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

InCyT træningsmoduler

Informationssikkerhed for ledere **Enhed nr. og Uge nr.: Enhed-2 Uge-4** **Navn på enhed: Informationssikkerhedsstyring -2**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑ **Andet** Streaming webinar, tekst, selvevalueringsøvelser, øvelser med svar på diskussionsfora og blive diskuteret med træner/mentor
Læringsansvarlig	• Fatma Gökdemir • Ali Gökdemir
Læringsaktivitetsmål	1. Trussels- og sårbarhedsvurdering 2. Trussels- og sårbarhedshåndtering 3. Typer af sårbarhedsvurdering 4. Cyberkontinuitet i driften 5. Cyberaktiv 6. Evaluering af effektiviteten af cybersikkerhedspolitikker
Færdigheder, der skal opnås	• ER 1 • ER 3 • MS 5
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?*** • Mellemliggende computerfærdigheder

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

Kort information om modulet

Beskrivelse
Styring af aktiver har en vigtig plads inden for rammerne af ISO 27001 Information Security Management System. Faktisk er identifikation og klassificering af informationsaktiver et af de første trin i opsætning af informationssikkerhed. At identificere og tildele værdi til aktiver i en organisation er et grundlæggende trin i risikoanalyseprocessen. Der udarbejdes en aktivopgørelse for at tildele værdi til aktiverne. En sonderende undersøgelse, der dækker alle medarbejdere, bør udføres forud for aktivopgørelsen. Med denne undersøgelse er afdelingens aktivopgørelse udforsket og listet med mulige risici og fortrolighedsgrad. Aktivopgørelse bør foretages én efter én på basis af de omfattede processer. Mens du forbereder aktivopgørelsen; aktivgruppen, miljøet, som det angivne aktiv befinder sig i, klassifikationskoden bestemmes, og aktivværdien (fortrolighed, integritet, tilgængelighed) beregnes. I henhold til beregningsresultatet fastlægges prioritetsstatus, og handlingsbeslutninger træffes. Når aktivopgørelsesarbejdet er afsluttet, udarbejdes en detaljeret inventarliste for de fundne software-hardware-opgørelser. Betingelser/kontroller vedrørende asset management i ISO27001-standarden er samlet under bilag A.8. I dette modul vil vi undersøge betingelserne for ansvar for aktiver defineret i A.8.1.

Lærematerialets indhold

1. Vurder ledelse af informationssikkerhed

I den første fase af asset management ville det være nyttigt først at afsløre og liste, hvilke aktiver vi har. Hvad en institution har eller ikke har, bør først vides. Så skal deres ejerskab defineres. Ingen forretning eller transaktion bør efterlades uden opsyn. Derefter bør reglerne for brugen af disse aktiver fastlægges.

For detaljer om emnet bør ISO27002-standarden undersøges. Forventningerne til Asset Management i ISO27002 er inkluderet i standardens 8. artikel:

Asset management og ansvar for aktiver

Formål: At identificere organisationens aktiver og definere passende beskyttelsesansvar.

1. Aktivbeholdning

Kontrol: Aktiver relateret til informations- og informationsbehandlingsfaciliteter bør identificeres, og en opgørelse over disse aktiver bør laves og vedligeholdes.

Anvendelsesvejledning: En organisation bør identificere relevante aktiver i informationslivscyklussen og dokumentere deres betydning. Informationens livscyklus bør omfatte oprettelse, behandling, lagring, transmission, sletning og destruktion. Dokumentation bør vedligeholdes i overensstemmelse med eksisterende opgørelser eller specifikt.

Aktivbeholdning; skal være aktuelle, konsistente, nøjagtige og kompatible med andre opgørelser.

Aktivejerskab bør allokeres for hvert identificeret aktiv (se artikel 2), og dets klasse bør bestemmes.

Andre oplysninger: Aktivbeholdning hjælper med at give effektiv beskyttelse og kan også være nødvendig til andre formål, såsom sundhed og sikkerhed, forsikring eller økonomiske (aktivforvaltning) årsager.

ISO/IEC 27005[11]-standarden giver eksempler på aktiver, som organisationen muligvis skal overveje, når aktiver identificeres. Processen med at udarbejde en aktivopgørelse er en vigtig forudsætning for risikostyring (se ISO/IEC 27000 og ISO/IEC 27005[11]).

2. Ejerskab af aktiver

Kontrol: Ejertildelinger skal foretages for alle aktiver, der opbevares på lager.

Anvendelsesvejledning : Enkeltpersoner og andre enheder med godkendt ledelsesansvar for aktivets livscyklus er berettiget til at blive udpeget som aktivejere.

En proces bruges ofte til at sikre, at ejerskab af aktiver bestemmes rettidigt. Ejerskab skal fastlægges, når aktiver oprettes eller overføres til organisationen. Aktivejeren bør være ansvarlig for den korrekte forvaltning af aktivet i hele aktivets livscyklus.

Aktivejer:

a) Sørg for, at aktivbeholdning er registreret,

b) Sikre, at aktiver er korrekt klassificeret og beskyttet,

c) Definere og periodisk gennemgå begrænsninger for adgang til væsentlige aktiver og deres klassificering under hensyntagen til den gældende adgangskontrolpolitik,

d) Sikre, at der tages passende skridt til at slette eller destruere aktiver.

Andre oplysninger : Det kan være en person eller en enhed med godkendelse til ledelsesansvar at kontrollere et aktiv i hele dets livscyklus. Den identificerede ejer har ingen ejerandel i aktivet.

Rutineopgaver kan uddelegeres; (f.eks. en depotbank, der dagligt passer på et aktiv), men ansvaret påhviler aktivejeren.

At identificere grupper af aktiver i komplekse informationssystemer kan være nyttigt til at levere funktioner sammen. I dette tilfælde er denne tjenesteejer ansvarlig for leveringen af tjenesten, herunder driften af aktiverne.

3. Acceptabel brug af aktiver

Kontrol: Regler vedrørende acceptabel brug af information og aktiver relateret til informations- og informationsbehandlingsfaciliteter bør fastlægges, dokumenteres og implementeres.

Ansøgningsvejledning : Medarbejdere og eksterne brugere, der bruger eller har adgang til organisationens aktiver, bør gøres opmærksomme på informationssikkerhedskravene for organisationens aktiver i forbindelse med informations- og informationsbehandlingsfaciliteter og -ressourcer. Disse brugere bør være ansvarlige for brugen af alle informationsbehandlingsressourcer og for enhver brug, der sker under deres eget ansvar.

4. Tilbagelevering af aktiver

Kontrol: Alle medarbejdere og brugere af eksterne parter skal returnere alle virksomhedsaktiver i deres besiddelse ved ophør af ansættelse, kontrakt eller aftale.

Ansøgningsvejledning: Opsigelsesprocessen bør formuleres, så den omfatter tilbagelevering af ejerskab af alle tidligere tildelte fysiske og elektroniske aktiver eller deponeringer i organisationen.

Når en medarbejder eller ekstern bruger køber eller bruger organisationens udstyr, følges procedurer for at sikre, at alle relevante oplysninger overføres til organisationen og slettes sikkert fra udstyret.

Hvor en medarbejder eller ekstern bruger har oplysninger, der er vigtige for den løbende drift, skal disse oplysninger dokumenteres og overføres til organisationen.

I opsigelsesperioden skal organisationen; kontrollere uautoriseret kopiering af relateret information, såsom intellektuel ejendomsret, af opsagte medarbejdere og entreprenører.

2. Trussel og sårbarhed vurdering og ledelse

Næsten enhver organisation har følsomme og værdifulde aktiver, som skal beskyttes. Det er dog ikke alle organisationer, der har en omfattende og gennemtænkt strategi til at beskytte disse aktiver. Inden for cybersikkerhed er sårbarhedshåndteringsstrategier grundlaget for et stærkt forsvar. Typisk er strategier til håndtering af sårbarheder designet til at hjælpe en organisations systemer, netværk, applikationer osv. Den anvender en holistisk og kontinuerlig tilgang til håndtering af sikkerhedssårbarheder i Disse sårbarheder identificeres, evalueres og rettes så hurtigt som muligt.

Sikkerhedstrusler og -tendenser udvikler sig konstant, hvilket kræver en effektiv, forebyggende indsats for at håndtere trusler og sårbarheder, der kan kompromittere dine data. For at identificere alle potentielle mål for et brud eller angreb skal dets risiko først mindskes ved at udføre en aktivopgørelse. Målene skal derefter klassificeres og løbende overvåges for nye potentielle sårbarheder. En trusselsmodel, der identificerer organisationens mest værdifulde aktiver med høj risiko, bør derefter udvikles og testes. Det primære formål med trussels- og sårbarhedstestprocessen (vurdering) er bedst at forstå aktivers kritiske karakter, sårbarhederne for disse aktiver og reducere de nødvendige foranstaltninger til effektivt at beskytte disse aktiver.

2.1. Hvad er sårbarhedsvurdering?

Sårbarhed vurdering er _ processen med at identificere , identificere , klassificere og prioritering sårbarheder i computeren systemer , applikationer og netværksinfrastrukturer . _ _

Sårbarhed vurderinger også give en organisation med det viden , bevidsthed og risikobaggrund nødvendig til forstå og svare til trusler til dens miljø . En sårbarhed vurdering behandle mål til identificere trusler og det risici, de udgør . Ofte involverer de det brug af automatiseret afprøvning værktøjer , såsom netværkssikkerhed _ scannere , hvis resultater er opført i en sårbarhed vurdering rapport .

Organisationer af enhver størrelse, endda personer med øget risiko for cyberangreb , kan drage fordel fra en eller anden form for sårbarhed vurdering , men stor organisationer og Andet typer af organisationer udsat til igangværende angreb vilje fordel mest fra sårbarhed analyse .

Fordi sårbarheder kan tillade hackere til gevinst adgang til IT- systemer og applikationer , er det kritisk til organisationer til identificere og rette op sårbarheder før de er udnyttet . En omfattende sårbarhed vurdering kombineret med et ledelsesprogram kan hjælpe virksomheder forbedre det deres sikkerhed _ systemer .

2.2. Vigtigheden af sårbarhedsvurderinger

Til bedre belyse det vigtigheden af sårbarhed vurdering , lad os overveje det igennem det fysiske øjne _ ejendom ejer . Hvis du eje en værdifuld bygning , dig sandsynligvis træffe en række foranstaltninger _ til beskytte det: Dig vedligeholde det, forsikre det og sørg for _ døre , vinduer , er låst , og alarmer er aktiveret . Alle disse _ trin kan betegnes som styring risikoen for _ det ejendom og dens indhold .

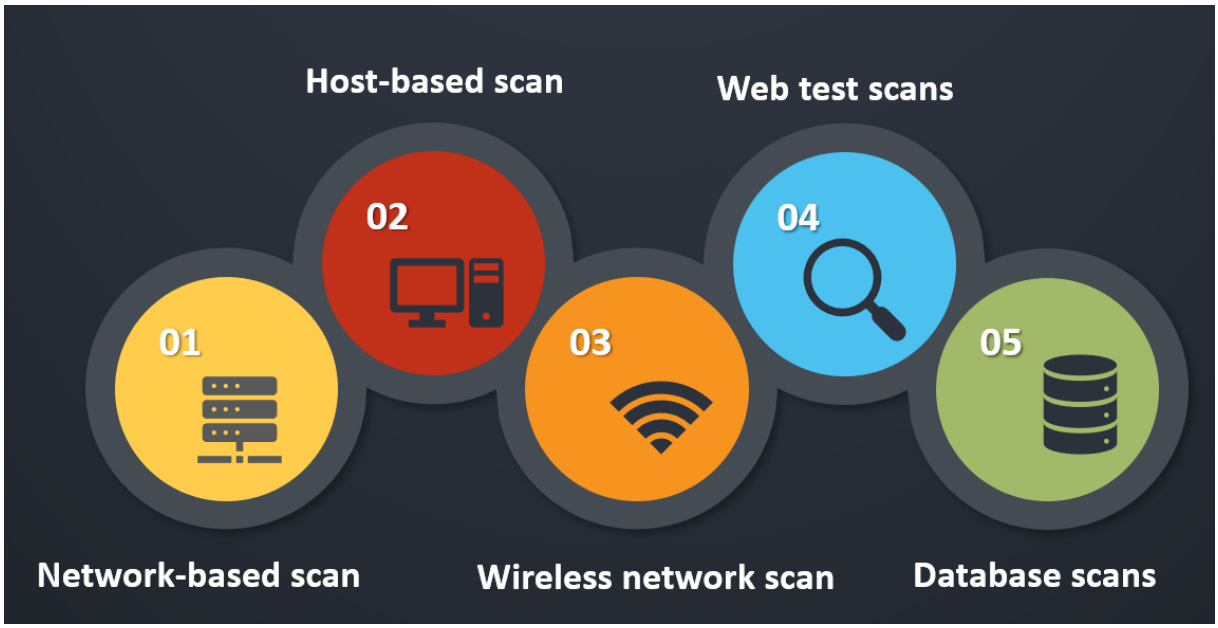
Nu hvad hvis du kunne leje nogen at teste og rapporter om din alarmer og ydre forsvar ? Cybersikkerhed sårbarheder er henvendt sig i en lignende måde . Sårbarhed ledelse er en overordnet og igangværende strategi , mens sårbarhed vurderinger er en specifik værktøj brugt i dette bredere ledelse strategi .

En sårbarhed vurdering giver en organisation med detaljeret Information om nogen sikkerhed svagheder i dens miljø . Det også giver vejledning om hvordan vurdere det risici forbundet med Disse svagheder . Dette behandle giver det organisation med en bedre forståelse af det aktiver , sikkerhed mangler og samlet risiko, reducerende det sandsynligheden for en cyberkriminel brud dens systemer og fangst det forretning af vagt .

2.3. Typer af sårbarhedsvurdering

Sårbarhed vurderinger opdage forskellige system eller netværkssårbarheder . _ Dette midler at det vurdering behandle omfatter ved hjælp af en række værktøjer , scannere og metoder til identificere sårbarheder , trusler og risici .

Nogle af de forskellige typer af sårbarhed vurdering scanninger inkludere (figur 1):



Figur 1. Typer af sårbarhed vurdering

- **Netværksbaseret _ scanninger** er Brugt til identificere potentiel netværkssikkerhed _ angreb . Dette type scanning kan også _ opdage sårbar systemer på kablet eller trådløs netværk .
- **Værtsbaseret _ scanninger** er Brugt til finde og identificere sårbarheder i servere , arbejdsstationer eller _ andre netværksværter . _ Dette type scanning _ som regel undersøger havne og tjenester , som også kan ses i netværksbaseret _ scanninger . Det tilbyder dog større sigtbarhed ind i det konfiguration indstillinger og lappe historik for scannet systemer , herunder eftermæle systemer .
- **Trådløse netværksscanninger af** en organisations Wi -Fi- netværk tit fokus på angreb punkter i _ trådløs netværksinfrastruktur . _ I tilføjelse til identificere Rogue adgang point , trådløs netværksscanning kan også _ verificere at en virksomheds netværk er sikkert konfigureret .
- **Web scanning test** websteder til opdage kendte softwaresårbarheder _ og fejlkonfigurationer i applikationer , netværk eller webapplikationer .

- **Databasescanninger** kan identificere _ svag pletter i en database til forhindre ondsindet angreb.SQL indsprøjtning angreb .

2.4. Sårbarhedsvurderinger og penetrationstest

En sårbarhed vurdering tit omfatter en penetration afprøvning komponent til identificere sårbarheder i en organisations personale , procedurer eller _ processer . Sårbarhed vurderinger del mange af de samme egenskaber som penetration tests fordi begge tillade organisationer til strengt undersøge deres forsvar . Disse sårbarheder kan normalt ikke opdages _ via netværk eller system scanninger . Det processen er nogle gange henvist til som sårbarhed vurdering / penetration afprøvning eller **VAPT** .

Dog penetration _ test er ikke tilstrækkeligt som en komplet sårbarhed vurdering og er faktisk en separat proces . En sårbarhed vurdering mål til afdække sårbarheder i et netværk og antyder passende afbødning eller afhjælpning til afbøde eller eliminere risici .

En sårbarhed vurdering bruger automatiseret netværkssikkerhed _ scanning værktøjer . Det resultater er opført i _ sårbarhed vurdering rapport , som fokuserer på at yde organisationer med en liste over sårbarheder at brug for fiksering . Det gør det dog dette uden vurderer bestemt angreb mål eller scenarier .

Organisationer skulle gerne regelmæssigt udføre sårbarhed afprøvning til sikre det deres sikkerhed _ netværk , især hvornår ændringer er lavet . Til eks . test skal gøres hvornår tjenester er tilføjet , ny udstyr er installeret , eller havne er åbnet .

I kontrast , penetration afprøvning involverer identificere sårbarheder i et netværk og forsøg til brug dem til angreb det system . Selvom Sommetider udføres i sammenhæng med sårbarhed vurderinger , den primær formålet med penetration test er at kontrollere om en sårbarhed rent faktisk eksisterer . Derudover penetration _ afprøvning forsøg til bevise at udnyttelse af en sårbarhed kan skade det Ansøgning eller netværket .

Mens en sårbarhed vurdering er normalt automatiseret til dække en bred række upatchede _ sårbarheder , penetration afprøvning tit kombinerer automatiseret og brugervejledning teknikker , hjælpe testere yderligere undersøge sårbarheder og gearing dem til få netværksadgang i en kontrolleret miljø .

2.5. Sårbarhedsstyring og risikostyring _

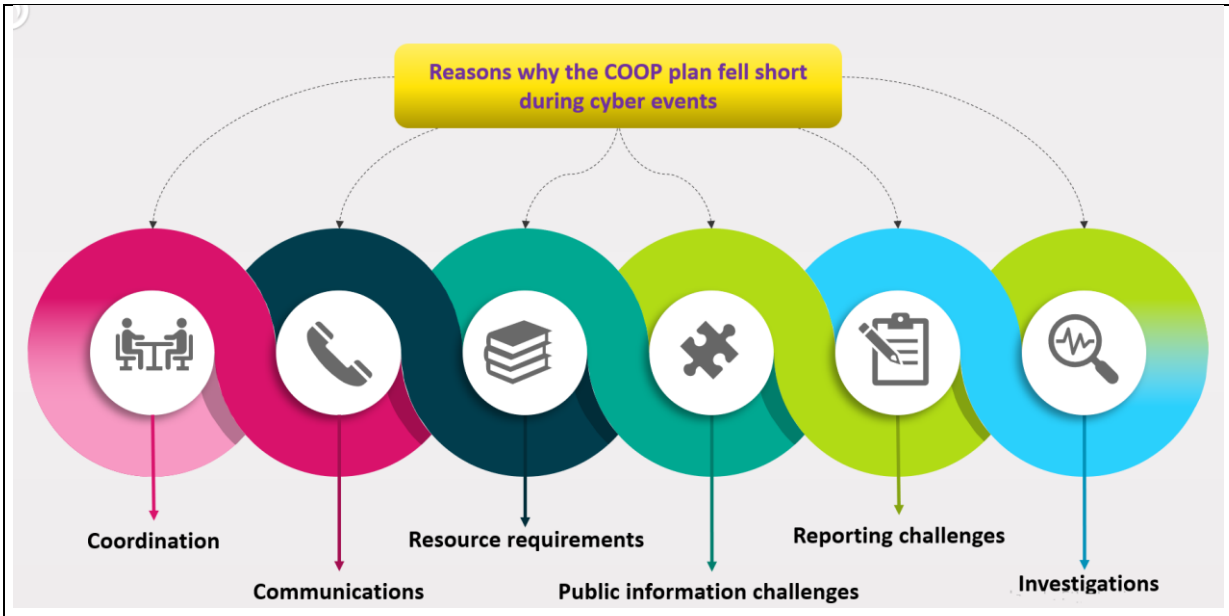
Mens sårbarhedsstyring er en løbende proces til håndtering af sårbarheder, tager risikostyring et bredere blik på alt, der kan udgøre en trussel mod en organisation. En sund risikostyringsstrategi gør det muligt at identificere, analysere og effektivt mindske risici. Denne tilgang hjælper organisationer med at forstå ikke kun de sårbarheder, der eksisterer, men omfanget af skader, der kan opstå, hvis de misbruges. En risiko- og sårbarhedsvurdering udført under paraplyen risikostyring kan give et særligt bredt perspektiv på styrken af en organisatorisk sikkerhedsposition.

3. Cyber Kontinuitet i driften

Forøgelse af modstandsdygtigheden over for trusler om destruktiv malware kræver indsigt i den aktuelle sikkerhedsposition, planlægning og koordinering af vigtige defensive handlinger og justering af nøgledefensive ressourcer korrekt.

Cyber hændelser har ligeledes udfordret grundlæggende kontinuitet planlægning indsats . Mens mange jurisdiktioner har udstyr og strategier til identificere , opdage og _ beskytte mod cyberangreb , langt færre har arbejdet igennem de hårde realiteter af kontinuitet i deres operationer gennem en egentlig angreb . Hvornår cyberangreb rammer , mange _ påvirket jurisdiktioner finde at at deres grundlæggende COOP- planer ikke holde op . Mens det planer er tilstrækkelig til overgang til en suppleant arbejdssted , de har meget mindre til tilbud når det kommer til arbejder uden adgang til det systemer og datapersonale _ brug for til udføre deres mission vigtig funktioner . Eksisterende planer også mangel det specificitet havde brug for til guide det svar , og major interessenter såsom medlemmer af IT - medarbejderne _ er ofte ikke integreret ind i respons strukturer . Og planer er uafprøvet mod en øvelse eller virkelige verden hændelse .

Traditionelle COOP- planer efterår kort til kontinuitet i løbet af cyber hændelser i flere måder (figur 2):



Figur 2 . Grunde hvorfor COOP planlægger er utilstrækkelig til kontinuitet i løbet af cyber begivenheder

Koordinering : inkl som er involveret i beslutningstagningen når det kommer til ransomware , beslutninger til tage systemer offline, og beslutninger til aktivere det jurisdiktionelle Nødsituation Operationscenter . Derudover de fleste lokal regeringer ikke har klar eskalering niveauer for et angreb , ej heller det forbundet handling genstande til hver niveau . Respons ledelse og bemanding kan også være uklar ; det typer af emner stof ekspertise havde brug for til guide et fællesskab gennem en cyber utilsigtet hændelse er forskellige fra de der havde brug for til ekstrem vejret .

Kommunikation : herunder hvordan lokal ledere vilje hurtigt give Information til personale når et cyberangreb har været alvorligt kompromitteret kommunikation . Dette omfatter begge umiddelbar kommunikation forklarer hvad at gøre hvornår det angreb begynder og igangværende kommunikation , såsom hvordan lønninger vil blive leveret ved lønningsdag . Begge er kritisk til svar , og dog begge dele kan har skal videresendes _ uden det fordel af typiske nødsituation kommunikation systemer .

Ressourcekrav : Hvilken _ kan være meget forskellige fra de der for en mere traditionel svar . Til for eksempel personale magt kræve ren computere , rene servere , lokale printere og _ også selvom fax maskiner og papir . Vigtigt , personale krav kan stigning også selvom mere i løbet af genopretning end som svar , som afdelinger og agenturer kamp til replikere mangler eller mistænkelige data.

Offentlig Information udfordringer : Herunder offentlig Information betjente med lille til ingen uddannelse eller erfaring inden for cybersikkerhed , mangel på forskrift beskeder og _ uenighed om hvornår Information om det angreb skal laves _ offentlige . At sørge for Information til det offentligheden er kritisk fordi borgere bekymre om deres data og det nøglens troværdighed _ demokratisk systemer såsom at stemme og retfærdighed .

Indberetning udfordringer : Det kan forsinke svar , som udfald er det ikke rapporteret i en konsistent måde , forlader IT -afdelinger uden det nødvendig almindelige operationelle billede til hurtigt identificere et angreb . I desuden den _ rapporteringslinjer _ _ er tit uklart , og få mennesker uden for IT forstå hvilken systemer er tilsluttet begge inden for og ydre til det jurisdiktion .

Undersøgelser : Som er en sort boks til mange lokaliteter . Det involvering af en eller flere føderale organisationer og det grænser undersøgelser sted på afhjælpning indsats har det ikke godt forstået eller planlagt for . Dette gør kontinuitet planlægning ekstremt svært , fordi der er usikkerhed om hvordan og hvornår afhjælpning kan endda begynde .

3.1. Prioriteter til Øjeblikkelig handling med Koordineret Forsvar

• Udvikle en cyber ' Go Taske ' med vigtig procedurer og information .

  o Saml mobil cyber sikkerhed værktøjssæt at omfatte procedurer til etablering , implementering , vedligeholdelse og _ aktiverer det fortsættelse af cyber robust TTP'er inden for et COOP- udpeget anlæg

• Udvikle , teste og validere spillebøger , roller , ansvar og _ værktøjer .

  o Udpege bestemt cyber roller , tilknyttede ansvar , og det cyber værktøjer at kan blive indsat til sikre implementering af cyber COOP.

  o Definer standard cyber COOP spiller til individuel eller cyber hold udførelse ved brug af cyber ' Go Taske ' værktøj og elastik TTP'er .

  o Adfærd forskellige typer af cyber øvelser (f.eks . type minibordplade _ øvelser) ved hjælp af det cyber ' Go Taske ' og spillebog .

• Definer samarbejde processer og erhverve værktøjer til cyber forsvarere og utilsigtet hændelse respondere .

o Sikre både mobil og stationær cyber COOP processer indarbejde meddelelse og samordning svalehale til fremme tilstrækkelig styring af cyber forsvar , synergi blandt alle respons aktiviteter , og reduktion af sikkerheden dækning huller i løbet af genopretning aktiviteter .

Mens grundlæggende COOP- planer har fremmet lokal beredskab til mange af de trusler at jurisdiktioner ansigt , de falder kort i løbet af situationer at skabe et miljø meget forskellige end normen . Som IT -afdelinger rundt om det Land Blive ved til lave systemer og data så sikkert som muligt , det er oppe til nødsituation ledere til strække deres fantasi og planlægge for cyberangreb at helt seriøst indvirkning kritisk systemer og data.

3.2. Prioriteter til Øjeblikkelig handling med Omlægning

• Identificer mission og forretning fungere afhængighed af cyber ressourcer .

o Bestemme det mission formål med ressourcer så at bruger at øge risikoen uden nogen tilsvarende mission fordel kan identificeres og elimineret .

✓ Identificere og fjerne eller erstatte data feeds og forbindelser til hvilken risici opveje fordele .

o Overveje det gensidige afhængigheder mellem og blandt mission og ikke-mission forretning funktioner og organisationer at del kritisk roller i _ levering af NEF -kapaciteter .

✓ Omfordele ressourcer eller gentildele administrative og ledelse ansvar baseret på risiko for mission og forretning funktion .

• Identificer ikke-mission og forretning fungere afhængighed af eller brug af cyber ressourcer .

o Lave brug af mission flyde analyse , mission afhængighed analyse , bordplade øvelser , og Rød Teaming til afdække udokumenteret mission afhængigheder .

o Anmeldelse og korrelere mission og forretning funktioner med afhængighedsmodel kortlægning _ og indvirkning analyse aktiviteter og resultater .

o Identificere systemer , applikationer og ikke - missionsprocesser kritisk funktioner og det ressourcer at support dem .

✓ Vurdere de der funktioner mod en væske Cyber COOP implementering strategi til imødekomme prioritet operationer og bedre afhængighed udnyttelse eller eliminering .

4. Cyber Asset, Change and Configuration Management

- ✓ **Aktiv:** Lad os starte med definitionen af et aktiv. Ordbogsdefinitionen af et aktiv er en nyttig eller værdifuld ting eller person . På samme måde er en it-tjenesteudbyders aktiver dens værktøjer, applikationer, konfigurationselementer og alle andre værdifulde elementer, der hjælper med at levere tjenester til kunderne eller virksomheden. Aktiver er en del af serviceaktiver og konfigurationsstyring.

- ✓ **Konfigurationselement:** Konfigurationselement er forkortet til CI, og et konfigurationselement er enhver komponent, der skal administreres for at kunne levere en IT-tjeneste. Eksempler på konfigurationselementer er it-tjenester, hardware, software, bygninger, mennesker og formel dokumentation. Så kort fortalt er enhver komponent eller vare, der hjælper med at levere en IT-service til kunden, klassificeret som en Konfigurationsvare. Oplysninger om hvert konfigurationselement registreres i en konfigurationspost i Configuration Management System, og disse oplysninger vedligeholdes gennem dets livscyklus af Configuration Management .

- ✓ **Configuration Management Database:** Configuration Management-databasen er forkortet til CMDB. CMDB er en database, der bruges til at gemme konfigurationsposter gennem hele deres livscyklus. CMDB gemmer oplysninger om dine CI'er, som hver er kendetegnet ved en unik identifikator, herunder identificerende oplysninger som dets serienummer, MAC-adresse eller IP-adresse; dens nuværende version; dens placering; og dets leverandør- og leverandøroplysninger.

- ✓ **Configuration Management System:** Configuration Management System er forkortet som CMS og er et sæt værktøjer og databaser, der bruges til at administrere en IT-tjenesteudbyders konfigurationsdata. Data om konfigurationselementer gemmes i konfigurationsposter, og konfigurationsposter er inkluderet i Configuration Management System-databaserne. CMDB'erne fra en IT-tjenesteudbyder til at administrere konfigurationsdataene er inkluderet i serviceaktiveret og konfigurationsadministrationsprocessen. Konfigurationsstyringssystemet omfatter også information om hændelser, problemer, kendte fejl, ændringer og udgivelser, medarbejdere, leverandører, lokationer, forretningsenheder, kunder og brugere. Sammenfattende er alle nødvendige oplysninger om konfigurationselementer og it-aktiver inkluderet i Configuration Management System. Når det er nødvendigt, hentes disse oplysninger fra CMS'et og bruges hhv.

Konfiguration ledelse , hvilket i bund og grund er defineret som _ processen med at identificere , kontrollere , overvåge og revision ændringer lavet , er en kritisk del af en stærk sikkerhedsprogram . Lave om og konfiguration ledelse inden for en organisation har stærk links til revidere krav i næsten alle sikkerhed rammer og forskrifter .

Konfiguration ledelse er baseret på _ styring og frigivelse af div produkt versioner . Standard konfigurationer til i drift systemer og applikationer er generelt gearet hen imod let implementering _ og brug , ikke cybersikkerhed bedst praksis . I dag , konfiguration ledelse er en efterspørgsel disciplin med væsentlig cybersikkerhed implikationer , især som organisationer bevæge sig fra ud af boksen _ _ Standard konfigurationer til mere sikker Ansøgning og hardware konfigurationer .

I dag , konfiguration ledelse midler forskellige ting til forskellige mennesker . I nogle implementeringer , refererer det til det måde netværksenheder _ er konfigureret . I andre , det er om det version af en app , et team kører . Sommetider mennesker i _ industri forvirre it -aktiv ledelse med lave om og konfiguration ledelse . Mens de er lignende og ligeligt vigtig til det forretning , de er ikke samme . IT- ledelse løsninger overvåge , optimere og styre aktiver et kors det hel aktiv livsstil . I mellemtiden indsamler CM , opbevarer , administrerer , opdaterer og analyser alle konfiguration genstande .

Mens mange organisationer har umodne CM- programmer , det er de kritisk til den moderne cybersikkerhed landskab og vilje kun stigning i betydning som _ trussel landskab fortsætter til udvikle sig .

4.1. Configuration Management og Disaster Recovery

Når det kommer til moderne katastrofe recovery , konfiguration ledelse er afgørende . I det hændelse af en cybersikkerhed katastrofe , (76% af organisationerne har oplevet et IoT cybersikkerhed hændelse , efter alle) det kan være umuligt til gendanne til det mest nylig konfiguration hvis der er ingen dokumentation af nævnte konfiguration .

Det samme går til cybersikkerhed : det er umulig til hold til ved godt hvis noget er galt hvis der er ikke en standardiseret måde at konfigurere på , skiftende , og dokumentere det digital miljø .

4.2. Forandringsledelse

Lave om ledelse løber parallel med konfiguration ledelse dog _ de to ting er *ikke* det samme . Folk forvirrer dem alle tiden .
Mens konfiguration ledelse er _ processen med at identificere og dokumentere hardwarekomponenter _ og software og det forbundet indstillinger , ændre ledelse er et underliggende funktion af _ større konfiguration ledelse proces . Lave om ledelse vedrører til det forbundet processer og søger til skab stabilitet inden for et system og forhindre ukontrolleret eller

tilfældig ændringer eller til dokument lave om processer hvornår du har omsætning inden for det organisation . I Andet ord , det tillader virksomheder til plan for forandring , snarere end lige reagerer til det.

4.2.1. Forandringsledelsesprocessen

I dag er en velstruktureret lave om ledelse behandle vilje omfatte det følgende :

- Ændre anmodningsindsendelser
- Risiko- og konsekvensvurderinger
- Godkend/afvis ændringsfunktioner
- Afprøvning
- Planlægning/brugermeddelelse/træningsfunktioner
- Implementering
- Validering
- Dokumentation

En af de steder lave om ledelse trives er i nødstilfælde _ _ beslutninger , hvornår ændringer skal laves . _ Enkelt gang det forandring har været implementeret , bør det tilbageføres ind i det lave om ledelse proces , hvor det vil derefter fordel fra det validering og dokumentation protokoller at var allerede etableret .

4.3. Cybersikkerhed aktiv ledelse

Forvaltning af cybersikkerhedsaktiver er det indsamlingsprocessen _ _ aktivdata (enheder , sky tilfælde , og brugere) til styrke kerne sikkerhed funktioner , herunder :

- **Detektion og respons:** Sikring af detektions- og responsfunktioner giver dækning på tværs af virksomheden
- **Sårbarhedshåndtering:** Forstå hvilke aktiver der kan være sårbare over for udnyttelse, og sikre, at alle aktiver evalueres for sårbarheder
- **Skysikkerhed:** Sikring af, at cloud-instanser er sikre og konfigureret til at forhindre alt for tilladelige adgangsrettigheder, selv når de idriftsættes og nedlægges hurtigt
- **Hændelsesreaktion:** Brug af berigede, korrelerede data om aktiver til at fremskynde hændelsesreaktionsundersøgelser og afhjælpning
- **Kontinuerlig kontrolovervågning:** Identifikation af, hvornår sikkerhedskontrol mangler og skal anvendes

5. Evaluering af cyber sikkerhed politikker effektivitet

Udviklingen af et informationssystem skrider frem gennem flere adskilte faser fra analyse af problemet til implementering af systemet. I løbet af denne proces er hvert trin dokumenteret gennem en række leverancer, der spænder fra en gennemførlighedsundersøgelse til træningsmanualer og systemdokumentation. I udviklingen af en sikkerhedspolitik forekommer denne selvdokumentationsproces generelt ikke.

Mange politikker, der er udviklet i øjeblikket, forsøger at passe alt ind i sikkerhedspolitikken: begrundelsen for vigtighed og specifikke systeminstruktioner og beskrivelser. Sikkerhedspolitikken i sig selv er ganske vist allerede langhåret nok, uden at have detaljer om, hvordan dokumentet blev oprettet, hvem der blev konsulteret i dets produktion, eller hvordan politikformuleringen blev opnået. Der vil heller ikke være dokumentation for politiske problemer, der kan være opstået under implementeringen af politikken, eller af, hvordan man træner folk i politikken. Med brug af dokumentationsteknikker under udviklingen af politikken kunne en sikkerhedspolitik dog igen blive et principdokument. Andre spørgsmål, der ikke omhandler principperne for sikkerhedspolitik, vil blive dokumenteret andetsteds sammen med begrundelsen for politikken.

Den vigtigste information, der ofte mangler eller bare er utilstrækkelig, når vi forsøger at evaluere en sikkerhedspolitik i en organisation, er kravdokumentationen. Uden en klar forståelse af kravene er evaluering af kvaliteten af en sikkerhedspolitik næsten umulig. En analyse af de risici/trusler, som organisationen står over for, er kun en del af de krav, der er nødvendige for udviklingen af en sikkerhedspolitik. Organisationens målsætninger og andre politiske forhold, der har indflydelse på udvikling, implementering og accept af sikkerhedspolitikken, er lige så vigtige. Tilgængeligheden af omfattende dokumentation, herunder resultaterne af en omfattende kravanalyse, vil gøre det muligt for evalueringen af sikkerhedspolitikken at nå en større dybde i stedet for blot at evaluere slutproduktet overfladisk. I stedet for kun at koncentrere sig om, hvorvidt politikken er blevet implementeret på et bestemt område, kan evalueringen f.eks. nu også overveje, hvordan dette område er udviklet inden for politikken. Dokumenter kan evalueres for at afgøre, om politikken dækker alle problemer, der er identificeret inden for udvikling, tilstrækkeligt uden at udvande nogen af dem. Sikkerhedspolitikkerne varierer dog meget afhængigt af organisationens kontekst, og man ville forvente, at deres udvikling også ville variere. Der ville eksistere nogle fællestræk mellem politikker, selv når målområderne afviger. I modsætning til produktevaluering vil mange kriterier i sikkerhedspolitisk evaluering dog være af subjektiv karakter. Dette skyldes den subjektive karakter af at udvikle en politik og af det miljø, hvori politikken implementeres.

5.1. Vedligeholdelse Effektiviteten af it- sikkerhedspolitikker

Informationsteknologi, eller IT, er velsagtens århundredets teknologi. Det har helt sikkert forandret verden. Med alle fordelene ved IT er der dog også en masse sikkerhedsrisici trængt ind

i vores liv. Organisationer skal designe effektive informationssikkerhedspolitikker for at sikre, at deres forretningsaktiviteter forbliver sikre fra ondsindede ubudne gæster og data til tyven. Ironisk nok er en glimrende måde at bevare effektiviteten af sikkerhedspolitikker mod det skiftende IT-risikolandskab at bruge mere IT.

Her er nogle af de måder, hvorpå it kan opretholde effektiviteten af sikkerhedspolitikker:

- **Bedre risikovurdering :** Sikkerhedsrisikovurdering er afgørende _ _ første skridt i design nogen Information sikkerhed politik . Til adresse det trusler opstår fra det hurtigt IT - sektor i udvikling , IT er den kun modgift . Siden risici lave om konstant , IT er et must til holde det ny trusler i skak . Det tillader du til let opdage ny risici baseret på din Tidligere overholdelse optegnelser , rang og klassificere risikofaktorerne _ _ og vurdere det skader det kan forårsage . Derfor er det vigtigt til lære fra det ny udvikling – godt eller dårligt i IT. Dette vilje forbedre din risikovurdering samt din _ _ _ beredskab , hvis en trussel er overhængende .
- **Bedre compliance** : IT hjælper du overvåge hvor godt det medarbejdere og det dine hoveder _ organisation forblive kompatibel med det regulerende myndigheder såvel som dine _ organisationsspecifik sikkerhed politikker . Gennem en enkelt software kan du holde øje med adgangen autorisationer , usikker datadeling , usikker websurfing , utilstrækkelig datakryptering og _ _ _ _ utallige Andet faktorer der kan alvorligt påvirke din sikkerhed .
- **Konstant opgradering er et must** : Da IT - verdenen ændrer sig med hver åndedrag vi tag , dig skal konstant være på pas på til ny ændringer der kan knække din system . Overvåge det udviklingen i _ verden af cyber-risici , cyber - kriminalitet og cyber-sikkerhed . Opgrader din Information sikkerhed politikker og din sikkerhedssoftware ofte _ og regelmæssigt , fordi de kan få forældet _ _ meget hurtigt . Dette måde , du kan vedligeholde det effektiviteten af din sikkerhed politikker .
- **Hurtigt afbødning** : Hvis din organisation gør står over for en forestående sikkerhed trussel der kan føre til potentielt tab af data eller tyveri , dig skal have en afbødning eller afhjælpningsplan ved hånden . IT hjælper du planlægger afbødning på en enkel og effektiv måde . Med IT kan du tildele og link risikobegrænsning trin til forskellige potentiel risici hvornår du design din sikkerhed politikker . Dette vilje lave afbødning rettidigt og mere effektivt altså _ vedligeholde det effektiviteten af din sikkerhed politikker .
- **Forbedret ansvarlighed** : Ingen information politik kan forblive effektiv hvis mennesker afholdes ikke _ ansvarlig og ansvarlig til risici , compliance og _ afbødning . IT gør det nemmere til sikre det ansvarlighed for afhjælpning handling . Det kan i høj grad forbedre det Synlighed af risici og Modenhed vurdering , overholdelse og _ det afhjælpning foranstaltninger at din organisation påtager sig . Dette midler at din medarbejdere vil være

mere hurtig og mere ansvarlig hen imod det trin opført i din Information sikkerhed politikker .

5.2. Evaluering Sikkerhedsrisici

Risikovurdering, efter at have bestemt, hvilke informationsaktiver der skal beskyttes, vælges risikovurderingsmetoden, og risiciene defineres. I henhold til den valgte risikovurderingsmetode placeres informationsaktiver på risikokortet vist i figuren. Efter vurderingen er foretaget, dækker risikovurderingskortet processerne med at forbedre og kontrollere risici for trusler med høj effekt og sandsynlighed. Da placeringen af informationsaktiver i risikokortet kan ændre sig, bør risikovurderingskortet opdateres regelmæssigt, og de nødvendige forholdsregler bør tages.

Risiko er defineret som kombinationen af sandsynligheden for en begivenhed og dens udfald. Risikovurdering, som er et trin i risikostyring, er en proces, hvor risici defineres, og virkningerne og prioriteterne af disse identificerede risici fastlægges. Risikostyring er at bestemme et acceptabelt risikoniveau, at vurdere den aktuelle risiko, at tage de nødvendige skridt til at reducere denne risiko til et acceptabelt niveau og at opretholde dette risikoniveau. Information og andre aktiver, trusler mod disse aktiver, sårbarheder i det eksisterende system og kontrolsystemer til sikkerhedssystemer er de komponenter, der bestemmer den aktuelle risiko. Identifikation af oplysninger eller aktiver, der skal beskyttes; at bestemme, hvor værdifulde disse aktiver er for virksomhederne; afsløre, hvilke af de kendte og mulige trusler mod disse aktiver, der vil blive forsøgt forhindret; at undersøge, hvordan mulige tab kan opstå; identifikation af omfanget af mulige trusler mod hvert aktiv; Undersøgelse af, hvad der i første omgang kan gøres for at reducere omfanget og sandsynligheden for tab, der kan forekomme i disse aktiver og planlægning af de skridt, der skal tages for at holde de fremadrettede trusler på et minimumsniveau, er visse faser af risikovurderingen. Omkostningerne ved det sikkerhedssystem, der skal etableres og implementeres som følge af risikostyring, er et andet vigtigt spørgsmål, der skal overvejes. Omkostningerne til sikkerhedssystemet bør begrænses af værdien af de beskyttede oplysninger og risikoen bestemmes ved at undersøge mulige trusler. Sammen med princippet om, at der ikke vil være 100 % sikkerhed, realiseres den ideelle konfiguration af informationssikkerhed gennem tre processer. Disse processer er forebyggelse, detektion og respons (respons eller reaktion).

Forebyggelse ; Det er den proces, som sikkerhedssystemer fokuserer på og fungerer mest. Forskellige tiltag udvikles til at isolere systemet mod trusler og angreb mod computersystemer, såsom sikkerhedsforanstaltninger, der bruges i dagligdagen, såsom indhegning af et huss have og brug af en ståldør. Med hensyn til personlig computersikkerhed, at have installeret virusscanningsprogrammer, udføre disse programmer og operativsystemservicepakker og fejlretning og opdateringer med jævne mellemrum, ved at bruge en adgangskodebeskyttet

pauseskærm på computeren, forlade systemet efter at have været væk fra computeren i en lang tid, er det svært at vurdere de anvendte adgangskoder. at bestemme, holde disse adgangskoder fortrolige og ændre dem med jævne mellemrum, være forsigtig med diskdeling, være opmærksom på filer, der downloades fra internettet eller sendes via e-mail, beskytte vigtige dokumenter med en adgangskode eller holde dem krypteret, e-mail fortrolige eller vigtige oplysninger, websteder uden sikkerhedscertifikater. Nogle af de tiltag, der kan virke enkle, men som redder liv, såsom ikke at blive sendt via usikre midler, at slukke for internetadgang, når den ikke er i brug, tage regelmæssige sikkerhedskopier af vigtige oplysninger og dokumenter. Forebyggelsestrin, der skal implementeres i computersikkerhed i virksomhedsmiljøer, er bredere og mere komplekse. Nogle af de ting, der gøres om forebyggelse i sådanne systemer, hvor sikkerhedseksperter arbejder:

- Periodisk gennemgå servicepakkerne _ _ og opdateringer af _ i drift system og software,
- Beholde bruger rettigheder til et minimum, kører ikke ubrugt protokoller , tjenester , komponenter og processer ,
- Kryptering teknikker i datatransmission , sårbarhed scannere ,
- Brug af virtuelt privat netværk,
- Det brug af offentlig Nøgle Infrastruktur og e - signatur kan angives som brug af Biometrisk-baseret systemer .

Faktisk, hvis fremskridtene i forebyggelsesprocessen kunne være perfekte, ville der slet ikke være behov for yderligere processer. Alle angreb ville i værste fald være blevet forhindret. Men intet sikkerhedsprodukt er perfekt eller komplet. Derudover opdages der næsten hver dag forskellige sårbarheder i transmissionssystemer, internettjenester, webteknologier og sikkerhedsapplikationer. Fra dette synspunkt øges brugen af detektions- og matchningsprocesser.

Beslutsomhed; Sikkerhed er ikke kun et spørgsmål om forebyggelse. Det at et museum er godt beskyttet, at museet er omgivet af hegn, at dørene er lukkede og låste, kræver for eksempel ikke brug af vagter om natten på det pågældende museum. På samme måde øges også brugen af metoder til at opdage angrebsforsøg på computersystemer. Forebyggelse er at bygge en barriere, der enten gør angreb stærkere (men ikke umulige) eller fraråder (men ikke ødelægger) angribere. Forebyggelse uden påvisning og respons kan kun have begrænset fordel. Hvis kun forebyggelse var tilstrækkelig, ville de fleste angreb ikke engang have været kendt. Med detektion kan tidligere kendte eller nyligt opståede angreb rapporteres og gives passende svar. Det første og mest grundlæggende trin i detektion er at overvåge hele systemets tilstand og bevægelse og at føre optegnelser over disse oplysninger. På denne måde indsamles data og beviser også til analyse efter angrebet. Firewalls, indtrængningsdetektionssystemer, netværkstrafikmonitorer, portscannere, brug af honeypot, virus- og spywareværktøjer til beskyttelse i realtid,

kontrolprogrammer til kontrolsum for filer og netværkssniffer-sensorer er nogle af de mest almindelige metoder, der bruges i detektionsprocessen.

SvarTilbage ; Ligesom et sted udstyret med vagter, hunde, sikkerhedskameraer, sensorer kan tiltrække tyvenes opmærksomhed, er computersystemer med realtidsdetektionssystemer også attraktive for hackere og angribere. Hurtig reaktion fremstår som et væsentligt element, der komplementerer sikkerhedssystemet for at afvise disse angreb. Respons kan defineres som udførelse af handlinger, der vil reagere øjeblikkeligt eller hurtigst muligt på angrebsforsøg, der ikke kan håndteres af forebyggelsesprocessen og bestemmes af detektionsprocesser. Systemer til registrering af indtrængen kan give mening, hvis der er nogen eller et system til at reagere på denne detektering. Ellers går denne situation ikke ud over fordelen ved en bilalarm, som ingen hører og bekymrer sig om. I denne henseende er gensidighed et vigtigt led, der fuldender sikkerhedsprocessen. Også selvom angrebet ikke er fuldstændig forhindret; Det gør det muligt for systemet at vende tilbage til sin normale tilstand, at identificere årsagerne til angrebet, at fange angriberen, når det er nødvendigt, at identificere sikkerhedssystemets sårbarheder og at omorganisere forebyggelses-, detektions- og reaktionsprocesserne. Planlægning af de handlinger, der skal tages, når et angreb opdages på forhånd, vil sikre, at denne proces fungerer effektivt og ikke spilder tid og penge. Disaster recovery er i spidsen for de store worst case-planer, der er iværksat for denne fase.

Spørgsmål :

1. Hvilket af følgende er ikke et af faserne i formueforvaltningen.

A) Opgørelse af aktiver

B) Fastlæggelse af ejerskab af aktiver

C) Fastsættelse af omkostningsregnskabet

D) Fastsættelse af regler for brug af aktiver

2. Hvad er det primære formål med trussels- og sårbarhedstestprocessen?

A) For bedst at forstå aktivernes sikkerhedssårbarhed og træffe de nødvendige foranstaltninger for at beskytte disse aktiver effektivt.

B) Håndtering af sikkerhedssårbarheder

C) Indhentning af foreløbige oplysninger om aktivopgørelsen

D) Lukning af sikkerhedssårbarheder

3. Hvilket af følgende er ikke en form for sårbarhedsvurdering?

A) Netværksbaserede scanninger

B) Værtsbaserede scanninger

C) Databasescanninger

D) Serverbaserede scanninger

4. Hvilket af følgende er ikke en af processen for forvaltning af cybersikkerhedsaktiver?

A) Sårbarhedshåndtering

B) Omkostningsstyring

C) Kontinuerlig kontrolovervågning

D) Detektion og indgreb

5. Hvilket af følgende er ikke en måde for IT at opretholde effektiviteten af sine sikkerhedspolitikker?

A) Risikovurdering

B) Konstant opgradering

C) Hurtig afhjælpning

D) Sikkerhedspolitikker

6. Hvilken af følgende er ikke en af de tre processer, der udgør den ideelle konfiguration af informationssikkerhed?

A) Forberedelse

B) Forebyggelse

C) Bestemmelse

D) Svar tilbage

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

- **Hvad er sårbarhed i it-systemer**
- **Forklar og giv eksempler på sårbarhedsstyring og risikostyring**

Vedhæftede filer (PowerPoint-præsentation, uddelingskopier, udskrifter, links, video...):

Referencer:

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