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

Module de instruire InCyT

Securitatea informațiilor pentru manageri **Unitatea 2 Săptămâna 3** **Denumirea unității: Securitatea furnizorilor terți**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte**
Responsabil de învățare	• George Matache – et al.
Obiectivele activității de învățare	1. Riscuri în rețelele sociale 2. Măsuri pentru a avea Securitate și Confidențialitate în Rețelele Sociale 3. Tehnici de securitate 4. Cerințe privind achizițiile
Abilități de dobândit	• TS3 Securitatea retelei • TS4 Testare de penetrare (vulnerabilități exploatabile). • SS3 Analiza cognitivă și comportamentală
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?***
	• Abilități de management de bază • Abilități IT de bază • Abilități de bază de securitate

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

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

Informații scurte despre modul

Descriere
Cerințele de achiziții se referă la bunurile și serviciile care trebuie achiziționate de la organizații din afara organizației executante. Din mai multe motive, uneori organizațiile performante se bazează pe furnizori pentru a oferi ceea ce este necesar pentru a finaliza un proiect. De exemplu, luați în considerare producătorul de widget-uri care întreprinde un proiect pentru a-și automatiza sistemul de urmărire a inventarului. Unele dintre activitățile de lucru ale proiectului presupun relocarea containerelor de depozitare în depozitul lor principal. Unele dintre activitățile de lucru implică dezvoltarea de software personalizat. În ceea ce privește activitățile de dezvoltare software, producătorul de widget-uri nu are o resursă umană care știe cum să dezvolte aplicația software. În ceea ce privește activitățile de dezvoltare software, producătorul de widget-uri trebuie să achiziționeze aceste servicii. Rețelele sociale bazate pe web (WBSN) sunt comunități online care permit utilizatorilor să publice resurse (de exemplu, date personale, adnotări, bloguri) și să stabilească relații, eventual de alt tip, în scopuri care pot viza afaceri, divertisment, religie, întâlniri, si asa mai departe. În ultimii câțiva ani, utilizarea și difuzarea WBSN-urilor a crescut, aproximativ 300 de site-uri Web care colectează informațiile a peste 400 de milioane de utilizatori înregistrați. Drept urmare, „modelul net” este folosit astăzi din ce în ce mai mult pentru a comunica, a împărtăși informații, a lua decizii și a „face afaceri” de către companii și organizații. Atunci este o problemă dificilă conceperea unor mecanisme de securitate pentru rețelele sociale, capabile să protejeze informațiile private și să reglementeze accesul la resursele partajate. În acest articol, pe lângă o imagine de ansamblu asupra caracteristicilor mediului WBSN și a cerințelor sale de protecție, ilustrăm abordările actuale și tendințele viitoare ale securității rețelelor sociale, cu o atenție deosebită acordată tehnologiilor emergente legate de așa-numitul Web 2.0. Cursanții ar putea fi informați despre astfel de aspecte citind textul corespunzător, urmărind webinarii în flux și rezolvând exerciții în ritm propriu. Toate aceste documente se află pe

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

platforma digitală interactivă a proiectelor.
Cursanții își pot testa răspunsurile la exerciții de autoevaluare. Răspunsurile la alte exerciții ar trebui salvate pe forumul de discuții corespunzător și discutate cu mentorul la întâlnirea comună organizată o dată pe săptămână. Cursantul poate lucra în cooperare cu ceilalți și poate îndruma în special în timpul întâlnirilor. Aceștia vor fi sprijiniți să dezvolte un portofoliu electronic important pentru reflecția și evaluarea instruirii.

Conținutul materialului de învățare

Un furnizor terță parte este o persoană sau o companie care furnizează servicii pentru o altă companie (sau clienții acelei companii). În timp ce vânzătorii sunt considerați „terți", unele industrii diferențiază un „vânzător terță parte" în mod specific ca furnizor în baza unui contract scris, dar nu toți vânzătorii lucrează în baza unui contract. Din motive de claritate, termenul „vânzător terță parte" din acest articol se referă la orice persoană fizică sau companie care furnizează servicii unei alte companii cu sau fără contract.

Cooperarea este cheia succesului. Lucrul cu terți ajută companiile să-și crească productivitatea și eficiența, să producă produse și servicii mai bune, să angajeze experți cu înaltă calificare și să reducă costurile. Dar toate aceste beneficii vin cu prețul unor riscuri crescute de securitate cibernetică. Defecte minore în rutinele de securitate și confidențialitate ale furnizorului dvs. terț se pot transforma în deficiențe de securitate cibernetică pentru compania dvs. În acest articol, analizăm riscurile specifice de securitate cibernetică legate de terți și cum le puteți atenua.

Bunurile și serviciile obținute de la furnizori terți pot include, dar nu sunt limitate la acestea:

- Servicii de găzduire web în cloud. Un furnizor de găzduire în cloud poate oferi totul, de la spațiu pe disc și lățime de bandă până la criptare și soluții de securitate de înaltă tehnologie.
- Soluții software bazate pe cloud. Furnizorii de software SaaS oferă acces la programe software fie pentru afacerea dvs., fie pentru clienții dvs. De exemplu, platforme de automatizare a marketingului, CRM-uri, pachete de contabilitate etc.
- Întreținerea echipamentelor. Compania care vă repară copiatorul și echipa care vă gestionează securitatea rețelei sunt furnizori terți.
- Service HVAC. Compania locală HVAC care deservește unitatea dvs. oferă servicii de furnizori terți.
- Contractori de orice fel. Orice contractant, pe termen scurt sau lung, este un furnizor terță parte.
- Furnizorii de centre de apeluri. Dacă găzduiți centrul de apeluri la o altă companie, acesta este

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

considerat un furnizor terță parte.

- Contabilitate/auditori financiari. Orice persoană sau afacere angajată pentru a vă gestiona finanțele, bugetul sau auditarea finanțelor dvs. este un furnizor terță parte.
- Avocaţi. Uneori este necesar să consultați un avocat înainte de a semna contracte sau de a face achiziții mari. Toate serviciile juridice sunt considerate furnizori terți.

Pe măsură ce organizațiile se bazează din ce în ce mai mult pe furnizori terți pentru a furniza servicii esențiale, ele devin și mai vulnerabile la riscurile de securitate cibernetică legate de furnizor. Un studiu recent a constatat că aproape 60% dintre companii au suferit o încălcare a datelor din cauza unui furnizor terță parte în ultimul an. Dar care sunt cele mai comune lacune cibernetice ale furnizorilor de care organizațiile ar trebui să fie conștiente?

Care sunt beneficiile utilizării furnizorilor terți pentru furnizorii de servicii?

În lumea de astăzi, este imposibil să evitați utilizarea furnizorilor terți. Indiferent de câte departamente va crea compania dvs., nu veți acoperi niciodată fiecare serviciu de care veți avea nevoie vreodată. Nici tu nu ar trebui, deoarece companiile trebuie să stabilească echilibrul corect între competențele esențiale pentru afacere față de cele care pot fi externalizate. Iată ce se întâmplă când obțineți echilibrul corect:

Vei economisi timp. Nimeni nu are timp să învețe toate abilitățile sau să angajeze fiecare persoană necesară pentru a conduce o afacere. Furnizorii terți fac ca procesele de afaceri să funcționeze fără probleme obținând toate serviciile profesionale necesare pentru a opera și a onora comenzile pentru clienții dvs.

Vei economisi bani. Poate cel mai mare beneficiu este economiile de costuri. Contractarea unui furnizor terț pentru muncă, după cum este necesar, poate fi mult mai puțin costisitoare decât a avea întotdeauna profesioniști pe statul de plată al companiei. De exemplu, este mult mai puțin costisitor să angajezi un avocat atunci când ai nevoie de unul, mai degrabă decât să-l ții pe un avocat.

Veți obține o expertiză valoroasă. Compania ta nu are timp să dezvolte o nouă echipă de experți. Timpul și costul de a face acest lucru ar fi enorm. Angajarea unui furnizor terță parte pentru expertiză pe care nu o aveți în casă va aduce probabil rezultate mai bune.

Care sunt riscurile utilizării furnizorilor terți?

Este posibil ca terții să nu ia securitatea rețelei lor atât de în serios pe cât doriți. Știind acest lucru, hackerii pot alege să nu atace compania în mod direct. În schimb, ei pot căuta o țintă mai ușoară printre furnizorii dvs. terți. Un subcontractant compromis poate fi ușor transformat într-un punct

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

de intrare pentru infractorii cibernetici.

Dacă furnizorii dvs. nu reușesc să livreze, nu veți livra. Cu toate acestea, riscul este inerent oricărei relații de afaceri. Utilizarea furnizorilor terți implică multe riscuri, dintre care majoritatea pot fi atenuate.

Cel mai mare risc este alegerea unei relații cu o terță parte care nu se aliniază cu standardele dvs. de securitate. De exemplu, echipa de securitate a rețelei trebuie să urmeze protocoale de securitate care se ridică la standardele dumneavoastră specifice. Dacă compania dumneavoastră este obligată de reglementări precum asigurările de sănătate, nu vă puteți permite să angajați o companie de securitate a rețelei care nu respectă reglementările privind asigurările de sănătate. Aveți nevoie de un furnizor care înțelege reglementările și este dispus să se adapteze pentru a respecta aceste reglementări.

Când sunteți obligat de reglementările privind confidențialitatea datelor, trebuie să știți exact ce standarde de securitate sunt implementate și dacă furnizorii dvs. nu sunt la egalitate cu acestea, trebuie să încercați să remediați acest lucru. În caz contrar, vă expuneți compania la riscuri de securitate cibernetică, cum ar fi o încălcare a datelor.

Încălcările de date sunt extrem de perturbatoare, mai ales atunci când protejați informațiile personale. Din păcate, încălcările de date sunt în creștere și sunt mai frecvente decât oricând. Încălcările de date pot cauza întreruperi ale operațiunilor, consecințe financiare devastatoare, acțiuni în justiție și o reputație deteriorată. Pentru a evita acestea, nu vă puteți lăsa garda jos când vine vorba de securitatea proprie sau a furnizorilor dvs.

În funcție de natura compromisului furnizorului terță parte, o organizație se poate confrunta cu diferite riscuri. Să ne uităm la cele mai comune categorii de risc și la amenințările pe care trebuie să fii pregătit să le atenuezi. Un furnizor terț compromis poate duce la riscuri multiple care pot fi împărțite în patru categorii majore: Fig 1

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

Riscuri de securitate cibernetică — Subcontractanții au de obicei acces legitim la diferite medii, sisteme și date ale clienților lor. Atacatorii pot folosi un furnizor terță parte ca punct de intrare pentru a încerca să obțină bunurile dumneavoastră valoroase.

Riscuri operaționale — Infractorii cibernetici pot viza sistemele dvs. interne și serviciile pe care le utilizați în loc de doar datele dvs. Acest lucru poate duce la întreruperi parțiale ale operațiunilor sau chiar la oprirea lor totală.

Riscuri de conformitate — Standardele și reglementările internaționale, locale și specifice industriei stabilesc criterii stricte de securitate cibernetică pe care organizațiile ar trebui să le îndeplinească. În plus, terții care lucrează cu aceste organizații trebuie să respecte aceste cerințe. Nerespectarea conduce, de obicei, la amenzi substanțiale și daune reputației.

Riscuri de reputație — A avea datele și sistemele dvs. valoroase compromise servește drept semnal roșu pentru partenerii și clienții dvs., atât actuali, cât și viitori. Recăpătarea încrederii lor va necesita mult timp și efort. Și, din păcate, nu există nicio garanție că vă veți putea recupera cu succes reputația după un incident grav de securitate cibernetică.

Cerințe de achiziții

Din mai multe motive, uneori organizațiile performante se bazează pe furnizori pentru a oferi ceea ce este necesar pentru a finaliza un proiect. În special, IMM-urile. Prin urmare, cerințele de achiziție sunt de cea mai mare importanță pentru a lucra cu securitatea furnizorilor terți.

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

Deși este adevărat că achizițiile este un proces extrem de individualizat, există, de asemenea, câteva etape fundamentale care vor fi, în general, utilizate în general.

Cerințele de achiziții se referă la bunurile și serviciile care trebuie achiziționate de la organizații din afara organizației executante. Din mai multe motive, uneori organizațiile performante se bazează pe furnizori pentru a oferi ceea ce este necesar pentru a finaliza un proiect.

Etapele Achizițiilor
Etapa 1: Identificați nevoia de produse și/sau servicii.
Etapa 2: Creați și trimiteți o cerere de achiziție.
Etapa 3: Evaluarea și selectarea furnizorilor/furnizorilor.
Etapa 4: Negociați termenii unui contract cu furnizorul selectat.
Etapa 5: Finalizați o comandă de achiziție.

Primul pas în procesul de achiziție este identificarea cerințelor. Toate cerințele de achiziție încep cu percepția unei nevoi. Necesitatea de a traversa un corp de apă ar putea crea o cerință de a construi un pod, un feribot sau alte sisteme de transport.

Etapa 1: Identificați nevoia de produse și/sau servicii
Înainte ca procesul de achiziție să poată începe, trebuie recunoscută o nevoie specifică. De exemplu, o organizație poate fi interesată să achiziționeze noi monitoare de computer, să-și re-comandeze proviziile lunare de produse din hârtie sau să achiziționeze software actualizat. În funcție de structura companiei, acest pas poate fi gestionat de proprietarii de afaceri, șefii de departamente, echipa executivă, personalul și/sau managerii de achiziții. În această etapă, va fi stabilit un buget și va fi adesea evaluată o viziune cuprinzătoare asupra cheltuielilor.

În această etapă este necesar să se definească în mod clar nevoia, iar acest lucru se poate face prin intermediul unui studiu pentru a determina cel mai bun mod de traversare a corpului de apă (dată fiind situația actuală și nevoia viitoare prognozată), apoi tipul de pod către fie construit, sau o analiză comparativă cost/beneficiu pentru a determina cea mai bună soluție între o punte și alte alternative. Studiul ar trebui să includă dacă nevoia poate fi satisfăcută la nivel intern sau sub contract, cuantificarea estimării bugetare inițiale și o idee despre termenul de achiziție.

Etapa 2: Creați și trimiteți o cerere de achiziție
O cerere de achiziție (sau o cerere de achiziție) este o cerere formală pentru bunuri sau servicii și este în general transmisă utilizând un software specializat pentru achiziții. Adesea, cererea de achiziție va proveni de la un angajat sau manager, apoi va fi revizuită de echipa de achiziții a

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

organizației.

Când o cerere de cumpărare este aprobată, aceasta devine o comandă de cumpărare. Cu toate acestea, în cazul în care cererea este respinsă, aceasta va fi în mod obișnuit returnată celui care trimite o cerere cu o scurtă explicație. O comandă de cumpărare respinsă, deși nu este ideală, poate fi o bună oportunitate de învățare.

Etapa 3: Evaluarea și selectarea furnizorilor/furnizorilor
Următorul pas este evaluarea diferiților furnizori, apoi alegerea unuia care îndeplinește cerințele cheie. Unele organizații mențin un catalog de furnizori aprobați, prezentând diferiți furnizori care și-au dovedit deja ei.

Solicitarea furnizorilor este un proces care poate varia de la simplu la complex, cu sfera de aplicare determinată de cerințele în cauză. De obicei, mai multe cereri de ofertă (RFQ) vor fi trimise către diverși furnizori, astfel încât organizația/echipa de achiziții să poată compara prețurile și opțiunile.

Amintiți-vă că prețul nu ar trebui să fie singurul factor determinant atunci când alegeți un furnizor. Pentru cele mai bune rezultate, luați în considerare „imaginea de ansamblu” a ceea ce poate oferi un furnizor, inclusiv:
- Ușurința comunicării
- Etica companiei
- Responsabilitate
- Capabilitati de productie

După ce un furnizor a fost selectat, este important să investiți timp și energie în relație. O relație bună cu un furnizor poate debloca economii și servicii mai bune, oferind valoare maximă pe termen lung.

Etapa 4: Negociați termenii unui contract cu furnizorul selectat
Odată ce ați ales furnizorul cel mai potrivit, este timpul să treceți la negocieri contractuale. În ceea ce privește achizițiile de succes, aceasta este de departe una dintre cele mai critice etape. În această etapă veți sublinia – și veți fi de acord cu – prețul, precum și detalii precum programele de livrare, termenii și condițiile specifice și multe altele. Poate fi adesea util să evaluați contractele anterioare pentru a identifica oportunitățile de îmbunătățire, permițându-vă să adoptați o abordare mai informată în viitor.
Etapa 5: Finalizați o comandă de achiziție
După ce contractul final a fost aprobat, următoarea ordine de lucru este comanda de cumpărare (PO). Contractul guvernează de obicei întreaga relație cumpărător/furnizor, în timp ce o comandă

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

de cumpărare se apropie de o anumită achiziție.

- Gândiți-vă la acest document ca la un alt contract formal, care detaliază complet următoarele:
- Costuri totale/pret
- Descrierea detaliată a bunurilor și/sau serviciilor
- Cantitate
- Orice alți termeni și condiții specifice

Etapa 6: Gestionarea comenzilor

Pe măsură ce bunurile/serviciile sunt livrate, ar trebui să existe cineva responsabil, în mod ideal utilizatorul final al produsului sau serviciilor, să verifice dacă toate standardele au fost respectate termenele de livrare, cantitățile de produse și calitatea etc. Dacă există probleme cu articole (de exemplu, produse deteriorate), aveți opțiunea de a respinge livrarea. Comunicarea clară cu vânzătorul este esențială în cazul oricăror probleme de livrare.

Pe măsură ce tehnologia și comunicațiile permit companiilor să-și extindă lanțurile de aprovizionare, complexitatea gestionării riscurilor furnizorilor crește. Este probabil ca afacerea dvs. să lucreze cu mai mulți furnizori decât oricând înainte și fiecare dintre acești furnizori va prezenta un anumit nivel de risc pentru organizația dvs.

Managementul riscului de securitate al furnizorilor este o strategie concepută pentru a limita numărul de amenințări, vulnerabilități și puncte slabe cu care se confruntă organizația dvs. din cauza furnizorilor din lanțul dvs. de aprovizionare. Un furnizor este de obicei o organizație terță parte care vinde un produs, un serviciu sau un echipament de care afacerea dvs. are nevoie pentru a funcționa.

Fiecare furnizor, atunci când este conectat la organizația dvs., va suporta un anumit nivel de risc pentru securitatea cibernetică. Dacă nu reușesc să-și mențină finalul acordului sau dacă sunt victimele unui atac cibernetic, acest lucru ar putea afecta direct organizația dvs. O evaluare eficientă a riscurilor, ca parte a unui plan mai mare de gestionare a riscurilor furnizorului, se străduiește să identifice aceste puncte potențiale de eșec cu mult înainte ca acestea să devină o problemă și să le remedieze.

Ciclul de management al riscului furnizorilor

Gestionarea riscului de securitate al furnizorilor este un proces continuu și pe care îl veți executa cu fiecare furnizor pe care îl aduceți în lanțul dvs. de aprovizionare. De obicei, procesul arată astfel:

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

Pasul 1: Analiză – Compania identifică riscul inerent al relației și nivelul de due diligence care trebuie efectuat. În consecință, compania evaluează postura de securitate a terței părți și efectuează o analiză a decalajului.
Pasul 2: Implicare – Compania și terțul colaborează pentru a remedia lacunele.
Pasul 3: Remediere – Terța parte remediază lacunele cibernetice.
Pasul 4: Aprobare – Compania aprobă terțul sau îl respinge pe baza toleranței la risc.
Pasul 5: Monitorizare – Compania continuă să monitorizeze terța parte pentru a detecta eventualele lacune cibernetice

Rețelele sociale și riscurile de securitate ale furnizorilor

Rețelele sociale sunt foarte populare în lumea de astăzi. De obicei, o rețea socială este definită ca o rețea de lume mică, constând dintr-un set de indivizi (persoane, grupuri, organizații) conectați prin relații personale, de muncă sau de încredere. Rețelele sociale sunt atunci o noțiune destul de largă și generică, care în contextul Web ar putea fi aplicată oricărui tip de comunitate virtuală. De exemplu, utilizatorii înregistrați la un serviciu web, cum ar fi poșta web, jurnale online sau ziare care necesită abonament, pot fi considerați o rețea socială. În cele ce urmează, adoptăm definiția, conform căreia site-ul Web al unei comunități online poate fi considerat o rețea socială bazată pe Web numai dacă îndeplinește următoarele condiții:

- Relațiile sunt specificate în mod explicit de membrii săi și nu sunt deduse din interacțiunile existente (de exemplu, o listă de corespondență poate fi folosită pentru a deduce relații implicite).
- Relațiile sunt stocate și gestionate prin utilizarea tehnologiilor, cum ar fi sistemele de gestionare a bazelor de date, permițând analiza relațiilor și reglementând accesul și regăsirea datelor relațiilor.
- Membrii pot accesa informații despre relații, cel puțin parțial.

Termeni cheie

Controlul accesului bazat pe relații: o paradigmă de control al accesului special adaptată rețelelor sociale, conform căreia membrii rețelelor sociale autorizați să acceseze o anumită resursă sunt denumiți în termeni de relațiile la care trebuie să participe pentru a obține accesul.

Rețea de socializare: o rețea de lume mică constând dintr-un set de indivizi (persoane, grupuri, organizații) conectați prin relații personale, de muncă sau de încredere. De obicei modelat ca un grafic, unde nodurile corespund membrilor rețelei sociale, în timp ce marginile denotă relațiile existente între ele.

Retele sociale. Comunicarea și împărtășirea informațiilor cu cei din jurul nostru face parte din

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

viața fiecăruia și a evoluat de la simple mesaje text la e-mailuri și la ceea ce numim acum platforme de social media. Ceea ce nu este foarte bine cunoscut sau realizat este faptul că expunerea noastră în mediul online vine cu o mulțime de riscuri.

Rețelele de socializare și rețelele sociale sau aplicațiile de mesagerie pot prezenta o serie de riscuri de securitate și confidențialitate atât pentru organizații, cât și pentru persoane atunci când sunt utilizate într-un mod neadecvat sau nesigur. Cele mai populare și răspândite platforme pe rețelele sociale:

- Facebook cu peste 1.300.000.000 de membri;
- Flickr folosit pentru a stoca, organiza și partaja fișiere media;
- LinkedIn cu peste 300 de milioane de utilizatori;
- Instagram cu peste 30 de milioane de utilizatori;
- Twitter cu peste un miliard de membri;
- YouTube cu peste un miliard de utilizatori;
- Tinder cu aproximativ 12 milioane de utilizatori;
- TikTok cu peste 800 de milioane de utilizatori.

Controlul accesului în funcție de confidențialitate: În contextul rețelelor sociale, denotă o paradigmă de control al accesului în care cerințele de control al accesului ale membrilor rețelelor sociale sunt aplicate fără a dezvălui informații private despre relațiile la care participă.

Rețea socială bazată pe web: un sistem bazat pe web care permite membrilor săi înregistrați să stabilească relații cu alți membri și să partajeze diferite tipuri de informații (de exemplu, date personale, contacte, resurse multimedia).

Analiza rețelelor sociale: O disciplină care vizează colectarea datelor statistice din analiza topologiei rețelelor sociale.

Nivelul de încredere al relației: într-o rețea socială, denotă valoarea asociată cu o relație de încredere, oferind o măsură a cât de mult un membru dat consideră un alt membru demn de încredere. În funcție de scopul în care este folosită, această noțiune poate avea semnificații diferite. De exemplu, într-un mediu de evaluare colaborativă, denotă cât de multă încredere are un membru dat în opiniile altui membru cu privire la un subiect specific (încredere de actualitate) sau în general (încredere absolută). Prin contrast, într-un context de control al accesului, acesta are unele asemănări cu noțiunea de nivel de securitate utilizată în modelele de control al accesului obligatoriu.

Perturbarea marginilor: Tehnica de anonimizare a graficelor care vizează ascunderea relațiilor

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

reale de rețea socială prin efectuarea unui set de ștergere/inserții aleatoare ale marginilor în graficul rețelei.

Relație de rețea socială: o relație care privește doi membri ai unei rețele sociale. În WBSN, pe lângă relațiile personale/de muncă (de exemplu, prieten/coleg), pot fi acceptate și relațiile de încredere care denotă cât de mult are încredere un membru în altul. În reprezentarea grafică a unei rețele sociale, relațiile sunt de obicei notate prin margini, etichetate cu un tip de relație și/sau un nivel de încredere în relație.

Anonimizare grafică: tehnică care vizează ascunderea informațiilor private despre membrii rețelei sociale atunci când se efectuează analiza rețelelor sociale. Anonimizarea nodurilor și perturbarea marginilor sunt cele două tehnici principale de anonimizare a graficelor utilizate în prezent.

Anonimizarea nodurilor: Tehnica de anonimizare a graficelor care vizează ascunderea identităților membrilor rețelelor sociale prin etichetarea nodurilor corespunzătoare cu identificatori aleatori (anonimizare naivă) sau, în cazul în care nodurile sunt asociate cu atribute care pot fi folosite pentru a identifica utilizatorul corespunzător, prin utilizarea tehnicilor bazate pe pe k-anonimitate (Sweeney, 2002).

Riscuri

Geoetichetarea

- Reprezintă adăugarea de date de identificare geografică la fotografii, videoclipuri, site-uri web și mesaje text de către aplicații care vă pot citi locația sau au voie să facă acest lucru în setările dvs.;
- Asigurați-vă că dezactivați funcțiile de geoetichetare în locații sensibile pentru a evita dezvăluirea locației dvs. exacte, unde lucrați sau unde locuiți.

" Public"

- Este un termen general care se referă la cine este capabil să vadă și/sau să comenteze postările tale;
- Grupul tău de prieteni se poate schimba oricând și poate vedea o postare care conține informații despre tine. S-ar putea să le împărtășiți în mod intenționat „prietenilor”, dar ceea ce fac aceștia cu postarea este în afara controlului dumneavoastră personal.

Identitate

- Descrie gama de informații care se referă în mod specific la o persoană;
- Trebuie avut în vedere faptul că există persoane care folosesc rețelele sociale ca metodă de

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

cercetare pentru a căuta informații de identitate, cu posibile intenții rău intenționate, cum ar fi furtul de identitate, frauda, delapidarea sau intimidarea.

Măsuri

Parola

- Se recomandă utilizarea unei parole diferite pentru fiecare cont online;
- Ar trebui să aibă cel puțin 10 caractere și să conțină litere mari, litere mici, cifre și caractere speciale;
- Nu trebuie dezvăluit nimănui, indiferent cât de apropiată sau de încredere este persoana căreia vrem să o spunem
- Se recomandă să nu folosiți informații personale la crearea unei parole (ex.: numele părinților, data nașterii, numele animalului de companie etc.);
- Schimbați-vă parola periodic;
- Deconectați-vă de la contul dvs. atunci când utilizați un dispozitiv care nu este al dvs. sau este folosit de altcineva.

Faceți actualizările de securitate la timp!

- Platformele de social media introduc în mod regulat noi setări de confidențialitate și securitate. Acestea pot fi găsite în setările contului dvs. și este recomandat să le verificați în mod regulat;
- Utilizați opțiunea de autentificare cu doi factori (2FA) pentru a vă asigura că cineva nu încearcă să vă pirateze contul.

Nu accepta cereri de prietenie de la nimeni!

- Acceptați sau trimiteți cereri de prietenie doar de la/către persoane pe care le întâlniți în viața reală sau către persoane publice de care sunteți interesat, având grijă să le urmăriți profilurile oficiale;
- NU UITA! Dacă te simți atașat de anumite conturi, le poți restricționa accesul la postările tale sau poți bloca contul. De asemenea, aveți opțiunea de a raporta conturi sau postări din motive precum: cont fals, nume fals, postări cu conținut neadecvat, incitare la violență, informații false etc.
- NU dați clic!
- Mulți atacatori folosesc ingineria socială pentru a câștiga încrederea unei persoane pentru a obține ulterior acces la informații;
- Nu deschideți link-uri și atașamente din rețelele sociale dacă nu sunteți 100% sigur de sursă (de exemplu, site-urile web care oferă premii au adesea scopul de a fura informații);
- Dacă din chat-uri, un prieten pare să se comporte diferit (pune multe întrebări, devine foarte curios în legătură cu viața lui personală, cere bani) există posibilitatea ca contul său să fi fost spart și un atacator să îl folosească în scopuri rău intenționate. scopuri.

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

Gândește-te de două ori înainte de a posta!

- Social media oferă la fel de mult o oportunitate de a crea o reputație online pozitivă ca și una negativă, în plus, chiar dacă „ștergem" o postare, odată ce a apărut online aceasta nu poate fi ștearsă definitiv;
- Nu dezvălui prea multe detalii personale pe rețelele de socializare! Câmpurile „Despre mine" sunt opționale.
- Granița dintre viața profesională și cea personală în mediul online
- Nu divulgați online informații despre angajatorul dvs
- Nu postați fotografii de serviciu sau mesaje negative care pun angajatorul într-o lumină proastă.
- Gândește-te înainte de a posta și nu-ți risca jobul.

Închideți conturile vechi!

- Dacă aveți conturi vechi pe platformele de socializare pe care nu le mai folosiți, sau chiar conturi vechi pe aceeași platformă, încercați să le închideți. În acest fel creați cât mai puține link-uri, conturile curente fiind mai protejate de posibili atacatori;
- Este posibil ca conturile sau platformele mai vechi să nu fie la fel de sigure ca cele de astăzi.

Rețelele de socializare prezintă mari riscuri

- Rețelele sociale prezintă riscuri ridicate de securitate și confidențialitate datorită arhitecturii lor centralizate, a depozitului lor uriaș de informații de identificare personală pe care orice hacker i-ar plăcea să le aibă și a ignoranței generale a populației cu privire la modul de utilizare adecvată a rețelelor sociale. setări de confidențialitate pentru a le îmbunătăți siguranța online.
- Un alt risc foarte mare, mai ales în rândul adolescenților, este încrederea în alte persoane și tipul de informații personale dezvăluite online.
- Acest lucru poate fi combatet prin mijloace tehnologice și prin aplicarea politicilor de securitate.
- Ar trebui să considerăm că informațiile transmise prin intermediul rețelelor sociale sunt nesigure și, prin urmare, nu transmitem informații sensibile prin intermediul rețelelor sociale, astfel că responsabilitatea principală de a rămâne în siguranță revine UTILIZATORULUI

Obiceiuri proaste în rețelele sociale

- Rețelele sociale sunt platforme utilizate pe scară largă de utilizatori în prezent. Avem o gamă largă de posibilități.
- Unele sunt mai orientate spre încărcarea de fotografii sau videoclipuri, altele spre opinia noastră și în alte cazuri pur și simplu pentru a păstra legătura cu prietenii și familia. În orice caz, avem de-a face cu platforme care au mulți utilizatori în întreaga lume.
- Acest lucru îi face și pe hackeri să-și pună ochiul aici. Vom vorbi despre aceste obiceiuri care ar trebui schimbate în rețelele sociale dacă vrem să ne păstrăm confidențialitatea și securitatea.

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

- Există multe tipuri de platforme pe care le putem găsi în rețea care ne oferă posibilitatea de a trimite mesaje prietenilor sau familiei, comentând fotografii, videoclipuri...
- Acest lucru le face un mediu foarte popular atât pentru utilizatorii privați, cât și pentru companii.
- Cu toate acestea, acest lucru vă determină și să aveți un anumit risc pentru securitatea și confidențialitatea noastră. Hackerii pot urmări aici pentru a-și duce atacurile. Ei pot profita în special de obiceiurile proaste ale utilizatorilor atunci când folosesc aceste platforme.

Obiceiuri care trebuie schimbate

- Confidențialitatea și securitatea sunt factori foarte importanți pentru utilizatori.
- Cu toate acestea, ele nu sunt întotdeauna prezente.
- Putem fi victimele multor tipuri de atacuri care compromit acești doi factori.
- De asemenea, putem face greșeli atunci când folosim rețelele sociale și ne afectează.

Adăugați orice tip de contact

- O eroare foarte comună în rețelele sociale este adăugarea oricărui tip de contact. Acest lucru se poate întâmpla pe platforme precum Facebook.
- Este posibil ca ceea ce adăugăm să fie mai degrabă un bot decât un utilizator real.
- Trebuie să știi să le diferențiezi și să eviți să adaugi orice tip de contact pe care îl primește invitația ta.
- Uneori, boții sunt proiectați exclusiv pentru a colecta date despre utilizatori. Acest lucru ne poate compromite confidențialitatea. Trebuie să avem un filtru real asupra contactelor pe care le adăugăm.
- Este important ca printre prietenii noștri să avem oameni care nu reprezintă o problemă pentru securitatea și confidențialitatea noastră.

Nu vă conectați la rețelele sociale de oriunde

- Vă autentificați adesea prin rețelele sociale de pe orice site. Acesta este foarte confortabil, dar nu este cel mai bun pentru confidențialitate.
- Cu siguranță în multe ocazii găsim posibilitatea de a ne înregistra pe o pagină sau de a ne conecta la o platformă prin Facebook sau Twitter. Evităm să ne înregistrăm pe acel site și să completăm un formular lung. Problema este că furnizăm date personale acelui site prin intermediul Facebook. Aceste date/informații pe care le împărtășim pot fi folosite de terți în scopuri publicitare.

Nu furnizați mai multe informații decât este necesar

- Este cu siguranță unul dintre cele mai rele obiceiuri pe care le au mulți utilizatori. Ei introduc o mulțime de date personale, informații care nu sunt cu adevărat necesare, în rețelele de socializare.
- De exemplu, date precum numărul nostru de telefon, adresa de e-mail, informații despre locul

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

în care locuim... Toate acestea ne afectează publicitatea și ar putea fi folosite în scopuri rele.

- Nu oferi mai multe informații decât este cu adevărat necesar. În acest fel ne vom îmbunătăți confidențialitatea în rețea și chiar putem evita anumite probleme de securitate.

Răspândirea de știri false

- Problema știrilor false este prezentă și astăzi. Pot ajunge la ei prin multe mijloace, dar fără îndoială în rețelele de socializare sunt mai mult decât prezențe.
- După cum știm, este o știre falsă pe care o folosesc ca momeală și uneori chiar pot distribui malware.
- Este important să evităm distribuirea acestui tip de știri false și, de asemenea, să le accesăm atunci când le vedem pe rețelele sociale.
- Acest lucru ne va îmbunătăți securitatea.

Nu ne protejăm intimitatea

- O ultimă greșeală este de a nu proteja în mod corespunzător intimitatea. De exemplu, lăsăm profilurile noastre deschise pentru ca oricine să intre.
- Oferim informații oricărei persoane care le-ar putea colecta pentru a ne crea un profil și chiar pentru a trimite publicitate țintită sau pentru a efectua diverse atacuri care ne afectează securitatea.

Ingineria socială dintr-o perspectivă interdisciplinară

- Datorită tehnicii folosite de hackeri, este necesar să se abordeze o perspectivă interdisciplinară precum tehnologia informației, psihologia, afacerile și etica..

Disciplina tehnologiei informației

- Ingineria socială ar trebui să fie discutată în contextul sistemelor informaționale actuale și apărarea lor utilizată ca formă de atenuare a riscurilor.
- Autentificarea multifactorială este o modalitate comună și adesea eficientă pentru organizații de a confirma că persoana care accesează sistemele ar trebui să aibă de fapt acel acces
- Un factor suplimentar ar putea fi utilizarea unei rețele private virtuale (VPN), de ex. autentificare pentru a valida în continuare utilizatorul.

Disciplina psihologiei

- Este necesar să înțelegem conceptul și să înțelegem gândurile și comportamentele atât ale atacatorului, cât și ale victimei.
- Metodele sunt importante pentru ingineria socială, deoarece sunt folosite pentru a ocoli protecțiile care pot fi existente, cum ar fi firewall-urile și sistemele utilizate pentru a identifica intrușii.
- Ajută la înțelegerea acțiunilor angajaților care sunt una dintre principalele cauze ale încălcării

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

datelor.

Perspectiva afacerii

- este important deoarece ingineria socială poate afecta multe tipuri de afaceri și poate avea implicații asupra modului în care sunt structurate și gestionate organizațiile.
- ajută la determinarea factorilor care influențează atacurile de inginerie socială și este benefică dacă este luată în considerare în termeni mai specifici în raport cu următoarele domenii de afaceri: instruire și dezvoltare, politici documentate, proceduri de audit intern, bugete și cultură organizațională.
- poate detecta deficiențe în oricare dintre zonele care pot contribui la atacuri.

Perspectivă etică

- este important în contextul ingineriei sociale și al cercetării aferente, deoarece ideea de a manipula o altă ființă umană încalcă multe principii etice.
- ajută, în cazul unui eveniment de inginerie socială, la tratarea victimelor.

Este important de luat în considerare:

- fiecare disciplină, oferind informații despre cum să înțelegeți și să interpretați subiectul, să vă protejați împotriva diferitelor tipuri de atacuri și să înțelegeți impactul ingineriei sociale atât din perspectivă umană, cât și organizațională.
- că interpretarea fiecărei discipline a subiectului este utilă numai atunci când este privită în contextul celorlalte discipline.

Tehnici de securitate

- Inventarul echipamentelor
- Inventarul de aplicatii si sisteme de operare
- Controlul echipamentelor wireless
- Proiectarea securității rețelei
- Limitarea și controlul porturilor de rețea, protocoalelor de comunicație și serviciilor
- Protejarea zonelor perimetrale
- Acces fizic la locații
- Utilizarea controlată a privilegiilor administrative
- Monitorizarea și controlul conturilor de utilizator
- Evaluarea competențelor și formarea în securitate

VPN (Virtual Private Network)

O rețea privată virtuală este o conexiune sigură printr-o rețea nesigură, cum ar fi Internetul. Virtual înseamnă existența unei rețele unice, indiferent de topologie, adică un grup de

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

calculatoare distribuite geografic care comunică și pot fi administrate ca o singură rețea.

Privat înseamnă o rețea virtuală cu control acces. care asigură confidențialitatea, integritatea mesajelor și autentificări între utilizatori și computerele care participă la comunicare.

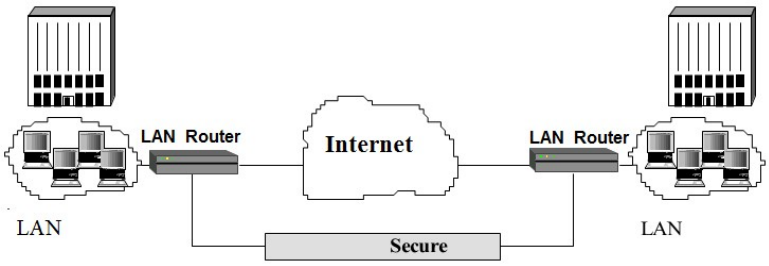

Fig. 2: VPN (Virtual Private Network)

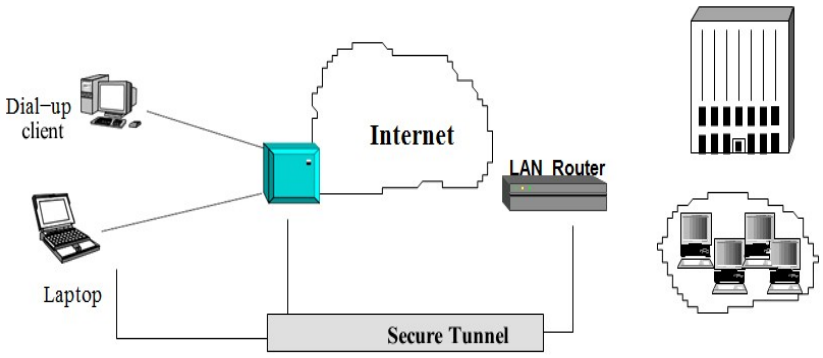

Fig. 3: VPN pentru acces la distanță

Crearea unei infrastructuri industriale sigure

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

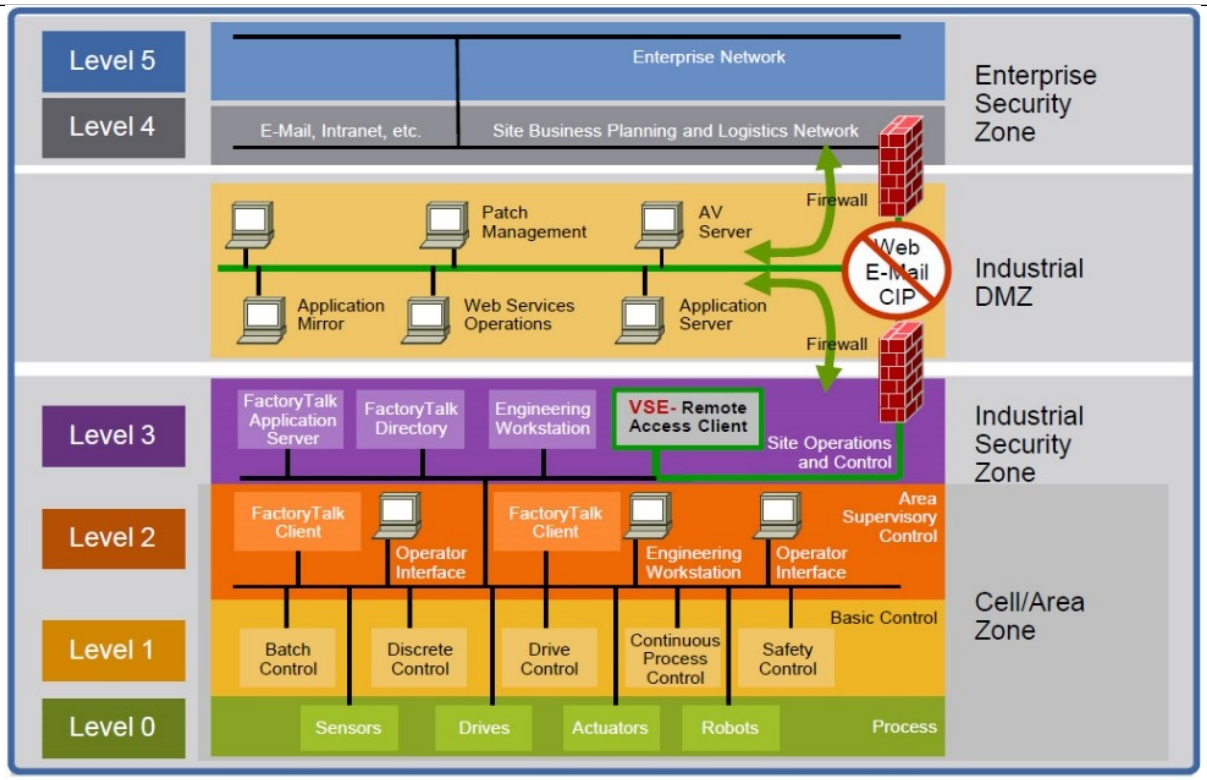

Fig. 4: Model logic ISA 95 - Sistem de automatizare și control industrial (IACS)

- Defense-in-Depth (DiD) sprijină această abordare. Pe baza noțiunii că un singur punct de protecție poate și probabil va fi învins, securitatea DiD stabilește mai multe straturi de protecție printr-o combinație de garanții fizice, electronice și procedurale.
- O bancă folosește mai multe măsuri de securitate – cum ar fi camere video, un paznic și un seif – acest lucru ajută la asigurarea faptului că amenințările îndeplinesc mai mult de o linie de apărare.
- O abordare de securitate în profunzime cuprinde șase componente principale:

1. Politici și proceduri
2. Fizic
3. Rețea
4. Computer
5. Aplicare
6. Dispozitivul

Crearea unei infrastructuri industriale sigure

- Securitatea fizică ar trebui să limiteze accesul personalului nu numai la zonele unei instalații, ci și la punctele de intrare în infrastructura fizică a rețelei, cum ar fi panourile de control,

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

cablurile și dispozitivele.

- Segmentarea zonelor fabricii în rețele locale virtuale (VLAN-uri) este o bună practică de securitate la nivel de rețea.
- VLAN-urile mai mici sunt mai ușor de gestionat și întreținut în comunicații în timp real.
- Ele pot ajuta la izolarea dispozitivelor de cele care au fost compromise, ceea ce păstrează impactul negativ într-un singur VLAN.
- Una dintre tehnologiile discutate ar trebui să fie o zonă industrial demilitarizată (IDMZ), care creează o barieră de protecție critică între întreprindere și zonele industriale.
- Un IDMZ restricționează traficul să circule direct între cele două zone și poate ajuta la o mai bună gestionare a accesului prin aplicarea autentificării sau monitorizarea traficului pentru amenințările cunoscute.

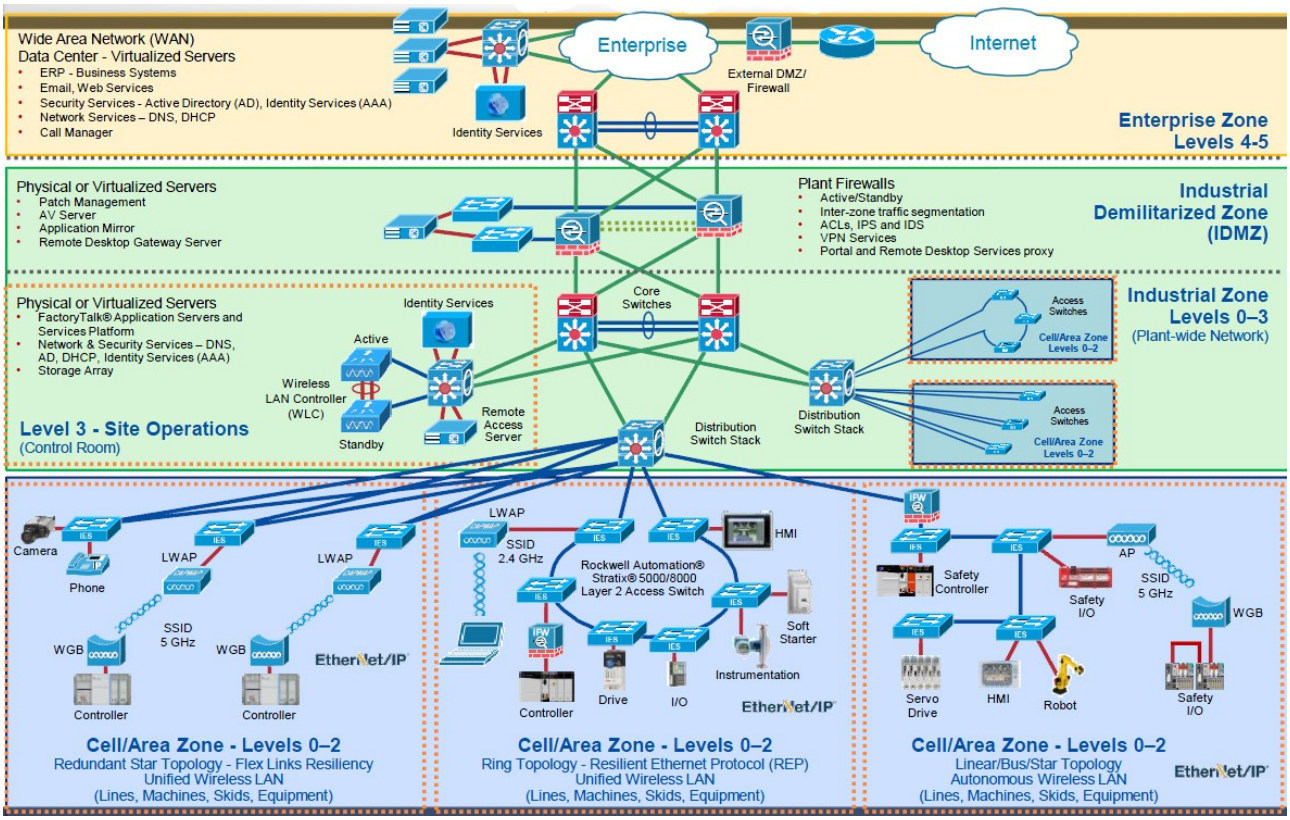

Fig. 5: IDMZ

Întrebări:

Forumul de discuții la care se răspunde cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat

1. Care sunt riscurile în rețelele sociale
2. Măsuri pentru a avea Securitate și Confidențialitate în Rețelele Sociale

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

3. Care sunt principalele tehnici de securitate în rețelele sociale

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

- Riscuri în rețelele sociale
- Securitate și confidențialitate în rețelele sociale
- Tehnici de securitate

Atasamente *(Prezentare PowerPoint, fișe, printuri, link-uri, video ...):*

Referințe:

Procurement Requirements
URL: Procurement-requirements
URL: https://www.ekransystem.com/en/blog/third-party-providers
Procurement Requirement Determination
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Security and Privacy in Social Networks
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Security and Privacy in Social Networks
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Privacy and Security in online social media
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Data Security Techniques and Privacy
URL: https://www.educba.com/data-security-techniques/
What is Security Techniques
URL: Security-concepts-developments-and-future-trends
Most Effective Security Techniques
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.