Zaštita IoT

Sadržaj

- Uvod
- Izazovi sigurnosti OT
- Praksa u sigurnosti OT
- Formalne strukture analize rizika (OCTAVE i FAIR)
- Fazna primjena sigurnosti u operativnom okruženju

Uvod

- Napadači sa ograničenim tehničkim mogućnostima ili bez njih sada imaju potencijal da pokrenu sajber napade.
- Uobičajena je zabluda da napadači uvijek imaju prednost i da ne postoje efikasne odbrambene mogućnosti.
- Važna prednost za adminstratore mreže je činjenica da su daleko bolje upoznati sa svojim okruženjem i bolje razumiju svoje procese, te tako mogu iskoristiti više tehnologija i mogućnosti za odbranu mreža od napada.
- Ovo je kritično jer će se mreže nastaviti suočavati sa sve evoluirajućim i promjenLjivim metodama napada od kojih će biti sve teže braniti se i na njih odgovoriti.

Uvod

- Komunikacione mreže se koriste u industrijskim okruženjima decenijama.
- Na primjer, daljinsko praćenje trafostanica i komunikacija između poluautonomnih sistema u industriji su dugogodišnji primjeri takvih OT mreža.
- Ovi komunikacioni sistemi specifični za OT su obično bili samostalni i fizički izolovani od tradicionalnih IT mreža kompanija.
- Iako slijedi tradicionalnu logiku, ovaj oblik podjele mreže doveo je do nezavisne evolucije IT i OT mreža, uz međusobne veze između okruženja koje su strogo odvojene i nadgledane.

Uvod

- Izolacija između industrijskih mreža i tradicionalnih IT poslovnih mreža podrazumijeva da između njih ne postoje veze.
- Iako postoje primjeri takve ekstremne izolacije u nekim industrijama, to zapravo nije tačan opis većine IoT mreža danas.
- Uopšteno govoreći, postoje različiti nivoi međupovezanosti između OT i IT mrežnih okruženja, a mnoge međuzavisnosti između njih utiču na nivo međusobnog povezivanja.

Uvod

- Pored politika, propisa i upravljanja koje nameću različita industrijska okruženja, postoji i određena količina preferencija krajnjih korisnika i dizajna specifičnog za implementaciju koji određuju stepen izolacije između IT i OT okruženja.
- Dok neke organizacije nastavljaju da održavaju striktno razdvajanje, druge počinju da dozvoljavaju određene elemente međusobnog povezivanja.
- Jedan uobičajen primjer ovoga je korišćenje Etherneta i IP-a za transportne sisteme upravljanja u industrijskim okruženjima.
- Koliko god se IT i OT mrežama i dalje upravlja odvojeno, preovlađujući trend je konsolidacija mreža zasnovanih na IT-centričnim tehnologijama kao što su TCP/IP, Ethernet i uobičajeni API-ji.

Uvod

- Ova evolucija sve prisutnijih IT tehnologija u OT prostoru donosi prednosti povećane pristupačnosti i veće baze obučenih administratora nego s nestandardnim i zaštićenim komunikacionim metodama u tradicionalnim industrijskim okruženjima.
- Izazovi povezani sa ovim dobro poznatim IT standardima su to što su sigurnosne ranjivosti šire poznate, a zloupotreba tih sistema je često lakša i dešava se u mnogo većem obimu.
- Ova dostupnost i obim čine sigurnost glavnim problemom, posebno zato što mnogi sistemi i uređaji u operativnom domenu nikada nisu bili zamišljeni da rade na zajedničkoj infrastrukturi zasnovanoj na otvorenim standardima i nisu dizajnirani i razvijeni uz visok nivo ugrađene sigurnosti.

Uvod

- Projekti u industrijskim okruženjima su često veoma skupi, sa očekivanim životnim vijekom koji se može mjeriti decenijama.
- Za razliku od IT-baziranih rješenja, OT implementirana rješenja obično nemaju razloga za promjenu jer su dizajnirana da zadovolje specifične funkcije i nemaju zahtjeve ili podsticaje za nadogradnju.
- Ogroman fokus i prioritet u OT-u je vrijeme neprekidnog rada sistema i visoka dostupnost, tako da se promjene obično prave samo da bi se popravile greške ili uvele nove sistemske mogućnosti kao podrška tom cilju.
- OT sistemi često imaju sporije cikluse razvoja i nadogradnje i mogu brzo postati neusklađeni sa tradicionalnim IT mrežnim okruženjima.
- Ishod je da su i OT tehnologije i znanje onih koji brinu o tim operativnim sistemima napredovali sporijim tempom od njihovih IT kolega.

Uvod

- Većina industrijskih kontrolnih sistema koji se danas koriste, njihove komponente i ograničeni povezani sigurnosni elementi dizajnirani su kada je poštovanje objavljenih i otvorenih standarda bilo rijetko.
- Vlasnička priroda ovih sistema značila je da je malo vjerovatno da će se pojaviti prijetnje iz spoljašnjeg svijeta.
- Rastući je trend u kojem su ranjivosti OT sistema bile izložene i prijavljene.
- Iako se broj prijava povećavao tokom proteklih godina, vjerovatno je da još uvijek postoje mnogi drugi koji nisu prijavljeni niti otkriveni.
- S obzirom na sporu stopu promjena i produžene cikluse nadogradnje većine OT okruženja, ulaganje u sigurnost industrijskih komunikacija i računarskih tehnologija je istorijski zaostajalo za ulaganjem u osiguranje tradicionalnih IT okruženja preduzeća.

Izazovi sigurnosti OT

Erozija mrežne arhitekture

- Dva glavna izazova u osiguranju industrijskog okruženja bili su početni dizajn i tekuće održavanje.
- Početni izazovi dizajna proizašli su iz koncepta da su mreže sigurne zbog fizičkog odvajanja kompanije s minimalnom ili nikakvom povezanošću sa spoljašnjim svijetom i pretpostavke da napadači nemaju dovoljno znanja da izvedu sigurnosne napade.
- U mnogim slučajevima, početni dizajn mreže je dobar i čak prati dobro definisane najbolje industrijske prakse i standarde, kao što je Purdueov model za hijerarhiju upravljanja.
- Izazov i najveća prijetnja „mrežnoj sigurnosti je da se standardi i najbolje prakse ili pogrešno razumiju ili da se mreža loše održava.

Izazovi sigurnosti OT

Erozija mrežne arhitekture

- Iz perspektive sigurnosnog dizajna, bolje je znati da su komunikacioni putevi nesigurni nego ne znati stvarne komunikacione puteve.
- Često, tokom vremena, za početak solidan dizajn postane narušen ad hoc ažuriranjima i pojedinačnim promjenama hardvera i mašina bez razmatranja šireg uticaja na mrežu.
- Svjedoči se pogrešnim procjenama širenja mreža i uvođenju bežične komunikacije, bez uzimanja u obzir njenog uticaja na originalni sigurnosni dizajn.
- Nekontrolisane ili loše kontrolisane evolucije OT mreže su, u mnogim slučajevima, tokom vremena dovele do slabe ili neadekvatne bezbjednosti mreže i sistema.

Izazovi sigurnosti OT

Erozija mrežne arhitekture

- Postoji širok izbor dizajna zaštićenih mreža unutar i među različitim industrijama.
- Elektroprivrede decenijama koriste moderne tehnologije za operativne aktivnosti, implementaciju bezbjednog mrežnog povezivanja i kontrole uz razumno propisane radnje.
- U drugim industrijama često ne postoje zakonski zahtjevi ili politike usklađenosti, što je rezultiralo raširenim razlikama u sigurnosnim politikama.
- U mnogim industrijama, kontrolni sistemi se sastoje od samostalnih komponenti koje mogu biti integrisane kao poluautonomni djelovi mreže.
- Ove komponente možda neće biti potpuno ili čvrsto integrisane u cjelokupni sistem kontrole, alate za upravljanje mrežom ili sigurnosne aplikacije, što rezultira potencijalnim rizikom.

Izazovi sigurnosti OT

Zastarjeli sistemi

- Zbog statične prirode i dugog životnog ciklusa opreme u industrijskom okruženju, mnogi operativni sistemi se mogu smatrati naslijeđenim sistemima.
- U elektroprivredi nije neuobičajeno da stara mehanička oprema još uvijek radi zajedno sa modernim inteligentnim elektronskim uređajima.
- U mnogim slučajevima, stare komponente nisu ograničene na izolovane mrežne segmente, već su prisutne i u IT operativnom okruženju.
- Sa sigurnosne perspektive, ovo je potencijalno opasno jer mnogi uređaji mogu imati slabosti koje nisu ažurirane, ili može biti da sigurnosne nadogradnje nisu ni dostupne zbog starosti opreme.

Izazovi sigurnosti OT

Zastarjeli sistemi

- Osim krajnjih tačaka, komunikaciona infrastruktura i zajednički centralizovani računarski resursi često nisu izgrađeni u skladu sa savremenim standardima.
- Njihove komunikacije i protokoli mogu biti stari generacijama i moraju biti interoperabilni sa najstarijim operativnim entitetom na komunikacionom putu.
- Ovo uključuje switcheve, rutere, firewalle, bežične pristupne tačke, servere, sisteme za daljinski pristup i alate za upravljanje mrežom.
- Svi ovi sistemi mogu biti iskorišćeni za napad i zato moraju biti zaštićeni.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

- Mnogi industrijski kontrolni protokoli, posebno oni koji su bazirani na serijskim komunikacijama, dizajnirani su bez sigurnosnih mehanizama.
- Njihov rad je često bio predviđen unutar sigurne mreže.
- Uz sve slabosti ili ranjivosti, njihovo operativno okruženje nije dizajnirano sa uzimanjem u obzir sigurne kontrole pristupa.
- Industrijski protokoli, kao što su nadzorna kontrola i prikupljanje podataka (SCADA), posebno starije varijante, pate od uobičajenih sigurnosnih problema.
  - česti nedostatak autentifikacije između krajnjih tačaka komunikacije,
  - nema sredstava za osiguranje i zaštitu podataka u mirovanju ili u pokretu
  - nedovoljna granularnost kontrole da bi se pravilno specificirali primaoci podataka.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

- Ovo je veoma kritično u samostalnim sistemima, ali je još kritičnije u WAN (posebno javni WAN) mreži.
- Struktura i rad većine ovih protokola često su javno dostupni iako ih je razvila privatna kompanija, radi interoperabilnosti, obično se objavljuju da bi ih drugi implementirali.
- Postaje relativno jednostavna stvar kompromitovati same protokole i uvesti zlonamerne aktere koji ih mogu koristiti da kompromituju sisteme kontrole bilo u svrhu izviđanja ili napada, što bi moglo dovesti do neželjenih uticaja u normalnom radu sistema.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

Modbus

- Modbus se obično nalazi u mnogim industrijama, kao što su komunalna i proizvodna okruženja, i ima više varijanti (na primjer, serijski, TCP/IP).
- To je jedan od najčešće korišćenih protokola u industrijskim primjenama, a njegovim razvojem upravlja Modbus organizacija.
- Nedostatak provjere autentičnosti komunikacionih krajnjih tačaka je omogućavalo napadaču da šalje neodgovarajuće komande primaocu.
- Da bi poruka stigla na svoje odredište, potrebna je ispravna Modbus adresa i poziv funkcije (kod).
- Neke starije i serijski bazirane verzije Modbusa komuniciraju putem broadcasta.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

Modbus

- Mogućnost zaustavljanja broadcasta ne postoji u nekim verzijama.
- Postoji potencijal da primalac djeluje na naredbu koja nije bila posebno usmjerena na njega.
- Nadalje, napad bi potencijalno mogao uticati na neželjene uređaje primaoca, smanjujući tako potrebu za razumijevanjem detalja topologije mreže.
- Provjera valjanosti sadržaja Modbus poruke također se ne vrši od strane aplikacije koja pokreće.
- Modbus zavisi o mrežnom steku za obavljanje ove funkcije.
- Ovo otvara potencijal za zloupotrebu protokola u sistemu.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

DNP3 (*Distributed network protocol*)

- DNP3 se koristi u više industrija.
- Uobičajen je u komunalnim djelatnostima i diskretnim/kontinuiranim procesnim sistemima.
- Kao i mnogi drugi ICS/SCADA protokoli, bio je namijenjen za serijsku komunikaciju između kontrolera i jednostavnih IED uređaja.
- Postoji eksplicitna "sigurna" verzija DNP3, ali postoje i mnoge nesigurne implementacije DNP3.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

DNP3 (*Distributed network protocol*)

- DNP3 posjeduje pouzdanu isporuku poruka što ima specifičnu slabost iz sigurnosne perspektive.
- Sigurnosni element koji nedostaje je sposobnost uspostavljanja povjerenja u stanje sistema, a time i sposobnost povjerenja u istinitost informacija koje se prezentiraju.
- Ovo je slično sigurnosnim propustima predstavljenim ARP porukama u Ethernet mrežama, što se rješava pomoću Dynamic ARP Inspection (DAI) u modernim Ethernet switchevima.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

ICCP (*Communications Protocol Inter-Control Center*)

- ICCP je uobičajen kontrolni protokol koji se često koristi za komunikaciju između komunalnih preduzeća.
- S obzirom na to da mora preći granice između različitih mreža, ima dodatni nivo izloženosti i rizika koji bi mogao izložiti komunalni sistem sajber napadu.
- Za razliku od drugih kontrolnih protokola, ICCP je dizajniran od početka da radi preko WAN-a.
- Početne verzije ICCP-a imale su nekoliko značajnih nedostataka u oblasti sigurnosti.
  - Sistem nije zahtijevao autentifikaciju za komunikaciju.
  - Enkripcija u cijelom protokolu nije bila omogućena kao zadati uslov, čime su veze izložene man-in-the-middle (MITM) i replay napadima.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

OPC (*OLE for Precess Control*)

- OPC je zasnovan na Microsoft metodologiji interoperabilnosti *Object Linking and Embedding* (OLE).
- Ovo je primjer gdje je IT standard koji se koristi u IT domenu i personalnim računarima iskorišćen kao kontrolni protokol u industrijskoj mreži.
- U industrijskim kontrolnim mrežama, OPC je ograničen na rad na višim nivoima kontrolnog prostora, uz zavisnost od Windows platformi.
- Problemi OPC-a su vezani za operativni sistem na kojem radi.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

OPC (*OLE for Precess Control*)

- Mnogi Windows uređaji u operativnom prostoru su stari, nisu u potpunosti "zakrpljeni" i pod rizikom su zbog mnoštva dobro poznatih ranjivosti.
- Iako novije verzije OPC-a imaju poboljšane sigurnosne mogućnosti, one su također otvorile nove načine komunikacije, koji imaju i pozitivan i negativan sigurnosni potencijal.
- Od posebnog značaja za OPC je zavisnost od protokola *Remote Procedure Call* (RPC), koji stvara dvije klase izloženosti.
- Prvi zahtijeva jasno razumijevanje ranjivosti povezane sa RPC-om, a drugi traži identifikaciju nivoa rizika koji ove ranjivosti donose za određenu mrežu.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

International Electrotechnical Commission (IEC) protokoli

- IEC 61850 standard je kreiran da bi omogućio inžinjering elektroenergetskih sistema nezavisno od proizvođača opr, što zauzvrat omogućava interoperabilnost između proizvođača i standardizovanih komunikacionih protokola.
- Prvobitno su definisana tri tipa poruka:
  - MMS (Manufacturing Message Specification),
  - GOOSE (Generic Object Oriented Substation Event)
  - SV (Sampled Values).
- Web je četvrti protokol koji je dodat kasnije.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

International Electrotechnical Commission (IEC) protokoli

- MMS (61850-8.1): MMS je klijent/server L3 protokol koji koristi TCP/IP. Pruža istu funkcionalnost kao i drugi SCADA protokoli, kao što su IEC 60870 i Modbus.
- GOOSE (61850-8.1): GOOSE je L2 protokol koji radi putem multicasta preko Etherneta. Omogućava IED-ovima da razmjenjuju podatke "horizontalno", između sistema, posebno za signale međusobnog zaključavanja, mjerenja i okidanja.
- SV (61850-9-2): SV je L2 protokol koji radi putem multicasta preko Etherneta. Nosi uzorke vrijednosti napona i struje.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

International Electrotechnical Commission (IEC) protokoli

- GOOSE i SV rade preko modela publisher/subscriber, bez mehanizma pouzdanosti koji bi osigurao da su podaci primljeni.
- IEC 61850 ima nekoliko poznatih sigurnosnih nedostataka koji se mogu iskoristiti za kompromitaciju kontrolnog sistema.
- Autentifikacija je ugrađena u MMS, ali je zasnovana na lozinkama sa čistim tekstom, dok autentifikacija nije dostupna u GOOSE ili SV.
- Firmver obično nije potpisan, što znači da ne postoji način da se provjeri njegova autentičnost ili integritet.
- GOOSE i SV imaju ograničen integritet poruke, što olakšava lažno predstavljanje publishera.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

International Electrotechnical Commission (IEC) protokoli

- Kada je standard prvi put objavljen, postojale su minimalne sigurnosne mogućnosti u ovim protokolima, što je riješeno pomoću IEC 62351 uvođenjem dobro poznatih mjera sigurnosti zasnovanih na IT-u, kao što je razmjena certifikata.
- EC 60870 se široko koristi za SCADA daljinsko upravljanje u Evropi, posebno u elektroenergetskoj industriji, i za široko geografski raširene sisteme upravljanja.
- Dio 5 standarda opisuje komunikacione profile koji se koriste između krajnjih tačaka za razmjenu poruka daljinske kontrole.

Izazovi sigurnosti OT

Nesigurni operativni protokoli

Drugi protokoli

- Ponekad su rasprave o sigurnosti industrijskih sistema samo fokusirane na protokole industrijske kontrole.
- Ovaj pristup je problematičan jer je potrebno identifikovati sve aspekte saobraćaja koji prolazi kroz mrežu prije implementacije bilo koje vrste kontrola ili sigurnosnih mjera u njoj.
- Od posebne važnosti su pravilno računovodstvo, rukovanje i razumijevanje najosnovnijih protokola, transportnih mehanizama i temeljnih elemenata svake mreže, uključujući ARP, UDP, TCP, IP i SNMP.
- Neka specijalizovana okruženja poput IoT mogu imati i druge kontrolne protokole.
- IoT mreže dosežu sve do pojedinačnih senzora, tako da se koriste protokoli poput CoAP i DTLS, što se mora uzeti u obzir.

Izazovi sigurnosti OT

Nesigurnost uređaja

- Osim komunikacionih protokola i kontrolnih sistema koji se koriste, sami elementi upravljanja i komunikacije su ranjivi.
- Prije 2010. godine, sigurnosna zajednica je posvećivala malo pažnje industrijskom računarstvu, i kao rezultat toga, OT sistemi nisu "preboljeli" sigurnosne probleme kao IT sistemi.
- Da bi se razumjela priroda nesigurnosti uređaja, važno je primijetiti da je većina sigurnosnih problema bila na višim nivoima operativne mreže, uključujući kontrolne sisteme kojima se vjeruje da upravljaju postrojenjima, prenosnim sistemima, naftovodima ili bilo kojom drugom kritičnom funkcijom koja je u upotrebi.

Izazovi sigurnosti OT

Nesigurnost uređaja

- Nije teško razumjeti zašto se takvi sistemi često smatraju ranjivim.
  - Mnogi sistemi koriste softverske pakete koji se lako mogu preuzeti i protiv kojih se može raditi.
  - Ovi sistemi rade na uobičajenom hardveru i standardnim operativnim sistemima, kao što je Microsoft Windows.
  - Windows i komponente koje se koriste unutar tih aplikacija dobro su poznati istraživačima sigurnosti koji su tradicionalno fokusirani na IT. Malo je potrebe za razvojem novih alata ili tehnika kada su oni koji su već dugo postojali dovoljno adekvatni da probiju odbranu mete.
  - Stuxnet, najpoznatiji od industrijskih kompjuterskih napada, u početku je bio uspješan jer je mogao iskoristiti ranije nepoznatu ranjivost u Windows-u.

Izazovi sigurnosti OT

Nesigurnost uređaja

- Zajednica proizvođača ICS-a zaostaje za IT kolegama u pogledu bezbjedonosnih mogućnosti i praksi, kao i saradnje sa nezavisnim istraživačima bezbednosti.
- Ipak, ova situacija počinje da dobija značajan fokus u industriji i poboljšava se kroz niz nedavnih inicijativa dizajniranih da se službeno pozabave bezbjedonosnim ranjivostima i testiranjem sistema u industrijskom okruženju.
- Iako postoje neki formalni standardi, kao što su ISO/IEC 15408 (Zajednički kriterijumi), ISO/IEC 19790, i nekoliko drugih, ostaje malo formalnih entiteta za testiranje bezbednosti.
- Osim formalnog testiranja, postoji malo regulatorne primjene uobičajenih kriterijuma koji se odnose na testiranje sigurnosti uređaja.

Izazovi sigurnosti OT

Nesigurnost uređaja

- Ne tako davno se na istraživačku zajednicu sigurnosti gledalo kao na prijetnju, a ne kao na cijenjenu i često besplatnu uslugu za razotkrivanje potencijalnih opasnosti.
- Iako se situacija poboljšala, operativni napori i dalje značajno zaostaju za inicijativama zasnovanim na IT-u, kao što su programi nagrađivanja za greške i napredni programi za pripremu ranjivosti, u skladu sa nečim poput *Microsoft Active Protections Program* (MAPP).
- U industrijskom području ne postoje čak ni paralele sa zakonima koji štite privatne podatke pojedinaca.
- Dok mnoge države i zemlje zahtijevaju obavještenje ako su lični i finansijski podaci pojedinca moguće izloženi, izvan elektroprivrede, vrlo mali broj zakona zahtijeva prijavljivanje incidenata koji su mogli ugroziti živote.

Izazovi sigurnosti OT

Zavisnost od proizvođača

- Iako moderna IT okruženja mogu prenijeti poslovne operacije ili određene funkcije obrade ili skladištenja u cloud, manje je uobičajeno da se od proizvođača originalne opreme IT hardverskih sredstava traži da upravljaju opremom, pri čemu taj nivo zavisnosti od proizvođača nije neuobičajen u nekim industrijskim prostorima.
- Direktan pristup i pristup na zahtjev kritičnim sistemima u pogonu ili na terenu ponekad je napisan „direktno u ugovorima ili je potreban uz valjane garancije za proizvode.
- Ovo ima jasne prednosti u mnogim industrijama jer omogućava proizvođačima da daljinski upravljaju opremom i nadgledaju je i proaktivno upozoravaju kupca ako se problemi počnu pojavljivati.

Izazovi sigurnosti OT

Zavisnost od proizvođača

- Iako ugovori mogu biti napisani da opisuju zahtjeve za praćenje opreme i upravljanje s eksplicitnim izjavama o tome koja vrsta pristupa je neophodna i pod kojim uslovima, generalno ne uspijevaju da se pozabave pitanjima zajedničke odgovornosti za kršenje bezbjednosti ili procesima kako bi se osigurala bezbednost komunikacije.
- Takva zavisnost i kontrola od proizvođača nije ograničena na daljinski pristup.
- Upravljanje na licu mjesta za ne-zaposlene kojima će se odobriti pristup računarima i mreži je takođe potrebno, ali opet, kontrolni uslovi i izjave o podijeljenoj odgovornosti tek treba da se ispoštuju.

Izazovi sigurnosti OT

Poznavanje sigurnosti

- U industrijskom operativnom prostoru, tehnička ulaganja su prvenstveno u povezivanje i računarstvo, dok je vidljivo manje ulaganja u sigurnost u odnosu na IT sektor.
- Drugi relevantan izazov u OT u smislu sigurnosne stručnosti je relativno starija radna snaga u industriji.
- Nove tehnologije povezivanja se uvode u OT industrijska okruženja koja zahtijevaju najnovije vještine, kao što su TCP/IP, Ethernet i bežično povezivanje koje brzo potiskuju serijski zasnovane naslijeđene tehnologije.
- Brza ekspanzija proširenih komunikacionih mreža i potreba za radnom snagom koja je svjesna industrijske kontrole stvara jednako ozbiljan jaz u svijesti o sigurnosti.

Izazovi sigurnosti OT

Poznavanje sigurnosti

- Ovaj jaz u poznavanju OT sigurnosti se aktivno rješava.
- Obrazovanje za industrijsko sigurnosno okruženje je u stalnom porastu, posebno u energetici, gdje propisi kao što su NERC CIP (CIP 004) i IEC 62351 (01) zahtijevaju stalnu obuku.
- Zbog važnosti sigurnosti u industrijskom prostoru, sve moguće tačke napada tretiraju se kao nesigurne.
- Nažalost, s obzirom na potencijalni ogroman javni uticaj provale ovih sistema, ostaje strah u vezi sa povezivanjem IT tehnologija i eksternih veza, uprkos ogromnom ulaganju u bezbjednost u ovim oblastima.
- Dovođenje industrijskih mreža do najnovijih i najsigurnijih nivoa je spor proces zbog dubokih istorijskih kulturnih i filozofskih razlika između OT i IT okruženja.

Praksa u sigurnosti OT

Purdue model za kontrolnu hijerarhiju

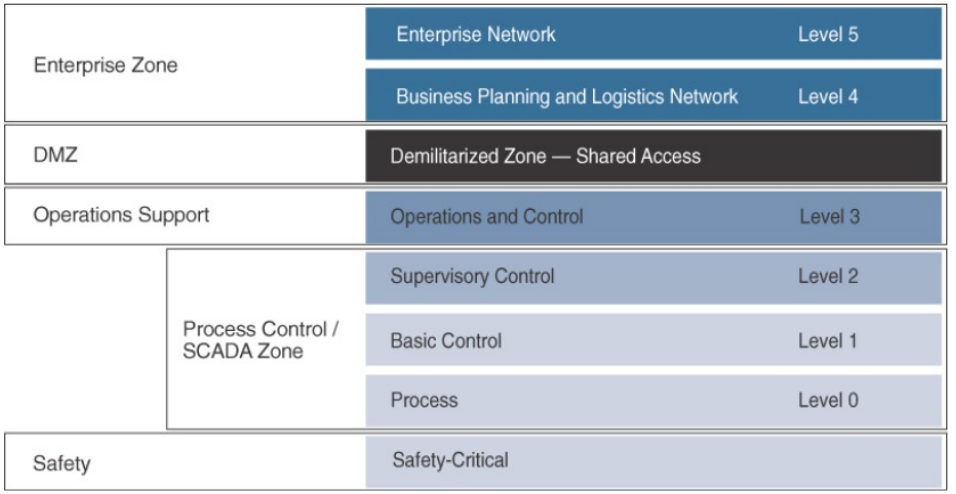
- IT informacije se obično koriste za donošenje poslovnih odluka, kao što su one u optimizaciji procesa, dok se OT informacije umjesto toga karakteristično koriste za donošenje fizičkih odluka, kao što je zatvaranje ventila, povećanje pritiska i tako dalje.
- Operativni domen takođe mora da se bavi fizičkom bezbjednošću i faktorima životne sredine kao dijelom svoje bezbjedonosne strategije što se obično ne povezuje sa IT domenom.
- Organizaciono, IT i OT timovi i alati su istorijski bili odvojeni, ali to je počelo da se mijenja i oni su počeli da se približavaju, što je dovelo do uvođenja tradicionalnih IT-centričnih rešenja za podršku operativnim aktivnostima.
- Sistemi kao što su firewall-i i IPS-ovi se koriste u IoT mrežama.

Praksa u sigurnosti OT

Purdue model za kontrolnu hijerarhiju

- Kako se granice između tradicionalno odvojenih OT i IT domena uklanjaju, oni moraju uskladiti strategije i bliže sarađivati kako bi osigurali sigurnost od kraja do kraja.
- Tipovi uređaja koji se nalaze u industrijskim OT okruženjima obično su mnogo bolje optimizirani za zadatke i operacije specifične za industrijski protokol od njihovih IT kolega.
- Industrijska okruženja se sastoje od operativnih i poslovnih domena.
- Da bi se razumjeli sigurnosni i mrežni zahtjevi za kontrolni sistem, potrebna je upotreba logičkog okvira za opisivanje osnovne kompozicije i funkcije.
- Purdueov model za kontrolnu hijerarhiju, je okvir koji se najčešće koristi u industrijskim okruženjima širom svijeta
- On segmentira uređaje i opremu prema hijerarhijskim nivoima funkcija i oblastima i ugrađen je u sigurnosni standard ISA99/IEC 62443.

Praksa u sigurnosti OT

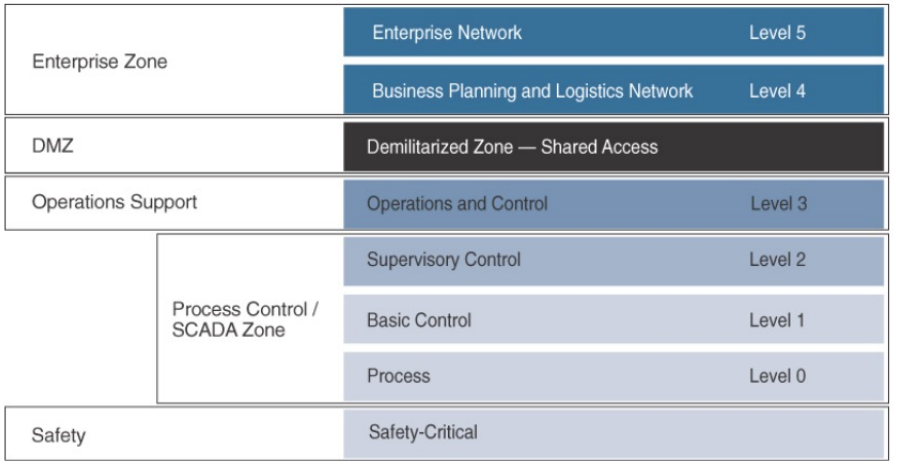


Purdue model za kontrolnu hijerarhiju

- Ovaj model identifikuje nivoe operacija i definiše svaki nivo.
- Preduzeća i operativni domeni su razdvojeni u različite zone i držani u strogoj izolaciji preko industrijske demilitarizovane zone (DMZ):
  - Zona preduzeća
    - Nivo 5: Mreža preduzeća: Na ovom nivou postoje aplikacije na korporativnom nivou kao što su planiranje resursa preduzeća (ERP), upravljanje odnosima sa klijentima (CRM), upravljanje dokumentima i usluge kao što su pristup Internetu i VPN ulazak iz spoljašnjeg sveta.
    - Nivo 4: Poslovno planiranje i logistička mreža: IT usluge postoje na ovom nivou „i mogu uključivati sisteme za planiranje, aplikacije protoka materijala, sisteme za optimizaciju i planiranje i lokalne IT usluge kao što su telefon, e-pošta, štampanje i sigurnosni nadzor.
  - Industrijska demilitarizovana zona
    - DMZ: DMZ pruža tampon zonu u kojoj se usluge i podaci mogu dijeliti između operativnih i poslovnih zona. Takođe omogućava jednostavnu segmentaciju organizacione kontrole. Podrazumijevano, nikakav saobraćaj ne bi trebalo da prolazi kroz DMZ; sve bi trebalo da potiče ili završava na ovom području.

Praksa u sigurnosti OT

Purdue model za kontrolnu hijerarhiju



- Operativna zona
  - Nivo 3: Operacije i kontrola: Ovaj nivo uključuje funkcije uključene u upravljanje tokovima rada za proizvodnju željenih krajnjih proizvoda i za praćenje i kontrolu cjelokupnog operativnog sistema. Ovo može uključivati planiranje proizvodnje, osiguranje pouzdanosti, optimizaciju kontrole na cijelom sistemu, upravljanje sigurnošću, upravljanje mrežom i potencijalno druge potrebne IT usluge, kao što su DHCP, DNS i mjerenje vremena.
  - Nivo 2: Nadzorna kontrola: Ovaj nivo uključuje zonske kontrolne sobe, status kontrolera, sistem upravljanja mrežom/aplikacijama i druge aplikacije povezane s kontrolom, kao što su interfejs čovjek-mašina (HMI).
  - Nivo 1: Osnovna kontrola: Na ovom nivou, kontroleri i IED-ovi, namjenski HMI i druge aplikacije mogu međusobno komunicirati kako bi pokrenuli dio ili cijelu kontrolnu funkciju.
  - Nivo 0: Proces: Ovdje uređaji kao što su senzori i aktuatori i mašine kao što su pogoni, motori i roboti komuniciraju sa kontrolerima ili IED uređajima.
- Sigurnosna zona
  - Kritična bezbjednost: Ovaj nivo uključuje uređaje, senzore i drugu opremu koja se koristi za upravljanje sigurnosnim funkcijama kontrolnog sistema.

Praksa u sigurnosti OT

Purdue model za kontrolnu hijerarhiju

- Jedna od ključnih prednosti projektovanja industrijske mreže u strukturiranim nivoima, kao i kod Purdue modela, je da omogućava ispravnu primjenu sigurnosti na svakom nivou i između nivoa.
- IT mreže se obično nalaze na nivoima 4 i 5 i koriste sigurnosne principe uobičajene za IT mreže.
- Niži nivoi su tamo gde se nalaze industrijski sistemi i IoT mreže.
- DMZ se nalazi između IT i OT nivoa.
- Da bi se zaštitili niži industrijski slojevi, sigurnosne tehnologije kao što su firewall, proxy serveri i IPS-ovi bi se trebali koristiti kako bi se osiguralo da se koriste samo ovlašćene veze iz pouzdanih izvora na očekivanim portovima.

Praksa u sigurnosti OT

Purdue model za kontrolnu hijerarhiju

- U DMZ-u, pa čak i između nižih nivoa, treba koristiti industrijske firewall-e koji poznaju OT kontrolne protokole kako bi se osigurao kontinuirani rad OT mreže.
- Iako sigurnosne ranjivosti potencijalno mogu postojati na svakom nivou modela, jasno je da zbog količine povezanosti i sofisticiranosti uređaja i sistema, viši nivoi imaju veće šanse za upad zbog šire površine napada.
- To ne znači da niži nivoi nisu toliko važni iz bezbjedonosne perspektive; prije, to znači da je njihova površina napada manja, i ako se tehnike ublažavanja pravilno implementiraju, potencijalno je manji uticaj na cjelokupni sistem.

Praksa u sigurnosti OT

OT mrežne karakteristike koje utiču na sigurnost

- Dok IT i OT mreže počinju da se približavaju, one i dalje zadržavaju mnoge različite karakteristike u smislu načina na koji rade i saobraćaja kojim upravljaju.
- Ove razlike utiču na to kako se prema njima postupa u kontekstu bezbjedonosne strategije.
  - IT mreže: U IT okruženju postoji mnogo različitih tokova podataka. Tokovi komunikacionih podataka koji potiču iz tipične IT krajnje tačke putuju relativno daleko. Oni često prolaze kroz mrežu kroz switcheve i na kraju dođu do skupa lokalnih ili udaljenih servera na koje se mogu direktno povezati. Podaci u obliku e-pošte, prenosa datoteka ili usluga štampanja vjerovatno će svi stići do centralnog centra podataka, gdje se na njih odgovara ili pokreće akcije u više lokalnih usluga, kao što je štampač. U slučaju e-pošte ili pretraživanja weba, krajnja tačka pokreće radnje koje napuštaju granice poslovne mreže.

Praksa u sigurnosti OT

OT mrežne karakteristike koje utiču na sigurnost

- OT mreže: Za poređenje, u OT okruženju (nivoi 0-3), obično postoje dvije vrste operativnog saobraćaja. Prvi je lokalni saobraćaj koji može biti sadržan u određenom paketu ili području kako bi se omogućilo lokalno praćenje i kontrola zatvorene petlje. Ovo je saobraćaj koji se koristi za procese u realnom vremenu (ili skoro u realnom vremenu) i ne mora napustiti nivoe kontrole procesa. Drugi tip saobraćaja se koristi za praćenje i kontrolu područja ili zona ili cjelokupnog sistema. SCADA saobraćaj je dobar primjer za to, gdje se informacije o udaljenim uređajima ili zbirne informacije iz funkcije dijele na nivou sistema tako da operateri mogu razumjeti kako funkcioniše cjelokupni sistem ili njegovi dijelovi. Oni tada mogu implementirati odgovarajuće kontrolne komande na osnovu ovih informacija.

Praksa u sigurnosti OT

OT mrežne karakteristike koje utiču na sigurnost

- Kada IT krajnje tačke komuniciraju, to su obično kratki i česti razgovori s mnogo veza.
- Priroda komunikacije je otvorena i gotovo svako može razgovarati s bilo kim drugim, na primjer putem e-pošte ili pretraživanja.
- Iako postoje jasne kontrole pristupa, većina tih kontrola je na nivou aplikacije, a ne na nivou mreže.
- U OT okruženju, komunikacija krajnje tačke je tipično od tačke do tačke, kao što je SCADA master prema SCADA slave-u, ili multicast ili broadcast, korišćenjem tipa modela publisher/subscriber.
- Komunikacija može biti TCP ili UDP ili neka treća.

Praksa u sigurnosti OT

OT mrežne karakteristike koje utiču na sigurnost

- Iako je mrežno mjerenje vremena u OT prostoru zasnovano na NTP/SNTP koji se koristi za podešavanje takta uređaja u odnosu na glavni izvor vremena, brojni slučajevi upotrebe zahtijevaju izuzetno precizan izvor vremena i izuzetno preciznu distribuciju vremena/sinhronizacije, kao i mjerljivu i konzistentna kašnjenja/varijacije kašnjenja.
- Neke industrijske aplikacije zahtijevaju mjerenje vremena putem IEEE 1588, PTP (*Precision Time Protocol*), tako da se informacije iz izvora i odredišta mogu precizno izmjeriti i uporediti u mikrosekundnim intervalima s komunikacionom opremom koja uvodi kašnjenja ne veća od 50ns.
- *Jitter* za slanje i primanje informacija mora biti minimizovan kako bi se osigurao ispravan rad.
- Poređenja radi, u biznis okruženju, govor se često smatra aplikacijom najvišeg prioriteta, sa tipičnim jednosmjernim kašnjenjem od 150 ms ili više.
- U brojnim operativnim okruženjima za naftu i gas, proizvodnju i elektroprivrede, kašnjenje mora biti ispod 10 mikrosekundi.
- Sigurnosni napadi koji uzrokuju kašnjenje, kao što su DoS napadi mogu uzrokovati kvar sistema isključivo ometanjem mehanizma za mjerenje vremena.

Praksa u sigurnosti OT

OT mrežne karakteristike koje utiču na sigurnost

- IT mreže su obično koriste najnovije tehnologije.
- Ove zrele moderne prakse umrežavanja su kritične za postizanje visokog stepena fleksibilnosti koji je potreban u IT okruženju.
- Virtuelno umrežavanje, virtuelni radni prostori i virtuelni serveri su uobičajeni.
- Vjerovatno je da postoji širok spektar tipova uređaja koji aktivno učestvuju u bilo kojoj mreži u bilo kojem trenutku što fleksibilna interoperabilnost čini kritičnom.
- Da bi se postigla interoperabilnost, obično postoji minimalna vlasnička komunikaciona aktivnost, a naglasak je tipično na otvorenim standardima.
- Prelazak na IPv6 se nastavlja, a mrežne usluge višeg reda, kao što je kvalitet usluge (QoS), su takođe uobičajene.
- Krajnje tačke upravljaju širokim brojem aplikacija od velikog broja različitih proizvođača.
- Otvorena priroda ovih računarskih sistema znači da širok spektar protokola prolazi kroz OT mrežu.

Praksa u sigurnosti OT

Sigurnosni prioriteti: integritet, dostupnost i povjerljivost

- Sigurnosni prioriteti su vođeni prirodom sredstava u svakom okruženju.
- U IT domenu, najkritičniji element i meta napada bile su informacije.
- U OT okruženju, kritična sredstva su učesnici procesa: radnici i oprema.
- Sigurnosni prioriteti se razlikuju na osnovu tih razlika.
- U IT postoje zakonske, regulatorne i komercijalne obaveze zaštite podataka, posebno podataka pojedinaca koji mogu ili ne moraju biti zaposleni u organizaciji.
- Ovaj naglasak na privatnosti fokusira se na povjerljivost, integritet i dostupnost podataka – ne nužno na sistem ili fizičku imovinu.
- Uticaj gubitka računarskog uređaja smatra se minimalnim u poređenju sa informacijama koje bi mogao da sadrži ili im omogući pristup.
- U OT gubitak uređaja zbog sigurnosne ranjivosti znači da se proizvodnja zaustavlja, a kompanija ne može obavljati svoju osnovnu operaciju.
- Gubitak informacija pohranjenih na ovim uređajima manje je zabrinjavajući, ali sigurno postoje povjerljivi skupovi podataka u operativnom okruženju koji mogu imati ekonomske posljedice, kao što su formulacije i procesi.

Praksa u sigurnosti OT

Sigurnosni prioriteti: integritet, dostupnost i povjerljivost

- Sigurnosni fokus je često vođen istorijom sigurnosnih uticaja koje je organizacija iskusila.
- U IT okruženju, najbolnija iskustva su obično bile kampanje upada u kojima se kritični podaci izdvajaju ili oštećuju.
- Rezultat je bilo značajno ulaganje u kapitalna dobra i ljude kako bi se smanjile ove vanjske prijetnje i minimizirali potencijalni unutrašnji zlonamjerni akteri.
- U OT istorija gubitaka zbog vanjskih aktera nije bila tako duga, iako je potencijal štete na ljudskim razmjerima očigledno znatno veći.
- Rezultat je da su sigurnosni problem proizašli više iz ljudske greške nego vanjskih napada.
- Interes i ulaganje u industrijsku sigurnost prvenstveno su bili u standardnim slojevima kontrole pristupa.
- Tamo gdje se OT u određenoj mjeri razilazio je da se naglasi kontrola sloja aplikacije između višeg nivoa kontrolera i prijemnog operativnog sloja.

Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

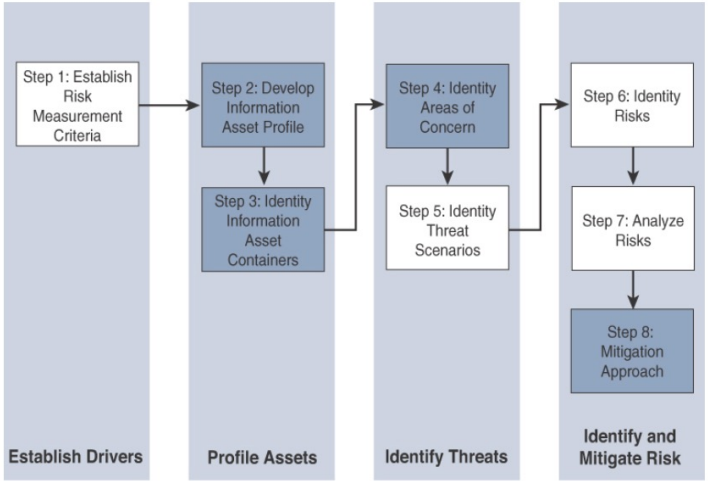
- U industrijskom okruženju, postoji niz standarda, smjernica i najboljih praksi koji su dostupni kako bi se razumio rizik i kako ga ublažiti.
- IEC 62443 je najčešće korišćeni standard na globalnom nivou u svim industrijskim vertikalama. Sastoji se od više dijelova, uključujući
  - 62443-3-2 za procjenu rizika i 62443-3-3 za temeljne zahtjeve koji se koriste za osiguranje industrijskog okruženja iz perspektive umrežavanja i komunikacija.
- ISO 27001 se široko koristi za organizacione ljude, procese i upravljanje bezbednošću informacija.
- Nacionalni institut za standarde i tehnologiju (NIST) obezbjeđuje niz dokumenata za kritičnu infrastrukturu, kao što je NIST Cybersecurity Framework (CSF).
- IEC 62351 je standard kibernetičke sigurnosti za elektroenergetske kompanije.
- Ključ za svako industrijsko okruženje je da se mora holistički pozabaviti bezbednošću, a ne fokusirati se samo na tehnologiju.
- Mora uključivati ljude i procese i treba da uključuje sve komponente ekosistema dobavljača koje čine kontrolni sistem.

Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*)

- OCTAVE je prošao kroz više iteracija.
- Verzija OCTAVE Allegro ima za cilj da bude lagani i manje opterećujući proces za implementaciju.
- Allegro pretpostavlja da snažan sigurnosni tim nije u pripravnosti ili odmah spreman da započne sveobuhvatnu sigurnosnu provjeru.
- Ovaj pristup i pretpostavke koje on donosi su sasvim prikladni, s obzirom na to da mnogim područjima operativne tehnologije na sličan način nedostaju ljudski resursi koji su usmjereni na sigurnost.



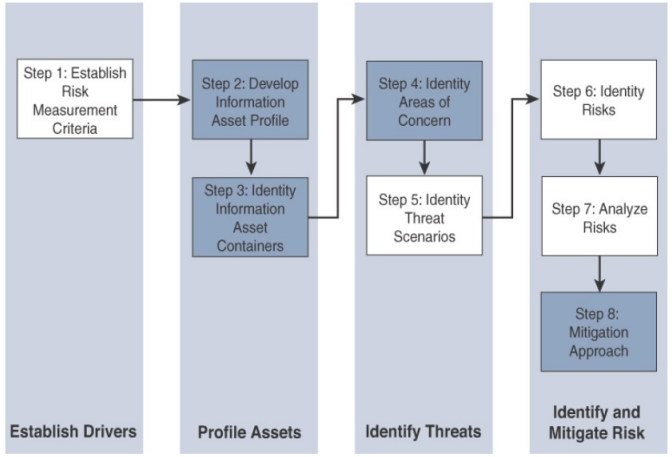
Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

- Prvi korak metodologije OCTAVE Allegro je uspostavljanje kriterijuma za merenje rizika.
  - OCTAVE pruža prilično jednostavan način da se to uradi sa naglaskom na uticaju, vrednosti i merenju.
  - Poenta postojanja kriterijuma mjerenja rizika je da se u bilo kojem trenutku u kasnijim fazama može izvršiti prioritizacija u odnosu na referentni model.
- Drugi korak je razvijanje profila informacione imovine.
  - Ovaj profil je popunjen sredstvima, prioritetima sredstava, atributima povezanim sa svakim sredstvom, uključujući vlasnike, eksplicitne sigurnosne zahtjeve i tehnološka sredstva.
  - Važno je naglasiti važnost procesa.
  - Potreba za zaštitom informacija ne nestaje, ali su operativna sigurnost i kontinuitet važniji.
  - Unutar ovog profila sredstava, procesi su višestruke podfaze koje dovršavaju definiciju sredstava.

  Neke od njih su jednostavno aktivnosti istraživanja i izvještavanja, kao što je identifikacija imovine i atributa povezanih s njim.



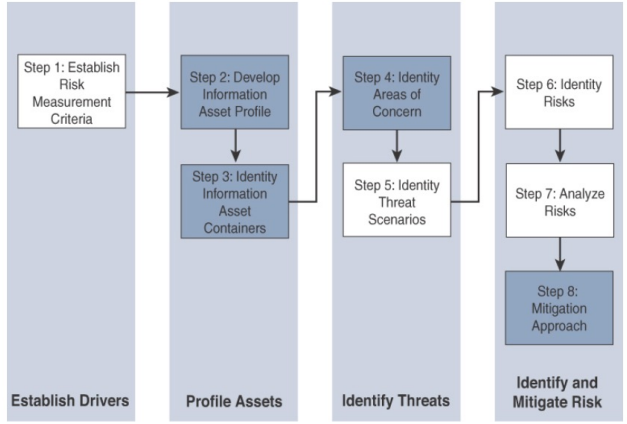
Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

- Treći korak je identifikacija kontejnera informacione imovine.
  - Ovo je opseg transporta i mogućih lokacija na kojima se informacije mogu nalaziti, što se odnosi na računarske uređaje i mreže pomoću kojih oni komuniciraju.
  - To može značiti i fizičke objekte kao što su štampani dokumenti ili čak osobe koje znaju informacije.
  - U OCTAVE, naglasak je na nivou kontejnera, a ne na nivou sredstava.
  - Vrijednost je smanjiti potencijalne inhibitore unutar kontejnera za rad informacija.

U OT svijetu, naglasak je na smanjenju potencijalnih inhibitora u kontejnerskom operativnom prostoru.



- Ako postoji neki atribut informacije koji je za njega endemičan, tada cijeli
- kontejner radi s tim atributom jer je informacija definišući element.
- U nekim slučajevima to možda nije tačno, čak i u IT okruženjima.
- Diskretni podaci na najnižem nivou mogu postati korisne informacije samo ako se vide u kontekstu ostatka podataka.
- Operativni podaci uzeti bez znanja o ostalim elementima takođe možda neće biti od posebne vrijednosti..

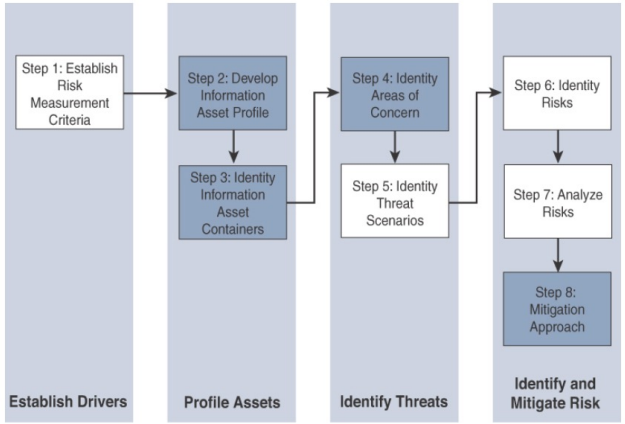
Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

- Četvrti korak je identifikovanje područja zabrinutosti.
  - U ovoj fazi, analitičari su fokusirani na poslovne slučajeve.
  - Analitičar razmatra profile rizika i ulazi u prethodno spomenutu analizu rizika.
  - To više nisu samo činjenice, već postoji i element kreativnosti koji može biti faktor u evaluaciji.
  - Istorija unutar i izvan organizacije je značajna.
  - Reference na slične operativne slučajeve upotrebe i incidente

sigurnosnih grešaka su razumne asocijacije.

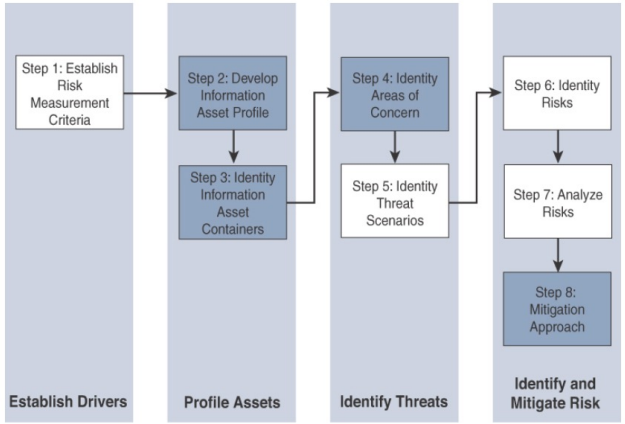


Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

- Peti korak je identifikacija scenarija prijetnji.
  - Prijetnje su široko (i ispravno) identifikovane kao potencijalni nepoželjni događaji.
  - Ova definicija znači da su rezultati i zlonamjernih i slučajnih uzroka održive prijetnje.
  - U kontekstu operativnog fokusa, ovo je vrijedno razmatranje.
  - Eksplicitna identifikacije aktera, motiva i ishoda.
  - Ovi scenariji su opisani u stablima prijetnji kako bi se pratio put do neželjenih ishoda, koji se zauzvrat mogu povezati s metrikom rizika.
- U šestom koraku se identifikuju rizici.
  - U okviru OCTAVE, rizik je mogućnost neželjenog ishoda.
  - Ovo je prošireno kako bi se fokusiralo na to kako se utiče na organizaciju.
  - Za fokusiraniju analizu, ovo se može lokalizovati, ali potencijalni uticaj na organizaciju mogao bi se proširiti izvan granica operacije.

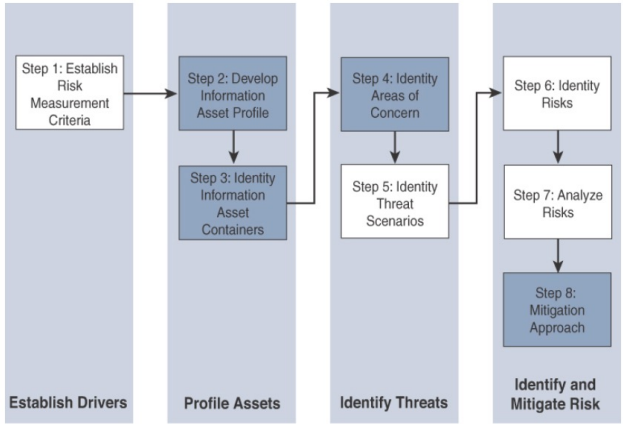


Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

- Sedmi korak je analiza rizika, uz napor uložen u kvalitativnu procjenu uticaja rizika pri čemu su kriterijumi mjerenja rizika definisani u prvom koraku eksplicitno unose u proces.
- Ublažavanje rizika se primjenjuje u osmom koraku.
  - Postoje tri rezultata ili odluke koje treba donijeti u ovoj fazi.
  - Jedan može prihvatiti rizik i ne učiniti ništa, osim dokumentovati situaciju, potencijalne ishode i razloge za prihvatanje rizika.
  - Drugi je da se rizik ublaži bilo kakvim kontrolnim naporom koji je potreban.
  - Vraćanjem kroz scenarije prijetnji do profila sredstava, uparivanje kompenzacijskih kontrola za ublažavanje tih parova prijetnja/rizik bi trebalo biti otkriveno i potom implementirano.
  - Konačna moguća radnja je odgađanje odluke, što znači da se rizik ne prihvata niti se ublažava.
  - To može podrazumijevati dalja istraživanja ili aktivnosti, ali to nije potrebno procesom.



Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

FAIR (Factor Analysis of Information Risk)

- The Open Group
- Dok je informaciona sigurnost u fokusu, baš kao i za OCTAVE, FAIR ima jasne primjene unutar operativne tehnologije.
- Kao i OCTAVE, on takođe dozvoljava nezlonamjerne aktere kao potencijalni uzrok štete, ali ide mnogo više da bi naglasio poentu.
- Za mnoge operativne grupe, to je dobrodošla potvrda postojećeg planiranja za vanredne situacije.
- Za razliku od OCTAVE, značajan je naglasak na imenovanju, sa definicijom taksonomije rizika kao vrlo specifičnom metom.
- FAIR stavlja naglasak i na nedvosmislene definicije i na ideju da su rizik i povezani atributi mjerljivi.
- Mjerljive metrike koje se mogu kvantifikovati su ključna oblast na kojoj se treba naglasiti, koja bi trebala biti pogodna za operativni svijet s bogatstvom operativnih podataka.

Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

FAIR (Factor Analysis of Information Risk)

- U svojoj osnovi, FAIR ima definiciju rizika kao vjerovatnu učestanost i vjerovatnu veličinu gubitka.
- Sa prethodnom definicijom, pojavljuje se jasna hijerarhija podelemenata, pri čemu je jedna strana taksonomije fokusirana na učestanost, a druga na veličinu.
- Ravnomjerna učestanost gubitka rezultat je djelovanja agenta prijetnje na imovinu i rezultirajući gubitkom za organizaciju.
- Ovo se dešava sa datom frekvencijom koja se zove učestanost događaja prijetnje (TEF), u kojoj određeni vremenski okvir postaje vjerovatnoća.
- Postoji više pod-atributa koji definišu učestanost događaja, a svi se mogu razumjeti pomoću nekog oblika mjerljive metrike.
- Učestalosti događaja prijetnje se primjenjuju na ranjivost.
- Ranjivost ovdje nije nužno neka slabost računarskog sredstva, već je šire definisana kao vjerovatnoća da će ciljano sredstvo propasti kao rezultat primijenjenih radnji.

Praksa u sigurnosti OT

Formalne strukture analize rizika: OCTAVE i FAIR

FAIR (Factor Analysis of Information Risk)

- Druga strana taksonomije rizika je veličina vjerovatnog gubitka, koja kvantifikuje uticaje, s naglaskom opet na mjerljivim metrikama.
- FAIR specifikacija čini poentom da se naglasi koliko prolazne neke od ovih procjena troškova mogu biti, a to bi zaista mogao biti slučaj kada je sigurnost informacija cilj diskusije.
- Na sreću operatera OT, značajan naglasak na operativnoj efikasnosti i analizi čini razumijevanje i kvantifikovanje troškova mnogo lakšim.
- FAIR definiše šest oblika gubitka, od kojih četiri eksterno fokusirana i dva interno fokusirana.
- Od posebne vrijednosti za operativne timove su produktivnost i gubitak zamjene.
- Gubitak odgovora se takođe razumno mjeri, sa novčanim kaznama i presudama koje je lako izmjeriti, ali je teško predvidjeti.
- Konačno, konkurentska prednost i reputacija su najmanje mjerljivi.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

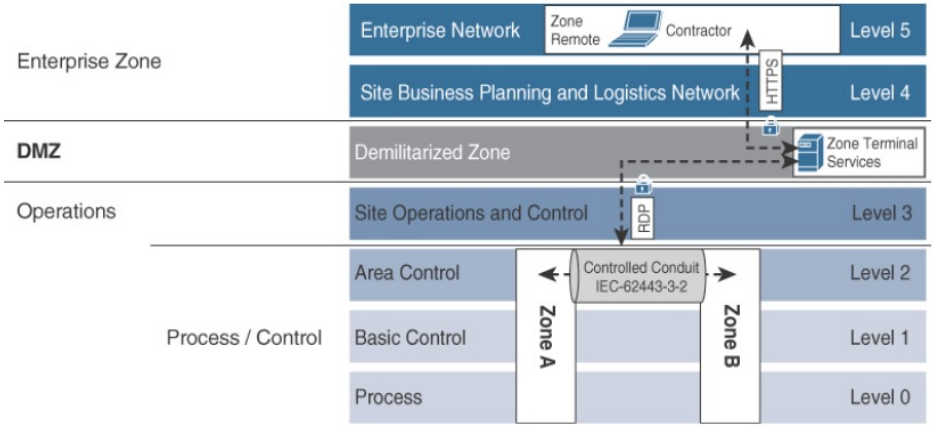
- Cilj stručnjaka za sigurnost je da bezbjedno osigura okruženje za koje je odgovoran.
- Za operativnog tehnologa ovaj proces je drugačiji jer se prioriteti i sredstva koja treba zaštititi jako razlikuju od IT okruženja.
- Mnogi procesi koje koriste stručnjaci za IT sigurnost su validni i mogu se koristiti u OT okruženju.
- Ako postoji jedan ključni koncept koji treba shvatiti, to je da je sigurnost za IoT okruženje trajni proces u kojem se mogu napraviti koraci naprijed, ali ne postoji prava ciljna linija.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- S obzirom na to da su mreže, računari ili operativni elementi u tipičnom IoT-u ili industrijskom sistemu vjerovatno postojali dugi niz godina i s obzirom da fizički izgled u velikoj mjeri definira operativni proces, ovaj fazni pristup uvođenju moderne mrežne sigurnosti započinje vrlo skromnim koracima.
- Kao prvi korak, mora se analizirati i osigurati osnovni dizajn mreže.
- Većina automatizovanih procesnih sistema ili čak hijerarhijskih sistema za distribuciju energije imaju visok stepen korelacije između dizajna mreže i operativnog dizajna.
- Osnovno je načelo ISA99 i IEC 62443 da funkcije trebaju biti segmentirane u zone (ćelije) i da komunikacija koja prelazi granice tih zona treba biti osigurana i kontrolisana kroz koncept vodova.



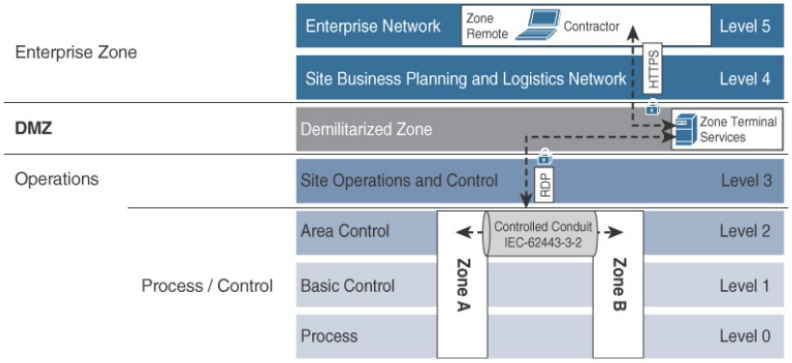
- Stručnjak za sigurnost treba da izuči stanje mreže i svih komunikacijskih kanala.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Normalni procesi otkrivanja mreže mogu biti vrlo problematični za stariju mrežnu opremu.
- Proces otkrivanja u potrazi za poboljšanjem sigurnosti, sigurnosti i operativnog stanja može rezultirati degradacijom sva tri.
- S obzirom na to stanje, proces otkrivanja mreže može zahtijevati ručnu inspekciju fizičkih veza, počevši od najviše dostupne tačke agregacije i radeći sve do posljednjeg pristupnog sloja.
- Ova aktivnost otkrivanja mora uključivati pretragu bežičnih pristupnih tačaka.
- Radi smanjenja rizika, bilo koje mrežno mapiranje na



žici treba da se radi pasivno što je više moguće.

- Mnogo je vjerojatnije da će ovaj propisani proces

uspjeti u manjem zatvorenom okruženju kao što je pod postrojenja.

- U geografski distribuiranim okruženjima, možda neće

biti moguće pratiti mrežu i u takvim slučajevima, dugolinijske veze možda neće biti fizičke ili ih može prenositi telekomunikacioni provajder.

- Za te dijelove operativne mreže potrebno je eksplicitno partnerstvo s drugim subjektima.

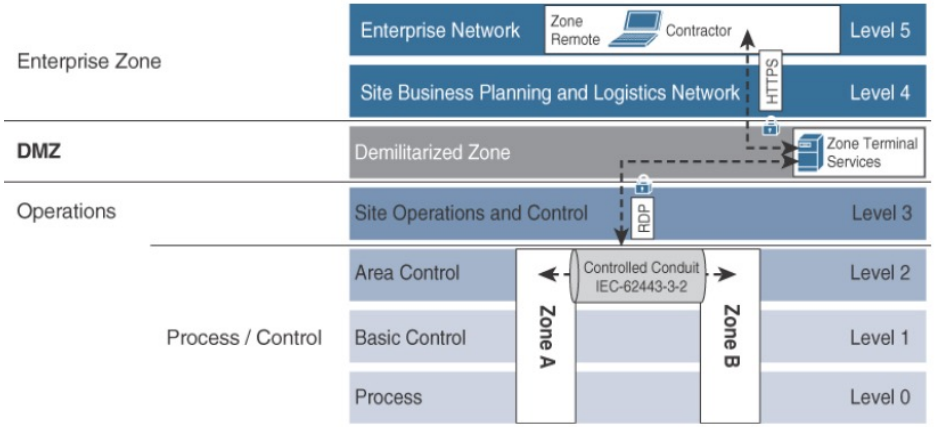
Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Sporedna aktivnost ovog procesa praćenja mreže je bilježenje stanja povezanosti fizičkih veza.
- Ovo nije samo provjera da se vidi koja su vlakna ili kablovi na kojim portovima, već da se razmotri korišćenje ili radno stanje drugih fizičkih veza, kao što su USB, SD kartica, alarmni kanal, serijski ili druge veze, na svakom mrežnom uređaju.
- Za modernija okruženja u kojima se koriste ažurirani mrežni uređaji i protokoli, alati kao što su NetFlow i IPFIX se takođ mogu koristiti za otkrivanje puteva mrežne komunikacije.
- Kako mrežno mapiranje dostigne tačku agregacije,

vrijedno je nastaviti do nivoa povezanog sredstva.

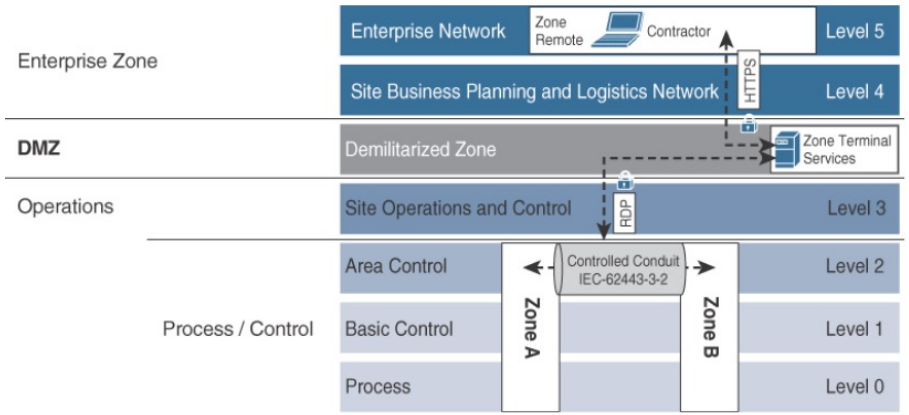


Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Obično, u IT okruženju, prva faza otkrivanja je fokusirana na sredstva povezana na mrežu.
- Sredstva ostaju kritična, ali iz perspektive efikasnosti i kritičnosti, uopšteno se preporučuje da se pronađu putevi podataka u i između zona (ćelija) umjesto serijske veze između uređaja unutar zone.
- Jedna stvar na koju treba stalno paziti je uvijek opasna, nesigurna i česta nedokumentovanost.
- Svaki fizički port koji nije fizički zaključan ili nema primjenjivu politiku zaštite je prijetnja.
- Nakon što je mreža fizički mapirana, sljedeći korak je izvođenje analize povezivanja kroz ARP tabele switch-a i rutera i DHCP zahtjeve unutar mrežne infrastrukture.
- Ovo bi trebalo pomoći da se dodatno rasvijetli dobra ili loša povezanost.
- Podaci o firewall-u i mrežnoj infrastrukturi mogu doprinijeti razumijevanju koji uređaji komuniciraju s drugim uređajima i putevima saobraćaja preko kojih se to radi.



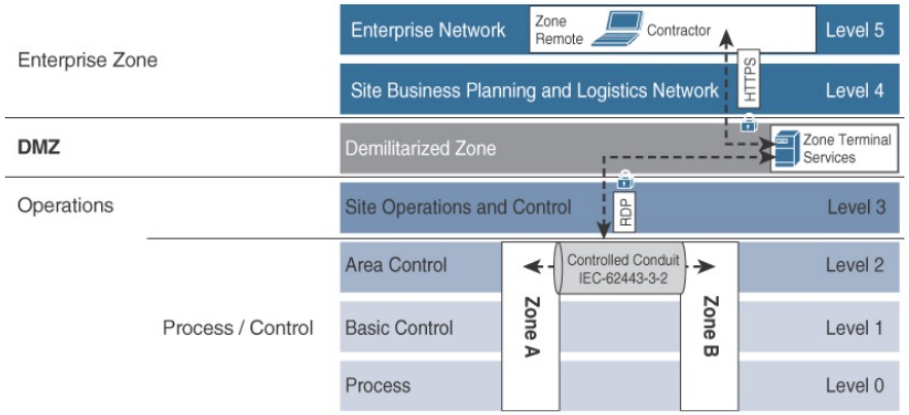
- U ovoj fazi, mreža bi trebala biti razumno dobro shvaćena i pripremljena za sigurno povezivanje.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Moderna mrežna oprema nudi skup mogućnosti kontrole pristupa i sigurnih komunikacja.
- Počevši od nivoa ćelije/zone, važno je osigurati da postoji jasna ulazna/izlazna tačka agregacije za svaku zonu.
- Ako su komunikacioni obrasci dobro identifikovani, može se primijeniti politika kontrole pristupa da se upravlja ko i šta može ući u te fizičke dijelove procesa.
- Ako nije lako eksplicitno kontrolisati saobraćaj, treba početi sa aktivnostima samo za upozorenje.
- S vremenom bi trebali biti dovoljno sigurni u svoje znanje da bi se primjenjivale kontrole.
- Na uzvodnim nivoima, treba uzeti u obzir kontrole saobraćaja kao što je zaštita od uskraćivanja usluge (DoS), aktivnosti normalizacije saobraćaja i kontrole kvaliteta usluge



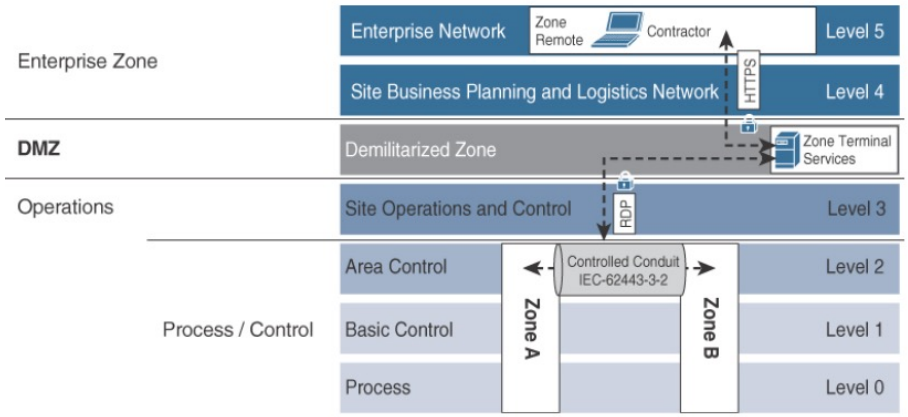
- Cilj je osigurati da ovi agregirani segmenti saobraćaja prenose saobraćaj visokog prioriteta bez prepreka.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Mrežna infrastruktura također treba da obezbijedi mogućnost da se osigura komunikacija između zona putem obezbeđenih vodova.
- Primarna metoda je šifrovana komunikacija u obliku virtuelnih privatnih mreža (VPN).
- VPN-ovi mogu biti u više oblika, kao što su site-to-site, što bi bilo prikladno između komunalne podstanice i kontrolnog centra, ili možda u komunikaciji od ćelije do ćelije.
- Kontrole daljinskog pristupa mogu se uspostaviti u više ad hoc situacija i koristiti pogodnost VPN-ova baziranih na pretraživaču sa VPN-ovima zasnovanim na *Secure Sockets Layer* (SSL).
- Ako problemi sa kašnjenjem nisu posebno veliki, modu se koristiti hop-by-hop šifriranje sigurnosti kontrole pristupa medijima (MACSec) kako bi se omogućili potencijalne kontrole i vidljivost na ključnim vezama.

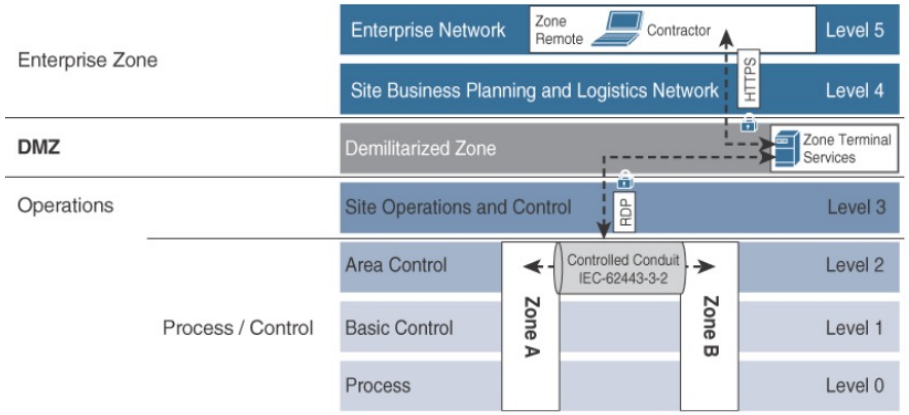


Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Sljedeća faza otkrivanja trebala bi biti usklađena sa softverom i konfiguracijama sredstava na mreži.
- U ovom trenutku, prava i uloge mrežnog administratora mogu biti nedovoljne za pristup potrebnim informacijama.
- Svakako, mrežna infrastruktura i njen status su unutar pogleda mrežnog administratora, ali pojedinačna sredstva vjerovatno nisu.
- U ovom trenutku za uspjeh je potrebna organizaciona saradnja.
- Za iskusnog IT-baziranog mrežnog stručnjaka ovo nije neobična situacija.
- Vrlo je uobičajeno, posebno u većim preduzećima, vidjeti razdvajanje odgovornosti i kontrola između komunikacionog transporta i sredstava na koje su povezani.



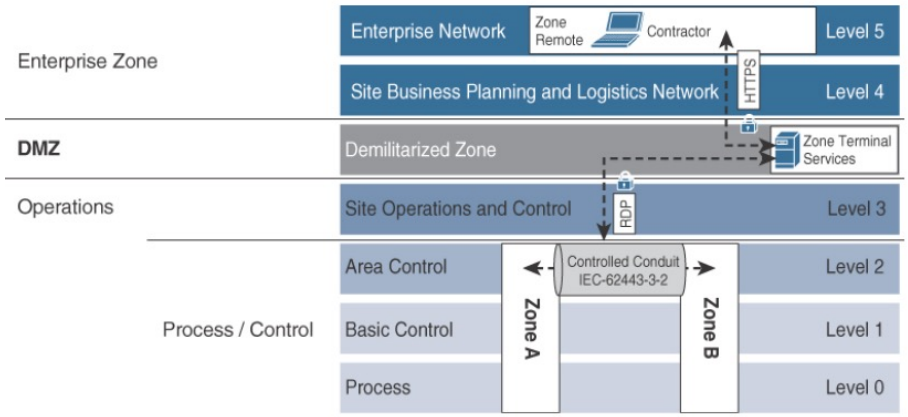
- Na operativnom nivou, potrebna je slična saradnja sa onima koji su odgovorni za održavanje imovine OT.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Osigurana mrežna infrastruktura i imovina

- Postoje razumni izvori informacija koji opisuju stanje konfiguracije OT sredstava.
- Kontrolni sistemi povezani sa procesima sadrže istorijske podatke koji opisuju šta je povezano i šta ta sredstva rade.
- Pregled istorijskih podataka treba da pruži ideju o tome koja su sredstva prisutna i koje operacije se na njima izvode, a trebalo bi da identifikuje stvari kao što su ažuriranja firmvera i zdravstveno stanje.
- Količina podataka za analizu može biti izazovna, ali ako je pravilno organizovana, bila bi dragocjena za razumijevanje funkcionisanja imovine.
- Sa završenim početnim inventarom imovine, može se pokrenuti analiza rizika na osnovu mreže i imovine i odrediti početni opseg sigurnosnih potreba.



Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Sljedeća faza je proširenje sigurnosnog otiska uz fokusiranu sigurnosnu funkcionalnost.
- Cilj je osigurati vidljivost, i sigurnost saobraćaja u mreži.
- Vidljivost pruža razumijevanje ponašanja primjene i komunikacije.
- Uz vidljivost, može se postaviti radnje politike koje odražavaju željena ponašanja za sigurnost među zonama i vodovima.
- Dok mrežni elementi mogu pružiti pojednostavljene prikaze sa istorijom povezivanja ili nekom vrstom podataka o toku, pravo razumijevanje dobija se uvidom unutar paketa na mreži.
- Ovaj nivo vidljivosti se obično postiže tehnologijama duboke inspekcije paketa (DPI), kao što su sistemi za otkrivanje/prevenciju upada (IDS/IPS).
- Ove tehnologije se mogu koristiti za otkrivanje mnogih vrsta saobraćaja od interesa, od jednostavne identifikacije o tome šta aplikacije govore, preko toga da li je komunikacija zamagljena, do toga da li su eksploatacije usmjerene na ranjivosti, do pasivnog identifikovanja sredstava na mreži.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- S ciljem identifikacije sredstava, IDS/IPS može otkriti kakva su sredstva prisutna na mreži.
- Pasivni programi za identifikaciju OS mogu uhvatiti obrasce koji otkrivaju osnovne operativne sisteme i druge aplikacije koje komuniciraju na mreži.
- Organizacioni jedinstveni identifikator (OUI) u uhvaćenoj MAC adresi, koji je mogao doći iz istraživanja ARP tabele, je još jedan način izlaganja.
- Zajedno sa fizičkim i istorijskim podacima spomenutim ranije, ovo je vrijedan alat za proširenje inventara imovine bez opasnog ili nametljivog pokretanja kritičnih sistema.
- IDS/IPS sistemi mogu otkriti i protokole specifične za aplikaciju.
- Za aplikacije sličnije IT-u, korisnički agenti su korisni, ali tradicionalno kombinacije brojeva portova i drugih diferencijatora protokola mogu doprinijeti identifikaciji.
- Neke aplikacije imaju ponašanja koja se nalaze samo u određenim izdanjima softvera.
- Poznavanje tih razlika može pomoći da se odredi verzija softvera koja se pokreće na određenom materijalu.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Unutar aplikacija i industrijskih protokola su dobro definirane komande i, često, pridružene vrijednosti parametara.
- IDS/IPS se može konfigurisati da identifikuje te naredbe i vrijednosti kako bi saznao koje se radnje preduzimaju i koje povezane postavke se mijenjaju.
- Sve ove radnje mogu se obaviti iz nenametljivog scenarija implementacije.
- Moderne DPI implementacije mogu raditi van opsega iz raspona ili dodira.
- Gledanje kopija paketa nema uticaj na performanse saobraćaja ili kašnjenje.
- To je najsigurnije sredstvo za sticanje dubokog uvida u aktivnosti koje se dešavaju na mreži.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Vidljivost i razumijevanje mrežne povezanosti otkrivaju informacije potrebne za pokretanje aktivnosti kontrole pristupa.
- Kontrola pristupa se obično postiže listama za kontrolu pristupa (ACL), koje su dostupne na gotovo svim modernim mrežnim uređajima.
- Za poboljšanu skalabilnost, bio bi poželjniji namenski firewall.
- Pružanje snažne segmentacije i kontrole pristupa zoni je prvi korak.
- Kontrola pristupa, međutim, nije ograničena samo na tipične identifikatore adrese i protokola.
- Moderni firewall-i imaju sposobnost da razaznaju atribute povezane sa korisnikom koji pristupa mreži, omogućavajući da se kontrole stave i na element „ko".
- Kontrola pristupa se može uskladiti s aplikacijama i ponašanjem aplikacija.
- Opremljen pravim skupom alata, moderni OT stručnjak može osigurati da samo oni operateri u određenoj korisničkoj klasi mogu pokrenuti bilo kakve eksterne komande za to određeno sredstvo.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Sigurnost je posebna prednost jer se kontrolama aplikacije može upravljati na rubu ćelije/zone preko IDS/IPS-a.
- Iste tehnologije koje posmatraju ko i šta takođe mogu upravljati vrijednostima koje se prosleđuju na ciljano sredstvo.
- U scenariju proizvodnje gdje robot radi, može postojati područje u koje posjećuju radnici koji su unutar potencijalnog raspona rada robota.
- Raspon je jedinstven za fizički raspored ćelije, a promjene parametara mogu uzrokovati fizičku štetu radniku u postrojenju.
- Sa IDS/IPS, sistem može otkriti da vrijednost parametra prelazi sigurnosni raspon i djelovati u skladu s tim kako bi osigurao sigurnost radnika.
- Identifikacija prijetnji i zaštita je ključni atribut IPS-a koji koriste DPI.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- IPS-ovi imaju hiljade identifikatora prijetnji, koji se odnose na cijeli niz tipova sredstava gdje su poznate ranjivosti koje se mogu iskoristiti.
- U nekim slučajevima, priroda identifikatora prijetnje je dovoljno generička da se bavi uobičajenom tehnikom bez potrebe da se povezuje s određenom instancom aplikacije tipa ranjivosti.
- Prioriteti postavljanja namjenskih sigurnosnih uređaja razlikuju se u zavisnosti od percepcije rizika od strane stručnjaka.
- Ako je vidljivost nepotpuna i zabrinutost nalaže da je potrebno dodatno znanje prije kreiranja proaktivne odbrane, sigurnosni uređaj treba postaviti tamo gdje se taj jaz uočava.
- Važno je primijetiti da je proces sticanja vidljivosti ili rješavanja rizika dinamičan.
- Mreže se mijenjaju, a kako se znanje stiče, novi prioriteti (bilo u obliku vidljivih prijetnji ili smanjenja praznina) stvaraju nove tačke naglaska.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Odluka se neizbježno mora donijeti.
- Postavljanje u operativnu ćeliju je vjerovatno najfiniji granularni scenario raspoređivanja.
- Pod finim granularnim se podrazumijeva da je to najniži dio mreže koji daje pristup baziran na mreži najnižem nivou operativnih sredstava.
- Kao što je ranije spomenuto, priroda raspoređivanja - van opsega ili u liniji - zavisi o nivou udobnosti organizacije za in-line "operaciju i želji da se stvarno izvrši kontrola.
- U oba slučaja, industrijski sigurnosni uređaj treba da bude priključen direktno na switch, koji označava pristupnu tačku u ćeliji.
- Ova lokacija daje najveći nivo kontrole za sigurnosne kontrole, vidljivost i prijetnje.
- Ako je dizajn mreže pravilno segmentiran na jednu ulaznu tačku zone, onda je ovo optimalna lokacija za implementaciju.
- Iz sigurnosnih razloga, može se izvršiti kontrola aplikacije kako bi se osiguralo da promjene aplikacije neće dozvoliti opasne postavke.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Prijetnje se mogu ublažiti dok prolaze kroz uređaj, a saobraćaj koji ulazi i izlazi iz ćelije može biti vidljiv.
- Posebno vrijedna funkcija je omogućena ako sigurnosni uređaj može prekinuti VPN-ove prilikom obavljanja dubinske inspekcije paketa.
- Sigurna komunikacija, potencijalno od predstavnika dobavljača izvan organizacije, može se prekinuti na ulazu u uređaj i zatim pregledati.
- Vrijeme prekida bilo bi slično onome što bi se uradilo na switchu, a onda je inspekcija šta radi taj udaljeni korisnik koji pristupa mreži izvodljiva.
- Svaki potencijalni saobraćaj prijetnji može biti zaustavljen.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Ako zona/ćelija sadrži kritičnu infrastrukturu i potreban je daljinski rad, savjetuje se redundantna konfiguracija visoke dostupnosti i za mrežnu i za sigurnosnu infrastrukturu.
- Za svrhu čiste vidljivosti, optimalno bi bilo aktivirati mirroring na switch-u.
- U većini slučajeva, poželjna lokacija je uzvodno od switcha za pristup zoni/ćeliji između sloja agregacije i zonskog switcha.
- Možda je izvodljivo imati sigurnosni uređaj između sredstava zone i switcha za pristup zoni.
- Za šire, manje detaljne nivoe kontrole, poželjan pristup je postavljanje namjenskih sigurnosnih uređaja uzvodno od agregacionih switcheva.
- Ako mreža ima više zona koje prolaze kroz agregacioni switch sa uglavnom redundantnom funkcionalnošću, ali bez komunikacije između njih, ovo može biti efikasnija tačka implementacije.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- U nekom trenutku, funkcionalni sloj iznad najnižeg zonskog sloja postaje povezan na mrežu, a trebao bi postojati uređaj koji se nalazi između tih funkcija i njihovih OT uređaja u zonama/ćelijama.
- Na tom sljedećem sloju mogu postojati HMI ili drugi operativni alati nižeg nivoa.
- Iz sigurnosnih razloga, vrijedna je kontrolna tačka između tog sloja i ćelije.
- Na višem nivou mreže nalazi se dobar broj sredstava više funkcije, kao što su standardni mrežni elementi (na primjer, serveri direktorijuma, alati za praćenje mreže, daljinski pristup plus proxy serveri, serveri za štampanje, elementi sigurnosne kontrole).
- Više operativno fokusirana funkcionalnost uključuje elemente kao što su inženjerske radne stanice i aplikacije za kontrolu operacija.
- U zavisnosti od raznolikosti i mrežnih topologija, ove operativne strukture bi se mogle replicirati unutar vlastitih podzona (podmreža) na istom nivou.
- Možda postoji opravdanje za korišćenje namjenskog sigurnosnog uređaja između podzona, zavisno o potrebi kontrole pristupa, ali uglavnom je ovo zona kojoj su potrebne kontrole postavljene iznad i ispod.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Iznad najvišeg nivoa, preporučuje se namjenski sigurnosni uređaj sa kontrolama prijetnji usmjerenim na IT.
- Ako su ovdje hostovane aplikacije slične prirode onima koje se nalaze u IT okruženjima (na primjer, aplikacije zasnovane na Windows-u ili Linuxu), to zahtijeva zajedničku mrežnu infrastrukturu i pristup baziran na webu radi pravilne vidljivosti, kontrole i zaštite .
- Primjena takvih kontrola na sve ulazne tačke (iznad i ispod) je važna.
- Ne bi trebalo postojati pretpostavke da prijetnja usmjerena na IT može proizaći samo iz sloja IT/preduzeća iznad DMZ-a.
- Napadači se ne bi ograničili na takvo razmišljanje.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- OS i softverske komponente, koje su pri kraju životnog vijeka, postoje u operativnim okruženjima.
- Previše uobičajen i problematičan atribut takvih sistema je da dalje nadogradnje za sigurnosne propuste vjerovatno neće biti dostupne.
- Kako bi zaštitili te sisteme nakon njihovog zvaničnog datuma završetka podrške, koncept sloja „virtuelne nadogradnje" bi mogao biti moguć.
- Ideja je da se zaštite od ranjivosti mogu primijeniti putem mrežnog puta kojim ovi sistemi komuniciraju.
- Iako ovo nije zamjena za praćenje nadogradnji, to može biti pristup ublažavanju koji odgovara politici prihvatanja rizika kompanije.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Uvođenje namjenskih sigurnosnih uređaja

- Na logičnom rubu operativnog prostora nalazi se DMZ (demilitarizirana zona)—sigurnosna granica između dva različita računarska područja.
- Sredstva u ovoj oblasti imaju za cilj da premoste komunikaciju na siguran način između IT područja preduzeća i industrijskog OT područja.
- Sigurnost treba primijeniti i iznad i ispod ovog sloja.
- Sigurnost je stalan process na bilo kojoj lokaciji.
- Primijenjene politike i stečeno znanje nikada ne smiju stagnirati.
- Uslovi će se neizbježno promijeniti, tako da se sigurnosna implementacija, a ponekad i same mreže, moraju promijeniti da bi se prilagodile.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Konvergencija politika višeg reda i praćenje mreže

- Još jedna sigurnosna praksa koja dodaje vrijednost umreženom industrijskom prostoru je konvergencija, što je usvajanje i integracija sigurnosti preko operativnih granica.
- To znači koordinaciju sigurnosti i na IT i na OT strani organizacije.
- Konvergencijom IT i OT prostora se spaja, ili barem postoji aktivna koordinacija preko ranije različitih IT i OT granica.
- Iz sigurnosne perspektive, vrijednost slijedi argument da je većina novih mrežnih i računarskih tehnologija koje dolaze u operativni prostor prethodno pronađena i uspostavljena u IT prostoru.
- Takođe se očekuje da će biti tačno da će prakse i alati povezani sa tim novim tehnologijama vjerovatno biti zreliji u IT prostoru.
- Postoje napredne prakse za cijelo preduzeće koje se odnose na kontrolu pristupa, otkrivanje prijetnji i mnoge druge sigurnosne mehanizme koji bi mogli koristiti OT sigurnosti.
- Kao što je ranije rečeno, ključ je prilagoditi pristup tako da odgovara ciljanom okruženju.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Konvergencija politika višeg reda i praćenje mreže

- Vjerovatnije je da će za nekoliko područja biti potrebna neka vrsta koordinacije u IT i OT okruženjima.
- Dvije takve oblasti su daljinski pristup i otkrivanje prijetnji.
- Za daljinski pristup, većina velikih industrijskih organizacija prenosi komunikaciju preko IT mreže.
- Neke komunikacije, poput e-pošte i pretraživanja weba, očigledne su vrste komunikacije koje će vjerovatno doticati zajedničku IT infrastrukturu.
- Često proizvođači ili konsultanti kojima je potrebna neka vrsta udaljenog pristupa OT ureajim takođe prelaze IT stranu mreže.
- Imajući to u vidu, bilo bi od velike vrijednosti za OT sigurnosnog stručnjaka da koordinira politike kontrole pristupa od udaljenog inicijatora preko sigurnosnih slojeva okrenutih prema Internetu, preko jezgra mreže i do tačke primopredaje na industrijskoj demarkaciji i dublje, prema IoT uređajima.
- Upotreba zajedničkih kontrola pristupa i operativnih uslova olakšava i štiti mrežna sredstva u većem stepenu nego postojanje različitih grupa koje stvaraju ad hoc metode.
- Korišćenje informacija o lokaciji, sigurnosni stav uređaja ućesnika, korisnički identitet i atributi cilja pristupa su sve standardne funkcije koje moderni alati politike pristupa mogu koristiti.
- Takva sofisticiranost je relativno nova praksa u industrijskim okruženjima.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Konvergencija politika višeg reda i praćenje mreže

- *Network Security Monitoring* (NSM) je proces pronalaženja uljeza u mreži.
- Postiže se prikupljanjem i analizom indikatora i upozorenja radi određivanja prioriteta i istrage incidenata uz pretpostavku da, zapravo, postoji neželjeno prisustvo.
- Praksa NSM-a nije nova, ali se ne primjenjuje često ili dovoljno temeljno čak ni u velikim kompanijama.
- Mnogo je razloga za ovu neiskorišćenost, ali nedostatak obrazovanja i organizacionog strpljenja su uobičajeni razlozi.
- Da bi se pristup pojednostavio, postoji velika količina lako dostupnih podataka koji bi, ako se pregledaju, razotkrili aktivnosti uljeza.

Praksa u sigurnosti OT

Fazna primjena sigurnosti u operativnom okruženju

Konvergencija politika višeg reda i praćenje mreže

- Važno je napomenuti da je NSM proces u kojem se otkrivanje događa pregledom dokaza i radnji koje su se već dogodile.
- Ovo ne znači da je riječ o vrsti aktivnosti na istorisjkim podacima.
- Ako se prepozna da su aktivnosti upada, slično kao i sigurnost, stalni procesi, tada se vidi da postoji sličan skup faza kroz koje napadač mora proći.
- Primijenjeni alati će usporiti taj proces i uvesti mogućnosti za otkrivanje i sprječavanje napadača, ali rijetko postoji jedan događaj koji predstavlja napad u cijelosti.
- NSM je disciplina koja će najvjerovatnije otkriti opseg procesa napada i, zauzvrat, definisati obim za njegovu sanaciju.