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

InCyT træningsmoduler

Informationssikkerhed for ledere **Enhed 3 - Uge 6** **Navn på enhed (modul): Tredjeparts leverandørsikkerhed**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑**Andet**
Læringsansvarlig	• George Matache – et al.
Læringsaktivitetsmål	1. Risici i sociale netværk 2. Foranstaltninger til at have sikkerhed og privatliv i sociale netværk 3. Sikkerhedsteknikker 4. Krav til indkøb
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?***
	• Grundlæggende ledelsesevner • Grundlæggende IT-færdigheder • Grundlæggende sikkerhedsfærdigheder

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
Indkøbskrav henviser til de varer og tjenesteydelser, der skal erhverves fra organisationer uden for den udførende organisation. Af forskellige årsager stoler udførende organisationer nogle gange på, at leverandører leverer det, der er nødvendigt for at fuldføre et projekt. Overvej f.eks. widgetproducenten, der påtager sig et projekt for at automatisere deres lagersporingssystem. Nogle af projektarbejdet involverer flytning af lagerbeholdere i deres hovedlager. Nogle af arbejdsaktiviteterne involverer skræddersyet softwareudvikling. Hvad angår softwareudviklingsaktiviteterne, har widgetproducenten ikke en menneskelig ressource, der ved, hvordan man udvikler softwareapplikationen. Med hensyn til softwareudviklingsaktiviteterne skal widgetproducenten anskaffe disse tjenester. Web-baserede sociale netværk (WBSN'er) er online-fællesskaber, der giver brugerne mulighed for at offentliggøre ressourcer (f.eks. personlige data, annoteringer, blogs) og etablere relationer, muligvis af en anden type til formål, der kan vedrøre forretning, underholdning, religion, dating, og så videre. I de sidste par år har brugen og udbredelsen af WBSN'er været stigende, med omkring 300 websteder, der indsamler oplysninger fra mere end 400 millioner registrerede brugere. Som følge heraf bruges "nettomodellen" i dag mere og mere til at kommunikere, dele information, træffe beslutninger og 'gøre forretning' af virksomheder og organisationer. Det er da et udfordrende spørgsmål at udtænke sikkerhedsmekanismer for sociale netværk, der er i stand til at beskytte private oplysninger og regulere adgangen til delte ressourcer. I denne artikel, udover at give et overblik over egenskaberne ved WBSN-miljøet og dets beskyttelseskrav, illustrerer vi de nuværende tilgange og fremtidige tendenser til social netværkssikkerhed, med særlig opmærksomhed på de nye teknologier relateret til den såkaldte Web 2.0. 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

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

blive støttet til at udvikle e-portfolio, der er vigtig for refleksion og evaluering af træningen.

Indhold af undervisningsmaterialet (🕓?? minutter eller 10-12 sider)

En tredjepartsleverandør er en person eller virksomhed, der leverer tjenester til en anden virksomhed (eller denne virksomheds kunder). Mens leverandører betragtes som "tredjeparter", adskiller nogle industrier en "tredjepartsleverandør" specifikt som en leverandør under skriftlig kontrakt, men ikke alle leverandører arbejder under en kontrakt. For klarhedens skyld henviser udtrykket "tredjepartsleverandør" i denne artikel til enhver person eller virksomhed, der leverer tjenester til en anden virksomhed med eller uden en kontrakt.

Samarbejde er nøglen til succes. At arbejde med tredjeparter hjælper virksomheder med at øge deres produktivitet og effektivitet, producere bedre produkter og tjenester, ansætte højt kvalificerede eksperter og reducere omkostningerne. Men alle disse fordele kommer til prisen af øgede cybersikkerhedsrisici. Mindre fejl i din tredjepartsleverandørs sikkerheds- og privatlivsrutiner kan blive til cybersikkerhedssvagheder for din virksomhed. I denne artikel analyserer vi de særlige cybersikkerhedsrisici relateret til tredjeparter, og hvordan du kan afbøde dem.

Varer og tjenester opnået fra tredjepartsleverandører kan omfatte, men er ikke begrænset til:

- Cloud webhostingtjenester. En cloud-hostingleverandør kan levere alt fra diskplads og båndbredde til kryptering og højteknologiske sikkerhedsløsninger.
- Cloud-baserede softwareløsninger. SaaS-softwareleverandører giver adgang til softwareprogrammer enten til din virksomhed eller dine kunder. For eksempel marketing automation platforme, CRM'er, regnskabspakker mv.
- Vedligeholdelse af udstyr. Firmaet, der reparerer din kopimaskine, og det team, der administrerer din netværkssikkerhed, er tredjepartsleverandører.
- VVS service. Det lokale HVAC-firma, der servicerer din enhed, leverer tjenester fra tredjepartsleverandører.
- Entreprenører af enhver art. Enhver entreprenør, kort- eller langsigtet, er en tredjepartsleverandør.
- Call center udbydere. Hvis du hoster dit callcenter hos et andet firma, betragtes det som en tredjepartsleverandør.
- Bogføring/finansrevisorer. Enhver person eller virksomhed ansat til at administrere din økonomi, budgettere eller revidere din økonomi er en tredjepartsleverandør.

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

- Advokater. Nogle gange er det nødvendigt at konsultere en advokat, før du underskriver kontrakter eller foretager store indkøb. Alle juridiske tjenester betragtes som tredjepartsleverandører.

Efterhånden som organisationer i stigende grad er afhængige af tredjepartsleverandører til at levere væsentlige tjenester, bliver de også mere sårbare over for leverandørrelaterede cybersikkerhedsrisici. En nylig undersøgelse viste, at næsten 60 % af virksomhederne oplevede et databrud på grund af en tredjepartsleverandør i det seneste år. Men hvad er de mest almindelige leverandørcyberhuller, som organisationer bør være opmærksomme på?

Hvad er fordelene ved at bruge tredjepartsleverandører til tjenesteudbydere?

I dagens verden er det umuligt at undgå at bruge tredjepartsleverandører. Uanset hvor mange afdelinger din virksomhed opretter, vil du aldrig dække enhver service, du nogensinde får brug for. Det bør du heller ikke, da virksomheder skal bestemme den rette balance mellem kompetencer, der er væsentlige for virksomheden kontra dem, der kan outsources. Her er, hvad der sker, når du får den rigtige balance:

Du vil spare tid. Ingen har tid til at lære alle færdigheder eller ansætte enhver person, der er nødvendig for at drive en virksomhed. Tredjepartsleverandører får forretningsprocesser til at køre problemfrit ved at opnå alle de professionelle tjenester, der kræves for at drive og udføre ordrer til dine kunder.

Du vil spare penge. Den største fordel er måske omkostningsbesparelserne. At kontrahere en tredjepartsleverandør til arbejde efter behov kan være betydeligt billigere end altid at have fagfolk på virksomhedens lønliste. For eksempel er det langt billigere at hyre en advokat, når du har brug for en, i stedet for at holde en advokat tilbage.

Du får værdifuld ekspertise. Din virksomhed har ikke tid til at udvikle et nyt team af eksperter. Tiden og omkostningerne ved at gøre det ville være enorme. At hyre en tredjepartsleverandør for ekspertise, du ikke har internt, vil sandsynligvis give bedre resultater.

Hvad er risikoen ved at bruge tredjepartsleverandører?

Tredjeparter tager muligvis ikke deres netværkssikkerhed så seriøst, som du ønsker. Ved at vide dette kan hackere vælge ikke at angribe din virksomhed direkte. I stedet kan de lede efter et lettere mål blandt dine tredjepartsleverandører. En kompromitteret underleverandør kan nemt gøres til et indgangspunkt for cyberkriminelle.

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.

Hvis dine leverandører ikke leverer, vil du ikke levere. Risiko er dog iboende i ethvert forretningsforhold. Brug af tredjepartsleverandører kommer med mange risici, hvoraf de fleste kan afbødes.

Den største risiko er at vælge et tredjepartsforhold, der ikke stemmer overens med dine sikkerhedsstandarder. For eksempel skal dit netværkssikkerhedsteam følge sikkerhedsprotokoller, der lever op til dine specifikke standarder. Hvis din virksomhed er bundet af regler som sygesikring, har du ikke råd til at hyre et netværkssikkerhedsfirma, der ikke overholder sygesikringens regler. Du har brug for en leverandør, der forstår reglerne og er villig til at tilpasse sig for at opfylde disse regler.

Når du er bundet af regler om databeskyttelse, skal du vide præcis, hvilke sikkerhedsstandarder der implementeres, og hvis dine leverandører ikke er på niveau med dem, skal du forsøge at afhjælpe det. Ellers udsætter du din virksomhed for cybersikkerhedsrisici såsom et databrud.

Databrud er ekstremt forstyrrende, især når du beskytter personlige oplysninger. Desværre er databrud stigende og er mere almindelige end nogensinde før. Databrud kan forårsage driftsforstyrrelser, ødelæggende økonomiske konsekvenser, retssager og et skadet omdømme. For at undgå disse kan du ikke svigte din vagt, når det kommer til din egen eller dine leverandørers sikkerhed.

Afhængigt af arten af tredjepartsleverandørkompromis kan en organisation stå over for forskellige risici. Lad os se på de mest almindelige risikokategorier og de trusler, du skal være forberedt på at afbøde. En kompromitteret tredjepartsleverandør kan føre til flere risici, der kan opdeles i fire hovedkategorier: Fig.

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

Cybersikkerhedsrisici - Underleverandører har normalt legitim adgang til forskellige miljøer, systemer og data fra deres kunder. Angribere kan bruge en tredjepartsleverandør som et indgangspunkt for at forsøge at få fat i dine værdifulde aktiver.

Operationelle risici — Cyberkriminelle kan målrette mod dine interne systemer og de tjenester, du bruger, i stedet for kun dine data. Dette kan føre til delvise afbrydelser af dine operationer eller endda stoppe dem helt.

Overholdelsesrisici - Internationale, lokale og branchespecifikke standarder og regler fastsætter strenge cybersikkerhedskriterier, som organisationer skal opfylde. Desuden skal tredjeparter, der arbejder med disse organisationer, også overholde disse krav. Manglende overholdelse fører normalt til betydelige bøder og skader på omdømmet.

Omdømmerisici — At få dine værdifulde data og systemer kompromitteret fungerer som et rødt flag for dine partnere og kunder, både nuværende og fremtidige. At genvinde deres tillid vil tage meget tid og kræfter. Og desværre er der ingen garanti for, at du vil være i stand til at genvinde dit omdømme efter en alvorlig cybersikkerhedshændelse.

Krav til indkøb

Af forskellige årsager stoler udførende organisationer nogle gange på, at leverandører leverer det, der er nødvendigt for at fuldføre et projekt. Især SMV'erne. Indkøbskrav er derfor af yderste vigtighed for at arbejde med tredjepartsleverandørsikkerhed.

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.

Selvom det er rigtigt, at indkøb er en meget individualiseret proces, er der også flere grundlæggende faser, som generelt vil blive brugt over hele linjen.

Indkøbskrav henviser til de varer og tjenesteydelser, der skal erhverves fra organisationer uden for den udførende organisation. Af forskellige årsager stoler udførende organisationer nogle gange på, at leverandører leverer det, der er nødvendigt for at fuldføre et projekt.

Stadier af indkøb
Trin 1: Identificer et behov for produkter og/eller tjenester.
Trin 2: Opret og indsend en købsanmodning.
Trin 3: Evaluer og vælg leverandører/leverandører.
Trin 4: Forhandle vilkårene for en kontrakt med den valgte leverandør.
Trin 5: Afslut en indkøbsordre.

Det første trin i indkøbsprocessen er at identificere krav. Alle indkøbskrav begynder med opfattelsen af et behov. Behovet for at krydse en vandmasse kan skabe et krav om at bygge en bro, en færge eller andre transportsystemer.

Trin 1: Identificer et behov for produkter og/eller tjenester
Inden indkøbsprocessen kan begynde, skal et specifikt behov anerkendes. For eksempel kan en organisation være interesseret i at købe nye computerskærme, genbestille deres månedlige levering af papirprodukter eller anskaffe sig opdateret software. Afhængigt af virksomhedsstrukturen kan dette trin administreres af virksomhedsejere, afdelingsledere, ledelsesteam, personale og/eller indkøbsledere. I denne fase vil der blive opstillet et budget, og der vil ofte blive vurderet et samlet overblik over udgifterne.

På dette stadium er det nødvendigt klart at definere behovet, og dette kan gøres ved hjælp af en undersøgelse for at bestemme den bedste måde at krydse vandmassen på (i betragtning af den nuværende situation og det forventede fremtidige behov), og derefter typen af bro til være konstrueret, eller en sammenlignende cost/benefit-analyse for at bestemme den bedste løsning mellem en bro og andre alternativer. Undersøgelsen bør omfatte, om behovet kan opfyldes internt eller udliciteres, kvantificering af det indledende budgetoverslag og en idé om leveringstiden.

Trin 2: Opret og indsend en købsanmodning

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

En købsanmodning (eller indkøbsrekvisition) er en formel anmodning om varer eller tjenester og indsendes generelt ved hjælp af specialiseret indkøbssoftware. Ofte vil købsanmodningen stamme fra en medarbejder eller leder og derefter blive gennemgået af organisationens indkøbsteam.

Når en købsanmodning er godkendt, bliver den en købsordre. Skulle anmodningen dog blive afvist, vil den typisk blive returneret til afsenderen med en kort forklaring. En afvist indkøbsordre, selvom den ikke er ideel, kan være en god læringsmulighed.

Trin 3: Evaluer og vælg leverandører/leverandører
Det næste trin er at vurdere forskellige leverandører og derefter vælge en, der opfylder de vigtigste krav. Nogle organisationer vedligeholder et katalog over godkendte leverandører, med forskellige leverandører, der allerede har bevist sig selv.

Indhentning af leverandører er en proces, der kan variere fra simpel til kompleks, med dens omfang bestemt af de(n) aktuelle krav. Normalt vil flere anmodninger om tilbud (RFQ) blive sendt til forskellige leverandører, så organisationen/indkøbsteamet kan sammenligne priser og muligheder.

Husk at prisen ikke bør være den eneste afgørende, når du vælger en leverandør. For de bedste resultater skal du overveje det "store billede" af, hvad en leverandør kan tilbyde, herunder:
- Nem kommunikation
- Virksomhedsetik
- Ansvarlighed
- Produktionsevner

Efter at en leverandør er blevet valgt, er det vigtigt at investere tid og energi i forholdet. Et godt forhold til en leverandør kan låse op for bedre besparelser og service og levere maksimal værdi på lang sigt.

Trin 4: Forhandle vilkårene for en kontrakt med den valgte leverandør
Når du har valgt den bedst passende leverandør, er det tid til at gå videre til kontraktforhandlinger. Med hensyn til succesfulde indkøb er dette et af de langt mest kritiske stadier. Det er i denne fase, du vil skitsere – og acceptere – priser samt detaljer såsom leveringsplaner, specifikke vilkår og betingelser og mere. Det kan ofte være nyttigt at vurdere tidligere kontrakter for at lokalisere muligheder for forbedringer, så du kan tage en mere informeret tilgang fremadrettet.

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

Trin 5: Afslut en indkøbsordre

Efter den endelige kontrakt er blevet godkendt, er den næste forretningsordre indkøbsordren (PO). Kontrakten regulerer typisk det fulde køber/leverandørforhold, mens en indkøbsordre zoomer ind på et specifikt køb.

- Tænk på dette dokument som en anden formel kontrakt, som fuldt ud beskriver følgende:
- Samlede omkostninger/pris
- Detaljeret beskrivelse af varerne og/eller tjenesteydelserne
- Mængde
- Eventuelle andre specifikke vilkår og betingelser

Trin 6: Ordrestyring

Efterhånden som varerne/tjenesterne leveres, bør der være en person, der er ansvarlig, ideelt set slutbrugeren af produktet eller tjenesterne, for at kontrollere, at alle standarder er overholdt leveringsfrister, produktmængder og kvalitet osv. Hvis der er problemer med varer (f.eks . beskadigede produkter), har du mulighed for at afvise leveringen. Klar kommunikation med sælgeren er nøglen i tilfælde af eventuelle leveringsproblemer.

Efterhånden som teknologi og kommunikation gør det muligt for virksomheder at udvide deres forsyningskæder, øges kompleksiteten af leverandørrisikostyring. Din virksomhed arbejder sandsynligvis med flere leverandører end nogensinde før, og hver af disse leverandører vil udgøre en vis grad af risiko for din organisation.

Leverandørsikkerhedsrisikostyring er en strategi designet til at begrænse antallet af trusler, sårbarheder og svagheder, som din organisation står over for på grund af leverandørerne i din forsyningskæde. En leverandør er typisk en tredjepartsorganisation, der sælger et produkt, en tjeneste eller et stykke udstyr, som din virksomhed har brug for at drive.

Hver leverandør vil, når den er forbundet til din organisation, bære et vist niveau af cybersikkerhedsrisiko. Hvis de undlader at opretholde deres afslutning på aftalen, eller hvis de er offer for et cyberangreb, kan det påvirke din organisation direkte. En effektiv risikovurdering, som en del af en større risikostyringsplan for leverandører, stræber efter at identificere disse potentielle fejlpunkter længe før de bliver et problem og rette dem.

Cyklus for leverandørrisikostyring

Leverandørsikkerhedsrisikostyring er en løbende proces, og en proces, du vil udføre med hver leverandør, du bringer ind i din forsyningskæde. Typisk ser processen sådan ud:

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.

Trin 1: Analyse – Virksomheden identificerer den iboende risiko ved forholdet og niveauet af due diligence, der skal udføres. I overensstemmelse hermed evaluerer virksomheden tredjepartens sikkerhedsposition og udfører en gap-analyse.
Trin 2: Engagement – Virksomheden og tredjeparten samarbejder om, hvordan man udbedrer huller.
Trin 3: Udbedring – Tredjeparten løser cyberhullerne.
Trin 4: Godkendelse – Virksomheden godkender tredjeparten eller afviser den baseret på risikotolerance.
Trin 5: Overvågning – Virksomheden fortsætter med at overvåge tredjeparten for at opdage eventuelle cyberhuller

Sociale netværk og leverandørsikkerhedsrisici

Sociale netværk er meget populære i dagens verden. Normalt defineres et socialt netværk som et netværk i den lille verden, der består af et sæt individer (personer, grupper, organisationer) forbundet af personlige, arbejdsmæssige eller tillidsforhold. Socialt netværk er da et ganske bredt og generisk begreb, som i websammenhæng kan anvendes på enhver form for virtuelt fællesskab. For eksempel kan brugere, der er registreret på en webtjeneste, såsom webmail, online-tidsskrifter eller aviser, der kræver et abonnement, betragtes som et socialt netværk. I det følgende vedtager vi definitionen, ifølge hvilken et online-fællesskabs websted kun kan betragtes som et webbaseret socialt netværk, hvis det opfylder følgende betingelser:

- Relationer er eksplicit specificeret af dets medlemmer og udledes ikke af eksisterende interaktioner (f.eks. kan en mailingliste bruges til at udlede implicitte relationer).
- Relationer lagres og administreres ved at bruge teknologier, såsom databasestyringssystemer, der tillader relationsanalyse og regulerer adgang og genfinding af relationsdata.
- Medlemmer er i stand til at få adgang til forholdsoplysninger, i det mindste delvist.

Nøglebegreber

Relationsbaseret adgangskontrol: Et adgangskontrolparadigme, der er specielt skræddersyet til sociale netværk, ifølge hvilket sociale netværksmedlemmer, der er autoriseret til at få adgang til en given ressource, er angivet i forhold til de relationer, de skal deltage i for at få adgangen.

Socialt netværk: Et netværk i en lille verden, der består af et sæt individer (personer, grupper, organisation) forbundet af personlige, arbejdsmæssige eller tillidsforhold. Normalt modelleret som en graf, hvor noder svarer til medlemmer af sociale netværk, hvorimod kanter angiver relationerne mellem dem.

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.

Sociale netværk. Kommunikation og deling af information med dem omkring os er en del af alles liv og har udviklet sig fra simple tekstbeskeder til e-mails og til det, vi nu kalder sociale medieplatforme. Hvad der ikke er særlig velkendt eller indset, er det faktum, at vores eksponering i onlinemiljøet er forbundet med en masse risici.

Sociale medier og sociale netværks- eller beskedapplikationer kan udgøre en række sikkerheds- og privatlivsrisici for både organisationer og enkeltpersoner, når de bruges på en upassende eller usikker måde. De mest populære og udbredte platforme på sociale netværk:

- Facebook med over 1.300.000.000 medlemmer;
- Flickr bruges til at gemme, organisere og dele mediefiler;
- LinkedIn med over 300 millioner brugere;
- Instagram med over 30 millioner brugere;
- Twitter med over en milliard medlemmer;
- YouTube med over en milliard brugere;
- Tinder med omkring 12 millioner brugere;
- TikTok med over 800 millioner brugere.

Privatlivsbevidst adgangskontrol: I forbindelse med sociale netværk betegner det et adgangskontrolparadigme, hvor adgangskontrolkrav for sociale netværksmedlemmer håndhæves uden at afsløre private oplysninger om de forhold , de deltager i.

Web-baseret socialt netværk: Et webbaseret system, der tillader dets registrerede medlemmer at etablere relationer med andre medlemmer og dele forskellige typer information (f.eks. personlige data, kontakter, multimedieressourcer).

Social Network Analysis: En disciplin rettet mod at indsamle statistiske data fra analysen af social netværkstopologi.

Relationstillidsniveau: I et socialt netværk angiver værdien forbundet med et tillidsforhold, hvilket giver et mål for, hvor meget et givet medlem anser et andet medlem for at være troværdigt. Afhængigt af det formål, det bruges til, kan dette begreb have forskellige betydninger. For eksempel, i et kollaborativt vurderingsmiljø, angiver det, hvor meget et givet medlem stoler på et andet medlems meninger med hensyn til et specifikt emne (aktuel tillid) eller generelt (absolut tillid). I modsætning hertil har det i en adgangskontrolkontekst nogle ligheder med begrebet sikkerhedsniveau, der bruges i obligatoriske adgangskontrolmodeller.

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.

Edge Perturbation: Grafanonymiseringsteknik, der har til formål at skjule de faktiske sociale netværksforhold ved at udføre et sæt tilfældige kantsletninger/indsættelser i netværksgrafen.

Social Network Relationship: Et forhold, der vedrører to medlemmer af et socialt netværk. I WBSN'er kan der udover personlige/arbejdsforhold (f.eks. ven/kollega) også understøttes tillidsforhold, som angiver, hvor meget et medlem stoler på et andet. I grafrepræsentationen af et socialt netværk er relationer normalt betegnet med kanter, mærket med en relationstype og/eller et relationstillidsniveau.

Grafanonymisering: Teknik, der har til formål at skjule private oplysninger om sociale netværksmedlemmer, når de udfører sociale netværksanalyser. Nodeanonymisering og kantforstyrrelse er de to vigtigste grafanonymiseringsteknikker, der i øjeblikket anvendes.

Node Anonymization: Grafisk anonymiseringsteknik, der har til formål at skjule sociale netværksmedlemmers identiteter ved at mærke de tilsvarende noder med tilfældige identifikatorer (naiv anonymisering), eller, hvis noder er forbundet med attributter, som kan bruges til at identificere den tilsvarende bruger, ved at bruge teknikker baseret om k-anonymitet (Sweeney , 2002).

Risici

Geotagging

- Repræsenterer tilføjelsen af geo-identificerende data til fotos, videoer, websteder og tekstbeskeder af applikationer, der kan læse din placering eller har tilladelse til at gøre det i dine indstillinger;
- Sørg for at deaktivere geotagging-funktioner på følsomme steder for at undgå at afsløre din nøjagtige placering, hvor du arbejder, eller hvor du bor.

"Publikum"

- Det er et generelt udtryk, der refererer til, hvem der kan se og/eller kommentere dine indlæg;
- Din vennegruppe kan ændre sig til enhver tid og være i stand til at se et opslag, der indeholder oplysninger om dig. Du kan med vilje dele noget med dine "venner", men hvad de gør med opslaget er uden for din personlige kontrol.

Identitet

- Beskriver rækken af information, der specifikt vedrører en person;

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

- Det skal huskes på, at der er mennesker, der bruger sociale medier som en forskningsmetode til at søge efter identitetsoplysninger med mulige ondsindede hensigter, såsom identitetstyveri, bedrageri, underslæb eller intimidering.

Foranstaltninger

Adgangskode

- Det anbefales at bruge en anden adgangskode for hver online-konto;
- Det skal være mindst 10 tegn langt og indeholde store bogstaver, små bogstaver, tal og specialtegn;
- Det må ikke videregives til nogen, uanset hvor tæt eller betroet den person, vi ønsker at fortælle, er
- Det anbefales ikke at bruge personlige oplysninger, når du opretter en adgangskode (f.eks .: forældres navne, fødselsdato, kæledyrs navn osv.);
- Skift din adgangskode med jævne mellemrum;
- Log ud af din konto, når du bruger en enhed, der ikke er din eller bliver brugt af en anden.

Lav dine sikkerhedsopdateringer til tiden!

- Sociale medieplatforme introducerer jævnligt nye privatlivs- og sikkerhedsindstillinger. Disse kan findes i dine kontoindstillinger, og det anbefales, at du tjekker dem regelmæssigt;
- Brug muligheden for tofaktorgodkendelse (2FA) for at sikre, at nogen ikke forsøger at hacke din konto.

Accepter ikke venneanmodninger fra nogen!

- Accepter eller send kun venneanmodninger fra/til personer, du møder i det virkelige liv eller til offentlige personer, du er interesseret i, ved at passe på at følge deres officielle profiler;
- GLEM IKKE! Hvis du føler dig knyttet til visse konti, kan du begrænse deres adgang til dine indlæg, eller du kan blokere kontoen. Du har også mulighed for at anmelde konti eller opslag af årsager som: falsk konto, falsk navn, opslag med upassende indhold, tilskyndelse til vold, falske oplysninger mv.
- KLIK IKKE!
- Mange angribere bruger social engineering til at vinde en persons tillid for senere at få adgang til information;
- Åbn ikke links og vedhæftede filer fra sociale medier, hvis du ikke er 100 % sikker på kilden (f.eks. er websteder, der tilbyder præmier, ofte beregnet til at stjæle information);
- Hvis en ven fra chatten ser ud til at opføre sig anderledes (stiller mange spørgsmål, bliver meget nysgerrig på sit personlige liv, beder om penge), er der en mulighed for, at hans konto er blevet hacket, og en angriber bruger den til ondsindede formål .

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

Tænk dig om to gange før du poster!

- Sociale medier tilbyder lige så meget en mulighed for at skabe et positivt online omdømme som et negativt, derudover, selvom vi "sletter" et opslag, kan det ikke slettes permanent, når det først er dukket op online;
- Afslør ikke for mange personlige detaljer på sociale medier! "Om mig"-felter er valgfrie.
- Grænsen mellem det professionelle og det personlige liv i onlinemiljøet
- Oplys ikke oplysninger om din arbejdsgiver online
- Post ikke arbejdsbilleder eller negative beskeder, der stiller arbejdsgiveren i et dårligt lys.
- Tænk dig om, før du poster, og far ikke dit job på spil.

Luk gamle konti!

- Hvis du har gamle konti på sociale medieplatforme, som du ikke længere bruger, eller endda gamle konti på samme platform, så prøv at lukke dem. På denne måde opretter du så få links som muligt, hvor nuværende konti er mere beskyttet mod mulige angribere;
- Ældre konti eller platforme er muligvis ikke så sikre som i dag.

Sociale medier udgør store risici

- Sociale netværk udgør høje sikkerheds- og privatlivsrisici på grund af deres centraliserede arkitektur, deres enorme lager af personligt identificerbare oplysninger, som enhver hacker ville elske at have, og befolkningens generelle uvidenhed om, hvordan man korrekt bruger sociale medier. privatlivsindstillinger for at forbedre deres onlinesikkerhed.
- En anden meget høj risiko, især blandt teenagere, er tillid til andre mennesker og den type personlige oplysninger, der afsløres online.
- Dette kan bekæmpes ved hjælp af teknologiske midler og håndhævelse af sikkerhedspolitikker.
- Vi bør betragte oplysninger, der overføres via sociale medier for at være usikre og derfor ikke overføre følsomme oplysninger via sociale medier, hvorfor det primære ansvar for at forblive sikker påhviler BRUGEREN

Dårlige sociale medievaner

- Sociale netværk er meget brugte platforme af brugere i dag. Vi har en bred vifte af muligheder.
- Nogle er mere gearet til at uploade billeder eller videoer, andre mod vores mening og i andre tilfælde blot at holde kontakten med venner og familie. Under alle omstændigheder har vi at gøre med platforme, der har mange brugere rundt om i verden.
- Dette får også hackere til at sætte sig ind her. Vi vil tale om disse vaner, som bør ændres i sociale netværk, hvis vi ønsker at bevare vores privatliv og sikkerhed.
- Der er mange typer platforme, som vi kan finde på netværket, der giver os mulighed for at sende beskeder til venner eller familie, kommentere billeder, videoer ...

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.

- Dette gør dem til et meget populært miljø for både private brugere og virksomheder.
- Dette medfører dog også, at du har en vis risiko for vores sikkerhed og privatliv. Hackere kan se her for at udføre deres angreb. De kan især drage fordel af dårlige brugervaner, når de bruger disse platforme.

Vaner, der skal ændres

- Privatliv og sikkerhed er meget vigtige faktorer for brugerne.
- De er dog ikke altid til stede.
- Vi kan blive ofre for mange typer angreb, der kompromitterer disse to faktorer.
- Vi kan også lave fejl, når vi bruger sociale medier, og det påvirker os.

Tilføj enhver form for kontakt

- En meget almindelig fejl i sociale netværk er at tilføje enhver form for kontakt. Dette kan ske på platforme som Facebook.
- Det er muligt, at det, vi tilføjer, er en bot snarere end en rigtig bruger.
- Du skal vide, hvordan du adskiller dem og undgå at tilføje nogen form for kontakt, som din invitation modtager.
- Nogle gange er bots udelukkende designet til at indsamle brugerdata. Dette kan kompromittere vores privatliv. Vi skal have et rigtigt filter på de kontakter, vi tilføjer.
- Det er vigtigt, at vi har mennesker blandt vores venner, som ikke er et problem for vores sikkerhed og privatliv.

Forbind ikke med sociale netværk hvor som helst

- Du logger ofte ind via sociale netværk på ethvert websted. Dette er meget behageligt, men ikke det bedste for privatlivets fred.
- Sikkert ved mange lejligheder finder vi muligheden for at registrere dig på en side eller oprette forbindelse til en platform via Facebook eller Twitter. Vi undgår at registrere os på den side og udfylde en lang formular. Problemet er, at vi leverer personlige data til denne hjemmeside via Facebook. Disse data/oplysninger, vi deler, kan bruges af tredjeparter til reklameformål.

Giv ikke flere oplysninger end nødvendigt

- Det er helt klart en af de værste vaner, som mange brugere har. De indtaster en masse personlige data, oplysninger, der egentlig ikke er nødvendige, i sociale netværk.
- For eksempel data som vores telefonnummer, e-mailadresse, oplysninger om, hvor vi bor ... Alt dette påvirker vores annoncering og kan bruges til dårlige formål.
- Giv ikke flere oplysninger, end det virkelig er nødvendigt. På denne måde vil vi forbedre vores privatliv i netværket, og vi kan endda undgå visse sikkerhedsproblemer.

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.

Spredning af falske nyheder

- Problemet med falske nyheder er stadig til stede i dag. Jeg kan nå dem på mange måder, men uden tvivl i sociale netværk er de mere end tilstedeværelser.
- Som vi ved, er det falske nyheder, som de bruger som lokkemad og nogle gange endda kan distribuere malware.
- Det er vigtigt at undgå at dele denne type falske nyheder og også at få adgang til dem, når vi ser dem på sociale medier.
- Dette vil forbedre vores sikkerhed.

Vi beskytter ikke vores privatliv

- En sidste fejl er ikke korrekt beskyttelse af privatlivets fred. For eksempel lader vi vores profiler stå åbne, så alle kan komme ind.
- Vi giver oplysninger til enhver, der måtte indsamle dem, for at oprette en profil til os og endda sende målrettet annoncering eller udføre forskellige angreb, der påvirker vores sikkerhed.

Social engineering fra et tværfagligt perspektiv

- På grund af den teknik, som hackere bruger, er det nødvendigt at nærme sig et tværfagligt perspektiv såsom informationsteknologi, psykologi, forretning og etik.

Disciplinen informationsteknologi

- Social engineering bør diskuteres i sammenhæng med nuværende informationssystemer og deres forsvar, der anvendes som en form for risikoreduktion.
- Multi-faktor autentificering er en almindelig og ofte effektiv måde for organisationer at bekræfte, at den person, der får adgang til systemer, faktisk skal have den adgang
- En yderligere faktor kunne være brugen af et virtuelt privat netværk (VPN), dvs. autentificering for yderligere at validere brugeren.

Psykologisk disciplin

- Det er nødvendigt at forstå konceptet og forstå både angriberens og offerets tanker og adfærd.
- Metoderne er vigtige for social engineering, fordi de bruges til at omgå beskyttelser, der måtte være på plads, såsom firewalls og systemer, der bruges til at identificere ubudne gæster.
- Det hjælper med at forstå medarbejdernes handlinger, der er en af hovedårsagerne til databrud.

Forretningsperspektiv

- det er vigtigt, fordi social engineering kan påvirke mange typer virksomheder og have

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.

betydning for, hvordan organisationer er struktureret og ledet.
- det hjælper med at bestemme de faktorer, der påvirker social engineering-angreb og er fordelagtigt, hvis det betragtes mere specifikt i forhold til følgende forretningsområder: uddannelse og udvikling, dokumenterede politikker, interne revisionsprocedurer, budgetter og organisationskultur.
- kan opdage mangler i ethvert af de områder, der kan bidrage til angreb.

Etisk perspektiv
- det er vigtigt i forbindelse med social manipulation og relateret forskning, fordi ideen om at manipulere et andet menneske krænker mange etiske principper.
- hjælper, i tilfælde af en social ingeniørbegivenhed, med at behandle ofrene.

Det er vigtigt at overveje:
- hver disciplin giver information om, hvordan man forstår og fortolker emnet, beskytter mod forskellige typer angreb og forstår virkningen af social engineering fra både et menneskeligt og organisatorisk perspektiv.
- at hver disciplins fortolkning af emnet kun er brugbar, når den ses i sammenhæng med de andre discipliner.

Sikkerhedsteknikker
- Udstyr inventar
- Opgørelse af applikationer og operativsystemer
- Trådløs udstyrskontrol
- Netværkssikkerhedsdesign
- Begrænsning og styring af netværksporte, kommunikationsprotokoller og tjenester
- Beskyttelse af perimeterområder
- Fysisk adgang til lokationer
- Kontrolleret brug af administrative rettigheder
- Overvågning og kontrol af brugerkonti
- Færdighedsvurdering og sikkerhedstræning

VPN (Virtual Private Network)

Et virtuelt privat netværk er en sikker forbindelse over et usikkert netværk såsom internettet. Virtuelt betyder eksistensen af et unikt netværk, uanset topologi, det vil sige en gruppe af geografisk distribuerede computere, der kommunikerer og kan administreres som et enkelt netværk.

Privat betyder et virtuelt netværk med adgangskontrol. som giver fortrolighed, integriteten af

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.

beskeder og autentificerer mellem brugerne og de computere, der deltager i kommunikationen.

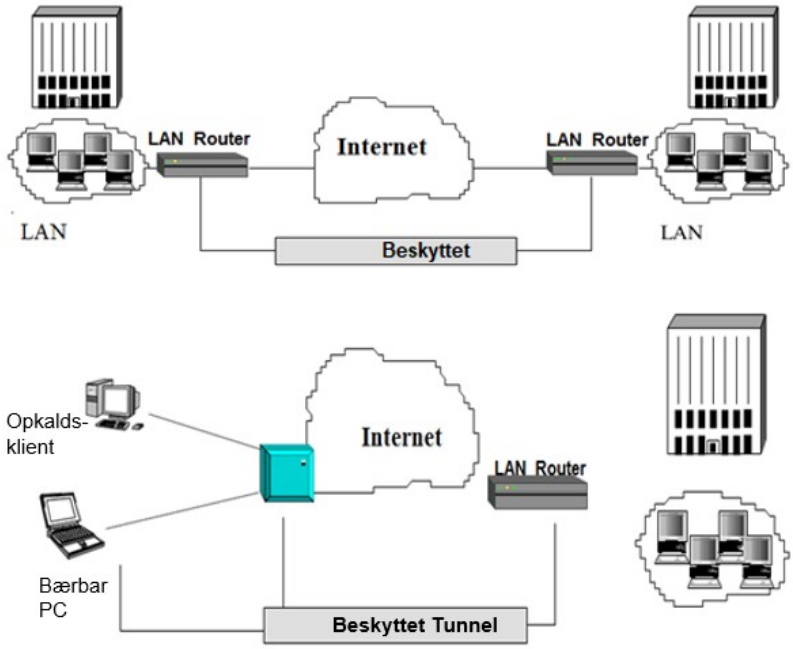

Fig. 2: VPN (Virtual Private Network

Fig. 3: VPN til fjernadgang

At skabe en sikker industriel infrastruktur

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

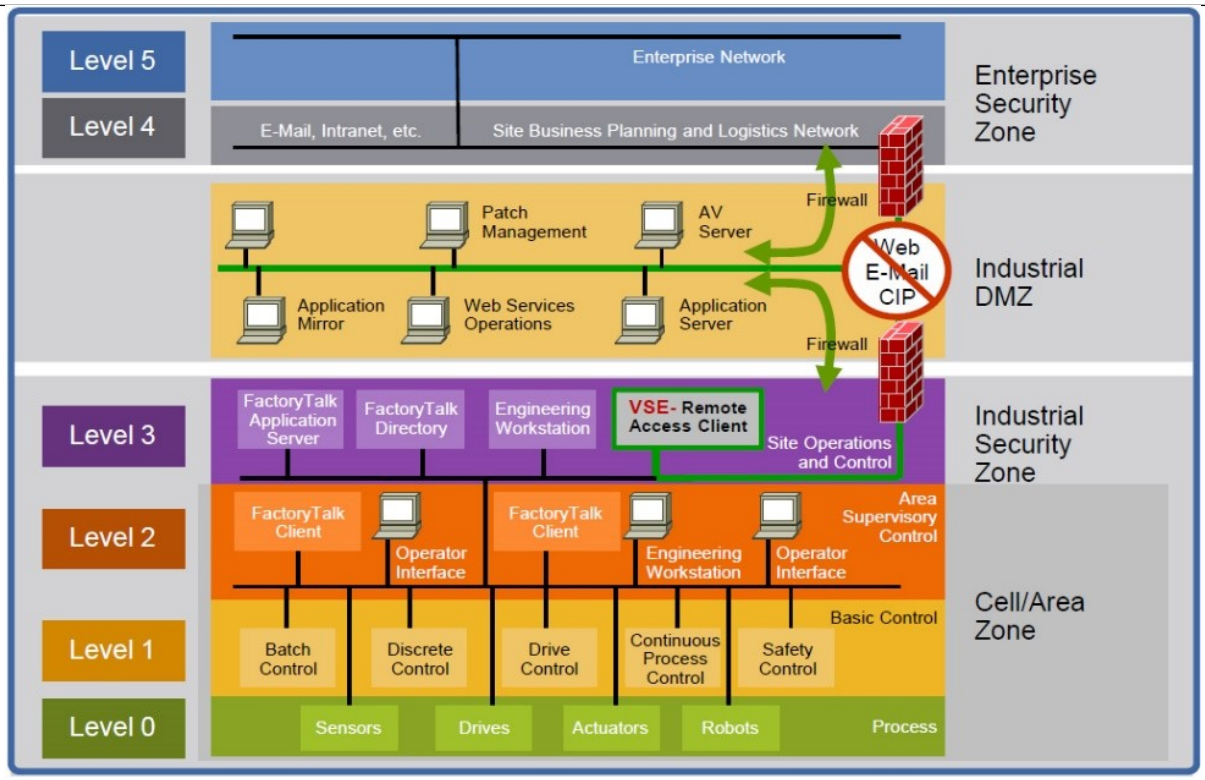

Fig. 4: ISA 95 Logic Model - Industrial Automation and Control System (IACS)

- Defence-in-Depth (DiD) understøtter denne tilgang. Baseret på ideen om, at et enkelt beskyttelsespunkt kan og sandsynligvis vil blive besejret, etablerer DiD-sikkerhed flere lag af beskyttelse gennem en kombination af fysiske, elektroniske og proceduremæssige sikkerhedsforanstaltninger.
- En bank bruger flere sikkerhedsforanstaltninger – såsom videokameraer, en vagt og en boks – dette hjælper med at sikre, at trusler møder mere end én forsvarslinje.
- En dybdegående sikkerhedstilgang omfatter seks hovedkomponenter:

1. Politikker og procedurer
2. Fysisk
3. Netværk
4. Computer
5. Ansøgning
6. Enheden

At skabe en sikker industriel infrastruktur

- Fysisk sikkerhed bør begrænse personaleadgang ikke kun til områder af en facilitet, men også til indgangspunkter til den fysiske netværksinfrastruktur, såsom kontrolpaneler, kabler og

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

enheder.

- Segmentering af anlægsområder i virtuelle lokalnetværk (VLAN'er) er en bedste praksis for sikkerhed i hele netværket.
- Mindre VLAN'er er nemmere at administrere og vedligeholde i realtidskommunikation.
- De kan hjælpe med at isolere enheder fra dem, der er blevet kompromitteret, hvilket holder den negative påvirkning inden for et enkelt VLAN.
- En af de diskuterede teknologier bør være en industriel demilitariseret zone (IDMZ), som skaber en kritisk beskyttende barriere mellem virksomheden og industriområder.
- En IDMZ begrænser trafikken fra at rejse direkte mellem de to zoner og kan hjælpe med bedre at administrere adgangen ved at håndhæve godkendelse eller overvåge trafik for kendte trusler.

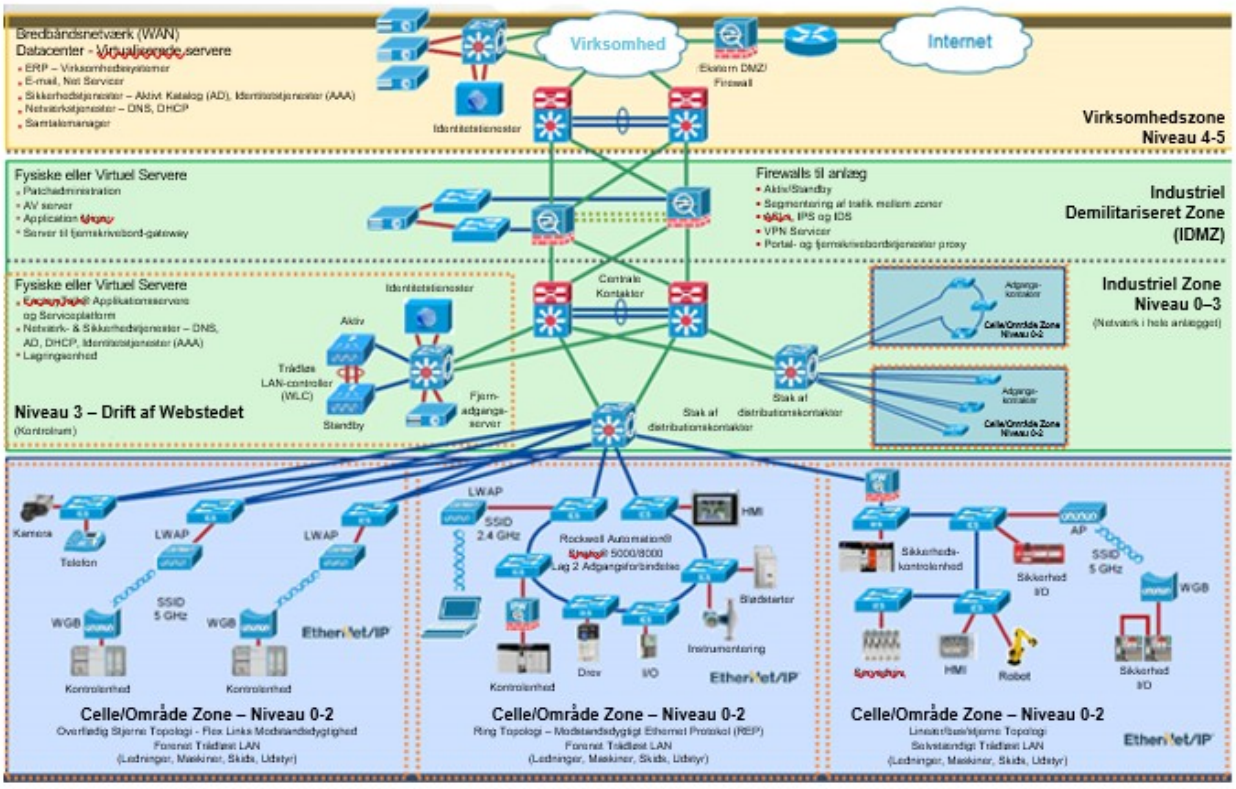

Fig. 5: IDMZ

Spørgsmål:

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

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.

1. Hvilke risici er der ved sociale netværk
2. Foranstaltninger til at have sikkerhed og privatliv i sociale netværk
3. Hvilke er de vigtigste sikkerhedsteknikker i sociale netværk

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

- Risici i sociale netværk
- Sikkerhed og privatliv i sociale netværk
- Sikkerhedsteknikker

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

Se vedlagte

Referencer:

Krav til indkøb
URL: Indkøbskrav
URL: https://www.ekransystem.com/en/blog/third-party-providers
Fastlæggelse af indkøbskrav
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Sikkerhed og privatliv i sociale netværk
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Sikkerhed og privatliv i sociale netværk
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Privatliv og sikkerhed i online sociale medier
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Datasikkerhedsteknikker og privatliv
URL: https://www.educba.com/data-security-techniques/
Hvad er sikkerhedsteknikker
URL: Sikkerhedskoncepter-udviklinger-og-fremtidige-tendenser
Mest effektive sikkerhedsteknikker
URL: https://dzone.com/articles/most-effective-security-techniques-part-1
URL: https://panorays.com/blog/what-is-a-third-party-vendor/

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.