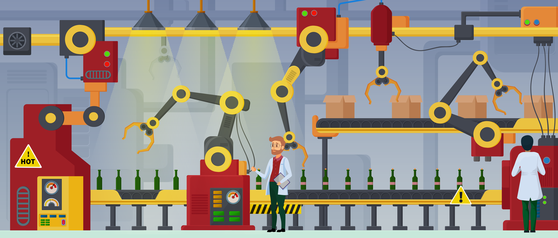

Kako (ne)varna so industrijska okolja in okolja kritične infrastrukture

Kibernetski napadi na OT okolja (specializirana informacijsko-komunikacijska okolja v industrijskih okoljih in okolja kritične infrastrukture, odgovorna za izvajanje procesov) so v porastu.

Prevladujejo ransomware oz. napadi z izsiljevalskimi virusi ter napadi na dobavne verige, ki povzročijo največ škode pri zagotavljanju neprekinjenega delovanja.

IoT naprave – najbolj prevladujoča točka vstopa napadalcev v omrežje, a pogosto spregledane, ko gradimo varnost.

Najbolj na udaru so okolja kritične infrastrukture

TRANSPORT

186 % porast tedenskih napadov med jun 20-jun 21

INDUSTRIJA

11 mio $ višina odkupnine (JBS Foods)

ZDRAVSTVO

113 mio $ poslovne škode (Scripps Health)

Prevladujoče grožnje

RANSOMWARE

Največ skrbi povzročajo napadi z izsiljevalskimi virusi z zahtevami po visokih odkupninah

AVTOMATIZACIJA STAVB

Fizični dostop, klimatizacija, ogrevanje - napad lahko povsem onemogoči poslovanje in delovanje sistemov

DOBAVNA VERIGA

Imajo zelo velik domet, saj lahko ena napadena rešitev/storitev prizadene ogromno končnih podjetij, ki jo uporabljajo

IoT BOTNETI

Omrežje kompromitiranih računalnikov, ki jih nadzoruje napadalec za izvajanje napadov (Meris, Emotet, BotenaGo)

Najbolj odmevne ranljivosti

Varnost naprav in rešitev v OT okoljih zaostaja za varnostjo, ki je običajna za IT okolja

+21 % RAST

Na novo odkritih ranljivosti

LOG4J

Zagotovo najbolj odmevna kritična **ranljivost Java knjižnice Apache Log4j**, ki napadalcu omogoča izvedbo poljubne programske kode na ranljivem sistemu ali krajo občutljivih informacij.

Posledice bodo podjetja čutila dalj časa – Log4j je del številnih komercialnih, odprtokodnih in lastnih aplikacij. **Mnoga podjetja niti ne vedo, da so izpostavljena tveganju.**

Zato je zelo pomembno, da imate seznam oz. podroben inventar programske opreme in aplikacij, ki uporabljajo ranljivo knjižnico, saj imate s tem ustrezen nadzor nad programsko opremo in lahko hitro izvedete ukrepe za zaščito.

OBLAČNE PLATFORME

So dragocena tarča napadalcev (Azure)

PROGRAMSKA OPREMA

Ki jo običajno najdemo v poslovnih okoljih

NADZORNI SISTEMI

Kamere in druge IoT naprave

Uspešne strategije za krepitev kibernetske varnosti v OT

Včasih smo se zanašali na fizično ločevanje procesnih sistemov t. i. "Air Gap", danes temu ni več tako, zato moramo **kibernetsko obrambo temu ustrezno prilagoditi**.

Spremljanje dogajanja v omrežju z razumevanjem, kaj je normalno delovanje, kaj pa odstopanje, nam pomaga hitro odkriti potencialne grožnje, jih povezati z anomalijami, prioritizirati alarme in tako ustrezno učinkoviteje ukrepati.

Bodite korak pred naprednimi grožnjami

Večplasten pristop k varnosti v OT okoljih vključuje poznavanje naprav, ki jih imate v OT omrežju, verzijo programske opreme in knjižnic, ki jih uporabljajo, odkrite kritične ranljivosti ter s čim oz. s kom naprave komunicirajo.

NEOVIRAN DOSTOP

Do vdelane strojne programske opreme naprav, ki se nahajajo v OT omrežju.

Možnost analiziranja naprav daje varnostnim inženirjem vse potrebne informacije, da določijo varnostni status naprave. **Pripravite seznam naprav**, do katerih ne morete dostopati oz. ocenite njihovega varnostnega statusa (PLC, IoT naprave...).

SPREMLJANJE OMREŽJA

Je eden ključnih gradnikov za obrambno strategijo.

Omogoča zgodnje zaznavanje anomalij – od začetne okužbe in kasnejšega poizvedovanja oz. prisluškovanja ter odpravo posledic napada.

Daje vam popoln pregled nad vašim kritičnim omrežjem (elementi in protokoli) z vidika kibernetske ogroženosti.

SEGMENTACIJA OMREŽJA

Skoraj vse oblike zlonamerne programske opreme se zanašajo na **bočno premikanje** po omrežju in s tem širijo okužbo na sisteme znotraj podjetja.

Zato je segmentacija v varnostna območja ključna taktika, ki **zavira širjenje zlonamerne programske opreme ali neavtorizirane prometa znotraj omrežja**.

Nadaljnji korak je mikrosegmentacija ali t. i. "Zero Trust" omrežje, ki popolnoma zaustavi širjenje zlonamerne programske opreme, saj se po omrežju lahko premika le promet, ki mu je to dovoljeno glede na omežno in varnostno politiko.

ZMANJŠANJE POVRŠINE NAPADA

Površina napada je tisti del sistema ali omrežja, ki je dostopen potencialnim napadalcem. Večja kot je, več je možnosti, da napadalci izkoristijo ranljivosti in tako pridejo v omrežje.

Ključne taktike za zmanjšanje površine napada:

- Segmentacija in "Zero Trust" omrežje
- Učinkovito upravljanje z viri in ranljivostmi
- Stalna izobraževanja in revizije postopkov

*** Informacije so povzete po poročilu Nozomi Networks Labs - OT/IoT Security Report, 2H 2021 Review.**

Zagotovite si napredno znanje in praktične izkušnje za vzpostavitev ali dvig kibernetske varnosti

Program 4-dnevnega specialističnega izobraževanja

SMART COM

Že vel kot 30 let delujemo na področju IT in smo eden izmed vodilnih sistemskih integratorjev v Jugovzhodni Evropi. Z ekipo vel kot 70 strokovnjakov in specialistov vzpostavljamo sodobna in zanesljiva komunikacijska omrežja, vpeljujemo hiperkonvergenčno infrastrukturo v podatkovne centre z enostavnim prehodom v računalniški oblak in varnostne rešitve za zaščito pred naprednimi kibernetskimi grožnjami. Z vpeljavo tehnoloških rešitev, ki temeljijo na strojnem učenju in umetni inteligenci ter avtomatizacijo in orkestracijo poskrbimo za zaščito IT in OT infrastrukture.

Smart Com d.o.o., Brnčičeva 45, 1231 Ljubljana - Črnuče
tel.: 01 561 16 06, info@smart-com.si

www.smart-com.si