IMPLEMENTACIJA SODELOVALNIH VIDIKOV KIBERNETSKE VARNOSTI

Andrej Bregar[1]
[1] Informatika d.o.o., Vetrinjska ul. 2, 2000 Maribor
andrej.bregar@informatika.si

Zaradi vse naprednejših tehnik napadov in naraščajoče izpostavljenosti, kompleksnosti in povezljivosti informacijskih sistemov, organizacijskih okolij ter IT in OT integriranih infrastruktur postajajo ključnega pomena sodobni proaktivni pristopi k zagotavljanju kibernetske varnosti. Posebej pereči so kaskadni učinki kibernetskih incidentov, ki lahko ogrozijo povezane vire različnih deležnikov. Prav tako sta za učinkovito upravljanje kibernetskih tveganj in groženj ter za uspešno strateško in taktično odločanje bistvena dobra obveščenost ter souporaba znanja, postopkov in modelov za zaznavanje napadov in odzivanje nanje. V ospredje tako prihajajo sodelovalni vidiki kibernetske varnosti in pristopi k njihovi implementaciji. Ti vidiki vključujejo izmenjavo obveščevalnih informacij za odločanje, standardizacijo in izmenjavo odzivnih procedur, vzpostavitev skupnosti z vpletenostjo varnostnih operativnih centrov in nacionalnih CERT-ov, uporabo pretočnih kanalov in platform za upravljanje s kibernetskimi dogodki ter številne druge mehanizme.

V prispevku analiziramo ter sistematično predstavimo različne vidike, pristope in tehnološke rešitve za sodelovanje in koordinacijo med deležniki na področju kibernetske varnosti. Obravnavamo platforme in standarde, kot sta MISP in STIX/TAXII za izmenjavo obveščevalnih informacij. Izpostavimo prednosti in priložnosti, ki jih na področju kibernetske varnosti prinaša implementacija mehanizmov sodelovanja. Dotaknemo se tudi možnosti, ki jih odpira umetna inteligenca na podlagi modelov, ki avtomatizirajo in izboljšajo zaznavanje ter odzivanje na kibernetske incidente z učenjem iz deljenega znanja.

Poseben poudarek damo na predstavitev nekaterih specifičnih rešitev in dobrih praks, ki jih vpeljujemo v okolju kritične energetske infrastrukture. Tako smo z mehanizmi skupinskega odločanja nadgradili odločitveni proces in sistem za analizo ter izbiro premostitvenih ukrepov proti kibernetskim grožnjam in napadom, ki smo ga predstavili na lanskoletni konferenci DSI 2023. Ta pristop vpeljuje tehniko Delfi ter zlivanje informacij, pridobljenih z analizo in preiskavo kibernetskih groženj oziroma incidentov na več organizacijskih nivojih. To vključuje povezane deležnike, ki upravljajo soodvisne IT in OT vire, ter različne vloge, kot so vodje informacijsko-kibernetske varnosti, varnostni inženirji na nivojih L1 do L3, IT strokovnjaki in višji poslovni kader, s čimer lahko enakovredno zajamemo tehnične, organizacijske in strateške vidike implementacije ukrepov za proaktivno zagotavljanje kibernetske odpornosti.

Predstavimo tudi ogrodje za standardizacijo, izmenjavo in avtomatizirano izvajanje odzivnih procedur. To ogrodje temelji na standardu CACAO. Podpira izvedbo procesa, ki pokriva vse faze odzivanja na kibernetske incidente, omogoča operacionalizacijo odzivnih procedur na podlagi analize indikatorjev groženj ter vpeljuje pravila za koordinacijo med varnostnimi operativnimi centri in odzivnimi ekipami.

Nazadnje naslovimo mehanizme za izmenjavo obveščevalnih informacij o kibernetskih grožnjah. Z njimi se vključujemo v nacionalne in mednarodne skupnosti, izboljšamo reaktivno odzivanje na napade in proaktivno preprečevanje le-teh, podpremo odločanje na strateškem in taktičnem nivoju ter dvignemo splošno odpornost IT in OT infrastrukture. Ključna platforma, ki jo apliciramo v tem segmentu, je MISP (Malware Information Sharing Platform). Z namenom neposredne izvedbe zaščite jo lahko integriramo z ostalimi temeljnimi tehnologijami za kibernetsko varnost, kot so požarne pregrade ali sistemi SIEM in SOAR. Prav tako pa so pomemben uporabljen vir za izmenjavo informacij o ranljivostih ter tehnikah napadov in obrambe standardne javne baze in repozitoriji, ki vključujejo NVD, MITRE ATT&CK, CAPEC, CIS Security Controls idr.

Ključne besede: kibernetska varnost; varnostni procesi in tehnologije; odzivne procedure; koordinacija in sodelovanje; izmenjava obveščevalnih informacij.

COLLABORATIVE ASPECTS OF CYBERSECURITY – AND THEIR IMPLEMENTATION

We provide a systematic review and analysis of different aspects, methodologies, and technologies for the collaboration and coordination between stakeholders in the field of cybersecurity. These aspects include CTI exchange, standardization and sharing of incident response playbooks, community building for VOCs and CERTs, integration of cybersecurity event-sharing platforms and feeds, etc. We focus on specific solutions and best practices which we are implementing in the ecosystem of electricity IT/OT infrastructure. We incorporate group decision-making and collaboration mechanisms in the process of proactive selection of mitigation countermeasures against cyber threats and attacks. We also present a CACAO-based framework for the standardization, sharing, and automated execution of playbooks. Finally, we address the implementation of MISP-based CTI exchange mechanisms and the integration of common cybersecurity resources including NVD, MITRE ATT&CK, CIS Security Controls, etc. This allows us to participate in international expert communities, improve reactive and proactive security strategies, enhance strategic and tactical decision-making, and leverage the cybersecurity posture of the integrated IT/OT infrastructure.

Keywords: cybersecurity; cybersecurity processes and technologies; incident response procedures and playbooks; coordination and collaboration; CTI exchange.