5G Varnost - 1. faza Industrijska raziskava, podfaza IR.3

Poročilo o varnosti in integriteti

Rezultat IR.11 naloge T.3.4 Celovita (end-to-end) varnost in integriteta

Tip dokumenta	Rezultat
Zapis v arhivu	5GVAR-IR3-R11_Javen
Narejeno za	5G Varnost
Avtor	Marko Pust, Andrej Kobal (OSI d.o.o.), Jauregi Lejona Urtzi (Iskratel, d.o.o., Kranj), Urban Sedlar (Univerza v ljubljani, Fakulteta za elektrotehniko), Dejan Šošter (Telekom Slovenije d.d.)
Stopnja zaupnosti	Javen

Obr.: 78-089c

1. Povzetek

Povzetek je narejen na podlagi dokumenta IR.11: Celostni pogled na varnost in opredelitev varnostnih vidikov v okviru rešitve projekta 5G Varnost, ki je rezultat naloge T.3.4.
Predstavljeni so prijemi, rešitve in tehnologije, ki temeljijo na široko sprejetih standardih in dobrih praksah s področja informacijske varnosti. Dokument podaja potrebne in priporočene ukrepe za zagotavljanje informacijske in kibernetske varnosti tako pomembnega sistema kot je 5G varnost in opisuje konkretne ukrepe, ki so v praksi uporabljeni v samem projektu.
V prvem delu dokumenta so na splošno predstavljeni ukrepi upravljanja informacijske varnosti. Podani so zakonodajni okviri ter standardi, s posebnim poudarkom na področje 5G in zagotavljanje varnosti na področju bistvene (kritične) infrastrukture, kamor PPDR vsekakor sodi. Za doseganje visoke stopnje informacijske varnosti tako kompleksnega sistema je potrebno uporabiti ustrezno ogrodje (ang. *framework*) in orodja, ki zagotavlja, da so vsi vidiki varnosti upoštevani. Kot osnovno ogrodje informacijske varnosti se najpogosteje uporablja standard ISO/IEC 27001, ki je primeren za širok spekter sistemov in storitev. Za posamezne podsisteme lahko kot razširitev ali dopolnitev uporabimo tudi druge standarde, npr. ISO/IEC 27032, ISA/IEC62443 ali NIST standarde. V primeru produkcijskega okolja je priporočljivo vzpostaviti tudi lastna merila in standarde, ki povzemajo, so blažja ali strožja od kontrol navedenih v standardih, odvisno od prepoznanih tveganj. Za potrebe projekta 5G varnost se naslanjamo na standard ISO/IEC 27001/27002 ter na priporočila ENISA za kibernetsko varnost 5G omrežij.
Peto poglavje je namenjeno modeliranju groženj (ang. *Threat modelling*). Preko teoretičnih okvirjev je bil izdelan model groženj za specifičen primer PPDR aplikacije, nato pa smo model uporabili v demonstracijskem okolju in določili grožnje. Sam model groženj je bil narejen s pomočjo UML diagramov in na osnovi tega smo analizirali konkretno postavitev v demonstracijskem okolju. Rezultat analize so podane smernice za izboljšanje kibernetske varnosti in odpornosti.
Posebno poglavje je namenjeno zagotavljanju varnosti v omrežju 5G. Proučeni so vsi vidiki varnosti od 5G jedrne infrastrukture, RAN omrežja do 5G dostopovnega (access) omrežja. Podane so tudi smernice glede varnosti vključitve 5G terminalov v omrežje ter glede mehanizmi kontrole dostopa.
Posebno poglavje je namenjeno varnostnim vidikom razvoja aplikacij. Pregledan je proces varnega razvoja in kontrolnih mehanizmov, ki pri tem obstajajo. Glede na značilnosti projekta 5G Varnost je bil velik poudarek na razvoju mobilnih aplikacij, kajti v okviru projekta se je razvijala aplikacija 112. Izveden je bil tudi ocena tveganja, identificirane so bile grožnje ter narejeno varnostno preverjanje aplikacije. Na osnovi tega so bile podane smernice, ki jih bo potrebno upoštevani pri nadaljnjem razvoju aplikacije.
Zadnji del dokumenta je namenjen zagotavljanju operativne varnosti. Podane so smernice izgradnje varnostno operativnega centra (ang. *SOC – Security Operation Center*). V tem poglavju je tudi opisana metodologija za izvedbo varnostnih testov. Predstavljen je sistem za operativno upravljanje incidentov in iskanje ranljivosti. Ta sistem je bil postavljen in preskušen v demonstracijskem okolju. V demonstracijskem okolju bo prav tako preizkušen prav sistem za beleženje revizijskih sledi, ki temelji na uporabi kriptografskih metod z uporabo tehnologije veriženja blokov (ang. *blockchain*).