Sodobni pristopi in rešitve za zagotavljanje kibernetske varnosti v OT okoljih

Igor Belina, Aljaž Stare, Saša Sokolić
Metronik d.o.o.
Stegne 9a, 1000 Ljubljana
igor.belina@metronik.si, aljaz.stare@metronik.si, sasa.sokolic@metronik.si

Modern approaches and solutions for ensuring cyber security in OT environments

New Industry 4.0 concepts, technologies and solutions bring many advantages and improvements in the field of process control, data processing, data insights, visualization, data exchange, etc. On the other hand, such operational environments (OTs) are becoming increasingly "open" and threatened by cyber-attacks or other accidental and unintentional employee errors, which can result in system shutdown or worse, it can lead to improper operation of a critical systems. All this can have significant negative impact on business performance or can lead to major accidents, either environmental or health and life threatening situations. In the past, companies usually completely disconnected OT (process) network from the rest of the world in order to prevent possible attacks. However, with the digitalization of the industry, these trends are changing. Therefore, in this paper modern cyber security approaches and solutions are presented. In addition, it is shown how these solutions, based on detailed analysis and understanding of industrial protocols and devices, offer a better insight into the OT environment and detect and eliminates potential malicious threats, changes or other accidental errors and activities performed by the workers in real time.

Kratek pregled prispevka

V zadnjem času se vse bolj srečujemo z novimi koncepti, tehnologijami in rešitvami, ki jih prinaša industrija 4.0 na področju avtomatizacije in digitalizacije sistemov. Nove tehnološke rešitve uporabnikom prinašajo številne prednosti in izboljšave na področju procesiranja in obdelave podatkov, vizualizacije, učinkovitejšega vpogleda v informacije, hitrejše izmenjave in dostopa do podatkov, itd. Po drugi strani pa postajajo takšna operativna okolja (OT) vse bolj „odprta" in ogrožena pred digitalno usmerjenimi napadalci ali drugimi naključnimi in nenamernimi napakami zaposlenih, kar lahko vodi do popolne zaustavitve sistema ali še hujše, do napačnega delovanja kritične infrastrukture. Vse to lahko izrazito negativno vpliva na samo uspešnost poslovanja podjetja, ali pa vodi celo do večjih nesreč, bodisi na okoljevarstvenem področju, bodisi na področju zdravja ter življenja ljudi. Podjetja so se zaradi tega v preteklosti zatekala celo k popolnemu zapiranju in odklapljanju OT (procesne) mreže od preostalega sveta. Z digitalizacijo industrije pa se ti trendi spreminjajo. V prispevku bomo zato pokazali, kakšne sodobne pristope in rešitve na področju kibernetske varnosti poznamo in kako le-te na podlagi podrobnega analiziranja in razumevanja industrijskih protokolov in naprav nudijo boljši vpogled nad delovanjem OT okolja in v realnem času zaznavajo in odpravljajo potencialne napade, spremembe ali nenamerne napake ter posege zaposlenih.

1 Uvod

Novi koncepti, tehnologije in rešitve, ki jih prinaša industrija 4.0 na področju avtomatizacije in digitalizacije sistemov omogočajo vrsto prednosti in izboljšav za podjetja. Vendar pa, da dosežemo čim večje učinke, ki jih prinaša digitalizacija, potrebujemo pogosto združevati podatke iz IT (poslovnega) okolja s podatki iz OT (procesnega) okolja. To pa pomeni, da moramo podatke iz procesa spraviti čez meje proizvodnih obratov v podatkovna skladišča poslovno-informacijskih sistemov. S tem pa izpostavimo OT okolje večjim varnostnim rizikom.

Večina podjetij ima že vrsto let vpeljane različne (IT) varnostne rešitve pred napadi in vdori. Vendar pa se pogosto dogaja, da podjetja kopirajo in prenašajo postopke zagotavljanja varnosti iz IT v OT okolja, saj se ne zavedajo ključnih razlik med obema svetovoma. V OT okolju se namreč nahajajo specifične (industrijske) naprave, ki komunicirajo preko namenskih industrijskih komunikacijskih protokolov. Zato teh naprav in protokolov s standardnimi varnostnimi rešitvami ne znamo in ne moremo učinkovito ščititi. Potrebujemo namensko zaščito, prilagojeno industrijski opremi.

Zaradi neprimerne OT zaščite smo bili v preteklosti tako že priča raznovrstnih napadov na industrijske objekte in naprave. Poznamo primer zlonamerne kode Havex, ki deluje kot trojanski program za oddaljeni dostop (RAT), ki lahko sproži nepooblaščen ukaz na SCADA napravah in povzroči škodo v kritični infrastrukturi. Poznamo primer trojanskega konja BlackEnergy, ki lahko ogrozi programsko opremo Human Machine Interface (HMI) za dostop do nadzornih sistemov. Poleg tega pa poznamo še Stuxnet, Dragonfly, Shamoon in mnogo drugih, kateri povzročajo škodo v OT omrežju [1].

Poleg samih usmerjenih napadov pa se v industrijskem okolju lahko srečamo tudi z raznimi nenamernimi napakami zaposlenih, ki imajo lahko enake ali še hujše posledice od zunanjih usmerjenih napadov ali vdorov. Tudi teh problemov se s standardnimi varnostnimi rešitvami ne da reševati.

V zadnjih letih zato čedalje bolj intenzivno nastajajo nove rešitve povezane z zagotavljanjem varnosti OT okolja. S temi rešitvami si podjetja lahko z že razmeroma majhno investicijo bistveno zmanjšajo rizike pred kibernetskimi napadi ali drugimi naključnimi napakami zaposlenih, ki imajo lahko katastrofalne posledice.

V prispevku bomo prikazali razlike med IT in OT omrežjem, problematiko varnosti OT omrežja in predstavili najnovejše tehnologije in rešitve za zaščito OT omrežij.

2 Varnost IT in OT omrežja

Ena glavnih ovir, ki preprečuje uspešno zaščito industrijskih sistemov, je nepoznavanje glavnih razlik med informacijskim (IT) in operativnim (OT) okoljem. V smislu, kako se prekrivata, kje se razhajata in kdo je odgovoren za varovanje česa.

2.1 Razlika med IT in OT omrežjem

OT in IT omrežje se razlikuje na več področjih. Vendar se najpomembnejša razlika kaže v smislu rezultatov napada. Napad na IT omrežje lahko privede do kraje podatkov (razkrijejo državne skrivnosti, ukradejo patente podjetja, spraznijo bančne račune…). Medtem napad na OT omrežje v večini primerov vpliva na fizični svet (poškodba in življenje ljudi, onesnaženost okolja, uničenje premoženja, stavb itd), kar predstavlja veliko razliko. Kljub tej razliki pa je pomembno omeniti, da se varnost IT in OT omrežja prekrivata in konvergirata. Ocenjuje se, da z IT tehnologijami pokrijemo 80% varnostnih težav, s katerimi se sooča OT, ostalih 20% pa so značilna samo za OT okolja, ki jih ne gre prezreti in so kritične narave (ljudje, okolje, premoženje). Torej pomanjkljiva zaščita na področju informacijskih sistemov

lahko privede do izgube podatkov, škodo za podjetje oz. blagovno znamko, ugled in dobiček. V OT okolju pa so posledice lahko bistveno hujše. Napadi na OT lahko privedejo do okvare jedrskih sistemov, elektrarn, sistemov za upravljanje železniškega prometa, zastrupitve ali onesnaženja vode in drugih kritičnih družbenih sistemov [1].

Na Sliki 1 so naštete glavne razlike, ki se pojavljajo med IT in OT omrežjem.

IT	OT
Je dinamičen	Je deterministične
Podatki so glavni	Proces je glaven
Zaupnost - prioriteta 1	Kontrola procesa - prioriteta 1
Pretočnost je pomembna	Pretočnost je sekundarna
Popravki so vsakdanjost	Popravki niso pogosti
Pogosta uporaba Gateway stikal	Redka uporaba Gateway stikal

Slika 1: Primerjava IT in OT omrežja.

2.2 Izzivi in kompetence kadrov

Na področju IT je specializacija kadrov v smislu kibernetske varnosti večja. IT strokovnjaki so posebej usposobljeni za zaščito aplikacij, zaščito omrežja, kodiranja ali drugih pomembnih veščin.

Na OT področju pa za varnost običajno skrbijo tehnologi, inženirji avtomatizacije, vzdrževalci, ki dobro poznajo in razumejo zahteve nadzorno-krmilnih sistemov in posebnosti industrijskih komunikacij. Niso pa specializirani za zagotavljanje varnosti OT omrežij, vendar se s tem srečujejo skoraj pri vsakodnevnem opravilu.

Da bi dosegli učinkovito varnost, bi moral OT imeti dostop do strokovnega znanja IT, IT pa bi moral bolje razumeti potrebe OT okolja. [1].

2.3 "White list" in "Black list"

Najbolj pogost način ščitenja (IT) opreme poteka preko »črnega seznama« (Black list). V temu primeru vsem iz seznama onemogočimo dostop do želenega cilja. Najdemo ga v protivirusnih programih in je bolj aktiven v smislu lovljenja groženj in odzivanju na varnostne luknje z namenom priprave popravkov še predno se incident zgodi. V IT okolju to deluje, namreč inženirji konstantno preiskujejo ranljivosti programskih orodij, ter jih odpravljajo s popravki. Lahko pa rečemo, da "Black list" princip ni idealen za OT okolja, saj je potrebno »Black listo« stalno posodabljati in izvajati redne preglede (scan-e), kar po eni strani upočasnjuje industrijske sisteme (npr. nadzorne sisteme), po drugi strani pa se rizičnih (validiranih, preverjenih) industrijskih sistemov marsikje ne smemo dotikati [1].

Za bolj statična OT okolja, kjer imamo unikatne naprave in opremo različnih dobaviteljev z znanimi komunikacijskimi protokoli, pa lahko omrežja zavarujemo preko »belega seznama« (White list). Ta privzeto ne dovoljuje zagona aplikacijam ali uporabnikom, ki niso na seznamu. Lažje povedano – če nisi na seznamu, te ni in nimaš nobenih pravic, da bi karkoli spremenil. Preko "White list" seznama lahko na enostaven način ustavimo večino zlonamernih programov ali preprečimo nenamerne napake zaposlenih.

3 Varnostne rešitve za OT omrežja

Zavedamo se, da obstaja del OT okolja nezaščitenega in sicer v smislu varovanja dostopov do perifernih naprav, varovanja industrijskih komunikacij nadzorno-krmilnih sistemov in preprečevanje nezaželenih posegov v upravljanje nadzornih sistemov. Ta del ostaja nezaščiten, hkrati pa je tudi najbolj kritičen sistem. Kaj se lahko zgodi, če se nezaželeno spremeni parameter na plinski peči, doziranje klora na vodovodu, parametri na turbini, ali kaj drugega na ostalih sistemih? Ali če nam nezaželeno ustavijo krmilje, spremenijo logično kodo? Vse to lahko privede do stroškov, tudi do ekoloških katastrof, stroje lomov, in do ogrožanja zdravja in življenja ljudi.

Grožnje, ranljivosti in varnostne rešitve so pri IT omrežjih že relativno dobro poznane. Tukaj imamo bogato paleto ponudnikov

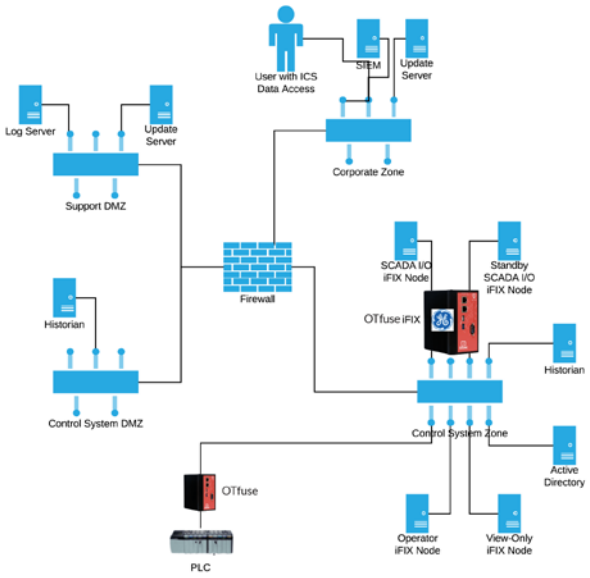
varnostne opreme za požarne zidove, odkrivanja in preprečevanje vdorov, nadzora uporabe in številnih drugih področij. Pri zagotavljanju varnosti OT okolja pa gre za relativno novo področje, kjer obstajajo manjši ponudniki, omejeni na določene industrijske protokole.

Še tako dragocene IT rešitve za zagotavljanje varnosti pa v OT okoljih v določenih primerih ne delujejo, saj so nevarnosti drugačne in posledice napadov težje. Zato se na trgu pojavljajo nove rešitve, ki so namensko razvite za OT naprave in sisteme. V nadaljevanju predstavljamo rešitve podjetja Bayshore Networks, ki se ukvarja z zaščito industrijskega okolja in naprav. Predstavili bomo orodja OTfuse in NetWall. OTfuse ščiti naprave pred nezaželenimi ukazi. NetWall pa deluje kot enosmerna dioda, ki fizično loči omrežja na varni in nevarni del. Predstavili bomo tudi rešitev podjetja Tosibox za zagotavljanje varnih kriptiranih povezav do naprav, tako znotraj podjetja kot oddaljenih lokacij. Rešitev je preprosta in vsebuje dvo-nivojsko avtentikacijo, ter je namenjena OT kadru, ki lahko preprosto upravlja dostope do kritičnih OT naprav in določa pravice razvijalcem, vzdrževalcem in ponudnikom opreme.

3.1 OTfuse – varovanje komunikacije

OTfuse postavimo pred napravo, ki jo želimo zaščiti (PLC, frekvenčni pretvornik, pametne naprave ipd., glej Sliko 2).

Je inteligenten industrijski varnostni element in sistem za preprečevanje vdorov (IPS), ki se konfigurira zelo preprosto. Deluje na principu lastnega učenja in spoznavanja industrijske komunikacije (ustvari se »White lista«), ki poteka med nadzornim sistemom in napravo. Na podlagi učenja in pravil OTfuse uveljavi »normalno« delovanje procesa v obratu, ter v realnem času aktivno preprečuje, da bi do zaščitenih naprav potekala katerakoli neznana komunikacija. Ščiti omrežje in naprave pred nepooblaščenimi spremembami, programskimi ali konfiguracijskimi, pred ponastavitvijo naprav, branjem naprav, in nezaželenimi spremembami vrednosti parametrov izven svojih mej. Podpira protokole kot so Modbus, Bacnet, Ethernet/IP, Siemens S7, SLMP, FINS, DNP3 in je zasnovan tako, da ga lahko uporabljajo tehnologi, vzdrževalci in inženirji avtomatizacije z znanjem računalništva in industrijskih komunikacijskih protokolov [2].



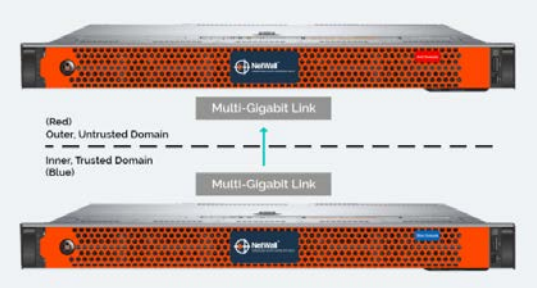
Slika 2: OTfuse ščiti krmilni sistem PLC, OTfuse iFIX pa ščiti komunikacijo med SCADA serverjema in SCADA odjemalci. [3]

3.2 NetWall – enosmerna fizična ločitev

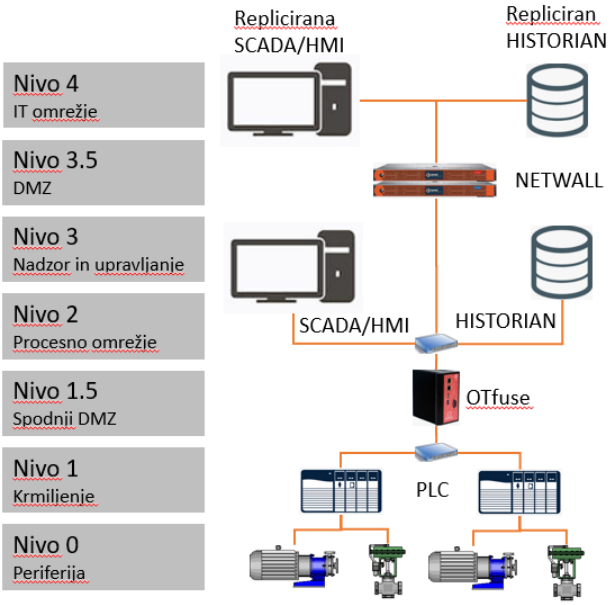
NetWall opremi pravimo tudi enosmerni varnostni prehod (dioda). Je strojna in programska rešitev, ki izvaja preslikavo podatkov samo v eno smer. Ob namestitvi razdeli omrežje na zaupanje vreden del in potencialno nevaren del. Varen del ščiti in izolira kritične elemente in občutljive dele omrežja pred kibernetskimi napadi in zlorabo.

Prenaša podatke iz zaupanja vrednega omrežja (obrata), ne da bi naprave izpostavil nezaupljivemu omrežju (korporacijska IT, poslovne destinacije). Ima funkcijo enosmerne podatkovne diode, ki zagotavlja industrijski most med omrežjema. S tem omogoča, da se podatki iz varnega dela omrežja (OT) neovirano pretakajo v nevaren (IT) del, v obratno smer pa ne. Prikaz strojne opreme Netwall si lahko pogledate na Sliki 4, primer uporabe v OT omrežju pa na Sliki 5.

NetWall podpira protokole OPC DA, A&E in UA ter Modbus / TCP, prenose datotek in vtičnic TCP / UDP.



Slika 4: Prikaz strojne opreme NetWall. Modra naprava se nahaja na varnem delu omrežja, rdeča pa na potencialno ogroženem delu omrežja. Podatki se prenašajo enosmerno iz modrega v rdeči del omrežja.



Slika 5: Z OTfuse ščitimo krmilni nivo, z NetWall pa enosmerno prenašamo podatke iz procesnega omrežja v IT omrežje.

3.3 *Tosibox – Oddaljen dostop do naprav preko interneta*

Tosibox rešitev je strojna oprema, ki na enostaven in hiter način vzpostavi point-to-point (VPN) kanal med dislociranim računalnikom in napravo. Rešitev je modularna, razširljiva in fleksibilna z vgrajenim požarnim zidom. Vse Tosibox komponente so kompatibilne, rešitev pa deluje tako znotraj podjetij, kot tudi na oddaljenih lokacijah.

Uporabljamo ga kot usmerjevalnik za priklop OT naprav, kjer se dostop preverja z dvo-nivojsko avtorizacijo. Vsebuje aplikacijo za enostavno upravljanje dodeljevanja pravic dostopov, ki je preprosta in namenjena uporabnikom brez specializiranih IT znanj. Omogoča tudi oddaljen dostop za vzdrževalce, integratorje, tehnologe, ponudnike naprav, glej Sliko 6. S pomočjo 4G omrežja je zmožen povezati tudi dislocirane enote na centralno enoto, tam kjer ni Ethernet priključka.

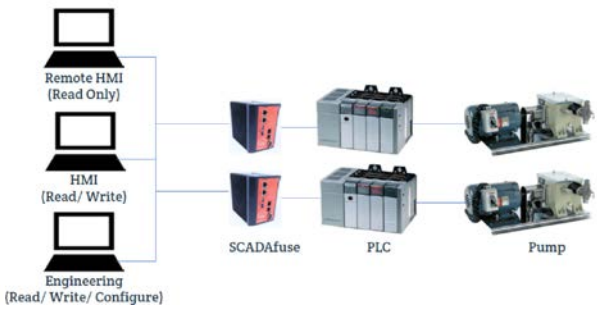
Slika 6: S kriptirnim ključem na strani računalnika dostopamo do naprav, ki so povezane s Tosibox Lock napravo. VPN povezava se vzpostavi samodejno.

4 Primeri uporabe

V nadaljevanju predstavljamo nekaj primerov uporabe rešitev podjetja Bayshore Networks in Tosibox.

4.1 *Bayshore Networks – zaščita vodovoda z OTfuse*

V primeru vodarne želimo pogosto zaščititi kritične PLC krmilnike in posledično črpalke pred zlorabo. S pomočjo OTfuse naprave, ki jo postavimo pred krmilno enoto (glej Sliko 7), želimo zaščiti komunikacijo med nadzornim sistemom in krmilnim enoto.



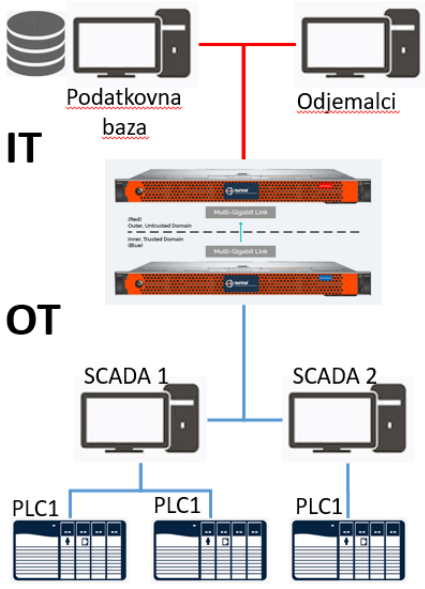
Slika 7: Primer OTfuse v procesnem okolju.[4]

OTfuse se avtomatsko nauči kaj je »znana« komunikacija in preprečuje izvajanje neznane komunikacije in ukazov. S tem smo zaščitili krmilno enoto pred nepredvideno uporabo, tako pred notranjimi kot zunanjimi grožnjami. Ščiti napravo pred nezaželeno spremembo konfiguracije, ponovim zagonom ali ustavitvijo naprave, pred spremembo logike programa in pred nedovoljenimi vrednostmi parametrov.

Na ta način lahko varujemo tudi druge naprave v različnih industrijskih panogah. Naprave, ki jih želimo ščititi morajo imeti s strani OTfuse podprte protokole. Rešitev pa ni omejena samo na krmilne enote, temveč tudi na druge naprave, ki uporabljajo podprte protokole, kot so na primer Modbus, Bacnet.

4.2 *Bayshore Networks – Zaščita podatkov z NetWall*

V podjetjih želimo pogosto fizično ločiti dostop do procesnega (OT) omrežja, a po drugi strani želimo iz IT mreže imeti na razpolago vse podatke o proizvodnji. Z NetWall tehnologijo fizično ločimo oba omrežja in z enosmerno komunikacijo zagotovimo, da ne more nihče posegati v sisteme izven OT omrežja. Arhitektura in umestitev orodja NetWall je prikazana na Sliki 8.

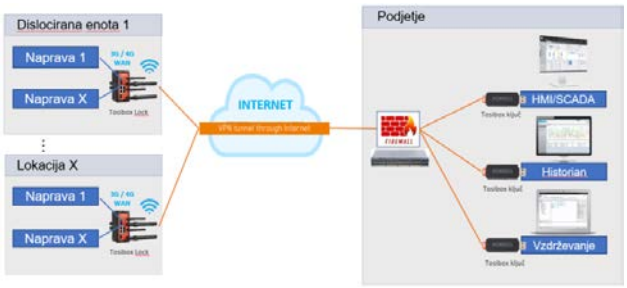


Slika 8: NetWall prepušča podatke iz procesnega (OT) omrežja v IT omrežje.

NetWall sinhronizira in replicira podatke med omrežjema, s tem pa ne razkriva občutljivih informacij o omrežju. NetWall ustvari popolno fizično ločitev med dvema omrežnima entitetama.

4.3 *Tosibox - Nadzor, upravljanje in vzdrževanje dislociranih IoT naprav*

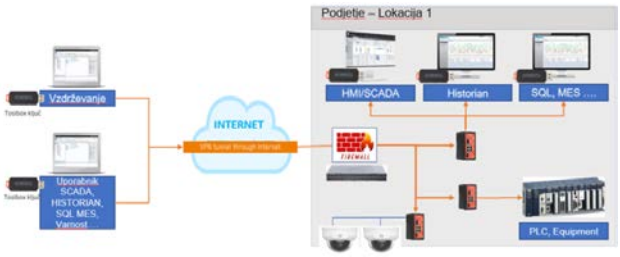
V kolikor želimo povezati dislocirane enote ali IoT naprave s SCADA sistemom ali kakšno drugo napravo in tako zagotoviti upravljanje, podatkovno zbiranje ali nadzor nad temi enotami, je Tosibox idealna rešitev. Tosibox rešitev zagotavlja varno povezavo in dostop do naprave preko interneta ali preko 4G omrežja. Pri tem mislimo na dostop do raznih IoT naprav, krmilnikov, frekvenčnih pretvornikov, črpališč, generatorjev, energetskih postaj, poslovnih stavb, nadzornih kamer, ipd.. Primer povezovanja dislociranih enot s SCADA sistemom je prikazan na Sliki 9, kjer imamo na strani dislociranih enot Tosibox Lock napravo in na strani SCADA sistema Tosibox kriptirni ključ. Z uparjanjem Lock naprave in ključa vzpostavimo kriptirano in varno povezavo point-to-point.



Slika 9: S Tosibox opremo lahko povežemo dislocirane enote s SCADA sistemom ali Historianom preko 4G ali internet komunikacije

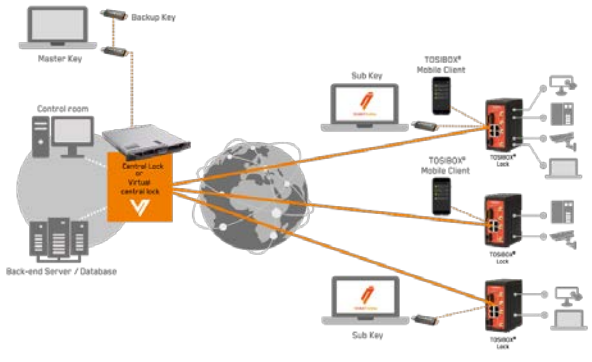
4.4 *Tosibox - Varen in preprost VPN dostop do ključnih proizvodnih lokacij*

Tosibox lahko uporabimo tudi kot varen VPN dostop do OT infrastrukture znotraj podjetja za namene vzdrževanja in izvajanja projektov na daljavo. Z uparjanjem ključa z Lock napravo vzpostavimo VPN povezavo v nekaj minutah, brez potrebe po specifičnih IT znanjih. Primer je prikazan na Sliki 10.



Slika 10: V primeru Tosibox uporabljamo za oddaljen dostop do naprav, kot so krmilni sistemi ali nadzorni sistemi, za namen vzdrževanja, pregleda tehnoloških nastavitev in varnostnih kamer. Vsaki Tosibox Lock napravi lahko določimo različne uporabnike.

Če integriramo Tosibox rešitev v OT omrežje, lahko OT kadrom prepustimo upravljanje dostopov do naprav (glej slika 11), ki je dokaj preprost. S tem podvojimo varnost, saj IT pravila še vedno veljajo. S celovito rešitvijo pokrijemo tako oddaljene dostope kot interne dostope uporabnikov do naprav. Lahko priklapljamo več lokacijsko oddaljenih objektov in agregiramo podatke na centralnem strežniku. Tosibox Lock skrbi, da do naprav lahko dostopa samo uporabnik, katerega ključ je uparjen z Lock napravo.



Slika 11: S pomočjo Tosibox VLC lahko upravljamo in nadziramo oddaljene dostope do različnih lokacij podjetja, notranjih ali zunanjih.

5 Zaključek

Ker se napadi na (OT) industrijske sisteme in naprave pojavljajo vedno pogosteje, in so ti napadi vedno bolj sofisticirani, so se razvijalci kibernetskih rešitev temu primerno prilagodili in razvili namenske rešitve za zaščito industrijskega okolja in varnega oddaljenega dostopa do procesnih naprav. Principi in tehnologije, ki smo jih dolga leta uporabljali na področju IT zaščite namreč ne pokrijejo vseh varnostnih lukenj, katerim je izpostavljano OT okolje. Vemo namreč, da ima OT okolje drugačne potrebe kot IT omrežje. Prav tako so posledice napada lahko bistveno bolj ogrožajoče za ljudi in okolje.

S podporo industrijskih protokolov lahko nove rešitve zaščitijo tisti (kritični) del sistema, ki se navezuje na avtomatizacijo proizvodnje, delovanje in upravljanje naprav. Rešitve učinkovito ščitijo krmilne, kot tudi nadzorne sisteme, in s tem preprečujejo, da ne pride do namernih ali nenamernih sprememb v delovanju procesa. Vse to pa lahko zagotovimo že z relativno majhnim investicijskim vložkom.

6 Literatura

[1] https://www.ge.com/fr/sites/www.ge.com.fr/files/an-executive-guide-to-cyber-security-for-operational-technology-whitepaper.pdf
[2] https://bayshorenetworks.com/products/otfuse/
[3] https://bayshorenetworks.com/products/otfuse-ifix/
[4] https://bayshorenetworks.com/products/netwall/
[5] https://www.tosibox.com/products/