Avviso pubblico denominato "Bando a cascata per Innovation Open Call n.01, Application Security" per la presentazione di Proposte progettuali per la realizzazione di attività di ricerca industriale e sviluppo sperimentale relative al Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 6 Software and Platform Security (UNIVERSITA' Ca' FOSCARI VENEZIA) ammesso a finanziamento con Avviso Pubblico nr 341 del 15-02-2022 "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base" – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3, finanziato dall'Unione europea – NextGenerationEU

Codice CUP H73C22000890001

Allegato Tecnico

SERICS Spoke 6 "Software and Platform Security" – Innovation Open Call

I servizi critici e tutte le infrastrutture moderne dipendono fortemente da software che viene eseguito su una varietà di piattaforme. Una vulnerabilità nel software o nella piattaforma sottostante potrebbe consentire attacchi di Denial of Service (DoS), compromettere l'integrità e la riservatezza dei dati e, nel peggiore dei casi, permettere l'esecuzione di codice da remoto. Le vulnerabilità del software e delle piattaforme vengono sfruttate dai malware e sono la causa principale di molti incidenti di sicurezza in una moltitudine di contesti, dai dispositivi mobili alle applicazioni web e basate su cloud. Negli ecosistemi critici, questi incidenti di sicurezza possono avere conseguenze disastrose, comportando in alcuni casi gravi perdite finanziarie e minacce fisiche per le persone.

Lo **Spoke 6** dell'iniziativa SERICS è coordinato dall'Università Ca' Foscari di Venezia e riunisce iniziative complementari per affrontare la linea tematica **"Software and Platform Security"** nella sua complessità e vastità. L'attività dello Spoke 6 si articola in due linee progettuali:

1. **SCAI** - *Supply Chain Attack Avoidance*, che ha lo scopo di esplorare soluzioni innovative per proteggere il processo di gestione e sviluppo del software;
2. **SWOPS** - *Securing softWare frOm first PrincipleS,* che affronta le basi formali della programmazione sicura, per consentire l'implementazione di sistemi software sicuri per costruzione (secure by design).

Maggiori dettagli di ciascuna linea progettuale sono forniti di seguito.

SCAI: Gli attacchi alla supply chain sono un approccio sempre più popolare per attuare una varietà di obiettivi malevoli. Il progetto esplora soluzioni innovative per proteggere il processo di gestione e sviluppo del software, eseguire test di sicurezza attraverso analisi dinamiche continue e proteggere il software, rilevando attività dannose e prevenendo o limitando il loro impatto, secondo un paradigma di *autodifesa*. In primo luogo, ci si occupa di mettere in sicurezza il processo di sviluppo del software considerando problematiche di usabilità dei meccanismi di sicurezza, proponendo tecniche innovative di valutazione del rischio cyber e metodologie per lo sviluppo di sistemi affidabili composti da componenti software eterogenei. Viene svolta attività di ricerca sulle vulnerabilità del software all'interno della supply chain, indagando strategie di testing di sicurezza specifiche per le varie fasi di sviluppo del software che includono lo sviluppo di nuove analisi a livello di API, nuove analisi statiche e dinamiche e nuove strategie di fuzzing. Infine, vengono studiate nuove tecniche per proteggere il software e rilevare comportamenti malevoli.

SWOPS. La complessità dei sistemi software richiede un importante cambiamento di prospettiva, in cui la sicurezza del software viene considerata fin dalle prime fasi del ciclo di vita del software. Il progetto affronta le basi formali per rivoluzionare la programmazione sicura al fine di semplificare l'implementazione di sistemi software sicuri per costruzione (secure by design). Più precisamente, il progetto ha tre obiettivi: il primo è sviluppare modelli semantici e astrazioni di programmazione di alto livello che consentano agli sviluppatori di scrivere codice robusto e sicuro per costruzione; il secondo è sviluppare metodi e tecniche per analizzare un software sia in fase statica che in fase di esecuzione per valutare continuamente le sue proprietà di sicurezza, garantendo che non sia stato

alterato, che esponga un comportamento accettabile e che sia privo di vulnerabilità; il terzo è contribuire alla progettazione, sviluppo e implementazione di meccanismi a livello di piattaforma che permettano l'esecuzione sicura e la composizione del software.

INNOVATION OPEN CALL

L'obiettivo delle Innovation Open Call è quello di sollecitare nel contesto progettuale di riferimento, sopra introdotto, proposte innovative volte a potenziare lo sviluppo di software sicuro, rafforzare la sicurezza cibernetica e promuovere un ambiente digitale più sicuro e affidabile.

Nello specifico, il bando per Innovation Open Call intende selezionare proposte finalizzate a:

- portare i risultati della ricerca a livelli avanzati di Technology Readiness Level (TRL), nel dominio di riferimento;
- realizzare applicazioni che siano sicure per costruzione e che considerino la sicurezza come un requisito fondamentale fin dalle prime fasi di sviluppo;
- individuare casi di studio pratici sui quali sperimentare i risultati della ricerca allo scopo di migliorare la sicurezza.

Saranno considerati e valutati i progetti che abbiano l'obiettivo di sviluppare idee ed applicazioni concrete sui seguenti temi:

Application Security

- **Software Security by Design**: Sviluppare tecniche avanzate per migliorare lo sviluppo del software incorporando tecniche di analisi statica e adottando principi e strumenti di programmazione che forniscano elevate garanzie di sicurezza. L'obiettivo è di collaborare in modo molto stretto con i partner accademici applicando alcuni risultati della ricerca al contesto di applicazioni reali in ambito aziendale.
- **Secure Software Development**: Adottare principi e tecniche robusti per lo sviluppo di software sicuro, considerando l'intero processo di sviluppo e gestione della supply chain. L'obiettivo è di innalzare la consapevolezza delle possibili minacce relative all'intera filiera di sviluppo del software incorporando strumenti di test e analisi che permettano un monitoraggio continuo del software e delle sue dipendenze.
- **Analysis of Existing Software and Platforms**: Analizzare sistemi software e piattaforme allo scopo di identificare vulnerabilità a diversi livelli: logico, implementativo, di configurazione, etc. L'obiettivo è di collaborare con i partner accademici al fine di applicare gli strumenti di ricerca ad applicazioni esistenti permettendo di identificare casi di studio rilevanti e, come fine ultimo, innalzando il livello di sicurezza delle applicazioni esistenti.

Ci attendiamo proposte che prevedano una o più delle seguenti attività:

1. La sperimentazione di alcuni tool di ricerca su casi pratici allo scopo di fornire feedback ai partner accademici sull'usabilità e la maturità degli strumenti stessi;
2. L'estensione dei tool in modo da innalzarne il TRL;

3. L'individuazione di casi di studio reali che possano essere analizzati con i tool e/o richiedano estensioni dei tool;
4. L'applicazione dei risultati della ricerca a sistemi industriali reali allo scopo di individuare e risolvere potenziali vulnerabilità migliorando la postura cyber dell'azienda stessa;
5. La progettazione di soluzioni innovative per migliorare la sicurezza di sistemi industriali esistenti.