CySEC

Manifesto della Value Chain

“CyberSecurity”

CLUST-ER INNOVATE
INNOVAZIONE NEI SERVIZI

Manifesto della Value Chain “CyberSecurity”

1. NOME/ACRONIMO DELLA VC

CySEC

2. BREVE DESCRIZIONE DELLA VC

Questa VC intende muoversi su due diversi orizzonti temporali.

A breve-medio termine, la VC intraprende attività atte a promuovere la cultura e le soluzioni di sicurezza che sono già note, ma che richiedono una diffusa applicazione a livello di tessuto produttivo e di pubblica amministrazione.

A medio-lungo termine, si intendono affrontare le sfide di sicurezza del cyberspazio del prossimo futuro, agendo per identificare i problemi di sicurezza nel contesto dell’Industria 4.0 e, in generale, dei CyberPhysical Systems (CPS), così da migliorare sicurezza, safety e affidabilità mediante la definizione e l’adozione delle migliori pratiche e di soluzioni tecnologiche innovative.

3. OBIETTIVI STRATEGICI DELLA VC

Obiettivi strategici a breve-medio termine:

- sviluppare una comprensione delle esigenze del peculiare contesto emiliano romagnolo al fine di identificare i problemi e gli ostacoli che impediscono l’acquisizione di soluzioni di sicurezza efficaci;
- promuovere una cultura top-down della sicurezza e del risk-management attraverso l’adozione consapevole di politiche e di procedure adeguate a ciascuna realtà industriale;
- individuare e promuovere buone pratiche per migliorare la continuità dei servizi informatici e la capacità di risposta del sistema di sicurezza;
- integrare le soluzioni di sicurezza tecniche con il necessario sviluppo dell’interoperabilità tra servizi e differenti tecnologie. Obiettivi strategici a medio-lungo termine:
- individuare e promuovere buone pratiche per l’adozione di modelli cost-effective orientati al miglioramento del livello di sicurezza delle imprese regionali in un contesto di Industria 4.0 e di ambiti ad elevato livello di rischio, quali quello sanitario e delle infrastrutture critiche;
- promuovere una modalità collaborativa per l’identificazione tempestiva delle minacce e delle vulnerabilità odierne e del prossimo futuro;
- individuare e proporre modifiche da apportare per promuovere l’innovazione permanente con modelli di security e privacy by design, il coinvolgimento continuativo del mondo accademico e l’individuazione di eventuali requisiti che richiedono l’acquisizione e adozione di soluzioni di sicurezza innovative.

4. DESCRIZIONE DELLA VC

STANDARD e NORME (soggetti interessati: aziende ICT, aziende di servizi con un forte reparto ICT, start-up)

- Norme nazionali ed europee sulla privacy e sulla riservatezza dei dati
- Standard e regolamenti relativi alla sicurezza informatica (ISO 27000, NIST)
- Standard relativi alla sicurezza delle infrastrutture critiche (NERC)
- Standard relativi alla sicurezza dei sistemi di pagamento elettronici (PCI-DSS)
- Direttiva europea NIS
- Common Vulnerability Scoring Systems (CVSS v3.0)
- Common Vulnerabilities and Exposures (CVE)
- Open Source Security Testing Methodology Manual (ISECOM OSSTMM)

R&D (soggetti interessati: università e centri di ricerca, laboratori rete alta tecnologia, aziende ICT, aziende di servizi con un forte reparto ICT, start-up)

- Sicurezza dei sistemi produttivi in un contesto Industria 4.0
- Sicurezza di Cyber Physical Systems
- Metodologie e testing di sicurezza di infrastrutture critiche
- Autonomous security
- Crittografia
- Anomaly detection
- Security analytics
- Cloud security

TECNOLOGIE (soggetti interessati: aziende ICT, aziende di settori verticali per l'integrazione)

- Analizzatori di traffico
- Sistemi per la rilevazione di attacchi informatici
- Protocolli di comunicazione sicuri
- Sicurezza per piattaforme virtuali
- Sicurezza per dispositivi mobili re BYOD
- Sicurezza per IoT
- Embedded security

PROCESSI PRODUTTIVI (soggetti interessati: aziende ICT, industria manifatturiera)

- Sviluppo software sicuro
- Security by design
- Privacy by design
- Security management
- Metodologie di testing

APPLICAZIONI

- Piattaforme software per la valutazione del livello di sicurezza sistemi informativi
- Piattaforme software a supporto della valutazione e della gestione del rischio informatico
- Sistemi avanzati per la rilevazione di attacchi informatici
- Sistemi di security analytics

BUSINESS MODEL

- Security as a Service: l'azienda cliente paga mediante un modello di subscription i servizi di sicurezza, offerti mediante piattaforme esternalizzate
- Consulenza: il cliente paga l'esperto di sicurezza per le attività di consulenza
- Licenze software: l'azienda cliente acquista una licenza di utilizzo per soluzioni software per la sicurezza, la crittografia e la security analytics

EDUCAZIONE E FORMAZIONE (soggetti interessati: Università, ITS, enti di ricerca e di formazione, pubblica amministrazione e policy makers)

- Educazione universitaria in corsi di Laurea triennale, Laurea magistrale e dottorati di ricerca
- Formazione continua mediante l'erogazione di corsi di perfezionamento e Master
- Organizzazione di eventi e seminari su specifiche tematiche relative alla CyberSecurity aperti a imprese e operatori nel settore della sicurezza informatica

ECONOMIA CIRCOLARE (soggetti interessati: tutti gli stakeholders)

- Miglioramento dei livelli di sicurezza dei sistemi e sensibilizzazione del personale, con conseguente riduzione di frodi e fenomeni d cybercrime
- Miglioramento dei livelli di safety relativi a infrastrutture critiche e Cyber Physical Systems

5. IL POSIZIONAMENTO DELLA REGIONE RISPETTO ALLA VC NEL CONTESTO NAZIONALE ED INTERNAZIONALE

Gli obiettivi perseguiti dalla VC Cybersecurity ricoprono una importanza strategica a livello regionale, nazionale e internazionale.

Il tessuto imprenditoriale emiliano romagnolo è caratterizzato dalla presenza di un elevato numero di PMI, che spesso operano su mercati internazionali proponendo prodotti e soluzioni connotate da proprietà intellettuali di grande valore e da un elevato livello di innovatività. Diffuse carenze nella gestione dei sistemi informatici di queste PMI hanno già consentito ad attaccanti informatici di creare un danno economico rilevante mediante attività di furto di dati e blocco delle attività produttive.
Il ricorso sempre maggiore a sistemi di automazione industriale, sia a livello regionale che nazionale, comporta rischi legati non solo alla sicurezza informatica, ma anche alla sicurezza fisica dei cittadini. Si consideri a tal proposito le potenziali ricadute di attacchi informatici portati a infrastrutture critiche, impianti industriali automatizzati, veicoli connessi e autonomi. Lo sviluppo di competenze di alto livello e di soluzioni tecnologiche avanzate per la sicurezza di infrastrutture critiche e Cyber Physical Systems rappresenta quindi una urgenza a livello nazionale e internazionale.

Analisi SWOT della VC

Strengths	**Weaknesses**
− Presenza sul territorio nazionale di centri di ricerca e laboratori con competenze di eccellenza nei settori della sicurezza delle informazioni e dei sistemi informatici − Presenza di filiere industriali significative (ad esempio nel settore dell'automotive) particolarmente interessate allo sviluppo di soluzioni di sicurezza innovative per Cyber Physical Systems − Capacità adattative delle PMI presenti nel territorio emiliano romagnolo	− Risorse limitate − Eccessivo ampliamento del perimetro (necessità di focalizzazione) − Carenza di personale dedicato a tempo pieno (necessità di rewarding) − Attuale carenza di competenze non tecnologiche
Opportunities	**Threats**
− Sostegno istituzionale − Periodo favorevole alla sensibilizzazione − Estrema e oggettiva necessità di interventi − Regione altamente industrializzata − Impulso derivante dalle iniziative nazionali Industria 4,0	− Incertezze sui ruoli, poteri attività − Incertezze sui mezzi per l'attuazione − Trasversalità della materia: necessità di integrazione con altre value chain − Valore aggiunto della value chain percepito dall'esterno − Problemi di IP nella collaborazione tra aziende − Resistenza al cambiamento