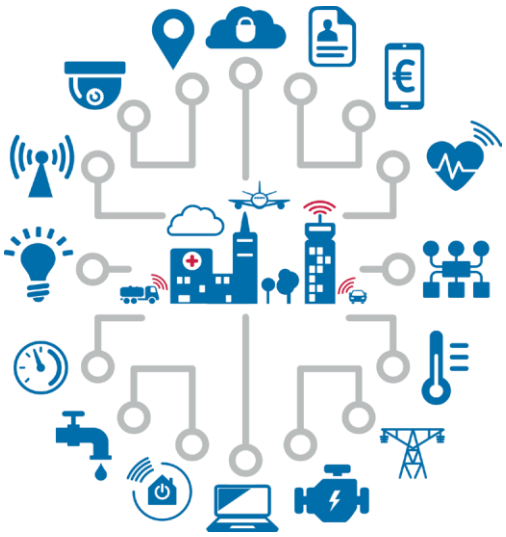
IoT i izazovi kibernetičke sigurnosti

Iotizacija – jesmo li pripravni?



Slika 1: IoT ekosustav i mogućnost primjene
(izvor: ENISA)

IoT uređaji su nestandardni pametni računalni uređaji koji se bežično povezuju na mrežu i imaju mogućnost prijenosa podataka. Osim što mogu komunicirati putem interneta, mogu se daljinski nadzirati i upravlja ti, te otvaraju brojne mogućnosti krajnje primjene. Posljednjih godina IoT uređaji doživljavaju streloviti rast te ne čudi činjenica kako je sve veća primjena zapažena u poslovanju, ali i u svakodnevnom životu. Mogućnosti primjene, brza implementacija i lako dosegljivi podaci rezultiraju snažnom pokrivenosti i sveobuhvatnom primjenom u ekosustavu. Je li pred nama nova era – Iotizacije?

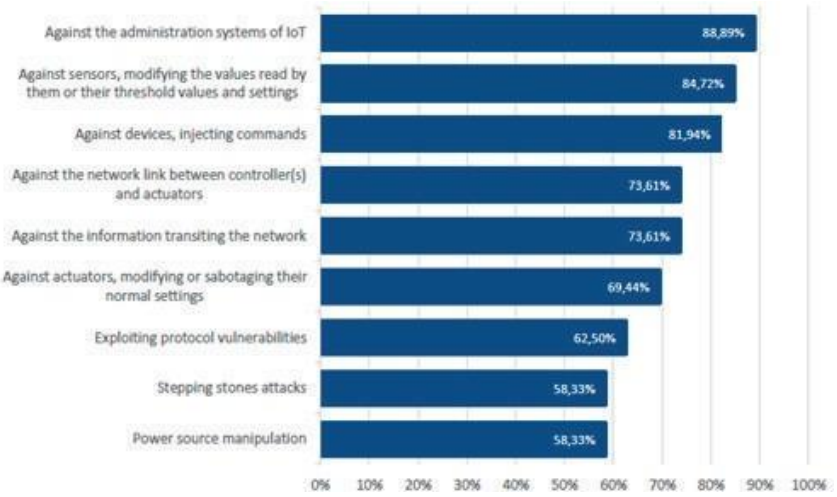
Recentna istraživanja idu u prilog naše tvrdnje, te vodeće analitičke kuće predviđaju snažan rast primjene IoT uređaja:

- Prema Gartneru, na svijetu će do 2020. godine biti u uporabi 20,4 milijarde IoT uređaja, a više od 65% tvrtki usvojit će IoT proizvode.
- IDC predviđa da će do kraja 2019. godine IoT doseći 745 milijardi USD i nadmašiti trilijun USD do 2022. godine.
- "CSOonline" navodi kako će do 2025. godine u upotrebi biti preko 75 milijardi IoT uređaja.

Sigurnost prije svega

Svim istraživanjima zajedničko je kako će rast biti eksponencijalan u narednih pet godina. Implementacija će biti jednostavnija, brza, a primjena šira i pokrivat će gotovo cijeli eko sustav. Upravo kroz taj rast sve veći značaj ima segment sigurnosti. Naime, IoT donosi velik broj novih prijetnji odnos- no ugroza uslijed korištenja pametnih uređaja koji često nisu adekvatno dizajnirani sa svim potrebnim sigurnosnim značajkama. Primjerice, nedostatak opcija za instaliran- je agenata, sigurnosna ažuriranja, neadekvatno upravljanje identitetima i pravima pristupa povećavaju broj sigurnosnih izazova s kojima se tvrtke ali i pojedinci moraju nositi.

U izvještaju "Zscaler" iz svibnja 2019. godine navodi se kako je čak 90% transakcija podataka na IoT uređajima nekodirano (primarno Set top boxes, pametni televizori i pisači). Jedno od zabrinjavajućih opažanja bilo je kako tvrtke na svojim mrežama imaju veliku količinu IoT uređaja jeftinijih razreda čime dodatno sigurnosno ugrožavaju vlastite poslovne procese, pogotovo ukoliko takvi uređaji nisu primjereno bili segmentirani i razdvojeni od mrežnih segmenata s kritičnim poslovnim sustavima i informacijama.



Slika 2: Kritični scenariji napada (izvor: ENISA)

Rastuća regulativa

Paralelno sa eksponencijalnim rastom tehnologija raste i broj raznih direktiva, regulativa i standarda iz domene sigurnosti.
European Union Agency for Network and Information Security (ENISA) je centar za ekspertizu mreža i informacijske sigurnosti unutar EU koji u svojim zadacima glede IoT-a i sigurnosti ističe:

- Promicanje usklađivanja IoT sigurnosnih inicijativa i propisa,
- Podizanje svijesti o potrebi kibernetičke sigurnosti u IoT,
- Definiranje sigurnosnih smjernica životnog ciklusa razvoja softvera i hardvera za IoT,
- Postizanje konsenzusa za interoperabilnost u IoT ekosustavu,
- Poticanje ekonomskih i administrativnih poticaja za sigurnost IoT-a,
- Uspostavljanje sigurnog upravljanja životnim ciklusom IoT proizvoda / usluga,
- Razjašnjenje odgovornosti među dionicima IoT-a.

Svjesna potrebnih zaštita, ENISA donosi i prepoznate tri glavne kategorija sigurnosnih mjera koje tvrtke moraju primjenjivati kako bi se efikasno zaštitile od prijetnji unutar svake IoT okoline:

- Donošenje politika i procedura,
- Organizacijske i procesne mjere, te ljudski resursi,
- Tehničke mjere.

IoT i sigurnosne mjere Verso Altima grupe

Verso Altima grupa u integraciji IoT tehnologija razvija softverska rješenja u svim segmentima implementacije IoT-a, od upravljačkih programa za uređaje i bazne stanice, pa sve do aplikacijskih sustava i sustava naplate. Do sada smo odradili tridesetak IoT projekata na četiri kontinenta, kao isporučitelj kompletnog rješenja ili kao dio konzorcija fokus- iran na LoRa komunikacijske infrastrukture. Sudjelovali smo u Smart City projektu za grad Shangai u Kini koji je u trenutku implementacije bio najveći Smart City projekt na svijetu. Recenti projekt koji je tim odradio je projekt Novog Mesta pod nazivom Pametno Novo Mesto koji uključuje mjerenje kvalitete zraka, m-parking, mjerenje potrošnje vode i plina te pametna rasvjeta izveden u suradnji s Telekomom Slovenije.

Kako se obraniti od hakerskih napada i prijetnji

Upravo informacijska sigurnost i SOC (sigurnosno operativni centar) čine snažnu obranu tvrtki naspram hakerskih napada i prijetnji koji nastoje otuđiti korisničke podatke, novac, poslovne tajne osobito alarmantno u IoT vremenima

Stručnjaci Verso Altima grupe u poslovanju uključuju razne elemente kako bi osigurali sigurnost unutar IoT ekosustava. Pritom ugrađuju i potrebne sigurnosne mjere vodeći računa o preporukama najboljih svjetskih praksi, standarda te sigurnosnih direktiva. Jedan od ključnih elemenata je uspostavljanje kvalitetnog sigurnosno operativnog centra ili SOC-a koji će osiguravatri pravovremenu detekciju, identifikaciju te analizu potencijalnih sigurnosnih prijetnji.

Nakon prve faze, stručnjaci će definirati i predvidjeti potre- bne obrane korisničkih sustava od napada i izvještavanje o incidentima koje podnese dionici procesa te osigurati pripravnost za eventualne buduće ugroze.
Donosimo primjere kibernetičkog napada u susjednoj Sloveniji: U kolovozu ove godine Ljubljanske ljekarne imale su problema s ransomwareom: nekoliko dana nije funkcionirao sustav e-recepti sustav (čak 60-ak poslovnica). Prvi dan nisu mogli izdavati lijekove, prebacivši se na papirnato poslovanje. Bilo je potrebno tjedan dana da se sustav upogoni, riješe naneseni problemi. S time da nije poznato kolika je bila tražena otkupnina.

Preporuke

Iako su IoT uređaji laka meta za kibernetičke napade preporuke su primjenjivati mjere sigurnosne zaštite kako bi se smanjile prijetnje i osiguralo sigurno korištenje i primjena. Minimalni koraci za smanjenje rizika:

- Promijeniti zadane sigurnosne postavke u što sigurnije. Ukoliko zaposlenici donose takve uređaje, sustavno primjenjivati kvalitetne politike lozinki,
- Segmentirati IoT uređaje u one mrežne s adekvatnim sigurnosnim razinama,
- Ograničiti pristup IoT uređajima s interneta što je više moguće. Blokirati sve nepo trebne servise na navedenim uređajima,
- Primjenjivati redovita sigurnosna ažuriranja softvera na IoT uređajima.