Studiu de caz

SECURITATEA CIBERNETICĂ ÎN INDUSTRIA 4.0

Cuvinte cheie: *Securitate cibernetică, tehnologie, atacuri cibernetice, siguranță*

Contextul studiului de caz

Multitudinea de noi tehnologii creează oportunități și spații pentru atacuri cibernetice, motiv pentru care asigurarea securității cibernetice este esențială pentru succesul Industriei 4.0. Este foarte important ca organizațiile să-și actualizeze cunoștințele și instrumentele pentru a face față provocărilor viitoare. Cele mai multe medii industriale nu au fost concepute având în vedere securitatea cibernetică ridicată. Sistemele de producție se îndreaptă acum către sisteme cyber-fizice, unde orice tip de vulnerabilitate ar putea fi detectat și exploatat de persoane rău intenționate.

Introducere în studiul de caz și relevanța acestuia pentru Industria 4.0.

Securitatea cibernetică este încă asociată cu protecția împotriva virușilor sau a programelor malware, dar în prezent amploarea și amenințarea sunt, cu siguranță, globale. Sunt tot mai multe infracțiuni financiare sau acte de spionaj, dar există chiar și atacuri asupra infrastructurii critice și a guvernelor. Pentru a minimiza amenințarea și a profita de oportunitățile oferite de Industria 4.0, este necesar să se disemineze și să se aplice bune practici de protecție împotriva amenințărilor cibernetice.

Securitatea digitală trebuie să fie rezultatul unei politici cuprinzătoare de management al conținutului IT și al îmbunătățirii competenței utilizatorilor. Factorul uman este mai dificil decât factorul infrastructură, deoarece cel mai frecvent mod de scurgere a datelor de la locul de muncă se realizează prin intermediul angajaților, prin utilizarea, de exemplu, a e-mailurilor private sau prin conectarea unor persoane neautorizate. Companiile suportă pierderi financiare importante în caz de scurgere de informații comerciale și industriale.

Prin urmare, protecția datelor începe cu punerea în aplicare și asigurarea respectării normelor de securitate de către angajați.

Proiect nr. 2019-1-PL01-KA202-064936
Sprijinul acordat de Comisia Europeana pentru elaborarea acestei publicatii nu constituie o aprobare a continutului, care reflecta doar opiniile autorilor, iar Comisia nu poate fi trasa la raspundere pentru orice utilizare a informatiilor continute în aceasta.

Cofinanțat prin programul Erasmus+ al Uniunii Europene

Studiu de caz

Studiul de caz și elementele Industriei 4.0: O imagine de ansamblu ilustrată

Internetul și Industria 4.0 deschid noi oportunități de comunicare și schimb de informații, dar securitatea inadecvată poate implica o serie de riscuri grave și pierderi financiare însemnate. Siguranța este un proces în cadrul căruia se desfășoară în mod constant un set de activități. Unul dintre modelele care descriu siguranța este modelul CID, pe care fiecare companie ar trebui să-l definească, să-l respecte și să-l mențină.

Modelul de securitate CID se bazează pe trei elemente de bază:
- Confidențialitate – datele și serviciile ar trebui să fie accesibile doar celor care au dreptul acesta
- Integritate – orice încercare de compromitere a datelor și serviciilor ar trebui detectată și înregistrată
- Disponibilitate – oricine are dreptul ar trebui să poată folosi resursele.

Proiect nr. 2019-1-PL01-KA202-064936
Sprijinul acordat de Comisia Europeana pentru elaborarea acestei publicatii nu constituie o aprobare a continutului, care reflecta doar opiniile autorilor, iar Comisia nu poate fi trasa la raspundere pentru orice utilizare a informatiilor continute în aceasta.

Cofinanțat prin programul Erasmus+ al Uniunii Europene

Studiu de caz

SECURITATEA CIBERNETICĂ ÎN INDUSTRIA 4.0

Elementul studiat în cadrul aplicației în Industria 4.0.	*Polski Tytoń Dystrybucja este unul dintre cei mai mari distribuitori de bunuri de larg consum și produse din tutun din Polonia. Compania oferă și servicii logistice și comerciale. Vânzările se realizează în cadrul Departamentului de vânzări și prin reprezentanți de vânzări, care ajung direct la clienți. Compania depune eforturi constante de îmbunătățire a calității serviciilor sale pentru a răspunde cât mai bine dorințelor clienților săi. Pentru a oferi servicii la cel mai înalt nivel, investește în pregătirea personalului și modernizarea sistemului.* *Polski Tytoń a implementat sistemul de management Axence nVision care permite administrarea și raportarea continuă a stării fiecăruia dintre dispozitivele conectate la rețea, crescând astfel nivelul de securitate al infrastructurii IT a companiei.* *Principala provocare a companiei a fost găsirea unui instrument care să permită controlul proceselor care au loc în rețea în sucursale individuale. Un alt domeniu care trebuia îmbunătățit a fost monitorizarea resurselor hardware din camera serverului și din stațiile de lucru individuale, precum și utilizarea computerelor și a dispozitivelor de rețea de către angajați.* *De la implementarea acestei soluții, compania a putut lucra cu o consolă la distanță care permite administratorilor autorizați să acceseze programul de pe orice computer, acest lucru facilitând monitorizarea continuă a parametrilor aplicației, vizualizarea jurnalului de evenimente sau a serviciilor de sistem. Utilizarea modulelor de rețea limitează conectarea dispozitivelor private externe și, de asemenea, permite monitorizarea condițiilor de mediu din camera serverului, ceea ce oferă protecție și duce la limitarea defecțiunilor.* *Administratorul este informat în cazul unei creșteri periculoase a temperaturii serverului sau a lipsei de spațiu de pe disc. De asemenea, compania a limitat afișarea profilurilor sociale și a serviciului Youtube, lucru care a avut un efect pozitiv în ceea ce privește performanța angajaților.* *Implementarea acestei soluții a adus companiei multiple beneficii:* *- Îmbunătățirea transparenței și a gradului de utilizare corporativă,*

Proiect nr. 2019-1-PL01-KA202-064936
Sprijinul acordat de Comisia Europeana pentru elaborarea acestei publicatii nu constituie o aprobare a continutului, care reflecta doar opiniile autorilor, iar Comisia nu poate fi trasa la raspundere pentru orice utilizare a informatiilor continute în aceasta.

Cofinanțat prin programul Erasmus+ al Uniunii Europene

	- Departamentul IT a primit acces pentru a monitoriza toate procesele care au loc în rețea, *- Perspectivă asupra datelor colectate și analizate de sistem,* *- Detectarea ușoară a defecțiunilor tuturor dispozitivelor,* *- Reducerea costurilor de întreținere în general și de întreținere a infrastructurii IT,* *- Creșterea eficienței asistenței tehnice,* *- Controlul asupra funcționării și utilizării rețelei,* *- Creșterea eficienței proceselor de afaceri,* *- Economie de timp prin posibilitatea de a reacționa rapid la erorile de sistem și de a oferi asistență de la distanță angajaților.*
Publicul țintă al aplicației:	*Rezultatele studiului de caz sunt destinate utilizării de către IMM-uri și antreprenori.*
Resurse utilizate:	*https://axence.net/files/pdf/media/case_study_polski_tyton.pdf* *http://ptdystrybucja.pl/o-firmie/*
Informații suplimentare:	*https://ik.org.pl/wp-content/uploads/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf* *https://axence.net/pl/o-nas* *http://websecurity.pl/pojecie-bezpieczenstwa-cia/*

Proiect nr. 2019-1-PL01-KA202-064936
Sprijinul acordat de Comisia Europeana pentru elaborarea acestei publicatii nu constituie o aprobare a continutului, care reflecta doar opiniile autorilor, iar Comisia nu poate fi trasa la raspundere pentru orice utilizare a informatiilor continute în aceasta.

Cofinanțat prin programul Erasmus+ al Uniunii Europene