Kibernetska varnost v industriji

Simon Vrbnjak
LAPP Slovenija
Družba 5.0, Kibernetska varnost, Zagotavljanje varnosti omrežja z uporabo ETHERLINE® ACCESS NF04T NAT/Firewall stikala, Industrijski internet stvari – IIoT, ETHERLINE GUARD
Simon.vrbnjak@lapp.com

Cybersecurity in industry

Cybersecurity in industrial networks is one of the highest priorities. The downtime of production plant can be expensive and regarding the GDPR the data is getting more sensitive than ever. Hackers are no longer satisfied with just encrypting your data. Today they want to stop the production or at least one part of it. Costs of downtime can go to the roof as well as ownership of network infrastructure. We must start thinking decentralized and analytical when it comes to network traffic.

Kibernetska varnost v industriji

Kibernetska varnost za industrijske mreže ima danes najvišjo prioriteto. Stroški ustavitve obratovanja so lahko zelo visoki, prav tako moramo poskrbeti za zaščito občutljivih osebnih podatkov. Hekerji niso več zadovoljni samo s kriptiranjem podatkov na serverjih. Danes nam ustavljajo proizvodnjo ali vsaj del proizvodnje. Stroški ustavitve so lahko visoki, prav tako pa postaja lastništva mreže vedno bolj draga. Zato moramo pri prometu na mreži začeti razmišljati decentralizirano in analitično.

1 Družba 5.0

Družbo, ki je osredotočena na človeka, je v ravnovesju z gospodarskim napredkom in skrbi za reševanje družbenih problemov s sistemom, ki močno povezuje kibernetski in realni fizični prostor imenujemo Družba 5.0.

V družbi 5.0 se ustvarjajo nove vrednote. Pri analizah enormnih količin podatkov v industriji vse bolj prihaja v ospredje umetna inteligenca (v nadaljevanju UI), ki bo sposobna te podatke obdelovati:

- načrtovala bo fleksibilno proizvodnjo, ki se bo odzivala na potrebe na trgu. Povezovala se bo z potrošniki, dobavitelji, proizvodnimi cikli, inventarjem, itd., skratka z vsem kar potrebujemo, da uresničimo zahtevek od kupca do končnega izdelka z minimalnimi stroški vseh procesov v verigi;
- z uporabo UI, robotov in usklajevanj med obrati bomo postali bolj učinkoviti, porabili bomo manj delovne sile in implementirali več tehničnih veščin, ki smo jih osvojili v preteklosti. S tem bomo dosegli visoko raznoliko proizvodnjo v malih serijah;
- distribucija bo postala bolj učinkovita, saj bodo industrije navzkrižno sodelovale pri dostavah, najemu tovornjakov, itd.;
- potrošnikom bomo zagotavljali blago po najnižjih možnih cenah, brez zamud in v skladu s potrebami.

S tem bomo pomembno izboljšali industrijsko konkurenčnost, povečali odzivnost na nesreče, ublažili problem pomanjkanja delovne sile, obravnavali raznolike potrebe, zmanjšali emisije in stroške.

Družba 5.0 dosega veliko stopnjo konvergence med kibernetskim (virtualnim) in fizičnim svetom. V pretekli družbi 4.0 so ljudje s pomočjo interneta dostopali do storitev v oblaku, iskali podatke in jih analizirali. V družbi 5.0 pa se v virtualnem svetu s pomočjo senzorjev oz. raznih interceptorjev generira ogromno podatkov. Te podatke nato UI analizira in rezultate v različnih oblikah posreduje človeku v realnem svetu.

2 Kibernetska varnost

Podatki postajajo iz dneva v dan dražji. V kolikor pa jih analiziramo s pomočjo UI, pa je ta vrednost še večja. Lahko bi rekli, da so danes podatki vredni več kot katera koli materija ali valuta na svetu.

Leta 2021 so bili hekerji v polnem zagonu. Izvedli so nekaj spektakularnih napadov, med drugim na kritične infrastrukture, kot so naftovodi in vodovodi. Tudi industrija je skoraj vsak dan izpostavljena napadom.

Profesor Axel Zimmermann iz Univerze uporabnih znanosti v nemškem Aalnu navaja, da se število incidentov vsako leto poveča za več kot 30 odstotkov. Medtem ko je bila še pred kratkim zlonamerna programska oprema, znana kot virusi, med hekerji še posebej priljubljena, je danes v ospredju t. i. metoda »phishing«, pri kateri kriminalci šifrirajo vse podatke svojih žrtev in nato zahtevajo odkupnino za dešifriranje. Verjetnost uspeha je visoka, saj podjetja le redko razkrijejo dejstvo, da so bila prizadeta. Po Zimmermannovih besedah je kibernetski kriminal prizadel že 61 odstotkov malih in srednje velikih podjetij v Nemčiji, strokovnjaki pa se strinjajo, da bo prej ali slej prizadel tudi preostala podjetja.

Lahko bi rekli, da smo se do danes ukvarjali predvsem s kibernetsko varnostjo na področju informacijskih tehnologij (v nadaljevanju IT), nihče pa ni razmišljal, kaj bi se zgodilo, če bi se nekdo odločil nagajati tudi v operativnih tehnologijah (v nadaljevanju OT). Rešitev se torej skriva v celovitih konceptih kibernetske varnosti.

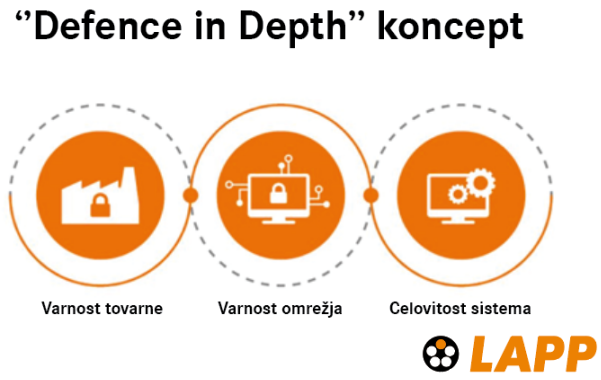
Večina industrijskih podjetij si tega ne more privoščiti, zato se zanašajo na zunanjo pomoč. Njihova prva kontaktna točka so običajno IT strokovnjaki, ki so jim podjetja primorana slepo

zaupati. Žal pa IT strokovnjaki nimajo dovolj znanja na področju OT, kjer ima prednost stroka v proizvodnji. Pri industrijski varnosti, znani tudi kot OT varnost, je namreč v ospredju razpoložljivost, saj lahko pri strojih in proizvodnih objektih že 300-milisekundna okvara predstavlja usodno težavo. Zato je izrednega pomena skoraj 100-odstotna razpoložljivost 24 ur na dan, 7 dni v tednu.

Mnoge izmed teh vidikov zajema standard IEC 62443. To je celovit in mednarodno sprejet standard za industrijsko varnost, ki podrobno opisuje razpoložljivost sistemov. Poleg splošnega dela obravnava tudi procese, sistem in posamezne komponente. Na tem standardu temelji tudi "defence-in-depth'' koncept. Gre za večplastni varnostni koncept, sestavljen iz treh delov: **varnosti sistema, varnosti omrežja** in **celovitosti sistema**.

2.1 ''Defence in depth'' koncept

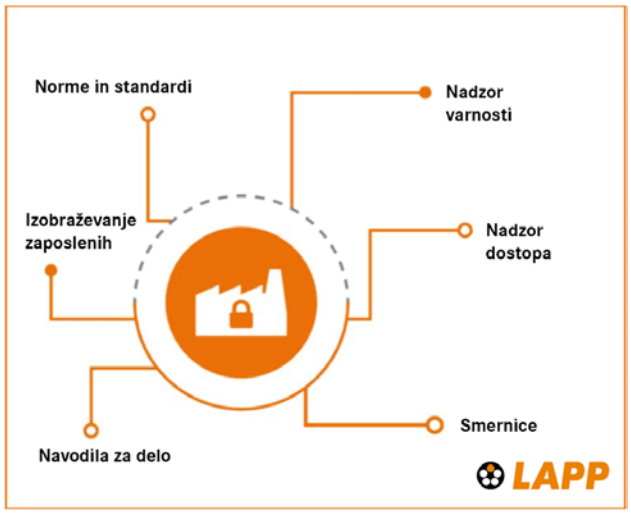
V nadaljevanju so predstavljeni trije deli koncepta "defence in depth": **Varnost tovarne, varnost omrežja** in **Celovitost sistema.**



Slika 1: "Defence in depth" koncept [1]

2.1.1 Varnost tovarne

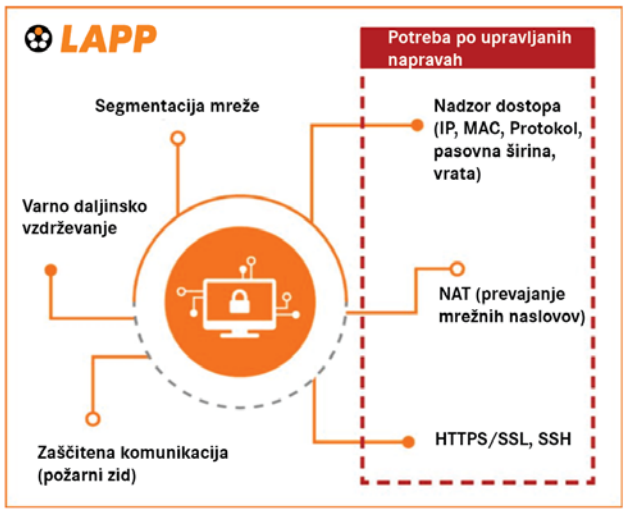
Predvsem zaklenemo sisteme, recimo uporabimo nadzorne omare, kjer ne more vsak dostopati do omrežja. To vključuje seznanjanje zaposlenih z delovnimi navodili in smernicami na ustreznih usposabljanjih.



Slika 2: Varnost tovarne v odvisnosti s podpornimi segmenti [1]

2.1.2 Varnost omrežja

Strategija je lahko segmentacija mreže, na primer z NAT (več v točki 2.2.1 ETHERLINE® ACCESS NF04T NAT/Firewall) ali VLAN napravami. Predlagamo uporabo IP in MAC filtrov, deaktivacijo neuporabljenih vrat (portov) za omejitev dostopnosti do mreže preko prostih vrat. Za varno komunikacijo z zunanjim svetom je obvezna tudi uporaba požarnega zidu. Obstajajo pametne rešitve, ki ločujejo posamezne stroje ali majhne proizvodne enote od preostalega omrežja podjetja. Uporabljati je treba varne protokole, na primer pri dostopu do spletnih mest.



Slika 3: Varnost omrežja [1]

2.1.3 Celovitost sistema

To se nanaša predvsem na utrjevanje sistema. Poznamo vsa privzeta gesla, kot je 0000, ki jih proizvajalec naprave posreduje ob dobavi komponent. Ta gesla je treba takoj zamenjati z varnimi gesli. Na ta način je hekerjem čim bolj otežen napad na omrežje. Druge možnosti so tako imenovani beli seznami in zaščite pred virusi. Beli seznam se uporablja, kadar podjetje ve, katere komponente lahko komunicirajo med seboj, vsaj na proizvodni ravni. Nasprotno pa se IT v glavnem zanaša na črno listo, saj ni mogoče vedeti, kdo želi dostopati do vašega spletnega mesta, kar pomeni, da obstajajo posebej prepovedana območja. Preverjanje pristnosti vključuje razvrščanje uporabnikov in upravljanje gesel (npr. RADIUS ali TACACS+).

Če upoštevate ta priporočila, v proizvodnem omrežju skoraj ni mogoče zaobiti upravljanih naprav. Podjetje LAPP ponuja obsežen nabor stikal za omrežno povezovanje v tovarnah, ki so opremljena z najvišjimi varnostnimi standardi, zaradi česar so hekerski napadi zelo oteženi. LAPP se zaveda drastičnih posledic izpadov strojev in tovarn. Kot ponudnik zanesljivih rešitev za povezave, se podjetje zavzema za reševanje tega vprašanja in zaščito svojih strank pred izpadi.

2.1.4 Zagotavljanje varnosti omrežja z uporabo ETHERLINE® ACCESS NF04T NAT/Firewall stikala

NAT usmerjevalnik ima 4, 8 ali 16 RJ45 vrat. Prva od teh vrat so WAN vrata za mreže višjega nivoja, sledijo LAN vrata za mreže na nivoju strojev. Naloga NAT stikala je preprečiti neavtoriziran dostop do strojne mreže. Zahvaljujoč individualni konfiguraciji se požarni zid enostavno prilagodi zahtevam strojne mreže. Če želimo realizirati enak IP naslovni razpon, ga lahko uporabimo tudi kot most.

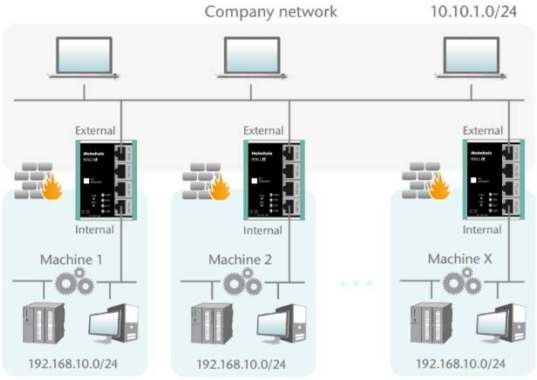
Slika 4: ETHERLINE® ACCESS NF04T NAT/Firewall stikalo [1]

Tudi ta je v izredno majhnem kompaktnem ohišju. Uporabi se ga lahko v treh možnih načinih delovanja:

- **Osnovni NAT**: stikalo uporablja NAT (NAT – Network Address Translation) operacije za podatkovni promet med raznimi IPv4 mrežami (OSI model – plast 3).

  Omogoča prevajanje naslova preko NAT in uporablja paketne filtre za omejitev dostopa do avtomatiziranega omrežja, ki se nahaja zadaj. Osnovni NAT, znan tudi kot "1:1 NAT" ali "Static NAT", je prevod posameznih naslovov IP, ali celotnih obsegov naslovov. Prevajanje poteka izključno na ravni IP, kar pomeni, da je vsa vrata mogoče nasloviti brez izrecnega posredovanja.

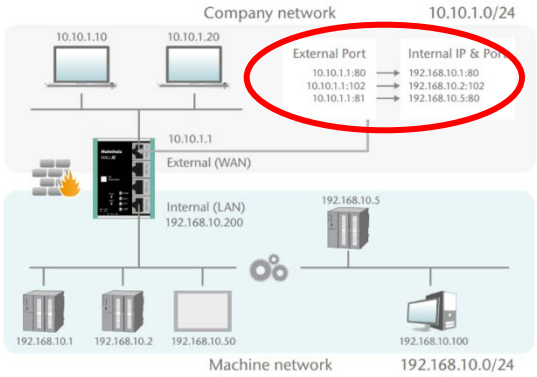
  Če posplošimo, stikalo NAT s 4 vrati uporablja NAT za dodeljevanje unikatnega IP naslova in treh naslovnih območij zunanjega omrežja WAN za vsak IP naslov v internem omrežju LAN. Tako lahko povežemo veliko strojev in računalnikov s proizvodno mrežo in obdržimo unikaten IP naslov iz zunanjega omrežja.



Slika 5: Osnovni NAT [2]

- **NAPT**: Prevajanje mrežnih naslovov in vrat NAPT (Network Address and Port Translation), znanih tudi kot "1:N NAT" ali "Masquerading – maskiranje", se uporablja takrat, ko želimo prevesti vse naslove v celici avtomatizacije v en naslov proizvodne mreže. Tako se naslovi pošiljateljev paketov in celice avtomatizacije zamenjajo z naslovom proizvodne mreže.

  Če še vključimo funkcijo posredovanja vrat (port forwarding) pa lahko nastavimo, da se paketi na določenih vratih TCP/UDP tega naslova posredujejo udeležencu v celici avtomatizacije (npr. 10.10.1.1:81 do 192.168.10.5:80 – slika 6).

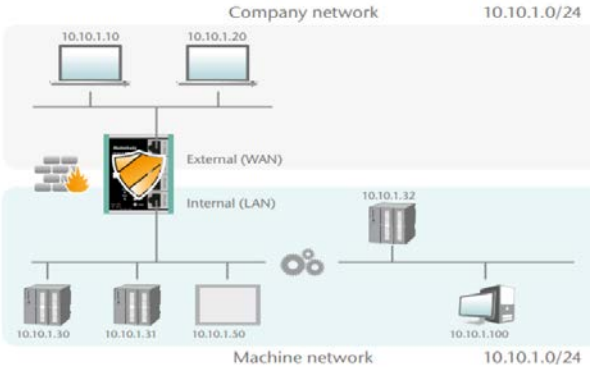


Slika 6: NAPT [2]

Če posplošimo, več stikal lahko organizira podatkovni promet med več internimi IPv4 mrežami v mrežo višjega nivoja. Tako dobijo interne mreže, računalniki in stroji enak IP naslov. Vsako stikalo prevede IP naslov z uporabo NAT.

Tako se lahko stroje in računalnike z istim IP naslovom unikatno naslovi kar iz omrežja podjetja.

- **Posredovanje vrat**: Če stikalo uporabimo kot tako imenovani most, se bo obnašalo kot stikalo plasti 2 med celico avtomatizacije in proizvodno mrežo. Uporabimo lahko tudi paketni filter in s tem omejimo dostope med območji. Tako lahko ločimo del proizvodne mreže brez da bi uporabili drugo mrežo.



Slika 7: Posredovanje vrat [2]

3 Industrijski internet stvari – IIoT

Pri zagotavljanju potreb družbe 5.0 igra Internet stvari (v nadaljevanju IoT) ključno vlogo, ko gre za daljinski prenos podatkov na naše naprave, saj lahko tako dobimo informacije takoj in ne glede na to kje smo.

Danes dodobra poznamo koncepte avtomatizacije in kontrolnih sistemov (v nadaljevanju IACS – Industrial Automation and Control Systems). Gre za OT, znane kot kibernetsko-fizični sistemi (v nadaljevanju CPS – Cyber-physical Systems), ki se uporabljajo v strojegradnji, robotiki, prehrambni, pakirni industriji in domala v vseh drugih panogah industrije. IoT se je prvič pojavil v domačih in industrijskih okoljih leta 1999.

Poznamo kar nekaj definicij na temo IoT, mi se bomo osredotočili na dogajanje v ozadju četrte industrijske revolucije ter predstavili industrijski internet stvari (v nadaljevanju IIoT – Industrial Internet of Things).

3.1 ETHERLINE GUARD

LAPP je prvi koncept IIoT predstavil maja 2020. Razvili smo modul za predvidevanje vzdrževanja PMBx (PMBx – Predictive maintenance box), danes ga imenujemo ETHERLINE GUARD. To je majhen, kompakten, robusten in prilagodljiv modul, ki ga lahko vključite v že obstoječe sisteme. Namen modula je ažurno ugotavljanje stanja Ethernet kablov. S tem preprečimo neželene in drage sistemske napake ter enostavno načrtujemo vzdrževalna dela. Prednost naše rešitve pred konkurenco je predvsem ta, da je naš modul serijsko povezan s podatkovnim kablom, torej ne potrebujemo dodatnih senzorskih elementov ali kakšnih drugih sekundarnih naprav. Zato je še posebej primeren za starejše obstoječe sisteme in ne samo za nove rešitve. Modul se lahko priklopi na gateway ali pa se uporabi v oblaku s pomočjo WiFi-ja, ki uporablja IoT protokol MQTT. Povežemo ga lahko tudi preko žičnega digitalnega izhoda ali IO povezave. Modul ima indikator predvidevanja LAPP, ki neprestano računa oz. predvideva kaj se bo dogajalo. V primeru, da izračuna potencialno nevarnost okvare, to nemudoma javi kot alarmno stanje, kakšen bo intervencijski prag, pa si lahko stranka določi sama. PMBx bo kmalu v uporabi za nekaj naših pilotnih strank na področju medicinske tehnologije, avtomobilskega in intralogističnega sektorja. Temu bo sledila serijska proizvodnja.

Modul je trenutno primeren za nadzor Ethernet kablov. Razvijamo pa tudi rešitve na področju napajalnih kablov.

Slika 8: ETHERLINE GUARD z WiFi modulom

Viri:
[1] Interni dokumenti podjetja LAPP
[2] https://www.helmholz.de/en/
[3] https://www8.cao.go.jp/cstp/english/society5_0/index.html
[4] https://www.lapp.com/en/de/solutions/industrial-communication/e/000231