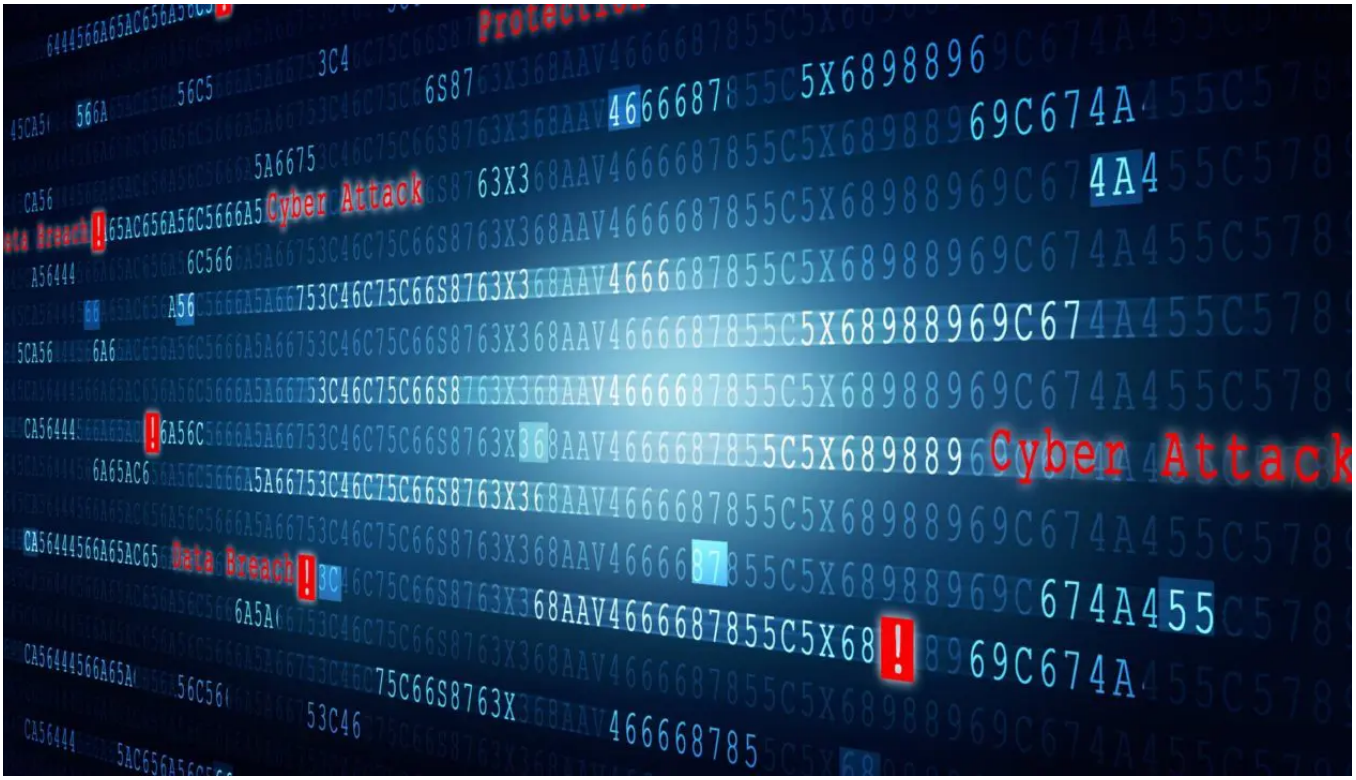
Le infrastrutture critiche alla base del sistema di fornitura dei servizi essenziali sono il perno delle funzioni chiave della società attuale. La loro protezione è centrale nelle iniziative Ue e in quelle nazionali. In questo contesto la creazione di partnership pubblico-privato è la sfida del futuro

8 ore fa

Fabio Lazzini

CISO e DPO di Sogei

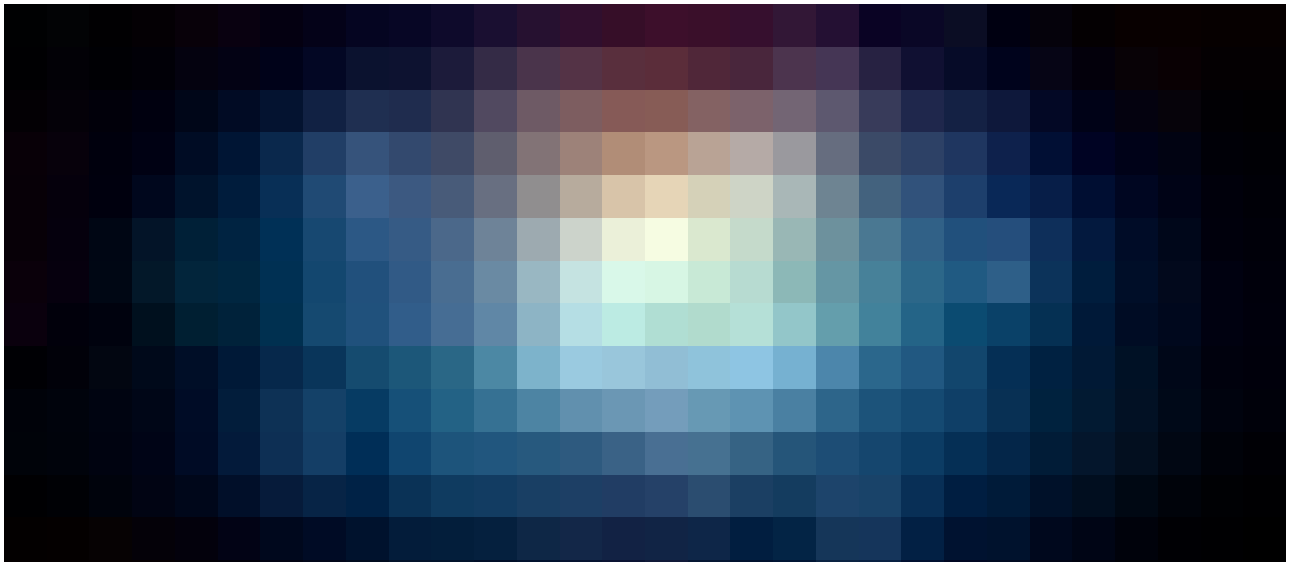


Lo straordinario aumento dell'utilizzo della rete e dei servizi digitali, come abbiamo visto durante la pandemia, ha creato **nuove opportunità** ma è stato accompagnato da un corrispondente incremento delle **vulnerabilità** e delle **minacce**.

Le organizzazioni, pubbliche e private, che gestiscono quotidianamente dati e informazioni digitali si trovano a dover **evolvere i propri processi di digitalizzazione** garantendo la disponibilità, l'integrità e la riservatezza.

Le **infrastrutture considerate critiche** per il Paese perché fornitrici di servizi essenziali, (luce, gas, acqua, ecc.), hanno il dovere di garantire il normale svolgimento della vita quotidiana dei cittadini.

La digitalizzazione è stata nel periodo pandemico uno straordinario driver di sviluppo svolgendo la funzione di ausilio e supporto e anche di miglioramento e rilancio di molti settori produttivi del Paese.



Indice degli argomenti

Il potenziamento dell'attività normativa

L'attenzione dell'Unione Europea per favorire e accelerare il potenziamento della capacità di difesa cyber negli Stati membri non passa solo da iniziative di finanziamento e incentivo, come il **Piano NextGenEU**, ma anche da **un forte potenziamento dell'attività normativa**.

La direzione intrapresa è **dotare l'Europa di strumenti normativi e operativi al fine di arginare le minacce provenienti dal cyber spazio**, minacce che attentano non solo alla sicurezza nazionale ed europea, ma anche alla crescita sociale ed economica.

La protezione delle infrastrutture critiche informatizzate costituisce l'ossatura del sistema di fornitura dei servizi essenziali, che sono alla base delle funzioni chiave delle società moderne e dei singoli che le compongono.

Nel campo della cybersecurity il quadro normativo si è arricchito di un ulteriore tassello come il **Perimetro di Sicurezza Nazionale Cibernetica (PSNC),** istituito a fine 2019. Il Perimetro include soggetti pubblici e privati che erogano o permettono di erogare servizi fondamentali per lo Stato dal cui malfunzionamento, interruzione, anche parziali, o dall'utilizzo improprio, potrebbe derivare un rischio per la sicurezza nazionale. L'obiettivo è assicurare un elevato livello di sicurezza alle reti, ai sistemi e ai servizi impiegati per l'esercizio di queste funzioni essenziali.

Il Governo ha istituito recentemente **l'Agenzia per la Cybersicurezza Nazionale (ACN)** e ha allargato ulteriormente il novero dei soggetti inseriti nel PSNC, sia pubblici che privati, aumentando il numero delle Funzioni o dei Servizi Essenziali in esso ricompresi. L'Agenzia è stata pensata come il referente per il PSNC e per il **Computer Security Incident Response Team**

italiano (CSIRT Italia), accentrando tutte le tematiche e iniziative del comparto intelligence orientate al contesto cyber. Lo Stato, quindi, perfeziona l'architettura di controllo e monitoraggio delle minacce cyber che punta a innalzare la resilienza di soggetti pubblici e privati, fondamentali per la sicurezza nazionale.

La creazione di partnership pubblico-privato

In questo contesto, la creazione di **partnership pubblico-privato** rappresenta una sfida importante per il futuro. Come riconosciuto anche nell'iniziativa del legislatore, la pratica **dell'information sharing** a livello europeo e nazionale è alla base del consolidamento di un atteggiamento costruttivo finalizzato al coordinamento politico e al progresso tecnologico, fondamentale per la trattazione adeguata della sicurezza cibernetica. Lo sviluppo del dialogo tra le parti, anche attraverso l'istituzione di opportuni meccanismi obbligatori di comunicazione previsti dalla legge, costituisce quindi un obiettivo importante per il futuro.

La **collaborazione e la condivisione**, se basate su un approccio e regole condivisi, può essere realizzata tra soggetti sia pubblici che privati. La pertinenza delle informazioni deriva dalla similitudine dei soggetti, definiti "peer" appunto, agli occhi degli attaccanti e non dalla somiglianza della loro forma giuridica. In quest'ottica, la partnership tra soggetti pubblici e privati è stata realizzata spesso con grande successo.

Il progetto Cyberkit4SME

Un ulteriore esempio del **valore di collaborazioni tra pubblico e privato**, in questo caso anche tra soggetti di "dimensione" diversa, è rappresentato per Sogei da **Cyberkit4SME**. Il progetto, avviato a giugno 2020 per una durata di 3 anni, mira a sviluppare un pacchetto di strumenti e metodologie che permettano alle PMI (in inglese SME) e alle micro-imprese (in inglese ME) di innalzare la loro consapevolezza e maturità nella gestione e mitigazione dei rischi cyber. Gli elementi del "toolkit" che verrà messo a punto sono pensati per essere facili da adottare, semplici da usare e da integrare nei processi di business, specificamente pensati per le PMI e le micro-imprese.

L'importanza del progetto nel contribuire all'aumento della resilienza delle PMI e micro-imprese negli stati membri, può significare per il nostro Paese **un passo avanti verso la creazione di una baseline per la cyber security**, componente fondamentale del tessuto industriale ed economico.

Conclusioni

CyberKit4SME costituisce un'importante iniziativa in progetti di Ricerca&Innovazione sulla cyber security in cui Sogei in qualità di hub di innovazione digitale per la PA e l'Italia può ricoprire un ruolo di rilievo e portare ulteriore contributo rafforzando il valore della collaborazione pubblico-privato.

Nel periodo dell'emergenza sanitaria è emersa la strategicità della digitalizzazione come driver di sviluppo e progresso. Sogei ha realizzato servizi e soluzioni specifiche e ha ampliato quelle preesistenti rafforzando ulteriormente il suo ruolo volto a semplificare la vita dei cittadini e a garantire la protezione degli asset strategici per l'azienda e il Paese: **i dati dei cittadini**.