Allegato 1) Elenco dei progetti di ricerca

Titolo: DeP-FiVE - Detection and Prevention for Fifth-generation Vulnerabity Emergence (Codice pratica: 95a04ac3)

Soggetto proponente
Denominazione: Università del Salento
Dipartimento/Istituto/Unità: Dipartimento di Ingegneria dell'Innovazione
Sede di svolgimento del progetto: Campus Ecotekne, via per Monteroni s.n.c. Lecce

Impresa privata
Denominazione: Deep Consulting Srl
Sede di svolgimento del progetto: Via Stradella Barone, 9, Bari

Ambito di ricerca dell'European Research Council (Livello 1):	Physical Sciences and Engineering
Ambito di ricerca dell'European Research Council (Livello 2):	Physical Sciences and Engineering
Filiera produttiva regionale:	03 - INFORMATICA

Descrizione del progetto di ricerca
Il progetto mira a supportare la definizione di nuove procedure di test e intervento adatte al monitoraggio e alla difesa pro-attiva di reti di dispositivi (device) connessi all'interno di reti 5G. La crescente diffusione di reti 5G si prospetta come un'opportunità per lo sviluppo di una radicale crescita di connessione tra device, sensori e attuatori con alta capacità di carico e ridotti tempi di latenza. Ciò si inquadra in un contesto dove tali device possono gestire ed elaborare dati, così come comunicare informazione, tanto su scala locale (e.g. edge computing) quanto globale (clud computing). Tale contesto, ormai consolidato a livello internazionale, trova una sua ampia realizzazione in Puglia: la Regione, in particolare la città di Bari, è una delle prime aree in Italia ad aver attivato la sperimentazione su connessioni 5G. Per poter trarre vantaggio da tali innovazioni, queste devono essere integrate da processi di comunicazione e di accesso sicuri, così come da metodi di test, di verifica e di reazione adatti al crescente numero di cyber-vulnerabilità, minacce e alla loro diversa entità. Difatti, da una parte le reti 5G possono abilitare l'acquisizione di dati da fonti eterogenee, permettendo analisi più fini e decisioni più consapevoli, garantendo nel contempo maggior controllo nelle applicazioni di automazione. D'altra parte, tali connessioni ampliano le superfici di attacco, potendo dar vita a nuove vulnerabilità; inoltre, nuove tipologie di vulnerabilità potrebbero emergere come risultato della combinazione di componenti digitali, ognuna delle quali può essere individualmente classificata come "sicura". Tale criticità coinvolge direttamente le imprese e gli enti operanti nel settore ICT all'interno del (o in collaborazione con) il contesto regionale ma, indirettamente, anche aziende che fruiscono di servizi IT su settori specifici (healthcare, trasporti, automotive): l'interazione con reti di dispositivi interna a un'Organizzazione, così come la fruizione di servizi esterni all'organizzazione richiedono apposite contromisure che non valutino un device solo localmente, ma immerso in un network le cui interdipendenze (potenziali fonti di

acquisizione di informazione o di attacco) sono complesse e, spesso, non visibili all'utente e al gestore della rete. L'obiettivo generale del progetto è definire un framework che, a partire dallo stato dell'arte nell'analisi delle cyber-vulnerabilità, identifichi e caratterizzi nuove tipologie e superfici di attacco, gli interventi necessari ad adeguare alcune delle principali metodologie, e i requisiti per la definizione di nuovi approcci ad hoc. Tali aspetti si traducono nei seguenti obiettivi realizzativi: OR1. Definizione di criteri o condizioni che invalidino l'efficacia delle attuali tecniche di testing (penetration test), analisi (malware analysis, statica o dinamica) o sistemi di monitoraggio (NIDS – Network Intrusion Detection Systems) OR2. Adattamento delle tecniche di testing a una rete di dispositivi 5G – metodologia, implementazione e validazione. L'output atteso dal progetto è duplice: D1. Caratterizzazione di una nuova classe di vulnerabilità emergenti dalla crescente complessità di reti connesse, con particolare attenzione alle componenti ridondanti e sinergiche in una rete IT e ai meccanismi che possono rendere tali componenti una fonte di potenziali vulnerabilità. D2. Metodologia e tool per exploitation e risoluzione (fixing) di una delle vulnerabilità succitate.