



hi!tech

Securitatea web

Necesitatea unei protecții avansate împotriva amenințărilor digitale

**Despre NIS2,
informații utile**

Directiva UE privind
securitatea cibernetică

**Digitalizarea
pârtilor de schi**

Condiții de schi
optimizate prin utilizarea
tehnologiei

**Focus pe comunitățile
de energie**

Cercetările privind
îmbunătățirea planificărilor
și a operațiunilor



Editorial

Dragi cititori,



Daniel Barciuc
CEO Siemens România



Coperta: Imagini Getty/E+/Doar_Super

Editură și tipar

hi!tech - Revista inovației a Siemens Austria
Editor și proprietar media - Siemens AG Austria,
Siemensstrasse 90, 1210 Viena
Publicat de - Katharina Swoboda
Redactor șef - Christian Lettner
Grafică și design - alaki-design
Litografie - R12
Contact - siemens.ro@siemens.com
siemens.ro/hitech

Într-o lume din ce în ce mai digitalizată, atât persoanele, cât și companiile devin extrem de vulnerabile în fața atacurilor cibernetice. În plus, folosirea inteligenței artificiale pentru accesarea frauduloasă a datelor sensibile este din ce în ce mai des întâlnită.

De aceea ne propunem ca în numărul actual al revistei noastre să vă punem la dispoziție articole interesante despre securitatea cibernetică, astfel încât să puteți afla opinii avizate ale experților Siemens din acest domeniu, dar și informații despre noul context legislativ, care să vă ajute în activitatea pe care o desfășurați.

Astfel, unul dintre subiectele căruia i-a fost acordat un larg spațiu editorial este actuala directivă europeană NIS (Securitatea rețelelor și a sistemelor informatice), a cărei formă adaptată și extinsă va deveni obligatorie de la 18 octombrie 2024, în toate statele Uniunii

Europene, sub denumirea de "NIS 2". Veți găsi exemple despre modul în care anumite organizații s-au pregătit pentru a putea respecta prevederile Directivei NIS 2, ținând cont că doar companiile cu mai puțin de 50 de angajați și o cifră de afaceri anuală mai mică de 10 milioane de euro nu sunt vizate de aceasta.

La nivel practic, digitalizarea și securitatea cibernetică fac parte din realitatea de fiecare zi atât a utilizatorilor de produse și servicii, cât și a producătorilor. De exemplu, datele relevante care rezultă din experiența de a conduce un anumit model de autoturism, odată partajate cu fabricantul, vor contribui la îmbunătățirea continuă a performanței autovehiculelor acestuia.

Cooperarea, transparența și cunoștințele solide sunt atuurile echipelor noastre, care vă stau la dispoziție pentru a răspunde împreună încercărilor viitorului. Vă urăm lectură plăcută și vă rămânem alături.

Cuprins

hi!biz

intro

Călătorește cu avionul, în siguranță
Suita de teste de securitate all-in-one

O mare de date, cu multe „phishing-uri”

Numărul infracțiunilor cibernetice crește de la an la an. Boți, virusi, phishing, achiziții frauduloase, apeluri false de la poliție și servicii de livrare non-existente - atacurile devin din ce în ce mai sofisticate.

Întotdeauna cu un pas înainte

Siemens și institutele de cercetare fac tot ce le stă în putință pentru a contracara hackerii cu măsuri sofisticate de securitate cibernetică.

NIS2 ar putea avea un impact și asupra voastră!

Începând cu octombrie 2024, noua directivă NIS2 a UE, care se adresează companiilor mijlocii și mari, precum și infrastructurilor critice, intră în vigoare.

Domeniu de schi digitalizat

Condițiile pârtiilor din stațiunea de schi pe ghețar din Sölden, Tirol, sunt optimizate printr-o soluție inteligentă. Aceasta reduce riscurile de a nu avea zăpadă în sezon și maximizează eficiența energetică a sistemului de producere a zăpezii.

hi!future

6 intro

Mai multă energie regenerabilă
Asistent cu inteligență artificială generativă
Soluție completă 5G

8 Blueprint pentru o sortare mai eficientă a deșeurilor

O soluție robotică inovatoare, îmbunătățită cu inteligență artificială, facilitează un proces automatizat și adaptabil de sortare a deșeurilor.

Noul update criptografic

Un algoritm de criptare a fost dezvoltat la Universitatea de Tehnologie din Graz, care se dovedește a fi extrem de adecvat pentru utilizarea în organizații mici, cu capacitate de calcul redusă - bazat pe Internet of Things.

Protejarea echipamentelor Internet of Things pentru domeniul industrial (IIoT)

Într-un proiect de cercetare, Universitatea de Tehnologie din Graz și Siemens colaborează pentru a dezvolta componente software industriale.

Rețele securizate cu Siemens Xcelerator

Prin intermediul instalației sale pilot unice, operatorul sloven de distribuție de energie electrică, Elektro Gorenjska, se află în pragul îndeplinirii cerințelor Uniunii Europene pentru securitatea rețelelor și a sistemelor de informații.

Focus pe comunitățile de energie

Prin intermediul a două proiecte de cercetare inovatoare, Siemens și partenerii săi lucrează pentru a optimiza funcționarea și planificarea comunităților locale de producție și consum de energie.

Schimbul de date în ecosistemele deschise

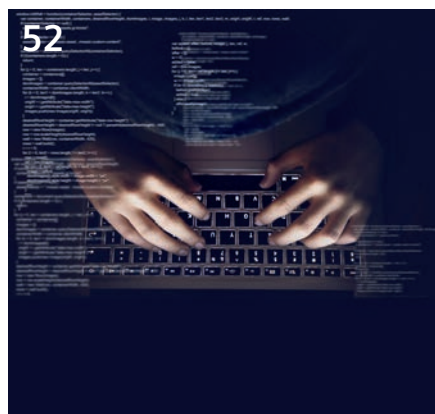
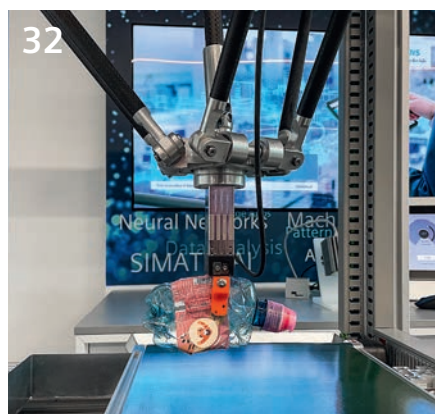
Suveranitatea datelor este esențială: colaborarea în afara granițelor companiei necesită reguli clare pentru partajarea datelor.

Securitatea cibernetică în viitor

Natalia Oropeza și Andreas Kind dezvăluie cum, alături de echipele lor, asigură protecția Siemens și a clienților săi împotriva atacurilor cibernetice.

hi!bye

Vă prezentăm o serie de reportaje de ultimă oră și alte informații relevante.



În această secțiune vă sunt prezentate descoperiri din lumea digitală.
Sub titlul „hi!tech acum 20 de ani” privim retrospectiv asupra edițiilor anterioare.



Calea europeană către digitalizarea economiei

Umanismul digital devine una dintre temele centrale ale digitalizării în economie. ChatGPT alimentează deja dezbaterile publice în jurul inteligenței artificiale și necesită răspunsuri adecvate atât din partea companiilor, cât și a politicienilor în ceea ce privește un comportament responsabil față de IA și tehnologiile digitale în general. Umanismul digital poate oferi răspunsuri, dar forma sa este prea puțin tangibilă în prezent.

Nu există aproape niciun standard sau proceduri testate pentru implementare și există doar câteva exemple în practica operațională care pot servi drept modele de urmat. Aici intervine această carte pe care v-o recomandăm. Aceasta descrie cum ideile umanismului digital pot fi implementate cu succes.

Sunt prezentate exemple și abordări ale unor mari companii din diverse sectoare, precum și noi soluții tehnologice sau procedurale. Politicieni și părți interesate, directori executivi ai unor companii renumite, printre care Patricia Neumann, CEO al Siemens Austria, precum și profesori remarcabili care sunt implicați în cercetare în acest domeniu, își prezintă abordarea cu privire la subiectul umanismului digital, obiectivele proprii, experiențele de implementare și exemple în acest sens.



hi!tech acum 20 de ani

Ediția hi!tech 2/2003 a abordat pilele de combustie ca alternativă la bateriile reîncărcabile convenționale pentru telefoane mobile și laptopuri. Am prezentat un „sistem de alimentare mobilă, o sursă de energie externă compactă cu o durată de funcționare deosebit de mare pentru funcționarea laptopurilor, telefoanelor mobile, PDA-urilor și a altor dispozitive electronice”. Acesta ar fi aproape de producția de serie și „conține metanol lichid sub forma unui cartuş de combustibil înlocuibil”. „Un singur cartuş poate alimenta un laptop pentru o zi întreagă de lucru”, se arată în comunicat. Potrivit producătorului Smart Fuel Cell (SFC), cu sediul în München, „dacă dezvoltarea continuă în același ritm, mini-centrala energetică ar putea fi în curând de dimensiunea unei baterii reîncărcabile”.

SFC Energy AG susține că este un furnizor de referință de pile de combustie cu hidrogen și metanol pentru soluții de alimentare cu energie hibridă staționară și mobilă. Compania comercializează produse premiate în întreaga lume și a vândut până în prezent peste 65.000 de pile de combustie. Noi încă așteptăm pila de combustie pentru laptop ... 😞.

Un alt producător a folosit dezvoltarea SFC pentru „Energy Docking Station”, iar un altul, avea în plan o „dispozitiv maraton”: „Stația de lucru PC completă oferă spațiu pentru șapte pile de combustie de rezervă. Acest lucru permite până la 50 de ore de funcționare continuă”.





Despre securitatea cibernetică industrială

Obiectivele industriale, clădirile de birouri din ce în ce mai conectate și utilizarea Internet of Things prezintă multe avantaje dar, în același timp, sporesc și riscul de amenințări cibernetice. Nimeni și nimic nu este în siguranță împotriva acestor atacuri, iar dezvoltarea și administrarea infrastructurilor critice sunt din ce în ce mai vizate de hackeri din întreaga lume. În seria de videoclipuri „Cybersecurity Industrial Talks” disponibilă scanând codul QR de mai jos, experții Siemens vorbesc despre pericolele pe care le reprezintă acești intruși și despre strategiile

ce pot fi folosite pentru a ne proteja.



Whitepaper „Transformarea clădirilor”



Criza energetică și schimbările climatice necesită acțiuni urgente - în special în cazul clădirilor. Există deja tehnologii revoluționare pentru crearea de clădiri inteligente și autonome.

Prin scanarea

codului QR, veți accesa un articol și veți afla cum să îmbunătățiți eficiența energetică a clădirilor și veți afla mai multe despre noile cerințe tehnologice pentru a depăși provocările schimbărilor climatice.



Ediția hi!tech 1/2003 a relatat despre lansarea din 1999 a UMTS (Sistemul Universal de Telecomunicații Mobile). Înainte de lansarea acestuia, în presă se spunea că: „atunci veți putea să vă uitați la televizor, să navigați pe internet și să faceți cumpărături prin intermediul telefonului mobil”. Toate aceste lucruri au devenit între timp



la un centru comercial mobil. Ulterior, se vor putea comanda mașini, cărți și CD-uri, prin simpla apăsare a unui buton”.

Ediția hi!tech 3/2003 a prezentat „mobilitatea” și „Sisteme telematice care fac drumurile și mașinile inteligente”.

La acea vreme, se introduseseră recent „panourile cu mesaje variabile controlate electronic”, prezente astăzi pe autostrăzi, care pot fi folosite pentru „a influența viteza și a menține fluiditatea traficului”. În ceea ce privește previziunile privind ceea ce vor putea face mașinile în viitor, hi!tech a dat lovitura: „parcare automată, evitarea coliziunilor din spate, avertizare înainte de a adormi la volan” și „identificarea semnelor de circulație”.



adevărate. „Ghidul orașului disponibil direct din telefon, care oferă informații despre toate atracțiile turistice precum și adresele acestora la cerere”, era o mini-sețiune a unei hărți a orașului. În ceea ce privește „mall-ul din telefon”, am specificat următoarele: „Amazon și eBay lucrează deja



Călătorește cu avionul, în siguranță

Sisteme de securitate modernizate la Aeroportul din Viena

Peste 100.000 de persoane vizitează Aeroportul Viena în fiecare zi în timpul sezonului de vârf. Pentru a proteja pasagerii și vizitatorii și pentru o eficiență ridicată a infrastructurii existente, sistemele de securitate trebuie să fie de ultimă generație.

În acest scop, aeroportul din Viena a dezvoltat un sistem de securitate inteligent împreună cu Siemens Austria, care a fost modernizat și extins în timpul operațiunilor curente și fără limitări pentru pasageri și vizitatori.

Astfel, centrul operațional de securitate oferă o imagine de ansamblu perfectă a accesului autorizat.

Noul sistem de gestionare a alarmelor integrează peste 1.800 de puncte de acces, cum ar fi ușile și porțile de acces, răspândite în peste 40 de clădiri ale Aeroportului Viena. În total, în sistem sunt integrate în jur de 2.700 de camere video. 1.300 de sisteme de control al accesului asigură că numai persoanele autorizate pot utiliza anumite zone de trecere.

În **centrul de operațiuni al terminalului**, angajații utilizează un sistem inteligent de control al ușilor pentru a ghida pasagerii prin zonele corecte de intrare. Cele mai înalte standarde de securitate sunt garantate cu ajutorul scannerului biometric SiPalm de la Siemens. Astfel, toate porțile de acces și alte zone

sensibile sunt protejate contra accesului neautorizat.

Această metodă biometrică de identificare a persoanelor este una dintre cele mai sigure din lume și, prin urmare, este utilizată în zonele de înaltă securitate.

Siemens a derulat proiecte de parteneriat cu Aeroportul din Viena de peste 20 de ani. În cadrul celui mai recent contract, compania a furnizat un sistem electric de sonorizare, sistemul de interfon și un sistem de control al ușilor.

În prezent, pe lângă tehnologia de securitate, distribuția de joasă și medie tensiune este un aspect esențial în prezent.

Suita de teste de securitate all-in-one

Pe măsură ce rețelele IT și OT din cadrul perimetrelor industriale sau de producție își continuă convergența, au crescut și provocările legate de securitatea cibernetică. În plus, reglementările legale obligă companiile industriale să sporească securitatea cibernetică în procesele lor de operare. Pentru a răspunde cererii tot mai mari de soluții de securitate cibernetică, Siemens și-a extins portofoliul de securitate cibernetică industrială și a lansat o suită de testare a securității all-in-one, pentru rețelele de comunicații industriale. „SINEC Security Inspector” este un cadru pentru diverse instrumente de securitate cibernetică care pot fi utilizate pentru a scana în mod activ dispozitive de rețea individuale, segmente de rețea sau întreaga infrastructură de rețea, în timpul perioadelor de mentenanță. Acesta combină o selecție de instrumente de testare moderne, integrate într-o singură interfață de utilizator.



biz-facts

10,5 trilioane \$ daune cauzate de criminalitatea cibernetică până în 2025 >> pagina 16

111 km de pârtii din Sölden sunt acoperite cu zăpadă într-un mod inteligent >> pagina 26

3,5 milioane de experți în securitate cibernetică lipsesc la nivel mondial >> pagina 52

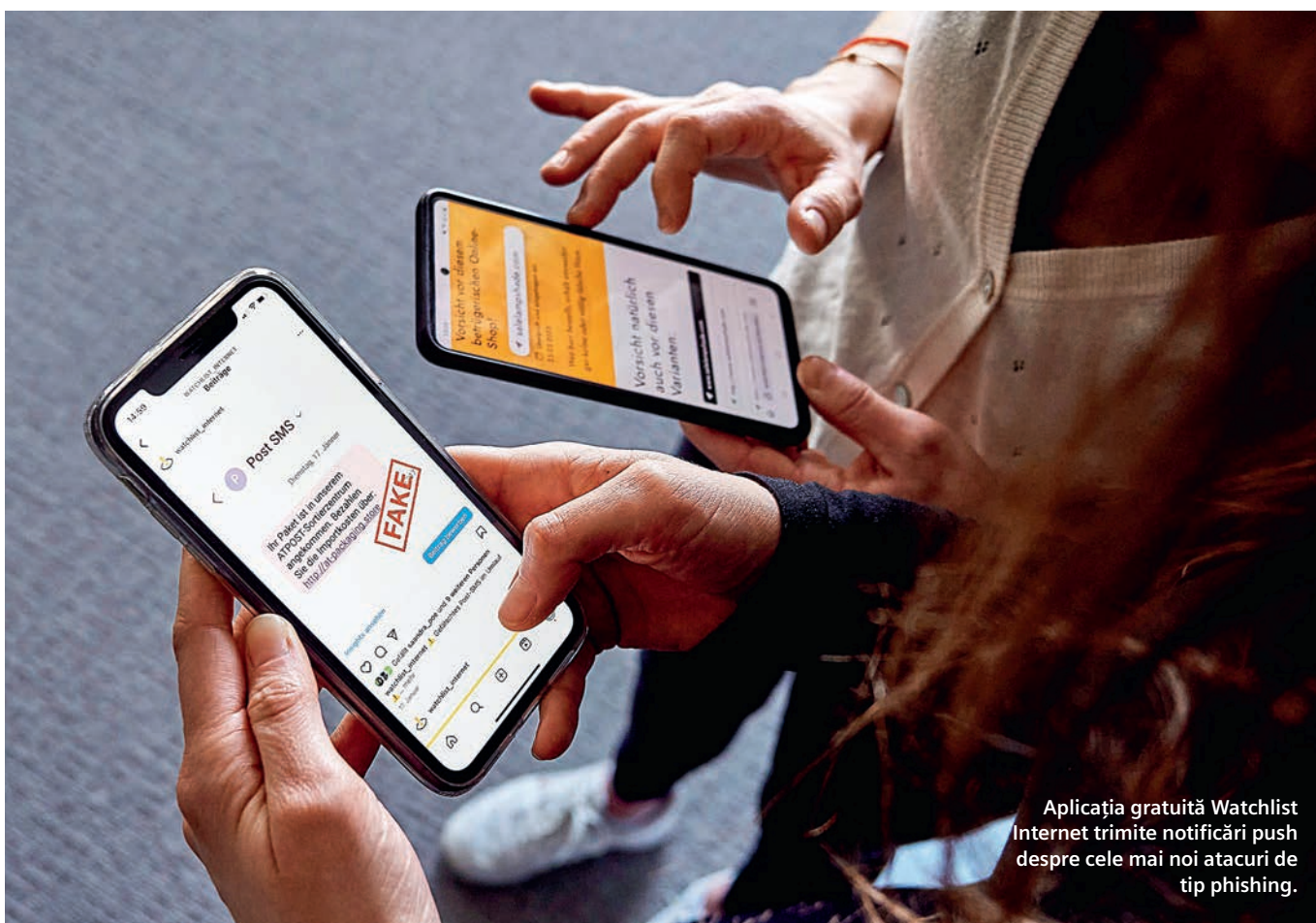
O mare de date, cu multe „phishing-uri”

Numărul infracțiunilor cibernetice crește de la an la an.

Boți, viruși, phishing, achiziții frauduloase, apeluri false de la poliție și servicii de livrare non-existente - atacurile devin din ce în ce mai sofisticate.

Revista hi!tech analizează care este cea mai bună soluție de protecție împotriva atacurilor cibernetice și dacă aceasta depinde mai mult de prudența oamenilor sau de soluțiile informatice.



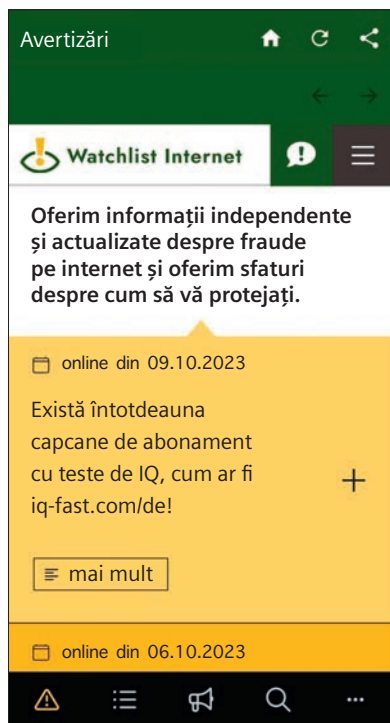


Aplicația gratuită Watchlist Internet trimite notificări push despre cele mai noi atacuri de tip phishing.

1 : phishing-ul

Ce se întâmplă în lume? Cum va fi vremea? Cu cine se întâlnește Taylor Swift? Ce face cea mai bună prietenă a mea? Când pleacă autobuzul? Am nevoie de acest tricou cool! Știrile, răspunsurile la întrebări urgente, distracția, cumpărăturile și mâncarea sunt, de obicei, la doar un clic distanță pe internet. 86% din populația Austriei este conectată la internet, iar aproximativ 90% dintre austriecii cu vârsta de 15 ani și peste, dețin un smartphone. „Raportul privind criminalitatea informatică în anul 2022” al Ministerului de Interne enumeră dezavantajele gradului înalt de disponibilitate și adopție a smartphone-urilor, precum și a utilizării intensive a acestora. Infracțiunile cibernetice au crescut cu aproximativ 30% în decurs de un an. „The Global State of Scams Report 2022” identifică fraudă online ca fiind cea mai frecventă infracțiune raportată în Europa. Cu toții putem deveni victime ale criminalității informatice.

Un e-mail de la administrația fiscală sau de la bancă, un apel telefonic de la un ofițer de poliție, chiar și mesajele de WhatsApp de la fiica dvs. pot fi false. Vestea bună este că aproape niciodată aceste posibile înșelăciuni nu pun în pericol viața cuiva. De cele mai multe ori este vorba despre bani. Suntem ușor de șantajat în situații neprevăzute sau dificile din punct de vedere emoțional. La nivel mondial, fraudă online a devenit o afacere de miliarde de dolari. Ofertele frauduloase se adaptează la obiceiurile noastre: campanii de strângere de fonduri, oferte de muncă, publicitate, rezervări la hoteluri, magazine online sau sponsorizări - totul poate fi o înșelătorie. Julia Krickl, cercetător la Institutul pentru Telecomunicații Aplicate din Austria (ÖIAT) și editor la platforma „Watchlist Internet”, a analizat 11.600 de rapoarte ale consumatorilor din 2022. Phishing-ul este escrocheria cea mai des



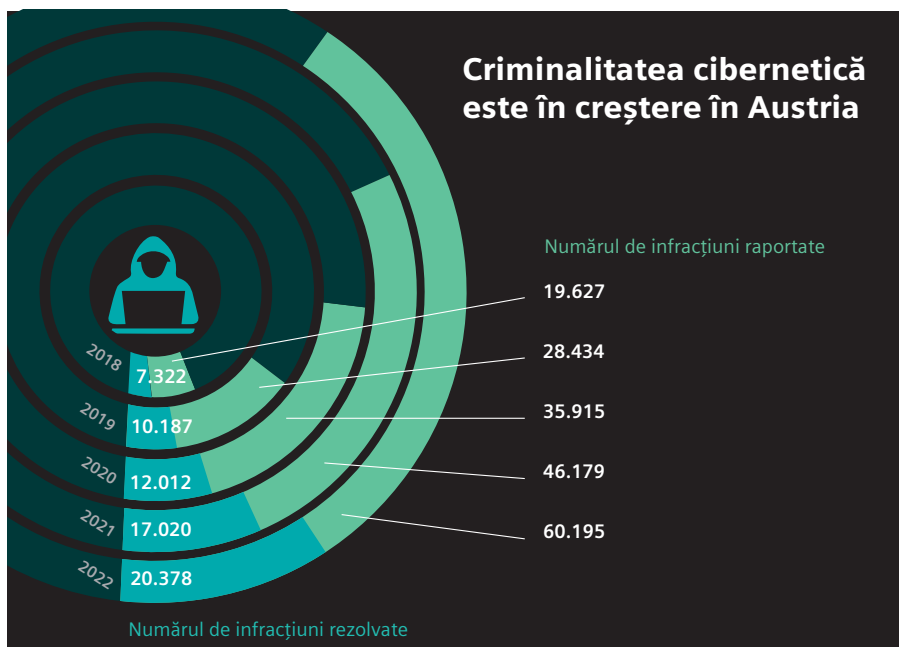
întâlnită: „Mesajele sunt trimise prin e-mail sau SMS și se încearcă accesarea detaliilor cardurilor de credit, obținerea autorizațiilor pentru debite directe mai mari sau înregistrarea pe dispozitive terțe, ca metode de plată, Apple Pay sau Google Pay”. Cea mai frecventă metodă utilizată a fost mesajul „Bună mamă, bună tată”, în care se pretindea schimbarea numărului de telefon mobil al copilului, care avea nevoie urgentă de un transfer de bani.

Frecvente sunt și mesajele text de phishing de la bănci, cu solicitări de actualizare a datelor sau de descărcare aplicațiilor. De asemenea, sunt frecvente mesajele de la presupuși curieri care pretind că nu pot livra fără un transfer bancar. În domeniul anunțurilor publicitare, vânzătorii și cumpărătorii pot fi afectați dacă accesează reclame false și dezvăluie informații despre cont sau detalii despre cardul de credit. Frauda telefonică cu „falsul polițist”

„Infractorii cibernetici creează o presiune cu încărcătură emoțională, iar cei afectați acționează impulsiv. De aceea e de preferat să faceți un pas înapoi și să vă întrebați dacă, totuși, o astfel de situație se poate întâmpla...”

Julia Krickl, cercetător la Institutul pentru Telecomunicații Aplicate din Austria (ÖIAT) și editor la platforma „Watchlist Internet”





(pierderi de peste 15 milioane de euro în 2022) a fost, cu siguranță, deosebit de neplăcută pentru Ministerul de Interne. Persoanele în vârstă sunt grupul țintă. Acestea sunt contactate telefonic și puse sub presiune sub acuzația unor fapte fictive urgente sau grave (infracțiuni, accidente). În acest fel, victimele sunt convinse să facă plăți în avans. Adolescenții și adulții tineri sunt cel mai adesea atrași de reclamele pentru platforme false de tranzacționare online pentru produse de brand, cărora li se face publicitate pe TikTok și Instagram. Julia Krickl a observat, de asemenea, o creștere a înșelăciunilor amoroase (Love-Scam) și a șantajului sexual (Sextortion) - așa cum este cunoscut șantajul cu imagini intime. Cei afectați sunt contactați prin WhatsApp sau prin intermediul aplicațiilor de dating și sunt implicați într-o rețea de minciuni: „Sumele implicate în acest tip de fraudă sunt uneori foarte mari. Inițial, se simulează apropierea personală prin contacte frecvente. De asemenea, varietatea înșelăciunilor este în creștere”, a spus Krickl. Nu doar singurătatea, ci și perspectiva banilor obținuți rapid ne fac vulnerabili. După primul contact prin intermediul unui mesaj pe Messenger sau al unei platforme de socializare, escrocii vorbesc mult și apoi recomandă o platformă comercială falsă sau cer o sumă de bani pentru acoperirea cheltuielilor de călătorie a ”partenerului de vis” care dorește să vină în vizită.

Platforme de verificare a potențialelor înșelăciuni cibernetic

Focus: Austria

PLATFORMA MIMIKAMA: mimikama.org

INSTRUIRE PENTRU COPII ȘI PĂRINȚI: saferinternet.at

PLATFORMA WATCHLIST INTERNET: watchlist-internet.at și aplicația

PENTRU COMPANII: watchlist-internet.at/warnungen-tipsps/unternehmensbetrug

SIMULARE DE PHISHING ȘI MANUAL DE CONȘTIENTIZARE A SECURITĂȚII

CIBERNETICE: watchlist-internet.at/warnungen-tipsps/unternehmensbetrug

DETECTOR DE MAGAZINE FALSE: fakeshop.at

PROTECȚIA CONSUMATORILOR LA NIVEL INTERNAȚIONAL: europakonsument.at

ETICHETA CYBER TRUST: cyber-trust.at

ALIANȚA GLOBALĂ ANTIFRAUDĂ (GASA): gasa.org

CENTRUL DE RAPORTARE A INFRAȚIUNILOR INFORMATICE AL BMI,

DISPONIBIL 24/7: against-cybercrime@bmi.gv.at

Monitorizare mass-media

FAPTIC: profil.at/faktiv

KOBUK: kobuk.at

CORECTIV: correctiv.org

VERIFICAREA FAPTELOR - APA: apa.at/service/faktencheck-2

TIKTOK: digitalerkompass.at/bait

Factură falsă - șef fals

Companiile pot fi, de asemenea, ținta infracțiunilor cibernetic. Infracțorii nu mai au nevoie de cunoștințe tehnice aprofundate deoarece infracțiunile de tip „Crime as service” pot fi cumpărate ca serviciu, după cum se menționează în Raportul privind criminalitatea informatică 2022. Pe darknet există instrumente

de hacking și programe malware care pot fi folosite ca ransomware.

„Ransom” înseamnă răscumpărare și aceasta trebuie plătită pentru a „elibera” o rețea informatică a unei companii paralizate de un atac cibernetic ce își găsește fișierele operaționale esențiale criptate de atacatori. Rețelele de boți care paralizează companiile prin atacuri concertate de tip „Distributed Denial of Service (DDoS)” sau prin e-mailuri spam sunt, de asemenea, disponibile. Toate acestea pot afecta companiile sau partenerii lor.

În mediul de afaceri, facturile falsificate, cererile de plată sau instrucțiunile de la falși manageri sunt frecvente. Cu ajutorul tehnologiei Deepfake, sub forma unei aplicații, se poate folosi clonarea vocii, adică recrearea vocii unui manager, pentru aprobarea plăților. Videoclipurile false cu sincronizarea mișcării buzelor sunt, de asemenea, din ce în ce mai numeroase.

Siemens se preocupă în mod deosebit de securitatea soluțiilor sale. În 2018, compania a lansat inițiativa de securitate cibernetică: Charter of Trust, în cadrul Conferinței de Securitate de la München, alături de alți parteneri.

De asemenea, Siemens se pregătește pentru a îndeplini cerințele UE pentru infrastructurile critice, începând cu octombrie 2024 (vezi pagina 22).

Având propria echipă de intervenție în caz de urgență cibernetică, Siemens se asigură în mod proactiv că operațiunile proprii și clienții sunt permanent protejați. Promisiunea de securitate se bazează pe trei piloni: securitatea produselor (pentru comunicații securizate, protecția integrității datelor, controlul accesului și monitorizarea end-to-end), securitatea sistemelor (interacțiunea optimizată și fiabilă a componentelor, produselor, proceselor și soluțiilor tehnice într-

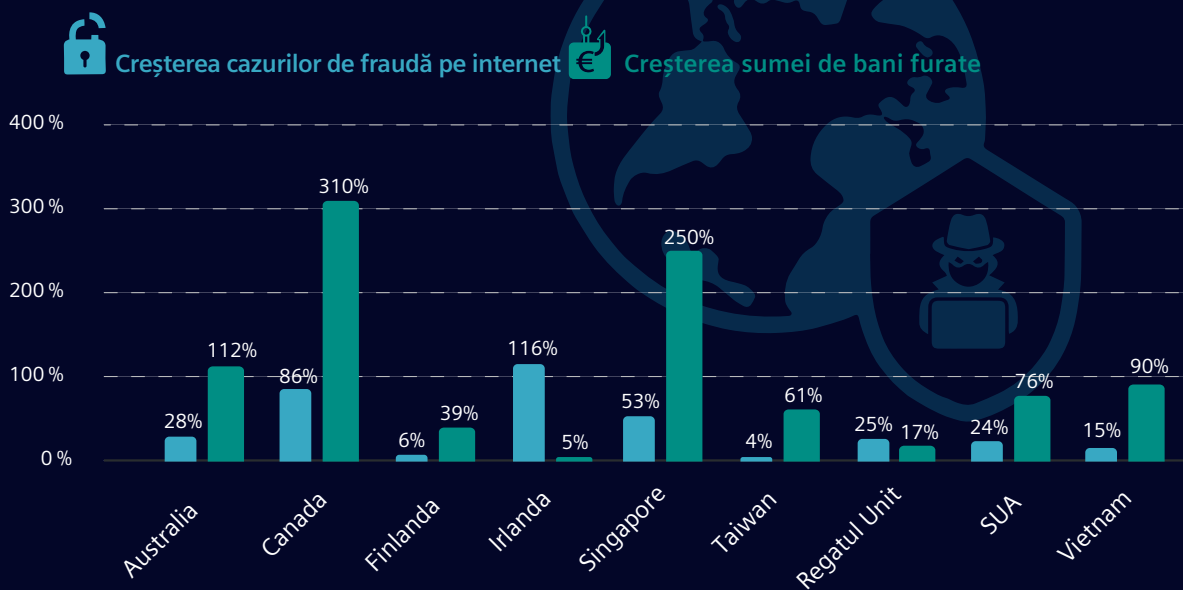
un sistem de înaltă securitate) și securitatea operațională (prin soluții de securitate cibernetică, de la consultanță până la servicii pe parcursul întregului ciclu de viață). Principiul „Zero Trust” se aplică tuturor proceselor, la fel și motto-ul „Never trust, always verify”. Toți cei care interacționează în sistemul securizat informatic sunt întotdeauna verificați pentru a vedea cine sunt cu adevărat și dacă au acces autorizat la acest sistem.

Să nu ai încredere în nimeni, să te retragi într-o peșteră, să îți pierzi încrederea în oameni - să fie aceasta soluția?

Înșelăciunile sunt tot mai adaptate la profilurile online ale persoanelor sau ale astfel fiind recomandate câteva sfaturi practice din partea Platformei Watchlist Internet:

- E-mailuri de phishing: Nu dați click pe linkuri, ci intrați în contul propriu și verificați dacă mesajul vine într-adevăr de la bancă/postă/instituții

Creșterea ratelor de cazuri de fraudă raportate pe internet (țări selectate)



Sursa: Global Anti Scam Alliance

„Un atac cibernetic este mai probabil decât un incendiu”

Georg Schwondra conduce departamentul de risc cibernetic la Deloitte Viena și oferă consultanță companiilor în domeniul securității informațiilor. În cadrul celui mai recent sondaj privind securitatea cibernetică, 350 de companii austriece au furnizat informații despre provocările actuale și despre modul în care le abordează.

Ce rezultat al ultimului sondaj Deloitte privind securitatea cibernetică v-a surprins?

Numărul total de atacuri a rămas același. Am fost surprinși însă de creșterea masivă a impactului acestora. În 2022, 76% dintre atacuri au putut fi combătute prin măsuri tehnice de infrastructură, iar în 2023 doar 41%. Așadar, atacurile sunt din ce în ce mai frecvente, iar infractorii lucrează din ce în ce mai profesionist.

Mesajele folosite pentru a lansa atacul sunt aproape imposibil de distins în viața profesională stresantă de zi cu zi. După ce utilizatorul și parola au fost introduse, programul malware începe să își facă treaba. În plus, capacitatea de recuperare prin backup-uri a scăzut cu o treime.

Ce înseamnă pentru companii faptul că, acum, hackerii pot cumpăra „Crime as a Service” (infracțiuni ca serviciu)?

Pe Darknet, acest lucru este organizat în funcție de diviziunea muncii. Există grupuri care creează noi ransomware și își vând „produsul” în schimbul unui procent din răscumpărare. Am văzut recent o demonstrație a modului în care Inteligența Artificială generativă ChatGPT poate fi folosită pentru a scrie programe malware în zece minute, practic fără cunoștințe de programare. Ransomware-ul este o afacere cu profituri mari și riscuri mici. Ne așteptăm ca o inteligență artificială puternică să faciliteze câștigarea de bani de către neprofesioniști, în special în țările în care nu există o legislație în domeniu. De asemenea, crearea de Deep Fakes este



din ce în ce mai facilă. „Punctul slab al omului” nu trebuie subestimat în acest context. În cadrul unui test am trimis recent o angajată îmbrăcată ca un grădinar cu o șapcă, o stropitoare și pantofi de lucru la o companie mare, iar aceasta a primit acces nelimitat.

Sunt afectate în mod egal companiile de toate dimensiunile?

Am intervievat organizații și companii cu cel puțin 50 de angajați. Companiile mici pot fi mai ușor de atacat, iar acest lucru poate fi mai profitabil - pentru infractori, deoarece șantajul implică mai puțin efort. O firmă de instalații cu cinci angajați poate fi afectată în aceeași măsură precum o companie de turism a cărei aplicație conține ransomware în macro-ul unui document Word.

În țara noastră, accentul este pus pe prevenire și mai puțin pe detectarea continuă, pe actualizări, pe măsuri tehnice și pe gestionarea accesului. De ce este mai bine să ne concentrăm eforturile pe toate aceste măsuri?

Conștientizarea este importantă și este o

măsură permanentă. Atunci când primesc un mesaj înșelător ce pare autentic de la Microsoft, cinci din 100 de persoane dau clic pe el - în ciuda unei instruiți adecvate. Infrastructura tehnică, cum ar fi rețelele segmentate, poate împiedica agravarea situației. Criptarea unui laptop ajută foarte mult și nu paralizează o companie întreagă. Oamenii trebuie să înțeleagă că gestionarea patch-urilor, adică eliminarea lacunelor cunoscute din infrastructură, trebuie să se facă prompt, deoarece ușa de acces este larg deschisă. De multe ori, lipsesc persoanele calificate. Observăm, de asemenea, că nu numai sistemele tehnice, ci și vechile instalații industriale au porți de acces pentru infractorii ciberneticici. Un mediu de automatizare vechi de 30 de ani reprezintă un risc de securitate.

Studiul arată că doar una din 5 companii are un plan de urgență pentru atacuri ciberneticice. Nu există aproape deloc exerciții periodice pentru situații de urgență. Exercițiile de evacuare în caz de incendiu sunt efectuate de două ori pe an, dar nu și exercițiile de acționare în cazul incidentelor ciberneticice. Cu toate acestea, acum acestea sunt mult mai probabile. Noi efectuăm periodic simulări în companii. Prezentăm un incident cibernetic, analizăm planul de urgență împreună cu consiliul director și discutăm pe subiect. Când vine vorba de extragerea datelor sensibile, de criptare și șantaj, prima decizie fundamentală și întrebarea crucială a managementului este: Aș plăti sau nu? Al doilea aspect este viteza de reacție necesară. În cazul în care un specialist IT observă un atac în curs de desfășurare în centrul de date,

este autorizat să i-a măsurile necesare, de urgență cu toate consecințele? Acestea sunt chestiuni de ierarhie. Primele cinci minute ale unui atac ransomware sunt importante. Cel de-al treilea punct este comunicarea, adică modalitățile prin care compania mai poate comunica cu angajații săi.

Ce altceva recomandați?

Comaniile trebuie să dezvolte capacități de detectare a pericolelor cibernetice ce pot apare. Aceste măsuri pot fi la nivel intern sau prin intermediul unui furnizor de servicii, pentru a identifica atacatorii din rețea într-un stadiu incipient. De obicei, aceștia se mișcă în rețea fără a fi identificați timp de 30 până la 90 de zile. Cu cât sunt depistați mai devreme, cu atât mai repede se pot lua măsuri și se pot minimiza daunele potențiale. Pentru a afla ce s-a întâmplat, este nevoie de expertiză criminalistică în domeniul încălcărilor de date. Există furnizori naționali și internaționali de servicii de securitate, pornind de la securitate IT de bază până la securitatea de vârf.

Ce recomandați atunci când trebuie stabilite priorități?

O abordare holistică care definește datele ce trebuie protejate și care sunt timpii maximi de nefuncționare ce pot fi tolerați, inclusiv cât de mare este expunerea la risc. Nivelul de securitate este apoi derivat pe baza riscului. În ciuda tuturor măsurilor de precauție, companiile trebuie să se întrebe cum vor reacționa în cazul unui incident și să reglementeze din timp răspunsul la incident. O echipă de experți, gata de intervenție, poate oferi asistență online în termen de două ore și se poate deplasa la fața locului în 24 de ore.

Ce pași urmați dvs. pentru propria securitate cibernetică?

Eu folosesc un seif pentru parole, folosesc parole diferite pentru toate aplicațiile și nu folosesc niciodată setările din fabrică ale router-ului. Nu am date de la companie acasă și am o copie de rezervă a datelor private pe un hard disk extern.



financiare etc.

- Programele malware sunt deseori ascunse în grafice sau în atașamente de e-mail.
- Mesajele SMS cu un link sunt întotdeauna suspecte!
- De îndată ce vi se solicită la telefon informații personale sau relevante din punct de vedere financiar, încheiați conversația!

Se recomandă întotdeauna scepticismul și o supraveghere constantă a propriilor tranzacții. Într-un moment de liniște, o escrocherie este observată rapid, dar infractorii creează o presiune cu încărcătură emoțională, iar cei afectați acționează impulsiv. De aceea, SMS-ul „Bună, mamă/ Bună, tată - am nevoie de bani” funcționează atât de bine, pentru că în acel moment de stres, când crezi că este în pericol copilul tău, nu mai gândești logic”, a spus Julia Krickl. Sfatul ei: priviți pentru o clipă situația în mod detașat, faceți un pas înapoi și gândiți-vă: Poate fi adevărat? Ar fi bine să vă asigurați și să verificați din nou. Standardul minim pentru cumpărăturile online de pe pagina unui comerciant

impune o pagină cu numele, adresa, persoanele de contact și termenii și condițiile.

Unele magazine afișează și anumite certificate, iar recenziile altor utilizatori pot oferi, de asemenea, informații.

Plățile ar trebui efectuate prin debit direct, prin card de credit sau prin factură, de preferat nu în avans. Atunci când plătiți și introduceți date, vă rugăm să vă asigurați că aveți o conexiune criptată (<https://> în bara de adrese).

Oficiul Federal de Poliție Criminală din Austria recomandă un program antivirus actualizat, un firewall și actualizări regulate pentru o protecție adecvată.

Aveți grijă la software-ul gratuit, la copiile piratate sau la programele suplimentare (tip „plug-in”). Platforma „Watchlist Internet” a dezvoltat o aplicație gratuită care trimite utilizatorilor notificări push despre noile falsuri și înșelăciuni din mediul digital.

În cadrul unui proiect de cercetare, Institutul Austriac pentru Telecomunicații Aplicate a dezvoltat un detector de magazine false, ca plug-in de browser pentru desktop. ○



Întotdeauna cu un pas înainte

Încă din anii 1970, când a început **lupta împotriva criminalității cibernetice**, a existat o cursă continuă între atacatori și specialiștii în securitate. În prezent, varietatea instrumentelor de atac este surprinzătoare. În acest context, companii de renume precum Siemens, alături de diverse instituții de cercetare fac tot posibilul pentru a contracara acțiunile hackerilor prin implementarea unor măsuri sofisticate.

Hacker? Acest termen era practic necunoscut la începutul anilor 1980. Lucrurile s-au schimbat odată cu lansarea filmului „Wargames”, în 1983.

Acesta prezintă povestea unui adolescent care, folosind un modem telefonic, reușește să pătrundă în Comandamentul de Apărare Aeriană Nord-American, provocând aproape

Milioane de locuri de muncă, fie că sunt în birouri sau la domiciliu, au devenit acum noi puncte de intrare pentru activitățile de criminalitate cibernetică.

10,5 trilioane \$ este valoarea estimată a daunelor cauzate de criminalitatea cibernetică la nivel mondial până în 2025

ARPANET (rețeaua Forțelor Aeriene ale SUA), precursorul internetului.

Pagube înspăimântătoare

Criminalitatea cibernetică, adică infracțiunile comise în spațiul virtual, are deja o istorie de peste jumătate de secol.

Compania IT Cybersecurity Ventures estimează că pagubele globale cauzate de criminalitatea cibernetică au ajuns la suma de 6 trilioane \$ în 2021. Experții prevăd că această sumă ar putea crește până la 10,5 trilioane \$ până în 2025. De-a lungul timpului, nu doar metodele atacatorilor au evoluat, ci și cele ale apărătorilor. Așadar, confruntarea în spațiul cibernetic a fost mereu un joc de-a șoarecele și pisica. De exemplu, antivirusul Reaper a fost dezvoltat rapid pentru a detecta și distruge primul virus, Creeper.

Multă vreme, atacatorii și-au concentrat eforturile asupra calculatoarelor personale sau asupra serverelor de date ale companiilor. În 1999, de exemplu, virusul Melissa s-a răspândit cu repeziciune prin e-mail, paralizând numeroase sisteme.

Totuși, în ultimii ani, atacurile împotriva inteligenței artificiale și a utilizării abuzive a datelor au crescut foarte mult. Piratarea sistemelor informatice prin intermediul camerelor de supraveghere, senzorilor sau al dispozitivelor interconectate, în cadrul așa-numitului Internet al lucrurilor (IoT), joacă un rol important. Multe dintre acestea sunt dotate cu hardware și software încorporate. Cu alte cuvinte, aceste

dispozitive sunt echipate cu procesoare pentru prelucrarea datelor la punctul de utilizare și dispun de interfețe pentru comunicarea cu lumea exterioară ceea ce le face vulnerabile la atacuri.

Virusul informatic Stuxnet, care a atacat sistemele de control Siemens utilizate în companii, în urmă cu zece ani, a fost un semnal de alarmă. Stuxnet a avut ca scop sabotarea fluxului operațional sau cel puțin întreruperea semnificativă a producției.

A devenit clar că atenția hackerilor nu se va limita doar la computere sau serverele de date ale companiilor, ci se va extinde către întregul sector industrial.

Siemens a realizat progrese semnificative în protejarea clienților ce utilizează tehnologia sa. Un departament distinct, numit Product-CERT, a fost înființat cu scopul de a supraveghea în mod constant produsele companiei și sistemele integrate. Acesta are rolul de a identifica eventualele vulnerabilități care ar putea fi exploatare de hackeri prin utilizarea noilor tehnologii de atac. În plus, clienții sunt ținuti la curent în mod regulat și primesc actualizări de software pentru a se asigura că sunt protejați în mod corespunzător.

Încrederea este bună, prevenția este și mai bună

Principiul "Zero Trust" (încredere zero) reprezintă o schimbare de paradigmă în domeniul securității cibernetice, care a câștigat teren în ultimii ani. Zero Trust

declanșarea celui de-al treilea război mondial. În acea perioadă, foarte puține persoane dețineau un computer personal. Computerele erau mai degrabă folosite în scopuri profesionale. Cu toate acestea, filmul a reușit să ilustreze existența unui univers tehnic extrem de interconectat - care era, de asemenea, vulnerabil la atacuri. De fapt, cu doar zece ani înainte, în 1971, fusese dezvoltat primul virus informatic din lume, programul malware numit Creeper.

Misiunea lui Creeper a fost de a paraliza

1.300 de experți

În timp ce în 1986, pentru securitatea rețelilor era nevoie de o mică echipă de securitate IT, astăzi este nevoie de gestionarea unui număr crescut de activități. Siemens monitorizează instalațiile industriale din întreaga lume pentru a detecta potențiale amenințări cibernetice, avertizează companiile în cazul unor incidente de securitate și coordonează măsuri proactive de contracarare. În prezent, compania dispune de aproximativ 1.300 de experți în securitate cibernetică, fiind astfel bine pregătită pentru a oferi produse și sisteme sigure atât pentru clienți, cât și pentru propriile sale nevoi. Siemens se numără printre primele companii care au adoptat o abordare holistică a securității cibernetice, cu scopul de a proteja cât mai eficient infrastructura, produsele, soluțiile și serviciile sale. Securitatea cibernetică este, de asemenea, una dintre așa-numitele „Company Core Technologies” (tehnologii de bază) ale companiei. Acestea reprezintă domenii de inovație și tehnologie de importanță strategică pentru companie, unde Siemens își propune să fie un lider tehnologic. Prin urmare, compania dispune de o expertiză vastă în domeniul securității cibernetice și în gestionarea provocărilor tot mai mari din acest domeniu.

„Produsele Siemens sunt la intersecția dintre lumea cibernetică și cea fizică, fiind controlate integral de software. Dacă acest software ar prezenta vulnerabilități, atunci și lumea fizică poate fi afectată în mod direct”.

Fabrizio De Santis, expert în criptografie la Siemens

contrazice ideea tradițională conform căreia o companie este protejată împotriva atacurilor în interiorul granițelor sale și este apărată de firewall-uri odată ce interacționează cu lumea exterioară. Într-o lume unde milioane de sisteme încorporate sunt interconectate în rețea, acest model nu mai este eficient.

În contextul pandemiei de coronavirus, milioane de oameni au început să lucreze de acasă. „Zero Trust înseamnă să privim fiecare computer și fiecare dispozitiv ca fiind potențial vulnerabil și să stabilim conexiuni sigure între toate dispozitivele”, a explicat Peter Stoll, responsabil Cybersecurity IT Siemens. „Sistemul verifică întotdeauna dacă un computer este autorizat să stabilească o conexiune sau să solicite date”. Pentru Siemens, Zero Trust este în prezent unul dintre cele mai importante subiecte în domeniul securității cibernetice. Principiu general este să nu avem încredere în nimeni. Trebuie să verificăm întotdeauna identitatea utilizatorului care se conectează. Siemens a implementat deja tehnologia „Zero Trust” la nivel global, asigurându-se astfel că utilizatorii sunt obligați să se identifice în mod constant, chiar dacă s-au autentificat deja. Soluțiile precum „Zero Trust” sunt concepute pentru a menține atacatorii mereu cu un pas în

urmă.

Fabrizio De Santis, expert în criptografie la Siemens, a subliniat: „Soluțiile Siemens combină lumea reală cu cea digitală. Toate acestea sunt controlate de software. Dacă software-ul este vulnerabil, atunci și lumea fizică este afectată”.

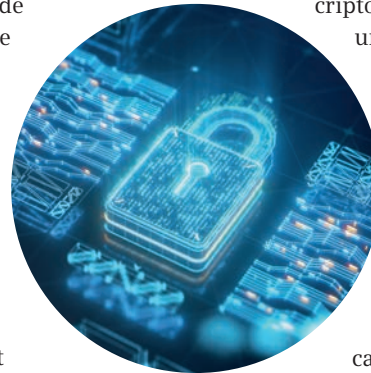
Pentru Siemens, procesele criptografice sunt, prin urmare, foarte importante atât pentru stocarea, cât și pentru transmiterea datelor.

De Santis a indicat o evoluție importantă pe care trebuie să o urmărim cu atenție în viitor - computerul cuantic, capabil de calcule la viteze

extraordinaire. „Nu putem

anticipa cu precizie momentul în care primul computer cuantic va fi disponibil pe piață, dar un lucru este cert: dacă un astfel de computer cuantic ar cădea în mâinile celor cu intenții malefice, aceștia ar fi capabili să anuleze toate protocoalele criptografice actuale”. Prin urmare, experții în securitate ar trebui să înceapă chiar de acum să elaboreze strategii de contracarare a hackerilor de computere cuantice din viitor.

La mai bine de 50 de ani de la apariția virusului Creeper, cursa dintre infractorii cibernetici și specialiștii în securitate continuă - evoluând într-o manieră mult mai complexă decât și-ar fi putut imagina cineva în anii 1970. ○





Securitatea cibernetică la Siemens Austria

Siemens AG Austria dispune de o politică fermă de securitate cibernetică.

Compania a obținut deja diverse certificări la diferite niveluri, cum ar fi ISO 27001, TISAX sau „CyberRisk Rating by KSV 1870” (Cyber Trust Austria Silver Label).

Prezența acestor certificări a devenit o condiție esențială pentru multe relații cu clienții și licitații.

„Atât gestionarea riscurilor în materie de securitate cibernetică, cât și gestionarea riscurilor furnizorilor de securitate cibernetică reprezintă instrumente esențiale în cadrul politicii noastre de securitate cibernetică.

Managementul continuității

activității, inclusiv realizarea de backup-uri, chiar și în mod offline și recuperarea datelor, împreună cu testele corespunzătoare, reprezintă elemente esențiale ale securității cibernetică.

Acestea sunt cruciale, în special pentru a ne pregăti în fața unui potențial atac de tip ransomware”, a declarat Johann Schlaghuber, Chief Information Security Officer (CISO) al Siemens AG Austria.

De asemenea, Schlaghuber reprezintă Siemens în cadrul unor organizații externe precum Centrul de Competență pentru Siguranța Austriei (KSÖ), Platforma de securitate cibernetică (CSP), EnergyCERT și Austrian Trust Circle (ATC), precum și

în relația cu Ministerul de Interne.

În calitate de CISO, Schlaghuber are responsabilitatea de a asigura conformitatea cu cerințele Directivei 2 a UE privind securitatea rețelelor și a informațiilor (NIS 2) (vezi materialul de la pagina 22). „Evaluările noastre interne preliminare indică faptul că suntem bine pregătiți pentru NIS2, dar la Siemens mai avem de lucru.

Vom putea face o evaluare concretă doar după ce legea NIS va intra în vigoare în Austria. Desigur, expertiza pe care am acumulat-o în acest proces este pusă la dispoziția clienților noștri, pe care îi putem sprijini în implementarea NIS2”, a spus Schlaghuber.

NIS2 ar putea avea un impact și asupra voastră!

Securitatea cibernetică este în continuare percepută de mulți ca o provocare majoră. Începând cu octombrie 2024, noua **directivă NIS2 a UE**, care se adresează companiilor mijlocii și mari, precum și infrastructurilor critice, ne va impune să facem față acestei provocări.

Comaniile pot stabili o fundație solidă pentru conformitatea cu directiva NIS2 prin implementarea unui număr relativ redus de măsuri.

„Există numeroase provocări”, a spus Adrian Pinter, expert în securitate cibernetică pentru sectorul industrial la Siemens, „și acestea nu par să se atenueze.

Toată lumea vorbește în prezent despre convergența IT/OT, dar mulți tind să simplifice prea mult lucrurile”. Deși integrarea datelor din ambele sisteme, adică IT (tehnologia informației) și OT (tehnologia operațională), progresează, Pinter consideră că este nerealist să ne așteptăm ca aceste două sisteme să se contopească într-un tot unitar: „Ar fi ca și cum raliul și Formula 1 ar concura în același campionat mondial”.

În ceea ce privește securitatea cibernetică, pur și simplu nu este posibil să securizăm complet Tehnologia Operațională (OT) cu resurse IT. Pinter a precizat: „Instrumentele sunt aceleași, dar le utilizăm în moduri diferite, deoarece trebuie să gândim diferit în domeniul OT, concentrați pe activitatea

continuă”. Dacă sunt necesare actualizări, acestea pot fi efectuate doar în timpul opririlor tehnologice - o sarcină dificil de realizat în industria metalurgică sau farmaceutică.

A doua provocare majoră este că multe sisteme informatice nu au fost actualizate. Pinter: „În multe cazuri, procesele rulează pe sisteme vechi, cum ar fi Windows 7, dar cum acestea continuă să funcționeze fără probleme, mulți operatori nu văd niciun motiv pentru a le actualiza. De asemenea, companiile ar trebui să renunțe la principiul de a nu umbla niciodată la un sistem funcțional”.

Conștientizarea costurilor asociate unei singure zi de întrerupere a activității cauzată de un atac cibernetic - inclusiv impactul asupra reputației companiei - este un prim pas. Ar trebui să urmeze apoi o analiză cuprinzătoare. Pinter: „În multe companii, există un conglomerat de sisteme și produse diferite, cu



Prin NIS2, UE își propune să îmbunătățească reziliența și să ofere un răspuns mai eficient la atacurile cibernetică în sectorul public și privat.

standarde de securitate diferite, care a crescut de-a lungul anilor - și adesea fără o documentație coerentă. Prin urmare, este necesară o evaluare a riscurilor cibernetică și eliminarea aspectelor care nu sunt legate de securitatea cibernetică. Odată finalizată analiza de risc, următorul pas este implementarea concretă a măsurilor de protecție, cum



ar fi segmentarea rețelei, un concept de firewall sau consolidarea sistemelor de securitate cibernetică.

Fiecare componentă inutilă reprezintă o poartă de acces pentru un atac cibernetic”, a avertizat Pinter.

În principiu, nu este necesar să se înlocuiască imediat tot ceea ce este vechi, a subliniat Pinter: „Noi avem competența necesară relevantă și știm

cum să integrăm sistemele noi și vechi într-un concept global de securitate cibernetică”. Serviciile personalizate ale Siemens pentru o varietate de sectoare industriale constituie un avantaj major. Siemens oferă soluții personalizate, independente de producător și le transpune în practică. Toate măsurile de securitate cibernetică implementate trebuie



„Fiecare componentă inutilă este o poartă de acces pentru un atac cibernetic”.

Adrian Pinter, expert în securitate cibernetică pentru sectorul industrial la Siemens Austria



Doar companiile cu mai puțin de 50 de angajați și o cifră de afaceri anuală mai mică de 10 milioane de euro nu sunt vizate de Directiva NIS2.

În viitor, Industria alimentară va fi supusă cerințelor regulamentului NIS2.



„Clienții noștri beneficiază de experiența noastră directă. Expertiza

și soluțiile pe care le punem la dispoziție și-au demonstrat eficacitatea în propriile noastre unități de producție”.

Johann Schlaghuber, Chief Information Security Officer al Siemens AG Austria.

monitorizate, evaluate și actualizate constant, ceea ce reprezintă o provocare în a asigura cea mai bună protecție posibilă. Probabil doar câteva companii vor fi capabile să gestioneze și această sarcină atât de dificilă - din cauza costurilor ridicate pe care le implică și a deficitului de forță de muncă calificată în sectorul IT. De aceea, credem că externalizarea către profesioniști reprezintă soluția optimă. Siemens pune la dispoziție servicii adecvate pentru companiile mici, mijlocii și mari, care aplică cerințele directivei NIS2.

„Clienții noștri beneficiază de experiența noastră directă. Expertiza și soluțiile pe care le oferim și-au demonstrat eficacitatea în propriile noastre unități de producție”, a spus Johann Schlaghuber, Chief Information Security Officer la Siemens AG Austria, care este, de asemenea, responsabil pentru implementarea conformității

NIS 2 în cadrul companiei (mai multe detalii despre activitățile de securitate cibernetică ale Siemens Austria se găsesc în caseta de la pagina 19).

Noul regulament NIS, din octombrie 2024

Actualul regulament NIS (Securitatea rețelor și a sistemelor informatice) va fi adaptat și extins la 18 octombrie 2024. UE își propune să îmbunătățească reziliența și reacția sectoarelor public și privat la atacurile cibernetice. „În timp ce companiile din infrastructura critică, cum ar fi furnizorii de electricitate, furnizorii de internet, băncile și spitalele au fost sub incidența NIS până în prezent, alte sectoare vor fi vizate, în viitor”, a menționat Adrian Pinter, care a observat că acest subiect este insuficient de cunoscut în rândul clienților săi. „Multe companii nici măcar nu-și dau seama că NIS2 se va

aplica și în cazul lor. Cu toate acestea, sancțiunile pentru neconformitate sunt drastice și, în cel mai rău caz, pot ajunge la milioane de euro”. Sectoarele vizate sunt foarte variate și, pe lângă infrastructura critică, includ acum și serviciile poștale și de curierat, gestionarea deșeurilor, produsele chimice, produsele alimentare, industria de prelucrare și de producție etc.

Doar companiile cu mai puțin de 50 de angajați și o cifră de afaceri anuală mai mică de 10 milioane de euro nu sunt vizate de Directiva NIS2.

Standardul minim european

Noua directivă, împreună cu normele de aplicare, are scopul de a stabili un standard minim la nivel european pentru a rezista atacurilor cibernetice.

NIS2 reprezintă un set de norme care cuprinde zece măsuri de gestionare a riscurilor ce trebuie implementate:

- Evaluarea riscurilor și securizarea sistemelor informatice;
- Gestionarea incidentelor de securitate;
- Managementul continuității activității și gestionarea situațiilor de criză;
- Securitatea lanțului de aprovizionare;
- Măsuri de securitate pentru achiziționarea, dezvoltarea și întreținerea TIC;
- Concepte și proceduri pentru evaluarea a eficacității măsurilor de gestionare a riscurilor;
- Practici de prevenție și formarea în domeniul securității cibernetice;
- Criptografie și criptare, dacă este necesar;
- Securitatea personalului, concepte pentru controlul accesului;
- Autentificare multifactor.

„NIS2 nu ar trebui în niciun caz tratată

cu superficialitate”, a avertizat Adrian Pinter, „și nu doar pentru că administratorii companiilor sunt personal responsabili. Dacă directiva NIS2 este ignorată, acest lucru poate avea consecințe grave”. Dar trebuie să se țină cont și de faptul că investițiile în securitatea cibernetică se fac pe termen mediu și lung.

Walter Wutzl, director de vânzări pentru produse de automatizare a energiei la Siemens, are o experiență îndelungată în securitatea cibernetică. Din punctul său de vedere, este necesară o abordare sistematică a acestui subiect.

Majoritatea clienților săi din sectorul energetic au fost deja sub incidența primei Directive NIS, care a intrat în vigoare în Austria în 2019, ca parte a infrastructurii critice. „Această experiență a condus în cele din urmă la un proces continuu de implementare a unor funcționalități actualizate a sistemelor noastre, care îndeplinesc atât cerințele clienților noștri, cât și directiva NIS”, a declarat Wutzl. Acest lucru a fost relativ ușor, deoarece specificațiile NIS pentru sectorul energetic erau destul de clare, iar cerințele tehnice puteau fi deduse cu ușurință. „Cu toate acestea, fiecare companie vizată de prima Directivă NIS a fost informată de către autoritate că trebuie luate măsuri și, mai ales, care sunt acestea. Acest lucru nu mai este valabil cu NIS2”, a subliniat Wutzl. „Fiecare trebuie acum să judece singur dacă intră sub incidența Directivei NIS2”. Acest lucru înseamnă că măsurile care trebuie luate trebuie să fie definite și de către companie. Cu toate acestea, în multe cazuri, sistemele existente nu pot fi integrate în tehnologiile actuale de securitate cibernetică decât într-o măsură limitată - prin urmare, trebuie utilizate alte soluții, cum ar fi izolarea unor părți specifice ale sistemului. „Aceasta este



„Integrarea sistemelor existente cu cele mai recente

tehnologii de securitate cibernetică este una dintre competențele noastre fundamentale”.

Walter Wutzl, Director de Vânzări pentru Produse de Automatizare a Energiei, Siemens Austria



„Dacă nu există interfețele dintre OT și IT, se pierd o mulțime de

date utile și, prin urmare, este afectat viitorul potențial al bazei de date”.

Werner Brandauer, șef al departamentului de consultanță pentru sisteme energetice, Siemens Austria

tocmai una dintre competențele noastre fundamentale”, a spus Wutzl, care menționează subiectul gestionării patch-urilor folosind exemplul unei substații. Toate acestea sunt controlate de la un centru de comandă, iar toate elementele de operare sunt disponibile în fiecare stație de transformare, pentru situații de urgență sau pentru funcționarea în timpul lucrărilor de întreținere.

În acest context și din cauza vechimii instalațiilor, apare provocarea ca, după actualizarea OT sau a securității în centrul de control, sistemele de la fața locului să funcționeze, pe deplin și în siguranță. „Din păcate, nu există personal care să detecteze imediat erorile. La Siemens, colaborăm cu clienții noștri pentru a maximiza siguranța și conformitatea cu NIS2 în aceste sisteme”.

Potrivit lui Werner Brandauer,

consultant pentru divizia Power Systems la Siemens, experiența și expertiza vastă a companiei în domeniul OT sunt extrem de valoroase pentru operatorii de rețele energetice.

„Aceștia trebuie să identifice în mod fiabil care dintre active nu mai pot fi integrate în mod sigur în cadrul sistemului de securitate cibernetică viitor”.

Acest lucru este cu atât mai important cu cât sectorul OT devine ținta unui număr din ce în ce mai mare al atacurilor cibernetice, întrucât IT-ul este acum bine securizat. Siemens oferă soluții care permit identificarea cu precizie a componentelor necesare reducerii potențialelor daune. Există clienți care adoptă deconectarea completă a unor părți specifice ale sistemului, care nu mai sunt actualizate. Aceasta poate fi o cale viabilă, dar nu întotdeauna adecvată,

conform lui Brandauer: „Dacă nu există interfețele dintre OT și IT, se pierde o mulțime de date utile și, prin urmare, este afectat viitorul potențial al bazei de date”. Pentru a păstra acest lucru, Siemens oferă un sprijin extins. Acesta începe cu analiza și evaluarea situației actuale a securității cibernetice. Pe baza acesteia, se recomandă măsuri foarte specifice și se stabilesc următorii pași împreună cu experții. Următorul punct menționat de Brandauer este identificarea vulnerabilităților prin scanarea mediului de rețea și eliminarea acestora. „Lucrând la aceste trei puncte, companiile pot atinge un nivel semnificativ mai ridicat de securitate cibernetică”, a afirmat Brandauer.

În plus, Siemens oferă posibilitatea de a îmbunătăți securitatea prin teste de penetrare, adică prin identificarea proactivă a vulnerabilităților, și prin



implementarea unui Security Operation Centre (SOC). „Este esențial să avansăm treptat - inclusiv în ceea ce privește directiva NIS2, care include acum și companiile mai mici, care trebuie acum să urmeze exemplul”. „Instalatorii și operatorii de clădiri din Austria nu acordă suficientă importanță securității cibernetice”, a spus Martin Krammer, expert Siemens în domeniul automatizării clădirilor. El crede că există un mare potențial de îmbunătățire, în special în rândul companiilor mai mici, unde adesea nu există personal dedicat acestei probleme. „Cu toate acestea, multe dintre aceste companii vor fi vizate de directiva extinsă NIS2, începând cu octombrie 2024”, a subliniat Krammer. Prin urmare, Krammer recomandă cu insistență fiecărei companii să evalueze dacă se încadrează în directiva NIS2. Pe lângă personalul și resursele necesare, costurile reprezintă o preocupare pentru multe companii atunci când vine vorba de o analiză mai atentă a securității cibernetice. „Mulți furnizori mici de servicii IT nu dispun de expertiza necesară actualizată, ceea ce poate duce la soluții inadecvate pentru clienții lor, în ciuda eforturilor depuse”, a spus Krammer. „Astăzi, întrebarea nu este dacă o companie va fi atacată, ci mai degrabă când”. Și, prea des, atacatorii reușesc prin metode simple.

Gândiți-vă din timp la securitatea cibernetică

Potrivit lui Krammer, un punct de plecare excelent este atenția îndreptată către securitatea cibernetică încă din faza de licitație și de planificare a unui proiect de construcție, utilizând o infrastructură de rețea sigură și produse de încredere, și implicând angajații în acest concept pe termen lung. Siemens oferă o gamă largă de servicii și o expertiză vastă pentru a ajuta



„Constructorii și administratorii de clădiri din Austria încă nu acordă suficientă importanță securității cibernetice”.

Martin Krammer, expert pentru automatizarea clădirilor la Siemens Austria

administratorii de clădiri să elimine rapid vulnerabilitățile critice - începând cu serviciile de actualizare și upgrade până la gestionarea patch-urilor, un serviciu pe care Siemens îl oferă acum pentru prima dată.

„Dacă o companie beneficiază de sprijinul Siemens, primește un pachet personalizat de soluții globale, care include și aspecte de securitate cibernetică”, a subliniat Martin Krammer, „iar acest lucru este complet independent de mărimea companiei sau a proiectului.

„Un lucru este clar: viitoarea directivă NIS2 necesită o abordare unitară asupra riscului. Krammer: „Companiile trebuie să efectueze o evaluare cuprinzătoare și nu trebuie să negligeze sub nicio formă automatizarea clădirilor etc”.

Datorită complexității mari, consultarea experților de la Siemens oferă avantaje deosebite.

În multe companii, securitatea în domeniul IT și securitatea în domeniul OT au fost strict separate până în prezent. „Dar lipsa comunicării între IT și OT și funcționarea intrinsecă a tehnologiei clădirilor nu mai sunt adecvate în contextul actual”, a spus Martin Krammer, fiind de acord cu argumentul lui Werner Brandauer în ceea ce privește rețelele energetice. Acest lucru este valabil în special pentru clădirile inteligente, care

utilizează tehnologii de ultimă generație pentru a maximiza confortul și eficiența energetică. Krammer: „Fluxurile de date între OT și IT devin din ce în ce mai importante”. Prin urmare, atacatorii ar putea să încerce să pătrundă în rețeaua OT prin intermediul rețelei IT - și invers. Măsurile de securitate fundamentale, cum ar fi un concept adecvat de segmentare a rețelei, actualizări regulate ale software-ului sau remedierea imediată a vulnerabilităților de securitate cunoscute, sunt esențiale în acest context.

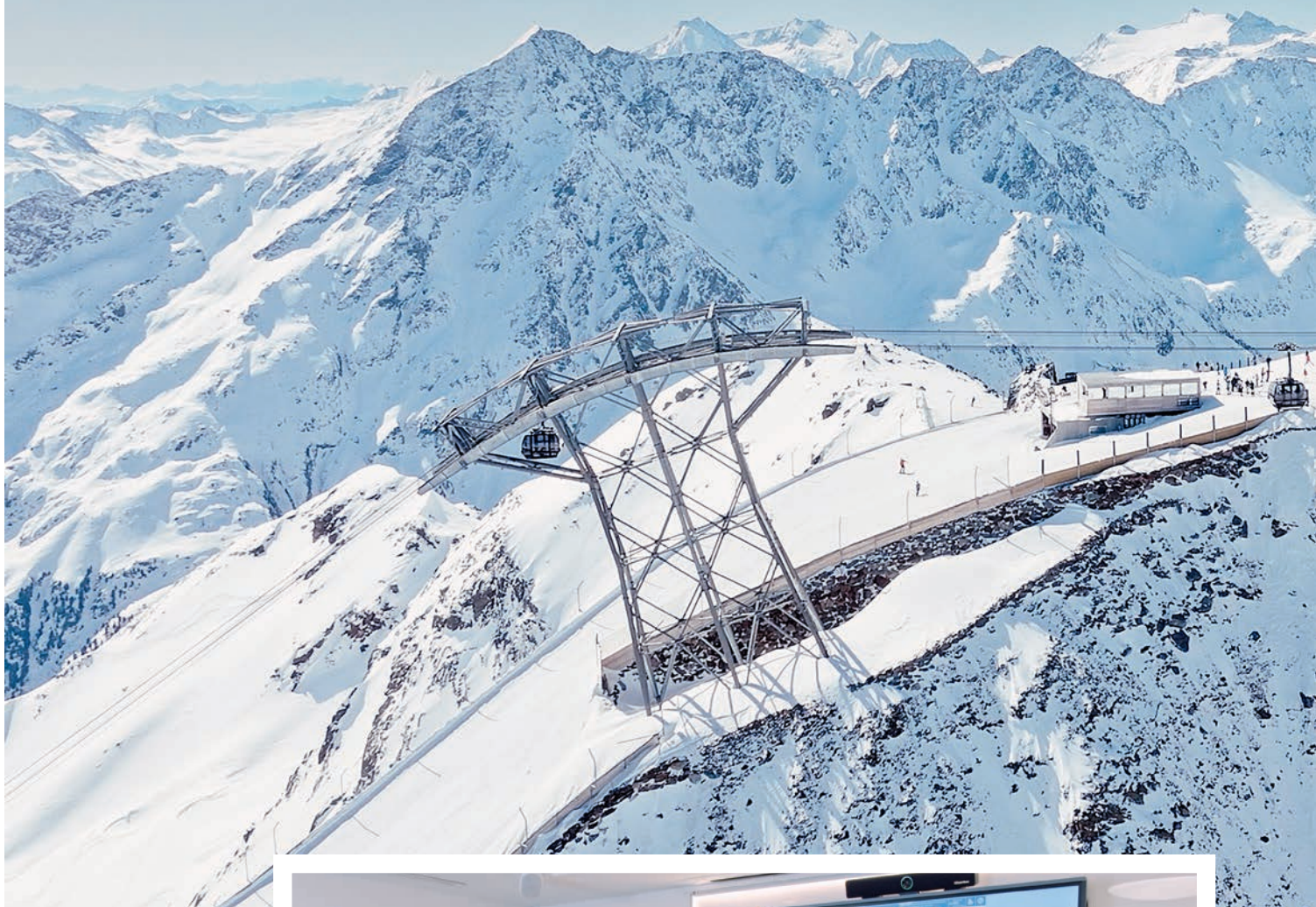
În cazul în care datele sunt transmise către cloud-uri sau companii externe, aceste fluxuri de date trebuie, de asemenea, securizate corespunzător. Impactul vulnerabilităților de securitate în acest domeniu este uriaș: „Începe cu posibilitatea ca atacatorii să manipuleze sistemul de încălzire, având efecte relativ minore. Dacă echipamentele dintr-un centru operațional sunt compromise, situația se schimbă radical”.

Este esențială segmentarea traficului de date, astfel încât datele să fie direcționate doar acolo unde este necesar, prevenind astfel accesul neautorizat al hackerilor. De asemenea, este crucial să se stabilească un sistem de gestionare a continuității activității (BCM) și de gestionare a situațiilor de criză în cazul unui atac cibernetic, care să stabilească cine trebuie să acționeze, ce măsuri trebuie luate și când, pentru a restabili funcționarea normală după un atac cibernetic.

„Acest lucru ar trebui exersat sau analizat periodic împreună cu angajații”, a recomandat Martin Krammer. În plus, planurile de urgență ar trebui să fie disponibile și în format tipărit, deoarece acesta este singurul mod de a garanta accesul la ele în timpul unui atac cibernetic.

Domeniu de schi digitalizat

Condițiile pârtiilor din stațiunea de schi pe ghețar din Sölden, Tirol, sunt optimizate printr-o soluție inteligentă. Aceasta nu doar că reduce riscurile de a nu avea zăpadă în sezon, dar și maximizează eficiența energetică a sistemului de producere a zăpezii.



Domeniul schiabil Sölden se bazează de peste 15 ani pe Siemens ca partener pentru digitalizare.





Situată între altitudinile de 1.350 și 3.340 de metri, stațiunea de schi Sölden din Tirol este un paradis pentru iubitorii de schi, oferind o gamă largă de atracții, inclusiv instalația cinematografică „007 ELEMENTS” la 3.040 de metri și Raliul BIG 3. Cu 144 de kilometri de pârtii ce se întind pe o suprafață totală de 450 de hectare, accesibile prin 31 de telecabine, Sölden promite o experiență de schi de neuitat, cu zăpadă garantată din luna octombrie până în mai. Aceasta este posibilă

datorită prezenței a doi ghețari și a unui sistem inteligent de producere a zăpezii, care economisește resurse. În contextul schimbărilor climatice și al creșterii costurilor energiei, Bergbahnen Sölden a luat măsuri proactive pentru a se asigura că această promisiune este îndeplinită în fiecare an. Acest angajament față de inovație și sustenabilitate face din Sölden o destinație de top pentru iubitorii de schi. Siemens a fost ales ca partener,

datorită sistemelor sale de comandă SIMATIC S7. În proiectele anterioare de licitație publică, compania a reușit să îndeplinească așteptările clientului în ceea ce privește standardizarea, fiabilitatea și scalabilitatea soluțiilor sale industriale, de proces și de automatizare. “În urmă cu peste 15 ani, am demarat primul nostru proiect de digitalizare, implementând o strategie pentru limitarea vârfurilor de sarcină”, rememorează Michael Maier, directorul tehnic adjunct al Bergbahnen Sölden. “Am instalat 320 de puncte de măsurare în întreaga zonă și 100 de kilometri de cablu de fibră optică în zona de schi. Punctele de măsurare sunt acum conectate la diverse alte sisteme de tehnologie a informației și comunicațiilor”. Cu ajutorul dispozitivelor multifuncționale bazate pe SENTRON PAC, vârfurile de sarcină din timpul verii pot fi identificate cu precizie.

Soluție aplicabilă în multiple scenarii

Deși, potrivit directorului tehnic adjunct al Bergbahnen Sölden, respectarea valorii maxime a energiei furnizate poate fi descrisă ca fiind principalul obiectiv la momentul respectiv - depășirea așa-numitului vârf de sfert de oră este foarte costisitoare - aplicabilitatea s-a extins considerabil de atunci. „Timpii morți în producția de zăpadă pot pune rapid în pericol sezonul pentru clienții noștri”, a spus Lukas Tauferer, specialist în automatizarea proceselor la Siemens, „de aceea este esențial ca nici transformatoarele și nici alimentatoarele de ieșire ale tunurilor de zăpadă să nu se supraîncarce. În același timp, există un potențial de economisire a energiei și a costurilor dacă zăpada este produsă în funcție de cerere”. Estimarea condițiilor reale de zăpadă din teren înainte de începerea sezonului, cantitatea de zăpadă produsă



Echipamentele pentru amenajarea pistelor pot măsura în timp real stratul de zăpadă de pe pârtii.



“În condiții ideale de mediu, perioada necesară pentru a obține un strat de zăpadă consistent nu depășește o săptămână înainte de Crăciun și adesea este chiar mai scurtă”.

Michael Maier, director tehnic adjunct al Bergbahnen Sölden

tehnic și necesară pentru o deschidere reușită a sezonului și condițiile de producere a acestuia - adică apa pentru zăpadă și aerul rece din mediul ambiant, în mod ideal cu mult sub punctul de îngheț - sunt responsabilitatea experților în materie de zăpadă artificială.

„Cu toate acestea, este foarte dificil de estimat dacă stratul de zăpadă are 1, 5 sau 10 metri, deoarece masa de zăpadă se adaptează la condițiile mediului. Ca urmare, experții noștri au creat un strat minim, atât de bază cât și sezonier, pentru a nu perturba experiența schiorilor”. Ruetz continuă: “Am trecut la următoarea inovație a domeniului de ski Bergbahnen Sölden - digitalizarea gestionării zăpezii, astfel încât să putem lua decizii bazate pe date precise”. În perioada 2014-2016, Bergbahnen Sölden, în colaborare cu Kässbohrer, a implementat proiectul SnowSAT. De atunci, echipamentele pentru amenajarea pistelor estimează în timp real înălțimea efectivă a stratului de zăpadă de bază de pe pârtii, utilizând tehnologii GPS și LIDAR. Fiecare tun de

zăpadă este asociat cu o anumită zonă și culoare, în funcție de cantitatea de zăpadă disponibilă, așa cum este reprezentată în sistemul SnowSAT. „Numai setările pentru stratul de zăpadă de bază se bazează pe cunoștințele și experiența specialiștilor noștri”, a explicat Manuel Köll din echipa IT de la Bergbahnen Sölden. Acestea sunt apoi transferate de la SnowSAT la sistemul de gestionare a zăpezii bazat pe WinCC, care este furnizat tot de Siemens. Aceasta indică volumul de apă necesar pentru producerea zăpezii în fiecare punct de alimentare care trebuie utilizat, în funcție de secțiunea de pârtie alocată. Când suprafața de zăpadă poate fi gestionată cu ajutorul echipamentelor pentru amenajarea pistelor, datele live privind măsurătorile din teren sunt transmise în timp real către sistemul central de control și comparate cu valorile țintă corespunzătoare. „Soluția utilizează diferența pentru a determina volumele de apă încă necesare pentru zăpadă. Prin urmare, sistemul garantează o pregătire a pistelor bazată pe necesități, economisind resurse și fiind eficientă din punct de vedere al costurilor”, a concluzionat Harald Ruetz.

Managementul energiei

Prin conectarea sistemului de control al tunurilor de zăpadă cu sistemul de gestionare a energiei, specialiștii primesc informații vizuale precise și clare privind gestionarea sarcinii pe domeniul schiabil.

Aceasta include, de exemplu, numărul de tunuri de zăpadă suplimentare care pot fi alocate la stația de acționare a unei telecabine, împărțite pe diferite pârtii. În același timp, din cauza dimensiunii sistemului de producere a zăpezii și a numărului de tunuri de zăpadă, alocarea punctelor respective poate fi aproximativă, într-o măsură limitată. În modul de vizualizare, se

utilizează benzi colorate pentru alocare și, cu un singur clic, se poate vedea la care dintre cele 11 stații de pompare sunt conectate generatoarele individuale.

În ceea ce privește gestionarea sarcinii, diagramele se extind până la transformator, unde poate fi atinsă puterea maximă.

Manuel Köll: „În plus față de modul de vizualizare, care, în configurația standard se bazează pe un tun de zăpadă pentru fiecare punct de alimentare, soluția noastră ne permite să monitorizăm întotdeauna consumul real pe teren - chiar dacă tunurile de zăpadă funcționează fără conexiune de date.

O alarmă se declanșează imediat dacă se apropie de limita de putere”.

Pe lângă vârfurile de un sfert de oră menționate la început și potențialele economii datorate utilizării precise a tunurilor de zăpadă în funcție de cantitatea de zăpadă măsurată, există un alt motiv important pentru gestionarea cu succes a energiei și a sarcinii întregului sistem de producere a zăpezii: „Din cauza condițiilor climatice, intervalul de timp pentru producerea unui strat de zăpadă de bază reușit, în condiții ideale, nu este mai mare de o săptămână înainte de Crăciun și adesea este chiar mai scurt”, a explicat Maier. Acesta a adăugat: „Dacă s-ar ajunge la o suprasolicitare și tunurile de zăpadă ar ceda, repornirea acestora ar putea dura câteva ore, în cel mai bun caz. Această întârziere ne-ar putea face să ratăm începutul sezonului. Cei de la Bergbahnen Sölden au fost întotdeauna conștienți de această provocare.

Prin ajutorul tehnologiei de nivel înalt și al digitalizării, sunt reduse riscurile, este maximizată eficiența energetică și sunt conservate resurse prețioase, eliminându-se necesitatea transportului zăpezii de către echipamentele de amenajare a pârtiilor.



Gestionarea zăpezii bazată pe date precise.



“În plus, diferitele noastre sisteme furnizează date valoroase care permit dezvoltări ulterioare”, a continuat Maier.

“Este bine cunoscut faptul că sarcina conectată a unui tun de zăpadă este comparabilă cu cea a unei case rezidențiale.

Cu toate acestea, putem demonstra că, în medie, fiecare dispozitiv funcționează doar 4,5 zile pe sezon”. Beneficiarii “splendorii albe” care rezultă din octombrie până în mai nu sunt doar angajații și compania, ci și întreaga regiune și turiștii care vin aici pentru a-și petrece vacanța.

111

Kilometri de pârtii (dintr-un total de 144 km) sunt acoperiți cu zăpadă în Sölden printr-o metodă inteligentă, care economisește resurse



Mai multă energie regenerabilă

Geamănul digital contribuie la îmbunătățirea capacităților de rețea în Aspern Seestadt

Un software inovator dedicat instalațiilor de joasă tensiune, numit Siemens LV Insights X, a fost lansat ca parte a proiectului de cercetare Aspern Smart City Research (ASCR). Acest software permite vizualizarea în detaliu a întregii rețele de joasă tensiune din Seestadt, un cartier din Aspern, Viena, unul dintre cele mai mari proiecte de dezvoltare urbană din Europa. Cu ajutorul unui geamăn digital al rețelei, pot fi identificate secțiunile critice, poate crește capacitatea utilizabilă a rețelei și poate integra energii regenerabile fără a fi nevoie de o extindere suplimentară a instalațiilor.

Pe baza datelor de rețea existente, se poate crea o imagine digitală completă

a rețelei de distribuție cu un efort redus și se poate planifica și exploata mult mai flexibil consumul datorită informațiilor obținute aproape în timp real.

Software-ul permite operatorilor de rețele de distribuție să reducă timpii de întrerupere cu până la 30%.

LV Insights X este parte a Siemens Xcelerator, o platformă digitală și deschisă care facilitează transformarea digitală pentru clienți.

LV Insights X este o soluție gata de utilizare, cu un timp scurt de implementare. Software-ul dispune de interfețe standard deschise care pot fi configurate printr-o simplă comandă drag-and-drop. Acest concept nou și flexibil se integrează perfect în coordonatele sistemului existent.

„Utilizarea resurselor de energie regenerabilă descentralizate reprezintă o componentă esențială a spațiilor urbane sustenabile. Flexibilitatea și transparența sporită este cheia optimizării planificării și gestionării rețelelor. Cu ajutorul LV Insights X, putem obține un nivel cu totul nou al digitalizării în Seestadt, Aspern”, a declarat directorul general al ASCR, Matthias Gressel.

LV Insights X este disponibil sub formă de Software-as-a-Service (SaaS). În comparație cu software-ul On Premises, SaaS garantează cel mai rapid timp de funcționare posibil, reduce semnificativ costurile și oferă standarde ridicate de scalabilitate și securitate cibernetică.

Asistent cu inteligență artificială generativă

Microsoft și Siemens își consolidează parteneriatul în domeniul inteligenței artificiale generative. Ca un prim pas, cele două companii au lansat Siemens Industrial Copilot, un sistem de asistență dezvoltat în comun și susținut de inteligența artificială pentru a îmbunătăți colaborarea dintre oameni și echipamente în sectorul producției. Siemens Industrial Copilot va permite utilizatorilor să genereze și să optimizeze rapid coduri de programare complexe pentru automatizare, să elimine erorile și să reducă semnificativ timpii de simulare. Acest lucru transformă un proces care durează săptămâni într-unul care durează doar câteva minute. „Copilot include tehnologia de automatizare și de simulare a proceselor oferită de Siemens Xcelerator și o extinde



aplicabilitățile prin Azure OpenAI Service de la Microsoft. Schaeffler AG, unul dintre principalii furnizori de componente pentru industria auto, este una dintre primele companii din domeniu care utilizează inteligența artificială cu scopul de a genera coduri fiabile pentru programarea sistemelor de automatizare industrială.

Soluție completă 5G

Pentru prima oară, Siemens introduce o infrastructură privată de comunicații mobile 5G, dezvoltată intern. Această soluție le permite companiilor industriale să își construiască propriile rețele 5G locale, oferind un suport optim pentru aplicațiile de automatizare. Infrastructura 5G a fost concepută de Siemens special pentru a răspunde



cerințelor specifice ale clienților și aplicațiilor industriale. Aceasta este formată dintr-un 5G-Core (nucleu 5G) și o rețea de acces radio (RAN). Diverse terminale 5G pot fi conectate la această infrastructură și pot comunica în cadrul rețelei private 5G. Soluția completă 5G este concepută pentru utilizarea în medii industriale dure. Pentru utilizarea integrată a rețelelor sunt folosite tablete, ochelari VR și instrumente inteligente. Dispozitivele Edge pot fi, de asemenea, utilizate în mod flexibil, de exemplu, în aplicații de tip brownfield, unde instalarea ulterioară a cablurilor este dificilă. Spre deosebire de alte tehnologii wireless, rețelele private 5G utilizează o bandă de frecvență cu licență și, prin urmare, pot fi operate fără interferențe.

200 de specialiști contribuie la dezvoltarea soluțiilor software Siemens în Graz
>> S. 38

14 parteneri lucrează în proiectul de servicii pentru gestionarea flexibilă a datelor UE DataBri-X
>> S. 44



Blueprint pentru o sortare mai eficientă a deșeurilor

O soluție robotică inovatoare, îmbunătățită cu inteligență artificială, facilitează un proces automatizat și adaptabil de sortare a deșeurilor.

Cu toate acestea, potențialul sistemului depășește cu mult această aplicație.

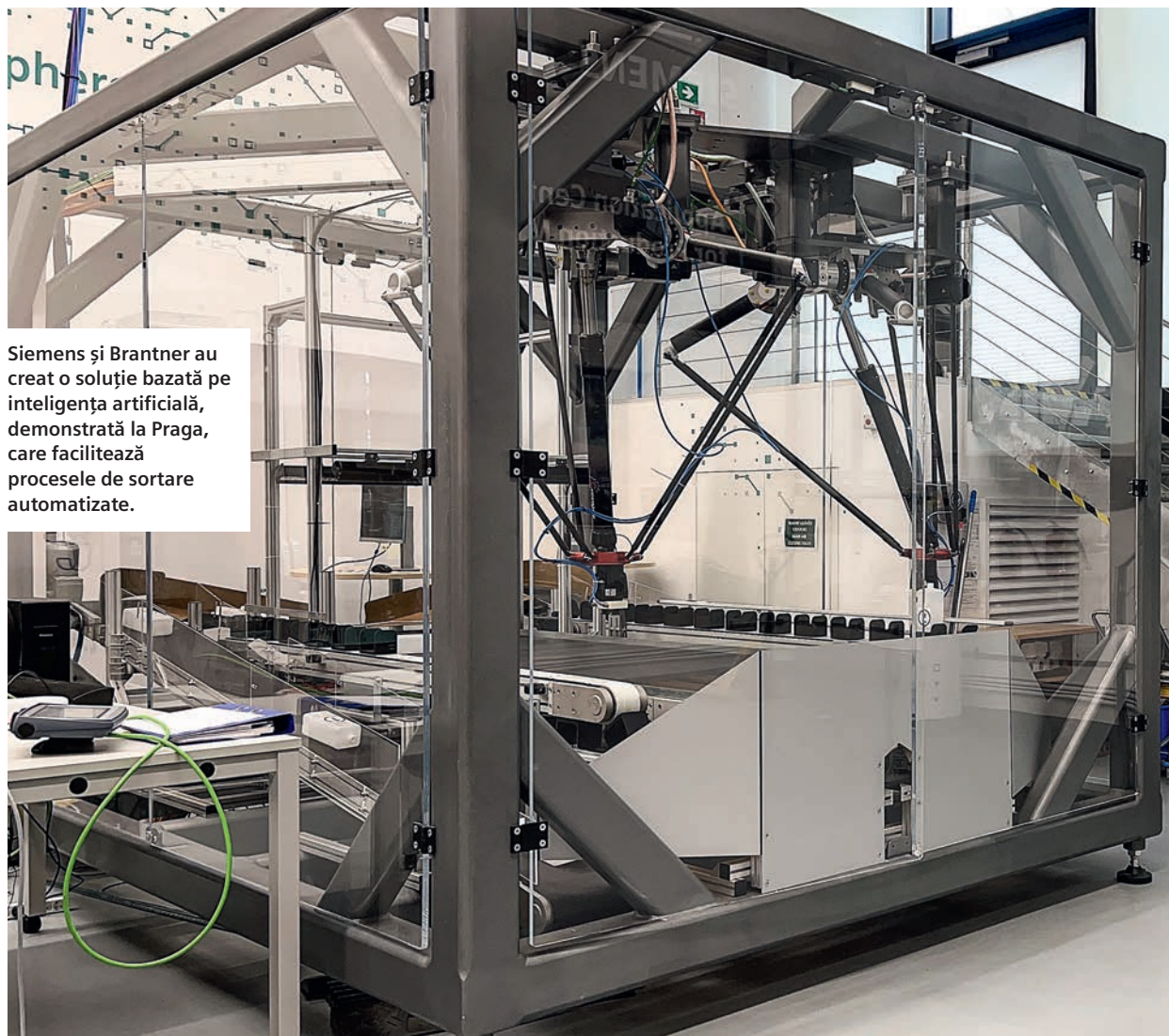
Reciclarea joacă un rol esențial în economia circulară, iar eficiența acestui model economic este în mare parte determinată de calitatea proceselor.

Cu alte cuvinte, metodele de sortare mai precise contribuie la o mai mare eficiență în domeniul reciclării. În acest context, Siemens, în colaborare cu Brantner, o companie internațională de

gestionare a deșeurilor din Krems, a dezvoltat o soluție care utilizează inteligența artificială pentru a permite un proces de sortare automată mai precis.

„Reciclarea va deveni din ce în ce mai importantă în viitor. Resursele noastre de materii prime sunt limitate și trebuie să le folosim în mod corespunzător. Folosim soluția dezvoltată în colaborare

cu Siemens în sortarea automată a plasticului, pentru a tria selectiv obiectele - înainte ca deșeurile să fie incinerate sau transformate în combustibili alternativi”, a explicat Christoph Pasching, șeful departamentului de soluții digitale și dezvoltare a afacerilor la Brantner. „În paralel, modelul nostru propriu de inteligență artificială, DeepSort,



Siemens și Brantner au creat o soluție bazată pe inteligența artificială, demonstrată la Praga, care facilitează procesele de sortare automatizate.

funcționează pe baza sistemului Siemens. Acesta permite recunoașterea obiectelor în timp real și implementarea măsurilor adecvate în funcție de proces. De asemenea, folosim această tehnologie în instalația noastră de sortare a materialelor plastice din Wölbling pentru a măsura adâncimea de sortare a instalației.

Inteligența artificială ne ajută să putem controla un robot care sortează în mod special recipiente PET, de exemplu”, a continuat Pasching.

„Dezvoltarea sistemului nostru, care funcționează cu soluții personalizate de inteligență artificială, marchează o etapă importantă în gestionarea și reciclarea deșeurilor.

În viitor, clienții noștri vor putea automatiza procesul de sortare într-un mod rapid și fără programare, prin învățarea unui model de inteligență artificială bazat pe fluxul individual de



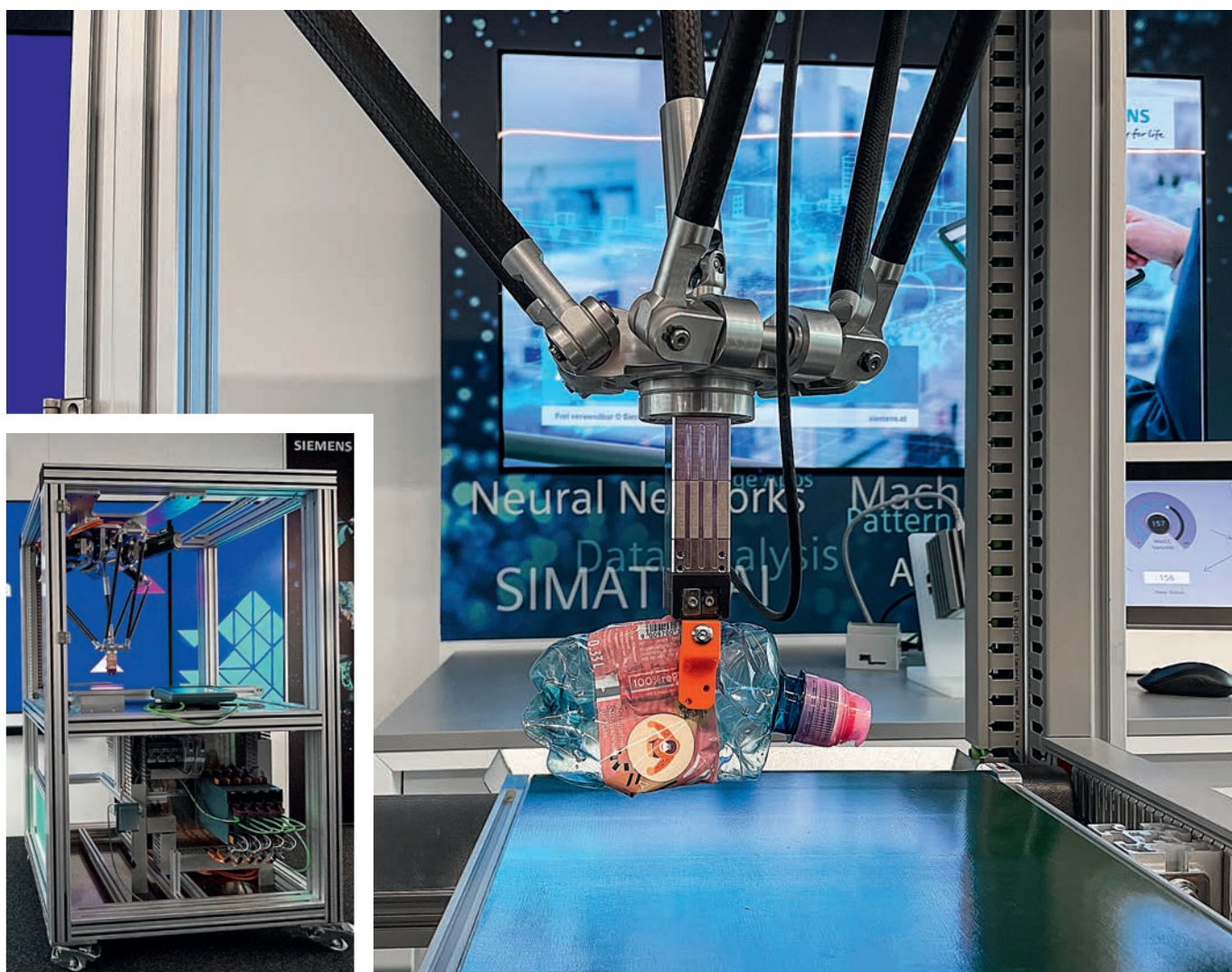
pentru sortarea automată a plasticului într-o manieră țintită”.

Christoph Pasching, Head of Digital Solutions & Business Development, Brantner

„Folosim soluția dezvoltată în colaborare cu Siemens

materiale”, a spus Daniel Schall, șeful grupului de cercetare Distributed AI Systems de la Siemens Technology din Austria.

Dar cum arată această soluție dezvoltată în comun de Brantner și Siemens? Sistemul modular este alcătuit din trei componente: un robot Delta-Picker, capabil să ridice obiecte cu ajutorul unui dispozitiv de prindere, o platformă Lifecycle pentru modelele de inteligență artificială și un Edge-Box, adică un PC industrial SIMATIC de la Siemens cu propriul sistem de operare, reprezentând creierul soluției de inteligență artificială. „Cea mai importantă dezvoltare a sistemului nostru Blueprint este platforma Lifecycle. Acesta poate efectua operațiuni de învățare automată, sau ML Ops pe scurt, pentru modelele de viziune computerizată”, a explicat Benedikt Häcker, inginer specializat în



Siemens DigiLab din Viena oferă clienților demonstrații practice ale sistemului său de modele, servicii care nu se limitează doar la industria de reciclare.

Machine-Learning la Siemens. MLOps pentru Computer Vision, adică vederea computerizată, integrează cele mai bune practici de dezvoltare de software în întregul ciclu de viață al modelelor de învățare automată vizuală: gestionarea structurată a datelor de imagine, instruirea și implementarea automată a modelelor în aplicații industriale de top, precum și monitorizarea continuă a performanței modelelor.

Nucleul platformei Lifecycle

Datele sunt colectate și etichetate în platforma Lifecycle, iar modelele adecvate sunt selectate, instruite, validate și reinstruite. Acest lucru permite depășirea provocărilor tipice din domeniul reciclării, cum ar fi schimbarea fluxurilor de deșeurilor sau noile reglementări legale.



„Dezvoltarea sistemului nostru, care se bazează pe soluții personalizate de inteligență artificială, marchează o etapă semnificativă în gestionarea deșeurilor și în reciclare”.

Daniel Schall, șeful grupului de cercetare Sisteme AI de distribuție, Siemens Technology Austria

„Platforma poate fi instruită în mod flexibil pentru a recunoaște noi obiecte în fluxul de materiale, iar sistemul sau modelul de inteligență artificială se adaptează automat în consecință, fără a necesita eforturi de programare”, a explicat Schall. Programele IA sunt, de asemenea, utilizate în sistemul de sortare. „Acestea sunt pachete de soluții configurabile care pot fi aplicate unui set de date și utilizate pentru a efectua o instruire pentru detectarea unui obiect. În același timp, programele conțin toate codurile, astfel încât acestea să poată fi executate în cele din urmă în Shopfloor pe Edge Device și să permită rezolvarea sarcinilor de predicție. De asemenea, ne referim la modelele de inteligență artificială ca fiind ”Pipeline”, deoarece, înainte și după ce modelul este aplicat în procesul de instruire sau predicție, se efectuează, de obicei, etape obișnuite de

procesare a imaginilor și a detecțiilor”, a spus Häcker, descriind programele de inteligență artificială, acestea sunt compuse din diverse modele de IA. Acestea oferă structuri predefinite, algoritmi eficienți și configurații de bază pentru cazuri de utilizare frecvente. Un astfel de program pentru sortarea deșeurilor, de exemplu, cuprinde funcții specializate de recunoaștere și clasificare a imaginilor, concepute pentru a identifica diferite tipuri de deșeuri.

Acesta include etape precum pregătirea datelor, formarea modelului, validarea și implementarea.

Astfel, dezvoltatorii pot să creeze mai rapid soluții de inteligență artificială, bazându-se pe metode deja testate și verificate, cum ar fi cele utilizate în industria de gestionare a deșeurilor. De îndată ce un model este gata de utilizare, acesta poate fi transferat în Edge-Box cu un singur clic, pentru a monitoriza în timp real fluxul de materiale al unui sistem de sortare a deșeurilor. Rezultatele sunt transmise către Delta-Picker, care este capabil să efectueze mișcări de prindere precise și eficiente pentru a selecta și sorta materialele destinate sortării.

Edge-Box, care acționează ca centrul de comandă al sistemului Blueprint, este echipat cu camere de ultimă generație și senzori în infraroșu apropiat (NIR), permițând detectarea și identificarea precisă a diferitelor materiale. Datele sunt colectate și transmise către platforma Lifecycle, unde modelele de inteligență artificială sunt instruite și optimizate.

Edge-Box, un PC industrial SIMATIC de la Siemens, este conceput pentru a rezista condițiilor dure care predomină în instalațiile de sortare a deșeurilor.

„Avem încredere că tehnologia noastră avansată va pune bazele economiei



„Clienții noștri nu primesc doar o soluție de inteligență artificială, ci au posibilitatea de a achiziționa de la noi o configurație completă”

Lukas Gerhold, Managerul Centruului de aplicații Siemens SIMATIC, Siemens Austria

circulare. Aplicarea inteligenței artificiale și a roboticii nu doar că eficientizează procesele de sortare necesare reciclării, dar reprezintă și pași semnificativi către un viitor sustenabil, unde resursele prețioase sunt păstrate și mediul este protejat”, a spus Schall. „Această evoluție este esențială, întrucât diminuează considerabil volumul de muncă al angajaților din stațiile de sortare a deșeurilor. Prin utilizarea sistemului de sortare, aspectele fizice epuizante și nesănătoase ale sortării manuale sunt eliminate, iar personalul poate fi recalificat în posturi mai puțin solicitante din punct de vedere fizic”, a continuat Schall.

Lukas Gerhold, Manager Siemens SIMATIC Application Centre, a adăugat: „De asemenea, a fost extrem de important pentru noi să păstrăm conceptul de automatizare („Blueprint”) cât mai standardizat și accesibil posibil. Clienții noștri nu primesc doar o soluție de inteligență artificială, ci au posibilitatea de a achiziționa de la noi o configurație completă. Aceasta integrează sistemele mecanice, acționările, sistemul de control, sistemul Edge și proiectul TIA Portal,

precum și interfețe deschise pentru inteligență artificială. Singura sarcină rămasă pentru client este instalarea sistemului.

În cazul în care nu există o soluție de inteligență artificială pentru o anumită problemă, îi putem asigura clientului instruirea necesară”.

Siemens oferă oportunitatea tuturor companiilor industriale interesate de a experimenta în timp real sistemul de sortare, sub forma unei celule robotizate mobile, la Siemens City din Viena. În plus, utilizarea acestora nu se limitează la domeniul reciclării, iar sortarea nu este singura sa capacitate. Soluția de inteligență artificială poate fi utilizată și pentru sortarea altor obiecte, cum ar fi produsele de panificație, sau pentru stivuirea plăcilor de lemn. De asemenea, sistemul de clasificare a obiectelor poate fi folosit, pentru controlul calității.

Grupul de cercetare Distributed AI Systems se ocupă cu explorarea potențialului imaginilor de cameră și a datelor din spectrul infraroșu apropiat (NIR) pentru clasificarea fluxurilor de materiale. Împreună cu institutul de cercetare Pro2Future GmbH și Montanuniversität Leoben, se concentrează pe un proiect finanțat de Agenția austriacă de promovare a cercetării (FFG), pentru a depăși limitele tehnologiei și a dezvolta soluții inovatoare pentru gestionarea deșeurilor.

Scopul principal este de a reduce efortul implicat în etichetare și de a cerceta modul în care modelele de inteligență artificială pot fi „alimentate” cu date NIR, în plus față de imagini. Aceste abordări sunt în curs de testare în cadrul Laboratorului de Cercetare Digitală a Deșeurilor de la Universitatea din Leoben (hi!tech).

Noul update criptografic

Criptografia, care constituie fundamentul matematic pentru securitatea informațiilor, trebuie integrată inițial într-o aplicație. **Un algoritm de criptare a fost dezvoltat la Universitatea de Tehnologie din Graz**, care se dovedește a fi extrem de adecvat pentru utilizarea în organizații mici, cu capacități de calcul redusă - bazat pe Internet of Things. Ulterior, dezvoltarea calculatoarelor cuantice va reprezenta o provocare majoră pentru companii, mai precis în actualizarea Post-Cuantică.

În era digitalizării, datele colectate și transmise constituie secretul comercial al companiilor.

Este de așteptat, și pe bună dreptate, ca autoritățile, sistemul de sănătate și furnizorii de servicii financiare să protejeze aceste date - de fapt, sunt obligați prin lege să o facă.

Deoarece am devenit din ce în ce mai digitalizați, sistemele de criptare „ușoare” sunt adesea esențiale. Maria Eichlseder, profesor la Institutul de Procesare Aplicată a Informației și Tehnologie a Comunicațiilor de la Universitatea de Tehnologie din Graz, este un pionier în acest domeniu.

Securitate prin criptografie

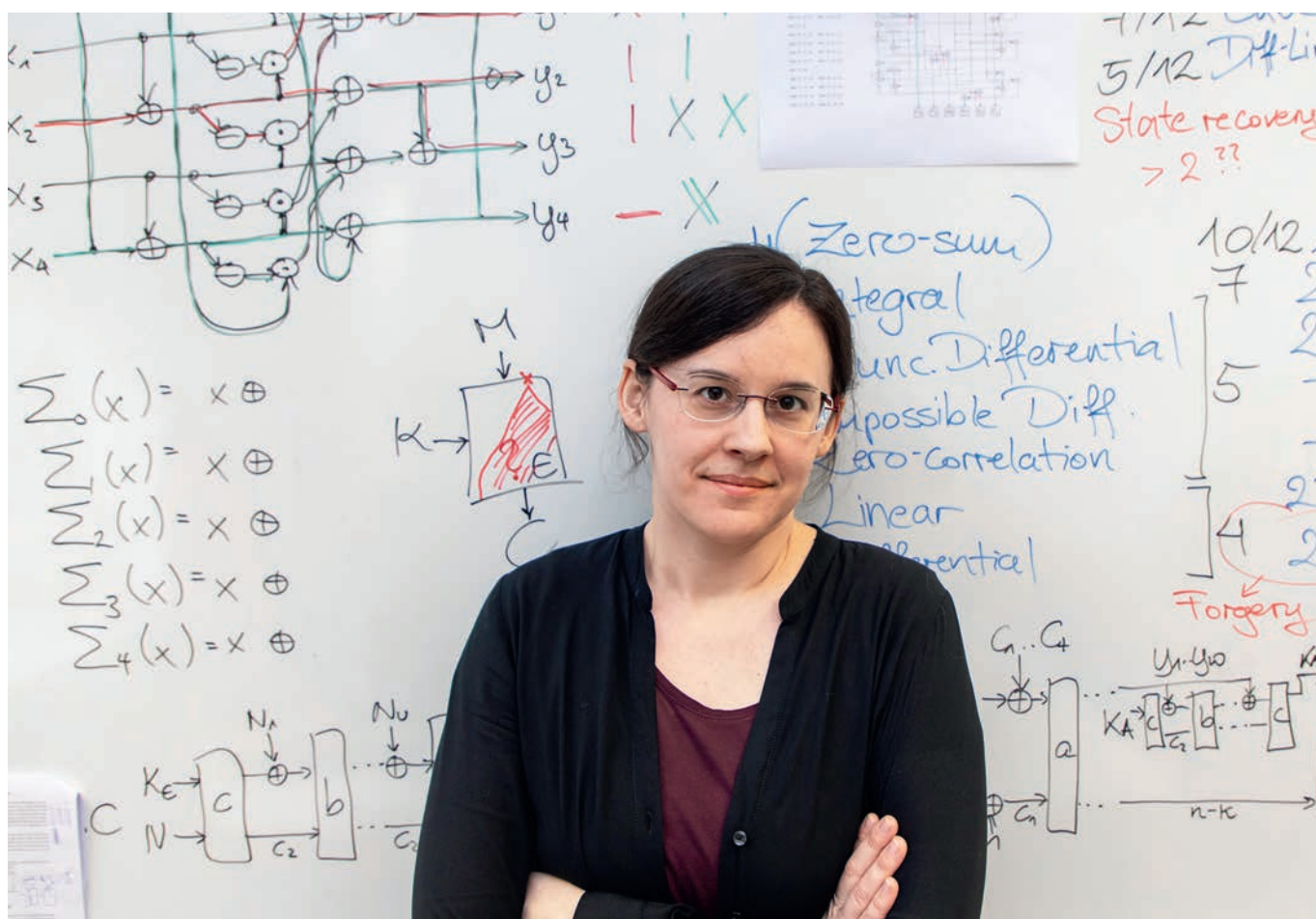
Criptografia, utilizată în mod tradițional pentru comunicare securizată, implică criptarea unui text simplu ce urmează a fi transmis, folosind o cheie secretă. În acest caz, mesajul poate fi transmis destinatarului prin intermediul unui canal de transmisie nesigur. Pe de altă parte, cheia trebuie să fie păstrată în siguranță și înlocuită. Scopul este de a cripta informațiile astfel încât persoanele neautorizate să nu le poată citi.

Maria Eichlseder, vorbind despre criptografie, afirmă că aceasta este fundamentul matematic al securității

informațiilor: „Avem nevoie de algoritmi matematici și de analizele acestora pentru a transforma datele sensibile, astfel încât să poată fi stocate și transportate în siguranță. Atunci când comunicăm prin canale nesigure și suntem supuși riscului de a fi interceptați, criptografia ne ajută să protejăm confidențialitatea și autenticitatea datelor. Prin urmare, este vorba „doar” de o dovadă matematică că modul în care sunt transportate datele este atât de sigur încât atacatorul nu poate contracara atingerea obiectivului de securitate decât cu un mare efort.

„Ceea ce criptografia nu poate ascunde atât de ușor este dimensiunea setului de date - de exemplu, cine comunică și cât de des”, a spus Maria Eichlseder, descriind principalele limitări ale utilizării criptografiei. Criptografia este esențială, deoarece fiecare persoană are dreptul la confidențialitate. Deși este un instrument necesar pentru protejarea secretelor, nu este suficient în sine. Protejarea vieții private în timpul colectării și utilizării datelor constituie un domeniu de cercetare distinct. Un algoritm de criptare, în sine, nu este suficient pentru a consolida securitatea cibernetică. Există o distanță considerabilă de la definiția matematică

a unui algoritm până la implementarea sa concretă ca produs. În momentul implementării hardware și software, pot apărea provocări suplimentare, cum ar fi gestionarea cheilor sau execuția securizată. Cu cât este mai mic dispozitivul care colectează și transmite date - cum ar fi sistemele încorporate, controlerele digitale sau Internetul obiectelor (IoT) - cu atât este mai probabil ca acesta să funcționeze într-un mediu securizat sau să necesite protecție fizică suplimentară. Maria Eichlseder lucrează la „criptografia ușoară”, care oferă un nivel adecvat de securitate cu resurse limitate, în special pentru dispozitivele mici cu capacități de calcul reduse. Dar cum putem identifica o criptare de calitate? Nu există un echivalent al TÜV (asociație de inspecție tehnică) pentru criptografie și, în ciuda evoluțiilor rapide din domeniul IT, este nevoie de mult timp pentru ca un algoritm să fie acceptat ca fiind sigur. Procedura ar trebui să ofere un nivel de securitate demn de încredere, să fie bine explicată, ușor de înțeles, precum și să prezinte o anumită eficiență și ușurință de utilizare, adaptându-se la scenariul de atac. Familia de algoritmi Ascon, dezvoltată la Universitatea de Tehnologie din Graz pentru criptare și hashing



autentificat (o metodă criptografică care convertește înregistrările de date și caractere de orice lungime în valori hash compacte de lungime fixă), a fost testată pe parcursul mai multor ani de către prestigiosul Institut Național de Standarde și Tehnologie și, în cele din urmă, a fost selectată ca standard din peste 50 de concurenți internaționali. Un algoritm este considerat practic sigur doar atunci când specialiștii în criptografie demonstrează că nu pot decodifica procesul timp de mai mulți ani.

Algoritmi post-cuantici

O tendință care ar trebui să fie pe radarul tuturor companiilor în prezent este utilizarea viitoarelor calculatoare cuantice, care ar putea face ca algoritmi criptografici actuali să devină instantaneu învechiți. Mai devreme sau mai târziu, acestea vor trebui să fie înlocuite cu noi proceduri „Post-Quantum” (post-cuantice) care să fie sigure împotriva unor astfel de atacuri. Nu este vorba de un scenariu de science-fiction: „Post-Quantum este o sarcină cu care multe companii trebuie să se

„Actualizarea post-cuantică reprezintă o provocare actuală cu care multe companii se confruntă. Această schimbare va deveni necesară în următorii ani”.

Maria Eichlseder, Expert în criptografie și profesor la Institutul pentru Tehnologie Aplicată pentru prelucrarea Informației și a Comunicațiilor de la Universitatea de Tehnologie din Graz

confrunte în prezent. Această actualizare va fi necesară în următorii câțiva ani. Noii algoritmi necesari în acest sens sunt în curs de dezvoltare și au fost standardizați. Cu toate acestea, necesită mult mai multe resurse, ceea ce poate afecta capacitatea sau performanța în timp real a sistemelor existente, de exemplu”.

Precum orice tehnologie, criptografia poate fi folosită în scopuri greșite. Criptografia poate fi folosită în scopuri neadecvate, cum ar fi ransomware pentru a comunica discret despre activități ilegale sau în cadrul serviciilor militare și de informații. Cu toate acestea, beneficiile pozitive ale cercetării criptografice le depășesc în mod clar pe cele negative, așa cum a spus

informaticianul: „Oricine dorește să ascundă date cu intenții ilegale poate face acest lucru, deja. Nu mai e niciun secret în această privință. Cercetarea în vederea îmbunătățirii proceselor este esențială pentru a putea proteja datele importante în scenarii tot mai complexe”. Cercetătorul a observat o nevoie și mai mare în acest sens în analizele de securitate.

Se pot lua măsuri de remediere numai dacă procedurile sunt analizate în detaliu și dacă se identifică lacunele de securitate.

În caz contrar, adversarii ne vor depăși la un moment dat.

De asemenea, în Austria se lucrează intensiv la noi algoritmi și la sisteme de apărare împotriva atacurilor.

Protejarea echipamentelor Internet of Things pentru domeniul industrial (IIoT)

Conexiunile dintre acestea aduc noi provocări pentru securitatea cibernetică.

Într-un proiect de cercetare, Universitatea de Tehnologie din Graz și Siemens colaborează pentru a dezvolta componente software industriale. Este esențial să asigurăm și să dezvoltăm cerințele hardware necesare pentru a rula în siguranță software-ul necesar realizării conexiunilor dintre echipamentele IIoT.

IIoT reprezintă un mediu extrem de divers, cu rețele, hardware și software partajate, rezultat din îmbinarea sistemelor IT cu infrastructura industrială. Securizarea Industrial Internet of Things (IIoT) este o provocare complexă și nerezolvată: numeroși actori, precum producătorii de echipamente, furnizorii de sisteme și software, își doresc să își protejeze activele - cum ar fi datele senzorilor, software-ul de control, proprietatea intelectuală - împotriva atacurilor cibernetică, eventual fără a avea dependențe reciproce în ceea ce privește securitatea. În acest context, „Edge Devices” - adică dispozitivele folosite pentru a conecta componentele industriale la internet - sunt deosebit de importante în ceea ce privește securitatea cibernetică.

Acest lucru expune componentele la toate tipurile de amenințări cibernetică. Pentru a garanta o funcționare în siguranță, TU Graz, în special Institutul pentru prelucrarea aplicată a informației și tehnologia comunicațiilor (IAIK), condus de Stefan Mangard - un expert cu ani de experiență în domeniul

securității cibernetică - a încheiat un parteneriat cu Siemens. În cadrul proiectului SEIZE, susținut de Agenția austriacă de promovare a cercetării (FFG), care a debutat la începutul anului 2022 și se va desfășura până la sfârșitul anului 2024, partenerii colaborează pentru a asigura securitatea componentelor software industriale și pentru a dezvolta cerințele hardware necesare rulării de software pe acestea într-un mod fiabil.

Valoare adăugată prin abordarea ecosistemică

Siemens și Universitatea de Tehnologie din Graz (TU Graz) au o colaborare de lungă durată.

Proiectele comune de cercetare se desfășoară la nivel local în cadrul a 16 rețele de cooperare distribuite global - împreună cu cercetători, clienți, fondatori, studenți și minți creative și inovatoare. Scopul acestei abordări ecosistemice este de a dezvolta produse, soluții și servicii pentru clienții Siemens care să îi facă mai eficienți, mai sustenabili.

Sub egida Universității de Tehnologie



din Graz, Siemens colaborează cu alți parteneri pentru a efectua cercetări comune pe teme și tehnologii. Sucursala Siemens din Graz se concentrează pe dezvoltarea de software și firmware; accentul se pune în principal pe securitatea cibernetică, siguranță, comunicare industrială și gestionarea eficientă a resurselor în procesul de reciclare. Dezvoltarea de software a început în 2014 cu 45 de angajați, iar compania acum are aproape 200 de angajați. „Departamentul nostru de software dezvoltă produse și soluții



care sunt implementate într-o varietate de aplicații industriale la nivel global. Punem un accent deosebit pe cercetare, inovație și sustenabilitate. De asemenea, urmărim acest lucru într-o serie de colaborări cu institute de cercetare universitare și parteneri din industrie”, a declarat Herbert Tanner, care este responsabil de dezvoltarea software-ului industrial și care conduce, de asemenea, locațiile Siemens din Styria și Carintia. Proiectul de cercetare SEIZE se focalizează pe îmbunătățirea securității execuției software în dispozitivele

industriale Edge.

Acestea pot să analizeze datele obținute din fluxul de producție, dar și să controleze anumite operațiuni.

„Prin urmare, este esențial să existe încredere din partea clienților că aplicațiile lor vor funcționa exact așa cum au fost concepute și nu vor fi afectate de un atac sau de alte aplicații. Abordarea noastră este de a proteja software-ul cu mecanisme hardware, astfel software-ul poate fi mai puțin susceptibil la atacurile cibernetice”, a explicat Sandra Dominikus, manager de

Siemens și Universitatea de Tehnologie din Graz au o colaborare de lungă durată.

Universitatea de Tehnologie din Graz face parte din ecosistemul global de cercetare și inovare al Siemens.



Securizarea IIoT este o provocare nerezolvată și complexă

proiect SEIZE în cadrul echipei de software de la Siemens Graz.

„Întrebarea centrală a cercetării la care lucrăm este: Cum pot diferite companii să opereze pe aceeași platformă Edge și să își protejeze activele fără a fi dependente de securitatea componentelor altor organizații?”, a spus Dominikus.

În cazul platformelor Edge, hardware-ul și, eventual, sistemul de operare sunt stabilite de producător.

Clienții folosesc această platformă pentru propriile aplicații și software.

„Provocarea este următoarea: cum își pot proteja clienții propriile echipamente și aplicații fără a se baza doar pe securitatea cibernetică oferită de platforma Edge?”, a explicat Sandra. În plus, „Din punctul nostru de vedere apare următoarea întrebare: Cum se poate securiza platforma astfel încât clienții care o folosesc să nu aibă acces total la datele și aplicațiile lor?” Astfel, echipele lui Stefan Mangard și Sandra Dominikus din cadrul proiectului SEIZE abordează și problema securizării dispozitivelor Edge, astfel încât acestea

să poată funcționa în siguranță, chiar și în fața unui atac cibernetic.

Evaluarea diferitelor abordări

TU Graz și Siemens analizează și evaluează mai multe opțiuni tehnologice în cadrul cercetărilor lor, iar în primul rând, un mediu hardware securizat. Aici pot fi stocate și executate programe deosebit de importante, acest mediu fiind protejat împotriva accesului extern.

„Conceptul de bază este următorul: componentele software care

funcționează pe același dispozitiv ar trebui să fie izolate cât mai mult posibil una de cealaltă.

Asta înseamnă că resursele unei componente nu pot fi accesate de o altă componentă”, a explicat Mangard, directorul Institutului TU. În al doilea rând, sunt abordate sandboxurile: „Acestea reprezintă un mediu securizat unde un cod nesigur poate fi executat fără a avea un impact potențial negativ asupra sistemelor conectate.

Componentele software terțe ar trebui să fie limitate cât mai mult posibil în sfera lor de influență; acest proces este cunoscut sub numele de sandboxing”, a spus Mangard.

În plus, există și a treia soluție tehnică: Calculul Autentic. Componentele software ar trebui să poată demonstra că funcționează conform scopului lor. Atât accesul la resurse, cât și secvența programului în sine, ar trebui să fie autentificabile.

„În cadrul proiectului, cercetăm, prin urmare, tehnici de izolare robuste care permit separarea software-ului critic și eliminarea conexiunilor nedorite dintre echipamente.

În acest scop, ne axăm pe două tehnici complementare de izolare: mediul hardware securizat și sandbox-urile”, a conchis profesorul Mangard.

„Mediul hardware securizat ajută la protejarea software-ului critic (de control) de restul sistemului și oferă un scut împotriva unui sistem de operare compromis. Sandbox-urile oferă modelul invers de protecție, ajutând la izolarea codului potențial periculos provenit de la terți”, a explicat Dominikus.

„Nu numai că investigăm limitările actuale ale mediilor hardware securizate, dar explorăm și noi extensii. Majoritatea tehnicilor de sandboxing nu

au fost încă investigate în legătură cu mediile de hardware securizate. Astfel, ne concentrăm pe depășirea limitelor acestor tehnologii și, în special, pe integrarea lor cu mediile de hardware securizate”, a spus Mangard.

În prezent, metodele și conceptele dezvoltate sunt puse în aplicare ca prototipuri în cadrul proiectului și sunt analizate într-un mediu de laborator. Evident, aplicabilitatea rezultatelor este esențială pentru ambii parteneri.

„Vom implementa cele mai promițătoare abordări pe care le dezvoltăm la institutul nostru sub formă de prototipuri în tehnologia Siemens și vom verifica viabilitatea lor. Având în vedere restricțiile industriale, obiectivul este de limitare a creșterii costurilor operaționale din cauza implementării securității suplimentar, la 10-20%”, a spus Stefan Mangard.

„Acest proiect comun de cercetare ne oferă posibilitatea de a elabora cerințe pentru hardware-ul nostru, astfel încât să putem rula software-ul adecvat. Tehnologiile evaluate pot fi apoi integrate în dezvoltarea produselor noastre”, a adăugat Sandra Dominikus, Manager proiect SEIZE.

„Prin abordările și exemplele de implementare pe care le dezvoltăm în cadrul acestui proiect împreună cu cercetătorii de la TU Graz, dezvoltatorii noștri se familiarizează cu cele mai recente descoperiri din acest domeniu. Acest lucru ne aduce beneficii în dezvoltarea caracteristicilor de securitate pentru sistemele noastre de control industrial, unele dintre acestea fiind dezvoltate și implementate chiar în Graz”, a spus expertul în securitate, evidențiind valoarea semnificativă pe care proiectele de cercetare, precum SEIZE, o aduc pentru Siemens și clienții săi.



„Vom implementa cele mai promițătoare abordări pe care le-am dezvoltat la institut, sub formă de prototip, folosind tehnologia Siemens și vom verifica viabilitatea lor în condiții reale”.

Stefan Mangard, șef al Institutului pentru Tehnologia Aplicată a Prelucrării Informației și a Comunicațiilor, Universitatea de Tehnologie din Graz



„Tehnologiile evaluate pot fi ulterior integrate în dezvoltarea viitoarelor noastre produse”.

Sandra Dominikus, Manager de proiect SEIZE și lider de echipă dezvoltare software industrial, Siemens Austria

Rețele securizate cu Siemens Xcelerator

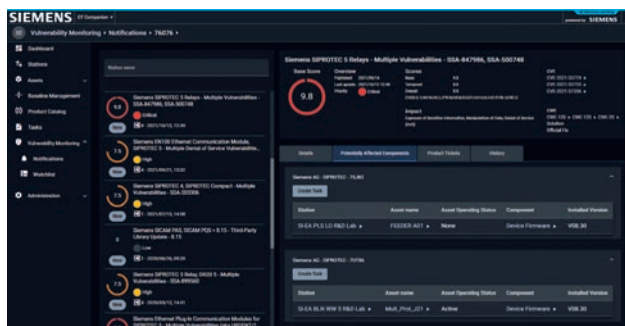
Prin intermediul **instalației sale pilot unice**, operatorul sloven de distribuție de energie electrică, Elektro Gorenjska, se află în pragul îndeplinirii cerințelor Uniunii Europene pentru securitatea rețelor și a sistemelor de informații.

Elektro Gorenjska, operatorul sloven de rețele de distribuție de energie, a stabilit un parteneriat cu Siemens în Slovenia pentru a se conforma viitoarei directive a UE privind securitatea sistemelor de rețele și de informații (NIS).

În cadrul Uniunii Europene, această directivă are ca obiectiv creșterea nivelului de securitate cibernetică în infrastructurile critice, inclusiv în cazul în operatorilor de sisteme de transport și distribuție a energiei electrice. Confruntându-se cu probleme de securitate cibernetică la stațiile sale de transformare, Elektro Gorenjska a apelat la Siemens pentru a îndeplini cerințele directivei NIS.

„Trebuie să ținem cont de faptul că problema securității OT într-o stație de transformare aduce cu sine cerințe suplimentare în comparație cu un mediu de birou”, a explicat Matej Grdadolnik, liderul diviziei de Electrification și Automatizare la Siemens în Slovenia. Prima provocare constă în identificarea componentelor software OT cu firmware-ul corespunzător în stația de transformatoare, urmată de verificarea actualizărilor.

Odată realizat acest pas, se pot analiza vulnerabilitățile software și deficiențele de securitate. Abordarea manuală a acestor probleme se dovedește a fi o activitate complexă și consumatoare de timp.



OT Companion este implementat într-o substație deținută de Elektro Gorenjska, cu scopul de a se conforma cerințelor NIS, urmând o lansare la nivelul întregii rețele.

OT Companion este soluția

OT Companion, soluția propusă de Siemens este o aplicație IoT bazată pe cloud care facilitează inventarierea continuă a activelor OT și gestionarea patch-urilor pentru operatorii de rețele

electrice din sectoarele energetic, industrial și de infrastructură.

OT Companion contribuie la păstrarea transparenței componentelor instalate pentru automatizarea rețelor de energie și la conformarea cu

Un atac cibernetic asupra
infrastructurii electrice a unei țări
poate avea un impact asupra
țărilor învecinate sau chiar
la nivel global



reglementările relevante în domeniul securității cibernetice.

„Pe baza datelor trimise de stația de transformare, care sunt apoi colectate în cloud, OT Companion identifică în mod automat software-ul instalat, efectuează o verificare a integrității pe baza software-ului original și evaluează potențialele vulnerabilități”, a spus Franziska Diestel, care este responsabilă pentru vânzările de software și digitalizare la Siemens Austria.

Instalarea proiectului pilot în stația de transformare

Soluția de transparență a activelor și de gestionare a patch-urilor, este testată în cadrul unui proiect pilot la o stație de transformare deținută de Elektro Gorenjska. Aceasta include mai multe componente care, în combinație, conduc la atingerea obiectivului dorit.

„Printre altele, tehnologia SICAM GridEdge de la Siemens este utilizată pentru a stabili conexiunea cu stația de transformare și pentru a colecta datele, pe care OT Companion le analizează și le

gestionează”, a relatat Vincent Dibon de la Siemens Austria, care a supervizat implementarea sistemului. SICAM Grid Pass de la Siemens este utilizat pentru a gestiona certificatele corespunzătoare generate între dispozitivele de teren și infrastructura cloud.

Diferențele dintre actualizări și baza instalată sunt evidențiate pe un tablou de bord.

Afișajul conține informațiile de configurare și firmware necesare pentru relee, unități terminale la distanță (RTU), routere și PC-uri. Disponibilitatea informațiilor despre patch-uri reprezintă un aspect important al protecției infrastructurilor esențiale împotriva atacurilor cibernetice. Astfel, patch-urile sunt gestionate în două etape: notificări de patch-uri (etapa 1) și recomandări de patch-uri (etapa 2).

OT Companion transmite ulterior aceste informații tehnicienilor, care pot aplica măsurile corective necesare.

OT Companion face parte din portofoliul Siemens Xcelerator. „Acest portofoliu ne oferă posibilitatea de a furniza clienților,

precum Elektro Gorenjska, inovații în continuă expansiune”, a declarat Diestel. Colegul ei sloven, Grdadolnik, a adăugat: „După faza pilot, am dori să extindem implementarea OT Companion în toate stațiile noastre de transformare. Având în vedere că unele dintre echipamentele instalate sunt vechi de câteva decenii, procesul rezultat va fi gradual.

Efortul va fi cu siguranță justificat, asigurându-se protecția infrastructurii esențiale împotriva atacurilor cibernetice, în conformitate cu NIS. Rețelele de energie electrică a statelor UE se pot confrunta cu aceeași amenințare, fiind conectate prin intermediul Rețelei europene a operatorilor de sisteme de transport (ENTSO) și al asociațiilor similare din sectorul rețelelor de transport și distribuție.

„Un atac cibernetic care vizează infrastructura critică din Slovenia ar putea avea, prin urmare, un impact și asupra transportului de energie în Carintia învecinată”, a subliniat Diestel. ○

Focus pe comunitățile de energie

Infrastructura din cadrul cercetării Aspern Smart City Research reprezintă cadrul perfect pentru studiul comunităților de energie.



Comunitățile de energie ar putea juca un rol semnificativ în îndeplinirea obiectivelor climatice.

Prin intermediul a două proiecte de cercetare inovatoare, Siemens și partenerii săi lucrează pentru a optimiza funcționarea și planificarea comunităților locale de producție și consum de energie.

Peste trei sferturi din emisiile de gaze cu efect de seră din Europa sunt generate de producția și consumul de energie.

Prin urmare, „Green Deal”, adică atingerea obiectivelor climatice până în 2030 sau neutralitatea climatică până în 2050, reprezintă o preocupare centrală a Uniunii Europene în lupta împotriva schimbărilor climatice și a degradării mediului. Comunitățile de energie reprezintă un instrument paneuropean pentru creșterea aprovizionării cu energie din surse regenerabile.

Acestea permit diferiților actori, cum ar fi populația, operatorii de clădiri, municipalitățile și companiile, să își unească forțele pentru a genera, stoca, comercializa și utiliza în mod colectiv energie (adică electricitate, căldură sau gaz) provenite din surse regenerabile. Implementarea cu succes a comunităților de energie este plină de provocări - atât în faza de planificare, cât și în timpul funcționării.

În faza de planificare, este esențial să se identifice combinația potrivită de participanți asigurând astfel o distribuție echitabilă a responsabilităților și să se aleagă cel mai potrivit mod de funcționare, în funcție de participanți, pentru a asigura

operarea fără probleme și viabilitatea economică a comunității după implementare. La fel de importantă, după implementare, este menținerea fără probleme a operațiunilor comunității și a viabilității economice a proiectului.

Rolul comunităților de energie în rețeaua electrică

În practică, comunitățile de energie reprezintă un alt jucător proactiv, dinamic și foarte complex în rețeaua electrică. Această complexitate poate limita transparența necesară într-un ecosistem digital - de exemplu, o mașină electrică nu a fost încărcată complet, în ciuda vremii însorite.

În prezent, se dezvoltă metode pentru a facilita planificarea și operarea viitoarelor comunități de energie, în cadrul a două proiecte de cercetare la care participă Siemens Austria (grupurile de cercetare a inteligenței artificiale, tehnologiilor de configurare și analiză a datelor și a soluțiilor IoT industriale inteligente).

Acestea sunt proiectul european DataBri-X, care se concentrează pe dezvoltarea metodelor de planificare, respectiv proiectul național SENSE, care se ocupă de metodele de operare.

DataBri-X, format dintr-un consorțiu de 14



În cadrul a două proiecte de cercetare, se elaborează metode menite să faciliteze planificarea și operarea viitoarelor comunități ce operează cu energie regenerabilă.

parteneri europeni, dezvoltă un set de instrumente și servicii (denumite Bri-X, sugerând ideea de cărămizi de construcție) pentru un proces flexibil de gestionare a datelor în contextul spațiilor europene de date. Spațiile de date reprezintă o infrastructură federată și deschisă pentru schimbul de date pe baza unor strategii, reguli și standarde comune. Procesul de gestionare a datelor dezvoltat în DataBri-X este conceput pentru a permite proiectarea și implementarea eficientă a proceselor bazate pe date. Un exemplu concret: să presupunem că trebuie analizat bilanțul unei comunități de energie.

Acest proces necesită, de obicei, câteva etape: în primul rând, datele trebuie să fie curățate și anonimizate, apoi evaluate folosind diverse metode de analiză. În cele din urmă, rezultatele analizelor sunt sintetizate într-o evaluare generală. Setul de instrumente DataBri-X este conceput pentru a permite proiectarea automată a unor astfel de procese. Serviciile (Bri-X), cum ar fi serviciul de

anonimizare a datelor, sunt propuse utilizatorilor pe baza unei evaluări a necesităților acestora. Ca urmare, procesul este apoi efectuat automatizat. Ce legătură are acest lucru cu planificarea comunităților de energie? Simulările permit testarea în avans a unor parametri importanți, cum ar fi rețelele de participanți și modurile de funcționare, precum și evaluarea viabilității economice a acestora. BIFROST a fost dezvoltat de departamentul de cercetare Siemens din Austria pentru a proiecta scenarii de simulare și a le executa.

Planificarea prin simulare

Proiectarea unor astfel de scenarii și, în special, pregătirea datelor pentru simulare reprezintă în prezent un proces intensiv, care are loc manual.

Datele corecte trebuie mai întâi identificate pentru un anumit scenariu și pregătite astfel încât să poată fi utilizate în cadrul simulării. Acest lucru face ca simularea comunităților de energie să fie un caz de utilizare interesant pentru proiectul de

cercetare DataBri-X, finanțat de UE. Infrastructura Aspern Smart City Research (ASCR) din Seestadt în Aspern, în cadrul căruia Siemens și municipalitatea din Viena colaborează pentru a modela viitorul energiei în zonele urbane, oferă mediul de testare ideal pentru acest lucru. Prin urmare, DataBri-X permite automatizarea procesului de pregătire a simulărilor, adică identificarea surselor de date necesare în spațiile de date și preprocesarea lor automată (prin Bri-X corespunzător) pentru simulare. Rezultatele simulării pot fi apoi postprocesate folosind Bri-X adecvat, salvate într-un spațiu de date și partajate cu alți parteneri interesați. DataBri-X facilitează procesarea simulărilor în planificarea bazată pe simulare a comunităților energetice. Acest lucru permite simularea rapidă a diferitelor scenarii (cu diferiți participanți și moduri de funcționare) și ajută la vizualizarea potențialului comunităților de energie. Operarea acestora reprezintă, însă, o

provocare. Mai presus de toate, trasabilitatea proceselor dinamice și complexe este o dificultate majoră. Pentru a ilustra mai bine acest lucru, să presupunem că avem o comunitate de energie formată din doi participanți la o rețea de distribuție - o clădire inteligentă dotată cu un sistem fotovoltaic cu o baterie de stocare, precum și o clădire rezidențială. În cadrul comunității clădirea inteligentă își vinde surplusul de energie fotovoltaică clădirii rezidențiale. Astfel, crește oferta de energie regenerabilă locală în rețeaua de distribuție.

Pentru a menține funcționarea optimă a rețelei de distribuție, operatorul acesteia poate stabili anumite specificații pentru comunitatea energetică, precum limitele de alimentare.

În cazul în care există acum o încălcare a specificațiilor, de exemplu prin depășirea aportului permis, este necesar să se identifice cauza.

În contextul exemplului tocmai menționat, cauza ar putea fi o baterie defectă în clădirea inteligentă, din cauza căreia energia generată de sistemul fotovoltaic nu a putut fi stocată temporar, așa cum era planificat.

O altă cauză posibilă ar putea fi faptul că prognoza de generare a energiei a fost imprecisă, adică s-a estimat o cantitate mai mică de energie fotovoltaică decât cea care a fost de fapt produsă.

Creșterea numărului de participanți adaugă complexitate sistemului, ceea ce complică identificarea surselor problemelor și diminuează claritatea evenimentelor din sistem.

În plus, sunt necesare motivații diferite în funcție de utilizator. De exemplu (în cazul prezentat mai sus), operatorul unei comunități energetice are nevoie de o motivație diferită pentru rezidenții blocului de apartamente sau pentru operatorul rețelei de distribuție de energie.

14 **colaborează pentru a dezvolta servicii care să faciliteze un proces flexibil de gestionare a datelor în cadrul proiectului de cercetare al UE, DataBri-X.**

Abilitatea de a interpreta evenimentele din sistem

În cadrul proiectului SENSE, finanțat de Agenția austriacă de promovare a cercetării FFG, se dezvoltă abordări pentru interpretarea evenimentelor sistemice în cadrul sistemelor dinamice de o complexitate extremă.

Aceste sisteme cuprind domenii fizice, digitale și umane, comunitățile de energie reprezentând un caz de utilizare centralizată.

SENSE dezvoltă metode în domeniul inteligenței artificiale (IA) neuro-simbolice. Inteligența artificială neuro-simbolică combină metode de inteligență artificială „clasică” bazată pe reguli (simbolică) cu rețele neuronale și „învățare profundă” (inteligență artificială sub-simbolică).

Prin această combinație, se pot depăși limitările metodologice existente.

Modelele simbolice, în timp ce sunt eficiente în reprezentarea cunoștințelor, se confruntă cu dificultăți în procesarea datelor nestructurate - o problemă cunoscută sub numele de fundamentarea simbolurilor. Acestea pot funcționa doar în limitele cunoștințelor pe care le reprezintă..

Pe de altă parte, rețelele neuronale și alte

metode de învățare automată pot avea dificultăți în generalizare, mai ales atunci când situația depășește contextul pentru care au fost instruite.

O altă provocare cu rețelele neuronale este că acestea pot apărea ca o “cutie neagră” pentru utilizatori. Deși aceste metode sunt eficiente în identificarea și clasificarea erorilor într-un sistem, răspunsul la întrebarea “de ce?” (adică, de ce a decis rețeaua să clasifice o intrare într-un anumit mod) rămâne adesea neclar, spre deosebire de abordările simbolice.

Rezultă necesitatea unei abordări combinate pentru a depăși aceste limitări.

Această incertitudine sau lipsa de claritate în explicarea soluțiilor, face dificilă utilizarea IA în aplicații critice pentru siguranță și ridică probleme de etică.

Combinând două abordări diferite, putem beneficia de cele mai eficiente caracteristici ale inteligenței artificiale. Pe de o parte, IA simbolică ne permite să structurăm sistemul. Pe de altă parte, IA subsimbolică ne ajută să extindem cunoștințele deja stocate cu ajutorul rețelelor neuronale.

În cadrul proiectului SENSE, aceste metode sunt utilizate în contextul detectării și explicării evenimentelor din sistemul energetic, un exemplu fiind funcționarea comunităților de energie. Acest proiect este, de asemenea, în curs de dezvoltare în cadrul ASCR din Aspern Seestadt, Viena. Prin utilizarea metodelor neurosimbolice, problemele operaționale sunt identificate, explicate într-un mod personalizat și ușor de înțeles pentru utilizator, iar soluțiile sunt generate automat pentru a ajuta utilizatorul să rezolve problema.

În plus față de aplicarea lor în sistemele energetice, abordările neuro-simbolice constituie un instrument valoros pentru portofoliul de automatizări Siemens în numeroase alte sectoare industriale, datorită capacității lor de a prezenta într-un mod ușor de înțeles raționamentul din spatele deciziilor sale.





Schimbul de date în ecosistemele deschise

În ecosistemele deschise, **suveranitatea datelor** este esențială: colaborarea în afara granițelor companiei necesită reguli clare pentru partajarea datelor.

Jacob, în vârstă de cinci ani, își întreabă părinții ce este împărțirea. Aceștia îi explică: „Dacă ai șase bucăți de ciocolată și le împarți cu sora ta, câte bucăți primește fiecare?” Jakob întreabă altceva: „Cum să împărțim? Egal?” Conceptul de dreptate și echitate ne este familiar încă din copilărie. Când vine vorba de împărțirea ciocolatei, este ușor de înțeles ce înseamnă împărțirea echitabilă: „Fiecare primește 3 bucăți”, a răspuns prompt Jakob. Cu toate acestea, atunci când vine vorba de schimbul de date industriale, există multă neîncredere cu privire la faptul că toată lumea se comportă corect - în special atunci când este vorba de date de producție

sensibile.

Negocierea contractelor poate fi un proces care consumă mult timp și resurse, făcând schimbul de date costisitor. Scopul inițiativelor europene, cum ar fi Gaia-X și Manufacturing-X, este de a facilita acest schimb de date.

La baza acestui schimb se află suveranitatea datelor. Compania care a generat datele decide singură cine este autorizat să le utilizeze, unde și pentru cât timp, în ce scop și la ce preț.

Amprenta ecologică a produselor

Un exemplu de schimb de date în domeniul sustenabilității este amprenta ecologică a produselor. În



viitor, va fi obligatoriu ca tot mai multe etichete de produse să includă amprenta de carbon (PCF). Imaginați-vă că fiecare produs nu are doar un preț, ci și o valoare care indică emisiile de CO₂ generate în timpul întregului proces de producție. Produsele cu un PCF mai mic vor avea un avantaj competitiv. Dar cum ne putem reduce la minimum amprenta de CO₂? Nu va fi suficient ca o companie de producție să încerce pur și simplu să își reducă la minimum propria contribuție la amprenta de carbon. De asemenea, trebuie luați în considerare factori precum achiziționarea de materii prime și componente. Pentru a calcula amprenta de carbon totală a

produsului, aceste cote trebuie adăugate la PCF-ul propriu al companiei. Siemens a dezvoltat instrumentul de gestionare a emisiilor SiGreen pentru a colecta date privind amprenta de carbon de-a lungul întregului lanț de aprovizionare. Astfel, există transparență în ceea ce privește locul în care este generată cea mai mare parte a amprentei de carbon a produsului și unde ar trebui să ne concentrăm eforturile de îmbunătățire. Un premiu Nobel a fost acordat pentru recunoașterea faptului că, dacă fiecare se concentrează doar pe propriile interese, nu se atinge în mod automat optimul general - ceea ce tehnicienii

numesc “optimul global”. Acest lucru se întâmplă și în cazul amprentei de CO₂. În viitor, fiecare companie din lanțul de aprovizionare se va strădui să își reducă la minimum propria contribuție la PCF - dar numai de la intrarea în companie până la ieșire, motiv pentru care se numește „gate-to-gate”. Acest lucru nu înseamnă că amprenta de carbon globală a produsului nu poate fi îmbunătățită și mai mult. Este necesar să se îmbunătățească și amprenta de carbon a produselor din întregul ecosistem al lanțului de aprovizionare. Un exemplu concret: amprenta de CO₂ a unei mașini este determinată în

mare măsură de cantitatea de oțel utilizată în construcția sa. Astfel, dacă un constructor de mașini dorește să obțină cea mai mică Amprentă de Carbon pentru mașina sa, ar putea proiecta mașina într-o formă mai puțin robustă, obținând astfel o amprentă de CO₂ mai mică la un preț similar sau chiar mai mic.

Cu toate acestea, dacă producătorul de mașini fabrică un produs de calitate inferioară și, prin urmare, produsul finit consumă mai multă energie pe întreaga sa durată de viață, atunci Amprenta de Carbon a Produsului pe întreaga durată de viață este mai mare

decât dacă utilajul ar fi fost construit mai robust de la început - iar utilajul în sine ar fi avut, deci, o Amprentă de Carbon a Produsului ușor mai mare. Prin urmare, este important să se ia în considerare întregul ecosistem și nu doar fiecare companie în parte de-a lungul lanțului de aprovizionare.

Schimbul de date în cadrul ecosistemului

În cadrul proiectului de cercetare austriac, ResearchLin-X, Universitatea Johannes Kepler din Linz își unește forțele cu companii de renume precum Siemens, Engel, Haidlmair,

Motan și Westcam, precum și cu Universitatea de Tehnologie din Viena.

Această colaborare are loc în fabrica LIT, situată în Linz și are ca scop analiza potențialului de reducere a amprente de carbon prin intermediul schimbului de date în cadrul ecosistemului.

Acest proiect se referă la minimizarea Amprente de Carbon a Produsului în procesul de turnare prin injecție. Acest proces implică utilizarea unei matrițe în care se toarnă materialul. Granulele de material trebuie uscate și preîncălzite corespunzător, iar



Este esențial să avem un schimb de date care depășește granițele companiei dacă dorim să abordăm în mod colectiv provocările semnificative ale erei noastre.

„Companiile care aspiră să se integreze în ecosisteme vor beneficia de un avantaj competitiv”.

Michael Freyny, Head of Siemens Digital Industries Austria, despre suveranitatea datelor în ecosistemele deschise.

sistemele de control ale mașinii de turnare prin injecție asigură eficiența producției. Prin facilitarea schimbului de date între diferitele etape ale procesului și, implicit, între companiile implicate, se poate obține o amprentă de CO₂ mai mică. Acest schimb de date permite o aliniere perfectă, optimizând astfel procesul și reducând impactul asupra mediului. Inițiative precum GAIA-X, AMIDS (Austrian Manufacturing Innovation Data Space) și Manufacturing-X contribuie la facilitarea schimbului de date. Acestea includ stabilirea unor reguli echitabile, cum ar fi contractele pentru schimbul de date, eliminând astfel necesitatea negocierilor.

Singura responsabilitate a companiilor este să aleagă opțiunea adecvată. Modelul de date este, de asemenea, conceput astfel încât destinatarul să poată înțelege datele imediat, fără a necesita un efort considerabil de traducere.

În cadrul proiectului de cercetare menționat anterior, se utilizează un sistem standardizat de administrare a activelor (AAS) pentru a descrie datele într-un mod uniform.

Conceptul „compute-to-data” merge un pas mai departe, unde nu mai sunt schimbate datele, ci doar algoritmul; calculul propriu-zis are loc la fața locului, fără ca datele să părăsească compania.

Deschiderea companiilor către schimbul de date și colaborarea în cadrul ecosistemelor, cu un grad mai mare de valoare, reprezintă o schimbare de paradigmă semnificativă în era noastră.

Doar prin eforturi comune putem depăși marile provocări care ne stau în față.

Companiile mici și mijlocii din Austria au un rol crucial în acest context, având la dispoziție numeroase oportunități în aceste noi ecosisteme. ○

Deși companiile au dorit întotdeauna să aibă control asupra propriilor date, asistăm acum la o schimbare de paradigmă către ecosisteme deschise.

Am lansat platforma digitală Siemens Xcelerator, care permite colaborarea între clienți, Siemens și partenerii certificați, pe lângă o gamă completă de soluții software și hardware capabile să utilizeze IOT.

Rețeaua noastră, care cuprinde de la companii mari de tehnologie până la dezvoltatori de software independenți, facilitează un schimb de date mult mai frecvent între participanți.

Pentru utilizarea datelor în ecosistemele deschise, avem nevoie de reguli verificate și testate, a căror corectitudine a fost testată și confirmată de o entitate independentă.

De ce tocmai acum este schimbul de date din ce în ce mai important?

Provocările majore, cum ar fi schimbările climatice, crizele geopolitice și dificultățile de livrare, au atins un nivel de complexitate care depășește capacitatea unei singure companii de a le gestiona. Problemele se extind dincolo de granițele unei singure companii. Să luăm ca exemplu amprenta de CO₂ a unui produs. Instrumentul nostru de gestionare a emisiilor, SiGreen, colectează date direct de la sursa emisiilor, în principal în producția din amonte. Utilizarea cheilor criptografice și a organismelor independente de certificare garantează un nivel ridicat de protecție a datelor și fiabilitatea informațiilor partajate.

Dar acesta este doar începutul. De exemplu, un producător de mașini



are acum cunoștințele necesare pentru a produce vehiculul său într-un mod care minimizează amprenta de carbon.

Datele relevante ar trebui să fie partajate cu compania sau persoana care utilizează mașina.

Ulterior, datele generate în timpul utilizării produsului ar trebui să revină la producătorul de mașini, astfel încât acesta să își poată îmbunătăți continuu mașinile. Acest proces duce la estomparea granițelor dintre companii și la optimizarea operațiunilor.

Ce le recomandați companiilor în ceea ce privește suveranitatea datelor?

Modul în care sunt utilizate datele și cine le utilizează are o importanță strategică pentru Europa.

Companiile ar trebui să elaboreze o strategie privind modul în care se pot integra în viitoarele ecosisteme. Ar fi riscant pentru ele să rămână izolate. Companiile care se integrează activ în ecosisteme vor avea un avantaj competitiv.

Interviul a fost publicat inițial într-o versiune extinsă în publicația „Starkes Land Österreich”, a editurii Ablinger Garber.



Securitatea cibernetică în viitor? „Avem încă multe de realizat!”

Securitatea cibernetică a reprezentat un punct de interes pentru Siemens încă din anii '80, perioadă în care amenințările și riscurile de securitate au evoluat semnificativ. În acest interviu, **Natalia Oropeza și Andreas Kind** dezvăluie cum, alături de echipele lor, asigură protecția Siemens și a clienților săi împotriva atacurilor cibernetice.

Siemens se mândrește cu o echipă dedicată securității cibernetice, care a acumulat peste trei decenii de experiență. Cum s-au transformat amenințările de-a lungul acestui timp?

Andreas Kind: În anii 1980, calculatoarele nu erau aproape deloc conectate în rețea. Programele malware și virusii informatici erau frecvent distribuiți pe computere prin intermediul dischetelor și altor medii de stocare. Furtul de date se realiza prin sustragerea fizică a acestor medii de stocare din sistemele informatice

sau prin interceptarea informațiilor de către persoane din interior.

În acea perioadă, Ingineria Socială era deja o amenințare majoră: cineva se dădea drept o persoană cunoscută, de exemplu un furnizor extern de servicii, în fața angajaților unei companii și astfel, obținea acces la sistemul informatic. Începând cu anii 1990, computerele au devenit din ce în ce mai conectate în rețea au început să interacționeze prin intermediul protocoalelor de comunicare. Pentru o lungă perioadă de timp, rețelele IT au constituit ținta principală

a atacatorilor și a experților în securitate cibernetică.

Totuși, pe măsură ce crește interconectivitatea, toate formele de sisteme industriale devin vulnerabile. Această sferă industrială este cunoscută sub numele de „Operational Technology, OT” (tehnologie operațională). Printre acestea se numără, de exemplu, mașinile și sistemele de control din fabrici, centralele electrice și trenurile. În prezent, un atac reușit al hackerilor poate duce la oprirea producției, la o pană de curent sau la devierea unui tren.



Andreas Kind deține rolul de responsabil pentru securitatea cibernetică în cadrul Siemens Technology.

Cum se poate garanta securitatea cibernetică în toate aceste domenii? Există mai multe moduri diferite de a ataca?

Natalia Oropeza: Un exemplu: în prezent, ne concentrăm asupra conceptului Zero Trust (încredere zero). Acesta presupune că un sistem IT își verifică în mod constant interlocutorii. În primul rând, sistemul informatic identifică persoana sau dispozitivul care solicită informații. Se verifică apoi starea de sănătate în care se află

„Pe măsură ce crește interconectivitatea, toate tipurile de sisteme industriale devin susceptibile la vulnerabilități”.

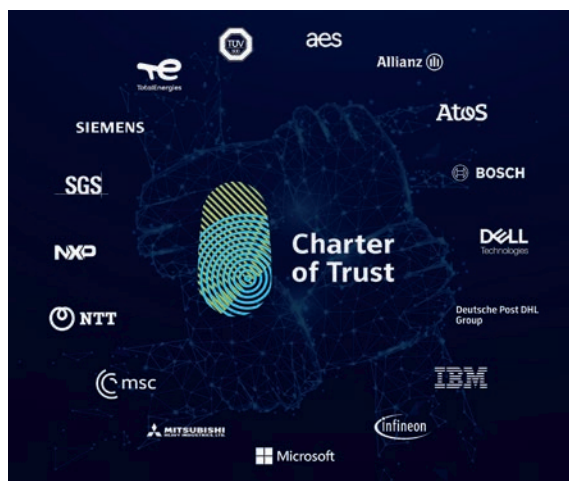
dispozitivul. Este acesta lipsit de viruși sau vulnerabilități? Având în vedere războiul din Ucraina și creșterea criminalității cibernetice, de ceva timp analizăm mai atent regiunile din care oamenii contactează sistemele noastre. Avem posibilitatea de a activa filtre specifice pentru a bloca anumite solicitări. Un alt exemplu este echipa Product-CERT (Computer Emergency Response Team), înființată în 2002, care monitorizează în mod continuu produsele Siemens pentru a identifica eventuale vulnerabilități. Dacă se descoperă vreo vulnerabilitate, echipa furnizează rapid clienților patch-uri, adică actualizări de software care remediază aceste vulnerabilități. Instalațiile industriale, precum centralele electrice, funcționează pe parcursul a numeroase decenii. Prin urmare, una dintre responsabilitățile Product-CERT este să asigure că produsele rămân actualizate în ceea ce privește securitatea pe întreaga durată de viață a acestora.

Și cum ne pregătim pentru viitor? Cum ne asigurăm că nenumăratele instalații din întreaga lume rămân protejate împotriva atacurilor pe parcursul anilor?

Kind: De exemplu, avem propria echipă de cercetare care analizează tehnologiile pentru a anticipa potențialele vulnerabilități viitoare. Privim cu trei până la zece ani în viitor și explorăm noile metode de inteligență artificială, de exemplu, pentru a afla cum le pot folosi atacatorii pentru a provoca daune sau pentru a descoperi vulnerabilități în noile tehnologii de inteligență artificială care ar putea fi vizate de hackerilor.

Poate Siemens să asigure în mod autonom securitatea cibernetică absolută?

Oropeza: Ar fi o iluzie să presupunem acest lucru. Reușita protecției cibernetice se datorează, printre altele, colaborării cu furnizorii și cu alte companii. Prin urmare, în 2018,



Siemens și-a unit forțele cu alte mari companii de tehnologie pentru a forma Carta încrederii, o inițiativă globală care lucrează la standarde comune de securitate, inclusiv de-a lungul lanțurilor lor de aprovizionare. În plus, există standarde industriale globale obligatorii pentru OT, cum ar fi standardul IEC 62443, care stabilește cum se poate realiza OT în condiții de siguranță.

Este bine cunoscut faptul că infractorii cibernetici descoperă constant noi modalități de atac. Care sunt provocările specifice pe care le anticipați pentru viitor?

Kind: Un subiect important este noua eră a computerelor cuantice. Siemens lucrează de ceva timp la proiecte în acest domeniu pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor și a sistemelor în viitor. Ne concentrăm pe testarea noilor procese criptografice sigure din punct de vedere cuantic pentru

aplicabilitatea în mediile industriale și pe dezvoltarea strategiilor de migrare.

Oropeza: O altă întrebare importantă pentru viitor este cum putem proteja industria în contextul incertitudinii politice crescânde - de exemplu, în situații precum conflictul din Ucraina, care este însoțit de atacuri cibernetice. Un alt aspect de luat în considerare sunt noile obstacole comerciale care ar putea apărea în viitor datorită standardelor de securitate cibernetică diferite din anumite țări.

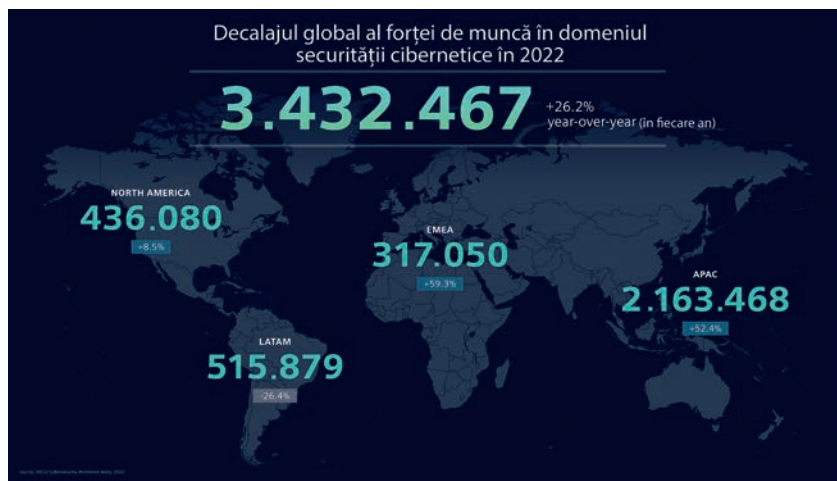
În plus, un aspect care nu trebuie neglijat atunci când ne gândim la viitor este deficitul de specialiști în securitate cibernetică. Conform unui studiu realizat de International Information System Security Certification Consortium, în prezent există un deficit de aproximativ 3,5 milioane de experți în securitate cibernetică la nivel mondial - iar tendința este în creștere. Cu alte cuvinte, amenințările se dezvoltă mult mai rapid decât formarea de noi specialiști calificați.

Pentru a combate acest deficit, Siemens a luat inițiativa de a înființa Academia Cyberminds în 2022. Aici, participanții sunt pregătiți ca experți în securitate pe parcursul unui an - nu doar tinerii, ci și persoanele mai în vârstă care doresc să își reorienteze cariera. Academia se străduiește să asigure o diversitate cât mai mare a participanților, incluzând femei, bărbați și persoane din diverse țări, din medii diferite și cu perspective variate, luând în considerare și faptul că amenințările cibernetice sunt extrem de diverse. Doar prin astfel de abordări putem continua să gestionăm, în măsura posibilului, riscurile crescânde ale lumii digitale. Cu toate acestea, mai avem mult de lucru.



Natalia Oropeza deține funcția de Chief Cybersecurity Officer la Siemens AG, având astfel responsabilitatea globală pentru securitatea cibernetică a companiei. Cu o experiență de aproximativ 30 de ani în tehnologia informației, a avut oportunitatea de a lucra în Mexic, SUA și Germania.

„Ceea ce nu trebuie să uităm atunci când privim spre viitor este deficitul de specialiști în securitate cibernetică”.



3,5 Milioane de experți în securitate cibernetică: lipsesc din forța de muncă necesară în întreaga lume - iar tendința este în creștere

În această secțiune, echipa editorială le transmite cititorilor câteva idei de final de revistă. Vă prezentăm o serie de reportaje de ultimă oră și alte informații relevante.



Accelerarea electrificării

Tranziția energetică implică o eliminare graduală sau o înlocuire progresivă a tuturor formelor de consum alimentate de combustibili fosili cu alternative sustenabile.

Electrificarea pare a fi în prezent una dintre cele mai viabile modalități de a realiza acest obiectiv.

Acest „Whitepaper” analizează modul în care clădirile, industria și mobilitatea pot fi decarbonizate și, în același timp, cum poate fi consolidată rețeaua electrică. Materialul analizează modul în care electrificarea „tuturor lucrurilor” va afecta cererea viitoare de energie electrică, în contextul creșterii producției de energie din surse regenerabile. De asemenea, se acordă o atenție deosebită pregătirii infrastructurii de rețea pentru viitor.



File de somon vegan imprimat 3D

De la 1 octombrie 2023, inovația „The Filet - Inspired by Salmon” - un filet de somon vegan imprimat 3D - conceput de start-up-ul vienez Revo Foods, este disponibilă în toată Europa. Necesitatea de a găsi alternative sustenabile la pește este mai urgentă ca niciodată.

Având în vedere că până la 60 % din stocurile de pește din lume sunt deja considerate supra-exploatate și că oceanele sunt afectate de o poluare semnificativă cu plastic, ecosistemele marine sunt amenințate în mod alarmant.

Fileul de somon pe bază de ciuperci filamentose micoproteice cu calitatea nutritivă „A” de la Revo Foods oferă o soluție



promițătoare la această criză ecologică.

Acesta nu numai că răspunde cererii tot mai mari de alternative sustenabile, dar oferă și o aromă autentică, care se adresează pieței flexitariene pretențioase. Revo Foods deține două brevete pentru o nouă tehnologie de imprimare 3D continuă a proteinelor.



IA în lumea industrială

Inteligența artificială (IA) nu este un obiectiv în sine, ci modul în care este aplicată face diferența pentru companii, societate și mediu. În ciuda tuturor progreselor deja realizate, IA are nevoie de oameni.

Provocările cu care ne confruntăm în domeniul vehiculelor autonome sunt similare cu cele din procesele industriale controlate de IA. Companiile care adoptă o strategie bazată pe parteneriate vor fi lideri în ceea ce privește potențialul de productivitate al inteligenței artificiale industriale.

Acest Podcast discută despre importanța inteligenței artificiale și a învățării automate în contextul industrial al zilei de astăzi.



Proprietar media și editor:

Siemens România

Strada Preciziei nr. 24

062204 București, România

Tel: +40 21 6296 400

Email: siemens.ro@siemens.com

siemens.ro

Tipărit în România de Still Print Forward SRL

Fotografii: Siemens, dacă nu este specificat altceva.

Informațiile din această revistă conțin doar descrieri generale, respectiv caracteristici de funcționare care nu se înregistrează întotdeauna în forma descrisă în cazurile concrete și care se pot modifica datorită dezvoltării în continuare a produselor.

Toate denumirile de produse pot fi mărci sau nume de produse ale Siemens AG sau ale altor companii furnizoare, iar utilizarea de către terți în scopuri proprii poate leza drepturile titularilor.

