Bob Iger se vrača na čelo Disneyja

PROFIL 15

Pri varjenju je robotizacija velika prednost

AVTOMATIZACIJA 11

Padci obveznic že dolgo niso bili tako globoki

BORZNA ANALIZA 15

Popolnoma avtomatizirana kibernetska varnost morda ne bo uporabna

Podjetja *Kibernetska varnost mora pri vsakem izdelku in vsaki rešitvi nastopati skozi celoten življenjski cikel*

»Pri razvoju varnostnih mehanizmov izvajamo lastne hekerske teste, v poznejših fazah pa sodelujemo s tretjimi osebami, ki potrdijo učinkovitost naših rešitev,« pojasnjuje Stefan Woronka. FOTO SIEMENS

V dobi interneta stvari, pametnih tovarn in digitalnih preobrazb je velik izziv proizvodnih podjetij kibernetska varnost. Stefan Woronka, direktor poslovnega razvoja industrijskih varnostnih storitev v družbi Siemens, je z nami delil svoje poglede na varovanje industrijskih okolij in zagotavljanje digitalne obrambe.

MIRAN VARGA

- Podjetje je lahko napadeno zaradi naključnega dejanja, ne pa, ker bi bilo v fokusu napadalcev.
- Ni univerzalnega odgovora oziroma rešitve, ki bi bila takoj primerna za vsako tovarno.
- Mnoga podjetja nimajo rednega posodabljanja opreme, kar zvišuje tveganja.

Digitalna revolucija v poslovanju ni brez nevarnosti. Kibernetska varnost skrbi vsa podjetja, ki vstopajo in delujejo v digitalnem svetu. Kako Siemens naslavlja to področje?

Siemens se kibernetske varnosti loteva celostno. To pomeni, da je ta pri vsakem izdelku in vsaki rešitvi upoštevana skozi celoten življenjski cikel – od začetka razvoja izdelka prek načrtovanja, proizvodnje do namestitve pri končnem kupcu, dokler po letih delovanja izdelka ne umaknemo iz uporabe. Pri tem upoštevamo tudi samo operativno infrastrukturo, kot je okolje IT. Poleg vključitve kibernetske varnosti v vsak izdelek in rešitev Siemens ponuja tudi storitve in podporo, ki stranke usmerjajo na njihovi digitalni poti, in sicer z zagotavljanjem preglednosti trenutnega stanja kibernetske varnosti v tovarni, izvajanjem preizkušenih in potrjenih rešitev kibernetske varnosti ter s stalno podporo med obratovanjem.

Kakšne varnostne strokovnjake zaposluje Siemens?

Ker kibernetsko varnost upoštevamo vedno in povsod, se vrsta potrebnega strokovnega znanja spreminja v vsaki fazi izdelka. Pri načrtovanju in projektiranju izdelka prevladujejo druge zahteve v primerjavi z namestitvijo in zagonom. Zato mora biti kibernetska varnost v glavi vsakega zaposlenega. Poleg tega Siemens zaposluje posebne strokovnjake za kibernetsko varnost, ki vsako organizacijo usmerjajo in podpirajo pri vsakodnevnih nalogah in skrbi za obvladovanje kibernetske varnosti.

Kako težko oziroma zahtevno je danes zaustaviti hekerje? S stališča laikov ti lahko naredijo ali dosežejo skoraj vse, kar si zadajo – napadejo vsako tarčo ...

Če si ogledamo vodilni standard za kibernetsko varnost v industrijski avtomatizaciji in krmiljenju – IEC 62443 –, ugotovimo, da ta opredeljuje različne stopnje varnosti glede na domnevno grožnjo. Najnižja raven pomeni ne prav dodelanih načinov napadov. Najvišja raven pa obravnava zelo dovršene, skrajno premišljene vrste napadov. Glede na to klasifikacijo zaznavamo, da prihaja do različnih vrst hekerskih napadov. V zadnjem obdobju so najpogostejši neciljani napadi, na primer uporaba izsiljevalske programske opreme. To pa pomeni, da je podjetje lahko napadeno zaradi naključnega dejanja, ne pa zato, ker bi bilo v fokusu napadalcev. Siemens za izboljšanje svojih izdelkov in rešitev uporablja več načinov za povečanje ravni varnosti. Najprej v okviru razvoja izvajamo lastne »hekerske« teste. V poznejših fazah sodelujemo s tretjimi osebami, ki potrdijo učinkovitost naših varnostnih mehanizmov in rešitev. To je razvidno iz različnih certifikatov, ki jih ima Siemens za svoje postopke in izdelke. Ne nazadnje pa tesno sodelujemo z varnostno skupnostjo in raziskovalci, ki preizkušajo naše izdelke in iščejo morebitne ranljivosti. Ko raziskovalci odkrijejo ranljivosti v naših izdelkih, Siemens to vzame resno ter na podlagi temeljite analize odpravi ranljivosti in izda varnostna priporočila ter popravke.

Kako se lahko podjetja, zlasti tovarne ali proizvodni obrati, kjer kibernetska varnost v preteklosti ni bila ravno pomembna tema, ustrezno zaščitijo?

Univerzalnega odgovora oziroma rešitve, ki bi bila takoj primerna za prav vsako tovarno, ni. Stranke do zanje najprimernejše obrambe pred digitalnimi napadalci in nevarnostmi usmerjamo s pomočjo pristopa v petih korakih. Podjetje lahko začne s katerim koli od teh korakov ali pa kakšnega tudi preskoči, če se mu ne zdi potreben. Teh pet korakov je: (1) Vedite, kaj imate! (2) Vedite, kako delate! (3) Vedite, kaj narediti! (4) Vedite, kako narediti! (5) Vedite, kako se izboljšati!

Prvi korak pomeni, da je izredno pomembno podrobno poznati linije, stroje, komponente (skratka sredstva), ki so nameščene v tovarni. To zahteva poznavanje ravni vdelane programske opreme, programske opreme in stanja nameščenih popravkov. V drugem koraku ocenjujemo organizacijsko zrelost. Kako dobro je organizacija pripravljena na izzive kibernetske varnosti – ali se zna nanje ustrezno odzvati.

Na podlagi rezultatov prvega in drugega koraka lahko Siemens v tretjem koraku pomaga načrtovati pot stranke do kibernetske varnosti tako, da predlaga, katere ukrepe je mogoče izvesti, in poda oceno stroškov ter koristi. To temelji na sredstvih iz prvega koraka, za katera lahko natančno poznamo »status zastarelosti« in morebitne ranljivosti, ki vplivajo na ta sredstva. Četrti korak zajema izvajanje ukrepov in usposabljanje organizacije za dvig ravni ozaveščenosti. V okviru petega koraka strankam pomagamo pri nemotenem delovanju njihove tovarne z vidika kibernetske varnosti, tako da zagotavljamo in implementiramo popravke ter smo pozorni na morebitne nove ranljivosti.

Stranke do zanje najprimernejše obrambe pred digitalnimi napadalci in nevarnostmi usmerjamo s pomočjo pristopa v petih korakih.

Večina varnostnih strokovnjakov trdi, da okolja OT na področju varnosti za okolji IT zaostajajo od pet do deset let. Se strinjate? Zakaj je tako?

Proizvodnja se osredotoča na proizvodnjo izdelkov. To pomeni, da je poudarek na ohranjanju stabilne proizvodnje v tovarni. Tovarne stremijo k čim boljšemu izkoristku naložbe oziroma opreme. Spremembe te mantre so v preteklosti pomenile potencialno tveganje izpada proizvodnje. Glede na to se mnoga podjetja niso odločala za redno posodabljanje ali modernizacijo proizvodne opreme. V nekaterih panogah proizvodno opremo uporabljajo, vse dokler izdelka ne proizvajajo več, to pa lahko traja tudi 15, 20 ali več let. Zato je treba pri uvajanju novih rešitev kibernetske varnosti v tovarni upoštevati, ali te dejansko delujejo s starejšo opremo. V praksi v tovarnah še vedno srečamo operacijski sistem windows XP, za katerega je njegov proizvajalec ukinil podporo že aprila leta 2014. Torej omenjena opazka žal drži.

Kako bi vi zaščitili okolje OT, kje bi začeli?

Začel bi s prej opisanimi koraki. Koraki od 1 do 3 bi mi pomagali ustvariti preglednost v tovarni stranke, saj bi identificirali nameščena sredstva in njihovo stanje (zastarelost, ranljivosti). Prav tako bi mi dali bolj jasno sliko, kako dobro organizacija, ki vodi proizvodnjo, skrbi za kibernetsko varnost. Na podlagi tega bi lahko podal jasne smernice o naslednjih možnih ukrepih. Ti bi seveda bili v skladu s standardom IEC 62443 in lokalnimi predpisi ter odražali tudi zavedanje podjetja glede tveganj, ki jim je izpostavljeno. To pomeni, da ima lahko podjetje v neregulirani panogi (na primer proizvodnja zamaškov) v primerjavi s podjetjem v regulirani panogi (recimo proizvodnja električne energije ali finančne institucije) višjo stopnjo sprejemljivosti tveganja in s tem drugačne varnostne ukrepe.

Varovanje tovarne ali pisarne ne pomeni le namestitve nekaj škatel in uvedbe par postopkov preverjanja. Izobraziti je treba tudi zaposlene, saj so ljudje najpogosteje najpomembnejši del varnostne enačbe. Kako lahko podjetja vzpostavijo varnostno kulturo?

Človek pogosto velja za najšibkejši člen v celotni verigi kibernetske varnosti, vendar številna podjetja kljub temu pozabljajo na usposabljanje svojih zaposlenih. Vsaj tista na ravni ozaveščenosti je treba izvajati redno. To rad primerjam z obveznimi usposabljanji za varnost pri delu. Ta so prav tako obvezna in pomagajo preprečevati nesreče pri delu. Enako velja za kibernetsko varnost.

Ali je kibernetsko varnost mogoče avtomatizirati?

Veliko naših rešitev, ki jih nameščamo, že vsebuje tehnologijo strojnega učenja ali celo umetno inteligenco. To pomaga pri izkoriščanju ogromne količine podatkov, ki prihajajo iz tovarne. Še vedno pa so po analizi podatkov in generiranju informacij potrebni ljudje, ki informacije umestijo v kontekst – se prepričajo, da so morebitne ugotovitve relevantne, in nato ustrezno ukrepajo.

Popolnoma avtomatizirana kibernetska varnost morda ni oziroma ne bo uporabna, saj lahko pripelje do tega, da se v primeru kibernetskega napada sistemi samodejno izklopijo. Samo pomislite, kaj bi to pomenilo pri sistemih, ki skrbijo za s človekovo varnostjo povezana področja. Te moramo ohraniti delujoče, da bi tako zagotovili, da lahko proizvodnjo spravimo v varen način delovanja.

Eden vaših sloganov je tudi »zaščiteno v vseh pogledih«. Kaj z njim sporočate strankam?

Za Siemens »zaščiteno v vseh pogledih« pomeni optimalno združitev robustnega področnega znanja in specifičnega industrijskega znanja s poglobljenim razumevanjem kibernetske varnosti. Izhajamo iz izkušenj v lastnih proizvodnih obratih, to znanje prenašamo na stranke ter ga vključujemo v naše izdelke in storitve, da izpolnimo našo obljubo: če je kibernetska varnost vaš cilj, vam ga pomagamo doseči.

Smernice za uporabo umetne inteligence

Usmerjanje *Pod okriljem Digitalnega inovacijskega stičišča (DIH) Slovenije nastajajo pravila za uporabo UI*

Čeprav umetno inteligenco že uporabljamo domala vsak dan, tehnologija umetne inteligence še vedno vzbuja nezaupanje. Zadržkov pri uporabi umetne inteligence v delovnih procesih se ne morejo otresti niti podjetja. To je bil povod za nastanek smernic za uporabo umetne inteligence v Sloveniji, ki podjetjem lajšajo njeno vpeljavo in uporabo. Nastale so pod okriljem Digitalnega inovacijskega stičišča (DIH) Slovenije.

- Umetno inteligenco v praksi že uporabljamo, pogosto nezavedno.
- Primer je aplikacija GoogleMaps, ki si zapomni naše potovalne navade.
- Podjetja skrbijo vprašanja nadzora, etike, zasebnosti in transparentnosti.

Varna in učinkovita raba UI

V sklopu dogodkov AI Governance, ki jih je DIH Slovenije v sodelovanju z Institutom Jožef Stefan in službo vlade za digitalno preobrazbo organiziral med predsedovanjem Slovenije Svetu EU, so predstavniki različnih fakultet v sodelovanju s podjetji analizirali področje UI z različnih vidikov njene uporabe. Ukvarjali so se s temami industrije 4.0, medijev in analize tekstovnih dokumentov, pametnih skupnosti, slike, videa in zvoka.

Na zaključnem dogodku so se osredotočili na razvoj UI skozi oči mladih, bodočih strokovnjakov, ki imajo do tehnologije manj predsodkov, saj z njo odraščajo. Študenti s šestih fakultet so svojo pozornost namenili predvsem regulaciji zbiranja podatkov, njihovi hrambi in nadaljnji uporabi, odgovornosti ustvarjalcev in nediskriminatornosti UI ter vzpostavitvi pravnih okvirov razvoja UI za varno in učinkovito rabo.

V razpravo so bili vključeni mladi strokovnjaki z različnih področij. FOTO DIH

Svež pogled mladih

V prvem delu dogodkov so soočili razvijalce rešitev, uporabnike, pravni in regulatorni vidik s področij, kjer je UI najbolj prisotna, je poudarila Katja Mohar Bastar, direktorica DIH Slovenije. Na zaključni dogodek so povabili študente pravne, elektro, računalniške in drugih smeri, ki so »dodali vidike generacije, ki vstopa v poslovni svet in je že od svojih začetkov vključena v sisteme, ki UI uporabljajo. Študentke in študenti so se aktivno vključili v pogovore o vidikih končnih uporabnikov, razvoju in regulaciji, mi pa smo pridobili svež pogled na problematiko.«

Z vsemi njihovimi idejami, pravi Mohar Bastarjeva, bodo zaključili smernice zaupanja vredne UI. Te bodo lahko podlaga vsem segmentom uporabnikov, da bodo delovali skladno z dogovori in skrbeli, da bo UI v slovenskem okolju uporabljena na dogovorjene načine, s katerimi se strinjajo vsi deležniki.

Samo Zorc s službe vlade za digitalno preobrazbo je mladim osvetlil razvoj evropske, na človeka osredotočene umetne inteligence. »Evropa si želi postati vodilna regija v svetovnem merilu pri razvoju in uporabi vrhunske, etične in varne umetne inteligence ter spodbujanju na človeka osredotočenega pristopa v globalnem kontekstu. 'Umetna inteligenca, izdelana v Evropi', ki izpolnjuje pričakovanja državljanov, se odziva na družbene potrebe ter spodbuja konkurenčnost,« je povedal Zorc. **P. D.**

Tehnologija

Avtobus na vodik opozarja na zeleni prehod

Minuli teden je promocijsko turo skozi Slovenijo opravil avtobus na vodik – začel je v Tolminu, nadaljeval v Novi Gorici ter skozi Šoštanj in Velenje zaključil v Celju. **Predstavitev avtobusa je bila del evropskega projekta JIVE 2 CEE Hydrogen Bus Roadshow**. V času turneje so v Tolminu, Kanalu, Desklah in Šoštanju potekale delavnice izobraževalnega programa H2STUDENT. V Termoelektrarni Šoštanj se je avtobus ustavil tudi zato, ker tam skupina HSE načrtuje postavitev večjih proizvodnih kapacitet vodika, podprtih z novimi lokalnimi sončnimi elektrarnami.

Obrt in podjetništvo

Znani so nominiranci za nagrade

Obrtno-podjetniška zbornica Slovenije (OZS) bo 8. decembra na Brdu pri Kranju podelila **prestižni priznanji obrtnik leta 2022 in podjetnik leta 2022, ki ju podeljujejo posamezniku, ki predstavljajo vzor odličnosti in kakovosti poslovanja**. Nominiranci za podjetnika leta 2022 so Ivan Cajzek, GIC Gradnje Rogaška Slatina, Marko Femc, Plan-net Solar Preserje, Miha Lavtar, Optiweb Škofja Loka, in Alojz Selišnik, Melu Luče ob Savinji. Nominiranci za obrtnika leta 2022 so Leon Kranjc, Klin Logatec, samostojni podjetnik Vinko Petkovšek z Iga in Andrej Rožmanc, Levček Logatec.

Odgovorno v kmetijstvu

Panvita je pristopila h kodeksu ravnanja v EU

Skupina Panvita je kot prvo podjetje v Sloveniji podpisala zaveze, ki jih opredeljuje kodeks Evropske unije o odgovorni živilski dejavnosti in trženjskih praksah, sprejet julija lani. **Zavezala se je, da bo do leta 2030 v procesu proizvodnje hrane znižala emisije toplogrednih plinov za 40 odstotkov**, povečala nabavo trajnostno pridelanih surovin na vsaj 90 odstotkov, pakirala vsaj 75 odstotkov izdelkov v reciklirano embalažo, znižala porabo vode za 20 odstotkov v primerjavi z letom 2020, izboljšala sestavo živil v smeri zdrave in trajnostne prehrane ter poskrbela, da bodo njihove živali v celotni verigi rejene skladno s standardi dobrobiti živali.

Paramount

Prodaje založbe Simon & Schuster (še) ne bo

Paramount, ameriška multinacionalka s področja zabavne in medijske dejavnosti, svoje založniške hiše Simon & Schuster ne bo prodal konkurentu Pengu-in Random Housu, saj je pristojno ameriško sodišče že pred tremi tedni prodajo blokiralo. **Konkurenca na ameriškem založniškem trgu, kjer je trenutno pet velikih igralcev, se tako za zdaj ne bo dodatno krčila. D. VI.**

Snopič ureja

Damjan Viršek

pd@delo.si