheden på personaleniveau.

Det repræsenterer grundlaget for alle andre komponenter af intern kontrol, hvilket sikrer en disciplin i organisationen, der skal respekteres, og en struktur i enheden, så det interne kontrolsystem kan anvendes effektivt. Det interne kontrolmiljø er et effektivt værktøj til at

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

forhindre korruption og svig.

De elementer, der definerer kontrolmiljøet, er:

- personlig og professionel integritet, de etiske værdier, der er etableret af ledelsen for alle medarbejdere, herunder en permanent støttende holdning til intern kontrol;
- en vedvarende ledelsesmæssig bekymring for personalets kompetence;
- " tonen givet fra oven" (ledelsens filosofi og aktivitetsstil);
- enhedens organisatoriske struktur;
- HR politik og praksis.

Typer af cybersikkerhedskontrol

Cybersikkerhedskontrol er mekanismer, der bruges til at forhindre, opdage og afbøde cybertrusler og -angreb. Mekanismer spænder fra fysisk kontrol såsom sikkerhedsvagter og overvågningskameraer til tekniske kontroller, herunder firewalls og multi-faktor autentificering.

En ensidig tilgang til cybersikkerhed er simpelthen forældet og ineffektiv. Og fordi det er umuligt at forhindre alle angreb i nutidens trusselslandskab, bør organisationer vurdere deres aktiver baseret på deres betydning for virksomheden og etablere kontroller i overensstemmelse hermed.

En tilføjelse til udfordringen er, at det er usandsynligt, at medarbejdere følger overholdelsesregler, hvis der implementeres strenge kontroller på tværs af alle virksomhedens aktiver. Sværhedsgraden af en kontrol bør direkte afspejle aktiv- og trusselslandskabet.

Konsekvenserne af, at en hacker blotlægger tusindvis af personlige kundedata gennem en cloud-database, kan for eksempel være langt større, end hvis en medarbejders bærbare computer kompromitteres.

Cybersikkerhedskontrol

"Der er mange forskellige måder at anvende kontroller baseret på arten af det, du forsøger at beskytte," sagde Joseph MacMillan, forfatter til Infosec Strategies and Best Practices og cybersikkerhed globalt sort bælte hos Microsoft.

"Hvad er arten af den trussel, du forsøger at beskytte dig imod?

Er det en ondsindet skuespiller?

Eller er det et ødelæggende angreb?"

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

Sikring af informationsaktiver

Det henviser til implementeringen af passende informationssikkerhedskontroller for aktiver. Vi ønsker at sikre, at vi fokuserer på stærke og effektive ideologier at forstå for at vælge de passende kontroller, hvilket betyder, at aktivet anses for "sikkert nok" baseret på dets kritik og klassificering. Der er forskellige klasser, der opdeler kontroltyperne:

- Administrative/ledelsesmæssige kontroller er virksomhedens politikker og procedurer. De er ikke så "seje" som en ny softwarekontrol, men de eksisterer for at give struktur og vejledning til enkeltpersoner og andre medlemmer af organisationen, for at sikre, at ingen får bøder eller forårsager et brud.
- Fysiske kontroller, der begrænser adgangen til systemer på en fysisk måde.
- Tekniske/logiske kontroller er dem, der begrænser adgang baseret på hardware eller software, såsom kryptering, fingeraftrykslæsere, autentificering eller betroede platformsmoduler (TPM).

De begrænser ikke adgangen til fysiske systemer, som fysiske kontroller gør, men derimod adgang til data eller indhold. Operationelle kontroller er dem, der involverer mennesker, der udfører processer på en daglig basis. Eksempler kan omfatte bevidsthedstræning, aktivklassificering og logfilgennemgang.

Typer af kontroller

Forebyggende kontroller findes for at forhindre en handling og inkluderer firewalls, hegn og adgangstilladelser.

Detektivkommandoer udløses kun under eller efter en hændelse, såsom videoovervågning eller indtrængendetekteringssystemer. Afskrækkende midler afskrækker trusler fra at forsøge at udnytte en sårbarhed, såsom et "vagthund" eller hundeskilt . Korrigerende kontroller er i stand til at handle fra en stat til en anden. Fejl åben og fejl lukket kommandoer behandles her.

Gendannelseskommandoer får noget tilbage fra et tab, såsom gendannelse af en harddisk. Kompenserende kontroller er dem, der forsøger at kompensere for mangler i andre kontroller, såsom regelmæssig gennemgang af adgangslogfiler. Dette eksempel er også en detektivkontrol, men kompensationskontroller kan være af forskellige typer.

Rækkefølgen af kontroller

Det afskrækker skuespillere fra at forsøge at få adgang til noget, de ikke burde være. Afvis/forhindre adgang gennem en forebyggende kontrol såsom adgangstilladelser eller

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

godkendelse.

Registrer risiko ved at sørge for at registrere detektion, f.eks. med endpoint-beskyttelsessoftware. Forsink processen fra at gentage risikoen igen, f.eks. med en "for mange forsøg"-funktion til at indtaste en adgangskode.

Ret situationen ved at reagere på kompromiset, f.eks. med en hændelsesplan. Gendan fra en kompromitteret tilstand, såsom en backup-generator, der gendanner tilgængeligheden til en server.

Derudover bør vi inden for løbende forbedringer overvåge værdien af hvert aktiv for eventuelle ændringer. Årsagen er, at vi muligvis skal genoverveje vores kontroller for at beskytte disse aktiver, hvis de bliver mere eller mindre værdifulde over tid eller under visse større begivenheder i din organisation.

Kontrol og genopretning

Når vi ser på kontroller, bør vi også tænke på inddrivelse, vi ønsker at være i stand til at komme os fra eventuelle ugunstige situationer eller ændringer i aktiver og deres værdi. Som eksempler taler vi om backups, redundans, gendannelsesprocesser og lignende.

Et koncept, der skal huskes, især i æraen med cloud, SaaS, PaaS, IaaS, tredjepartsløsninger og alle andre former for "en andens computer" er at sikre, at Service Level Agreements (SLA'er) er klart definerede og har maksimal tilladt nedetid aftaler, samt bøder for manglende overholdelse af disse aftaler. Dette er et eksempel på kompenserende kontrol.

Spørgsmål :

Spørgsmål Diskussionsforum skal besvares med en kort forklaring. Svarene vil blive drøftet med mentoren under mentorsessionerne

1. Heks er risiciene i virksomheden for cyberangreb ?
2. Kald nogle typer cybersikkerhedskontroller
3. Heks er interne kontrolstandarder
4. Sådan kontrollerer og gendanne oplysninger

Selvevalueringsspørgsmål. Efter besvarelsen kan eleven se resultaterne og sammenligne dem med disse gemt på platformen

- Risici i virksomheden for cyberangreb
- Interne kontrolstandarder og rutiner
- Kontrolmiljø

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

Vedhæftede filer

PowerPoint-præsentation

Video film

Referencer:

- Cyberangreb på virksomheder: Er du i fare?
- De stigende strategiske risici ved cyberangreb
- 10 almindelige cybersikkerhedsrisici for virksomheder
- Interne kontroller og datasikkerhed: Sådan udvikles kontroller, der opfylder dine IT-sikkerhedsbehov
- Intern kontrol over informationssystemer

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.