So industrijska okolja imuna na kibernetske napade?

Veljalo je, da so proizvodna oziroma industrijska okolja strogo ločeni sistemi, zato je dostop do njih zelo omejen. Nič več. Varnostne grožnje in pomanjkljivosti so v industrijskih okoljih, ki nimajo vzpostavljenih naprednih mehanizmov kibernetske varnosti, izredno nevarne.

S povezovanjem različnih proizvodnih sistemov ter njihovim zlitjem s poslovnimi aplikacijami in digitalizacijo procesov, ter na splošno »odpiranjem navzven« se je pojavil nov izziv. Kako varovati industrijska okolja ter kritično infrastrukturo pred digitalnimi napadalci.

Gartner research ocenjuje, da so podjetja že leta 2016 dnevno v svoja omrežja ali na internet »dodala« kar 5,5 milijona naprav, medtem ko bo Internet stvari (angl. IoT) leta 2020 sestavljalo okoli 21 milijard naprav samo v industrijskih okoljih. Povezovanje in križanje informacijskih tehnologij in industrijskih sistemov ni najbolj enostavna naloga. Sploh če gre za starejše rešitve, ki imajo vgrajeno bore malo ali sploh nič varnostnih rešitev oziroma mehanizmov. Slednje podjetjem povzroča povečana tveganja, ki se lahko kaj hitro spremenijo v dejansko škodo, če podjetje ali organizacijo na piko vzame kak heker ali skupina hekerjev.

Industrijska okolja so ranljiva zaradi povezovanja z »zunanjim« svetom

V industrijskem okolju komunikacije praviloma niso poznale internetnega protokola. Tehnologija požarnega zidu ni obstajala in se ni zdela potrebna. Tudi ko so se omrežja v industrijskih sistemih modernizirala in začela uporabljati Ethernet in protokole TCP/IP, so bila običajno fizično ločena od IT-sistemov in zaprta pred vstopi iz drugih sistemov. Digitalizacija procesov pomeni obvezno povezovanje z informacijskimi sistemi. Hitro se razvijajo tudi oblačne (angl. cloud) platforme za industrijske sisteme, IIoT (angl. Industrial Internet of Things), ki vodijo v povezovanje industrijskih sistemov in omrežij z »zunanjim« svetom. Vzpostavljajo se okolja, ki so namenjena poslovnim procesom (IT) ter procesni sistemi oz. omrežja (OT), tudi če sta v načelu fizično ločena. Ravno zaradi digitalizacije procesov prihaja do povezovanja med njima.

Zaradi tega moramo danes resno razmišljati o kibernetski varnosti. Industrijska kibernetska varnost je proces ohranjanja industrijskih nadzornih sistemov (ICS) brez namernih ali nenamernih kibernetskih groženj, ki motijo ali povzročajo škodo ljudem, procesom, opremi ali okolju. Varnostne grožnje in pomanjkljivosti so v industrijskih okoljih, ki nimajo vzpostavljenih naprednih mehanizmov kibernetske varnosti izredno nevarni. Izkoriščajo pomanjkljivosti in ranljivosti starejših operacijskih sistemov in naprav, ki se ne posodabljajo, saj so procesni sistemi bistveno bolj statični, od poslovnih procesov, kjer se varnostne posodobitve redno izvajajo.

To odpira velik potencial morebitnim napadalcem. Že okužen USB-ključ, ki je bil povezan na osebni računalnik in ga operater uporablja za delo v industrijskem okolju, lahko nosi škodljivo kodo ali viruse, preko katerih se zgodijo kasnejši varnostni vdori. Spomnimo se na posledice virusa Stuxnet ali večkratni razpad elektroenergetskega sistema zaradi varnostnega vdora v Ukrajini v letih 2015 in 2017.

Kako okrepiti kibernetsko varnost naše vitalne infrastrukture?

V industrijskih okoljih pridejo v poštev dodatne varnostne rešitve poleg tistih, ki jih podjetja že poznajo. Vedno več podjetij se odloča za uvedbo rešitev za spremljanje, odkrivanje in profiliranje proizvodnih virov kot tudi za rešitve, katerih naloga je odkrivanje

anomalij in ustrezno odzivanje na varnostne grožnje, sistemi, ki celovito preverjajo tako naprave kot komunikacijske tokove in na podlagi strojnega učenja in umetne inteligence zaznavajo nenavadne ali kritične odmike od normalnega obnašanja sistemov v takšnih okoljih.

Svetovni gospodarski forum je v svojem poročilu o najrazličnejših tveganjih Global Risks Landscape 2018 kibernetske napade po verjetnosti dogodkov uvrstil na izjemno visoko tretje mesto – takoj za ekstremnimi vremenskimi pojavi in naravnimi katastrofami. Na četrto mesto pa so se uvrstile kraje podatkov in prevare. Kaj to pomeni za industrijska okolja? Preprosto povedano: pričakovati je, da bodo napadena, zato velja tudi v ta »informacijska okolja« vpeljati ustrezne zaščite in procese odzivanja na varnostne incidente.

Proaktivno upravljanje varnostnih tveganj procesnih sistemov postaja naloga vodstva

Na vodstvu podjetja je vse večja odgovornost, da poskrbi za kibernetsko varnost celotne organizacije, tudi širše od poslovnih informacijskih sistemov, svojih zaposlenih, okolja in strank, ki so v primeru uspešnega kibernetskega napada lahko močno prizadeti.

Izboljšanje kibernetske varnosti v industrijskih okoljih je nujno, če želimo zagotoviti nemoteno delovanje kritičnih sistemov ter obdržati pozitivne finančne rezultate in ugled podjetja. Finančne posledice napadov, ki so povzročili motnje v delovanju kritičnih sistemov, lahko dosežejo več milijonov dolarjev. V podjetju Merck je nastalo 780 milijonov dolarjev izgube zaradi zaustavitve proizvodnje, izgube prodaje in stroškov sanacije. V Maersk je zaradi motnje poslovanja, izgube dobička in stroškov sanacije nastalo za 300 milijonov dolarjev. Podobna škoda s 300 milijonov dolarjev izgube dobička v enem kvartalu je nastala tudi v podjetju v Fedd Ex.

Strokovnjaki za kibernetsko omrežno in aplikativno varnost kot za zagotavljanje naprednih in zanesljivih komunikacijskih omrežij iz podjetja Smart Com izpostavljajo dva pomembna ukrepa, ki ju lahko uvedete, da omilite posledice OT tveganj oz. proaktivno pristopite k zmanjšanju kibernetskih tveganj v vašem industrijskem okolju.

Poenotenje ekip za poslovne in procesne sisteme

Z združevanjem tehnologij tudi sistemi postajajo vse bolj povezani, kar je priložnost tako za zmanjševanje tveganj, stroškov kot tudi pohitritev projektov.

Edini način, da zmanjšamo tveganja in povečamo varnost OT okolij kritične infrastrukture, je, da IT in OT združita moči – IT-ekipa ima več znanja s področja kibernetske varnosti in oblačnih storitev, medtem ko ima OT-ekipa več znanja o delovanju procesne infrastrukture in storitev. Sodelovanje obeh ekip pripore k identificiranju varnostnih slepih peg in zmanjšanju stroškov. Seveda se to

ne zgodi čez noč, potrebna je močna zaveza in usmerjanje vodstva. Začetni koraki naj obsegajo določitev odgovorne osebe tako za IT kot OT okolje ter prenos znanja in izobraževanje med obema ekipama. Čim več naj bo skupne tehnologije, ki jo uporabljata obe ekipi.

Investiranje v tehnološke rešitve, ki uporabljajo strojno učenje in umetno inteligenco

Zasnovane so tako, da izboljšajo vidljivost in kontrolo nad elementi in protokoli v OT-okolju ter povečajo odpornost na kibernetska tveganja. S tem vplivate na povečanje zanesljivosti, varnosti in produktivnosti zaposlenih ter izboljšate timsko delo.

IT-rešitve za OT okolja niso ustrezne, ker ne izpolnjujejo zahteve po 24/7/365 delovanju operativnih sistemov, kjer je prioriteta razpoložljivost in je pomembnejša od zaupnosti ali integritete.

Sodobne rešitve (kot npr. Nozomi Networks) so zasnovane na podlagi podrobnega poznavanja in razumevanja industrijskih omrežij in procesov. So popolnoma varne (ne vplivajo na delovanje sistemov – pasivno sledenje) in prinašajo popoln pregled nad delovanjem OT-okolja in zaznavanje kibernetskih groženj v realnem času.

Prednosti, ki jih pridobite z implementacijo tovrstnih rešitev:

- Enotna platforma za aktivno spremljanje in varovanje OT--sistemov (tako IT- kot OT-ekipa imata popoln pregled nad OT-omrežjem in elementi ter varnostnimi in procesnimi tveganji).
- Nadzor nad delovanjem omrežja in zaznava groženj v realnem času na način, ki ni škodljiv za izvajanje procesnih sistemov.
- Takojšnja zaznava obstoječih groženj v industrijskih omrežjih ter izboljšanje produktivnosti zaposlenih v IT- in OT-oddelku.
- Neopazna integracija z IT-infrastrukturo.
- Enostaven prenos podatkov z obstoječimi aplikacijami.

› *www.smart-com.si/ics*