

UPORABA VEČKRITERIJSKIH ODLOČITVENIH METOD V KIBERNETSKI VARNOSTI

Andrej Bregar¹

¹ Informatika d.o.o., Vetrinjska ul. 2, 2000 Maribor

andrej.bregar@informatika.si

Kibernetski napadi postajajo vse naprednejši, izkoriščajo številne ranljivosti ter ogrožajo kritične in kompleksne ekosisteme, ki vključujejo povezane vire iz soodvisnih omrežij. To znatno povečuje stroške za zagotavljanje kibernetske varnosti ter zahtevnost potrebnih proaktivnih in reaktivnih ukrepov. Za izvedbo le-teh je potrebno zagotoviti dobro obveščenost, sodelovanje kompetentnih strokovnjakov in deležnikov iz različnih organizacijskih nivojev ter premišljeno izbiro in načrtovanje aktivnosti. Pri tem lahko pomagajo metode večkriterijskega odločanja, ki se vse bolj uveljavljajo na področju kibernetske varnosti. Tradicionalno jih uporabljamo za ocenjevanje tveganj, vendar imajo potencial tudi v sklopu številnih drugih nalog in procesov, kot so izbira in implementacija premostitvenih ukrepov, izbira odzivnih procedur in aktivnosti, analiza stroškov in koristi, analiza obveščevalnih informacij, ocenjevanje resnosti kibernetskih dogodkov in incidentov, ocenjevanje časovno spreminjajočih se groženj, določitev nivojev potrebnega poročanja in koordinacije med deležniki v skladu z regulativnimi zahtevami, pa tudi pri oblikovanju pravil zaznavanja incidentov.

V te namene lahko uporabimo različne večkriterijske metode, kot so aditivni modeli koristnosti, mehki agregacijski modeli, AHP (Analytic Hierarchy Process), TOPSIS, ELECTRE, časovni modeli, simulacije tveganj in druge. Poseben pomen ima souporaba kvantitativnih in kvalitativnih metod, ki jo omogoča tudi sistem CVSS (Common Vulnerability Scoring System). Nekatere odločitve je potrebno zaradi širšega vpliva in izmenjave informacij sprejeti med različnimi organizacijskimi nivoji in deležniki, zato se dotaknemo še pristopov k skupinskemu odločanju, kot je tehnika Delfi.

V prispevku identificiramo in predstavimo področja kibernetske varnosti, na katerih je možno učinkovito in koristno uporabiti metode večkriterijskega odločanja. Prav tako analiziramo, katere metode so uporabne po posameznih področjih in za različne procese. Podamo priporočila, dobre prakse in scenarije uporabe odločitvenih metod. Opišemo generični model kibernetske varnosti, v katerem je odločitveni sistem osrednji povezovalni člen med tradicionalnimi komponentami, tehnologijami in procesi za upravljanje tveganj, varovanje virov, odzivanje na incidente, izmenjavo obveščevalnih informacij in sodelovanje. Večkriterijsko odločanje praktično demonstriramo na primeru uporabe iz elektroenergetske domene, kjer ga apliciramo v procesu oblikovanja časovno odvisnih premostitvenih ukrepov v IT in OT integriranem omrežju. Na tem primeru, ki temelji na naši metodologiji in tehnologiji za izbiro premostitvenih strategij ter ukrepov proti kibernetskim napadom, prikažemo tudi koristi uporabe večkriterijskih metod odločanja v kibernetski varnosti.

Ključne besede: kibernetska varnost; večkriterijske odločitvene metode; podpora pri odločanju; varnostne tehnologije in procesi, študija primera.

APPLICATION OF MULTI-CRITERIA DECISION-MAKING METHODS IN CYBERSECURITY

We identify and present potential cybersecurity areas where we can effectively apply different multi-criteria decision-making methods. We analyze suitable methods and map them to these areas and processes. We provide recommendations, good practices, and scenarios on how to use decision approaches. We introduce and describe a generic cybersecurity model in which the decision support system is a central block integrating the traditional components, technologies, and processes for risk and vulnerability assessment, asset management and patching, incident response, threat intelligence sharing, and cooperation. We practically demonstrate multi-criteria decision-making on a use case from the electricity distribution domain by applying it in the time-dependent mitigation selection process targeting an IT/OT integrated network. The case study utilizes our methodology and technology that facilitates multiple stakeholders and experts from different organizational levels in selecting remediation measures and strategies against cyber-attacks. It shows the benefits of using multi-criteria decision-making methods in cybersecurity.

Keywords: cybersecurity; multi-criteria decision-making methods; decision support; security technologies and processes; case study.