

Cybersecurity e sostenibilità sono complementari per lo sviluppo di una società migliore, secondo uno studio realizzato da Fondazione per la Sostenibilità Digitale con il contributo non condizionante di Gyla

- *Recentemente presentato alla Sala Stampa della Camera dei Deputati, il rapporto Sicurezza Informatica e Sostenibilità Digitale esplora le intersezioni tra sicurezza digitale e sostenibilità*
- *Sovranità Digitale, Privacy e Integrazione Tecnologica IT/OT sono gli elementi maggiormente impattanti sui diversi SDG*

Roma, 11 aprile 2024 – Presentato oggi il rapporto **“Sicurezza Informatica e Sostenibilità Digitale”**, realizzato dalla **Fondazione per la Sostenibilità Digitale**, la più autorevole istituzione di ricerca in Italia su temi della sostenibilità digitale, nonché il principale ThinkTank italiano dedicato alla relazione tra sostenibilità e trasformazione digitale, con il contributo di **Gyla**, azienda italiana che vanta una pluriennale esperienza in ambito difesa e fornisce al mercato soluzioni di cybersecurity innovative per proteggere le risorse strategiche IT/OT delle aziende pubbliche e private.

“Viviamo in un’era in cui il digitale permea ogni aspetto della nostra vita e ogni interazione, sia essa aziendale, istituzionale o personale. Questa realtà aumenta di fatto in modo esponenziale la superficie d’attacco dei sistemi e rende la cybersecurity una componente imprescindibile di ogni strategia di digitalizzazione. Parallelamente la sostenibilità, intesa come la capacità di soddisfare i bisogni attuali senza precludere alle generazioni future le stesse opportunità, emerge come un obiettivo globale, un imperativo per tutti gli attori della società”, ha commentato **Stefano Epifani, Presidente della Fondazione per la Sostenibilità Digitale**.

Il report esplora le intersezioni tra sicurezza digitale e sostenibilità, stabilendo priorità chiare, con l’obiettivo di proporre un quadro di riferimento che porti verso una **cybersecurity che sia al contempo sostenibile e motore di sostenibilità**, delineandola convergenza tra sicurezza informatica e sostenibilità, che non devono essere interpretate come entità distinte, ma complementari, orientandosi entrambe verso lo sviluppo di una società migliore.

È stato redatto a seguito di una approfondita analisi condotta attraverso focus group comprendenti una rappresentanza eterogenea di esperti, tra cui CISO, CIO, docenti e ricercatori universitari. Questa attività ha prodotto un elenco di priorità che riflette una visione olistica e multidisciplinare, essenziale per affrontare le sfide contemporanee in termini di sicurezza informatica e sostenibilità.

Sono emerse tre aree tecnologiche prioritarie, che impattano oltre la metà degli obiettivi di sviluppo sostenibile definiti dall’Organizzazione delle Nazioni Unite: **integrazione tecnologica IT/OT, privacy sovranità digitale**.

Nicola Mugnato, CTO e co-fondatore di Gyala, ha così commentato i risultati della ricerca: *“Crediamo fermamente che la sostenibilità può trovare nella tecnologia un elemento abilitatore e attuatore, e riteniamo che le tecnologie che si occupano di cyber siano un volano per lo sviluppo del Paese oltre a essere uno degli elementi di protezione della nostra forza produttiva, collaborando nella protezione delle istituzioni e delle singole aziende e stimolando il circuito dell’economia, del benessere e della crescita. Gli elementi che ci ha restituito questa ricerca confermano che l’approccio che Gyala ha nel suo DNA di guardare alla **sovranità digitale, all’integrazione tecnologica e alla privacy** connesse alla sostenibilità come elementi competitivi è corretto e può rappresentare un elemento chiave nel processo evolutivo, sostenuto da diversi anni dal Sistema Paese, che vede questi nuovi approcci come acceleratori della crescita del settore pubblico e privato”.*

LE TRE AREE PRIORITARIE

Integrazione tecnologica IT/OT

Con lo sviluppo delle tecnologie IoT (Internet of Things) è sempre più importante garantire integrazione tra le componenti digitali dell’IT e quelle fisiche dell’OT. Questo ha forti impatti su diversi SDG e sulle caratteristiche specifiche della sicurezza in termini di sostenibilità. La rilevazione ha evidenziato come rispetto all’integrazione IT/OT gli impatti maggiori siano percepiti in relazione all’area della **Sostenibilità Ambientale**. Al secondo posto si colloca la **Sostenibilità Economica** e al terzo la **Sostenibilità Sociale**.

Gli intervistati ritengono quindi che **l’integrazione IT/OT è fondamentale per supportare i processi legati alla salvaguardia e alla tutela dell’ambiente**, anche in relazione alla tenuta delle infrastrutture critiche ed al loro valore economico.

Il report pone in evidenza come l’adozione di **criteri di progettazione orientati al “Security by Design”** sia estremamente importante: il 66% del campione ritiene infatti che sia essenziale per garantire la sostenibilità. Analogamente, per il 61% **la sicurezza della catena di forniture** è un fattore essenziale per la sostenibilità. Per oltre la metà dei rispondenti (57%) è necessario che le **infrastrutture OT possano essere gestite con la stessa flessibilità delle infrastrutture IT**, in modo da poter garantire sicurezza e resilienza delle infrastrutture stesse. Infine, per il 51% dei CIO, la **gestione di infrastrutture resilienti richiede un elevatissimo livello di integrazione tra IT e OT**.

La sicurezza dei sistemi che integrano le componenti digitali dell’IT e quelle fisiche dell’OT richiede una visione integrata degli stessi sistemi di cybersecurity. Emerge una priorità trasversale ai diversi obiettivi di sostenibilità settoriali (medicina, elettricità, acque) che riguarda la sicurezza dei sistemi IT che si interfacciano con i sistemi OT (**SDG9**).

Il settore di maggiore rilevanza per l’integrazione IT/OT è quello **medico (SDG3)**, rispetto al quale la sicurezza degli apparati e dei dati ha un elevato livello di rischio legato alla salute dei pazienti, la cui vita dipende dal controllo dei dispositivi medicali impiantati o utilizzati nelle strutture ospedaliere o nella medicina a distanza.

Con analoga importanza emerge il settore **energetico (SDG7)** con la gestione delle reti smart grid, fondamentali nella gestione delle fonti rinnovabili, nelle loro diverse componenti: generatori, processori, sensori, smart meter. Seguono la gestione del flusso integrato delle acque (**SDG6**) e la gestione degli impianti di produzione dell’energia elettrica (**SDG7**).

Privacy

La sicurezza informatica, in un contesto di sostenibilità, va perseguita nel rispetto della privacy degli utenti e rappresenta allo stesso tempo un importante strumento di sostenibilità. Per gli intervistati, la privacy impatta principalmente sulla **sostenibilità sociale**, seguono la **sostenibilità economica** e quella **ambientale**.

La correlazione tra privacy e sicurezza in ottica di sostenibilità tocca in modo trasversale tutti i temi dell'indagine. **L'obiettivo di sostenibilità più importante è l'SDG3** (buona salute e benessere delle persone: la protezione dei dati dei pazienti rispetto ad attacchi esterni ed interni è riconosciuto come il più importante).

Gli altri ambiti hanno un'importanza minore, ma comunque significativa e sono: gestione dei sistemi di monitoraggio e controllo dei comportamenti degli utenti (**SDG7** Energia pulita ed accessibile); gestione della sicurezza dei sistemi nel rispetto della privacy dei lavoratori (**SDG8** Lavoro dignitoso e crescita economica); protezione dei dati degli studenti rispetto ad attacchi esterni (**SDG4** Educazione di qualità); protezione dei dati degli studenti rispetto ai gestori delle piattaforme (**SDG4**).

La gestione della sicurezza del paziente nel pieno rispetto della privacy è un elemento focale per il **62%** degli intervistati e per il **51%** dei rispondenti la sicurezza di un sistema informativo non deve in alcun modo confliggere con la privacy degli utenti del sistema stesso.

Sovranità Digitale

La modalità in cui uno Stato regola ed esercita il governo della tecnologia e dei servizi utilizzati in vario modo all'interno del perimetro nazionale (sovranià digitale) vede nella sicurezza informatica un elemento di grande criticità e, contestualmente, rappresenta un tema centrale in termini di sostenibilità.

Gli intervistati evidenziano una centralità della sovranità digitale nella sicurezza per garantire la sostenibilità economica, così come per la dimensione della sostenibilità sociale. La sostenibilità ambientale, rispetto alla sovranità digitale, è percepita come la dimensione meno rilevante.

L'elemento più rilevante per la sovranità digitale è con evidenza che **la garanzia che i dati coperti da segreto industriale di un'azienda e quelli delle infrastrutture critiche del Paese non possano essere acquisiti da Stati esteri (SDG8)**. Seguono gli altri ambiti che riguardano i dati relativi alle infrastrutture con: la garanzia che i dati delle infrastrutture energetiche non possano essere acquisiti da Stati esteri (**SDG7**); la garanzia che i dati delle infrastrutture idriche non possano essere acquisiti da Stati esteri (**SDG6**); la garanzia che i dati dei pazienti (**SDG3**) non possano essere acquisiti da Stati esteri.

Il **60%** degli intervistati ritiene che gli Stati debbano investire in cyber sicurezza favorendo gli attori nazionali e il **57%** pensa che per garantire la sostenibilità è necessario che le aziende che forniscono sistemi e soluzioni per la cybersecurity siano indipendenti da ingerenze di stati esteri. Poco meno del **50%** dei CIO intervistati ritiene infine che l'accesso ai dati, in particolar modo se questi non sono segregati all'interno dei confini nazionali, può essere compromesso da forzature sui fornitori stranieri.

Informazioni su Fondazione per la Sostenibilità Digitale:

La [Fondazione per la Sostenibilità Digitale](#) è la prima Fondazione di Ricerca in Italia che analizza le correlazioni tra trasformazione digitale e sostenibilità con l'obiettivo di supportare istituzioni e imprese nella costruzione di un futuro migliore. La sua mission è quella di studiare le dinamiche indotte dalla trasformazione digitale, con particolare riferimento agli impatti sulla sostenibilità ambientale, culturale, sociale ed economica. In quest'ottica la Fondazione

sviluppa attività di ricerca, fornisce letture ed interpretazioni della trasformazione digitale, offre indicazioni operative per gli attori coinvolti, intercetta i trend del cambiamento e ne analizza gli impatti rispetto allo sviluppo sostenibile. La Fondazione agisce attraverso una struttura costituita da esperti indipendenti, istituzioni, imprese e università.

Ai soci e partner della Fondazione si affianca la Rete delle Università che costituisce il sistema di competenze al quale fa riferimento la Fondazione per lo sviluppo dei suoi progetti e che rappresenta un esempio virtuoso di collaborazione tra istituzioni ed aziende nello sviluppo di progetti e di attività dedicati alla sostenibilità digitale. Tra le Università che fanno parte della Rete, **l'Università Sapienza di Roma, l'Università di Pavia, l'Università Ca' Foscari di Venezia, l'Università degli Studi di Cagliari, l'Università degli Studi di Palermo, l'Università degli Studi di Firenze, l'Università degli Studi di Trieste, l'Università degli Studi di Perugia, l'Università per Stranieri di Perugia, l'Università di Siena, l'Università degli Studi di Urbino Carlo Bo, l'Università degli Studi di Torino, l'Istituto di Studi Politici "S. Pio V", l'Università degli Studi di Sassari, Università del Salento.**

Informazioni su Gyala

Gyala, grazie a una profonda e pluriennale esperienza in ambito **Difesa** ha creato soluzioni estremamente innovative per proteggere le **risorse strategiche IT / OT** delle aziende pubbliche e private. L'obiettivo raggiunto è stato quello di introdurre un **diverso livello di Cyber Security** attraverso un sistema **«all-in-one»**, per qualsiasi tipo di dispositivo e sistema operativo, potenziato da un sofisticato sistema di AI di supervisione e reazione automatica in grado di garantire la stabilità e resilienza degli ambienti IT / OT.

www.gyala.com

Contatti per la stampa:

Prima Pagina Comunicazione

Vilma Bosticco: vilma@primapagina.it

Laura Castellazzi: laura@primapagina.it Cell: 3518739212