Data Protection e Cyber Resilience: all'Open Day SMI 2026 un confronto tra imprese, PA e partner tecnologici sulle sfide della resilienza digitale

La quarta edizione dell'evento organizzato da SMI Group ha riunito a Roma rappresentanti del settore pubblico e privato, aziende tecnologiche e decision maker per una giornata dedicata alla protezione del dato, alla continuità operativa e alla cyber resilience come leva strategica per il business

Roma, 5 giugno 2026 – La sicurezza del dato non è più soltanto una questione tecnologica: è un tema che riguarda **la continuità operativa, la competitività delle organizzazioni e la capacità di garantire la resilienza dei processi** in un contesto sempre più digitale e interconnesso. È da questa consapevolezza che ha preso forma la **quarta edizione** dell'**Open Day SMI 2026**, dedicata al tema *"**Data Protection and Cyber Resilience**"*, ospitata ieri 4 giugno negli spazi di **Villa Alberico** a **Roma**.

L'evento, organizzato da **SMI Group** – ecosistema di aziende tecnologiche composto dalla capogruppo **S.M.I. Technologies and Consulting**, **Younified**, **Wyl** e **SM Innovation Polska** – ha riunito rappresentanti di **Ministeri, enti pubblici, università, strutture sanitarie, aziende e partner tecnologici** in un momento di confronto dedicato alle strategie, alle tecnologie e alle competenze necessarie per proteggere dati e processi critici e garantire continuità al business.

Ad aprire i lavori **Cinzia Mingiardi**, Chief Marketing Officer di SMI Group, che ha illustrato il valore dell'Open Day come **occasione di incontro tra innovazione tecnologica, bisogni delle organizzazioni e applicazioni concrete**: «*L'Open Day SMI Group conferma la forza di un format nato per mettere a fattor comune competenze, esperienze e visioni diverse. La presenza dei nostri partner tecnologici rappresenta un elemento fondamentale di questo percorso: affrontare sfide complesse come la Data Protection e la Cyber Resilience richiede collaborazione, specializzazione e capacità di guardare insieme all'evoluzione del mercato*».

Tre le parole chiave emerse nel corso della prima parte della mattinata, **tre concetti cardine** su cui impostare ogni strategia di protezione del dato: **responsabilità**, **consapevolezza**, **fiducia.**

Cesare Pizzuto, CEO e Founder di SMI Group, ha posto l'accento sull'importanza della **responsabilità** e della **consapevolezza**: "Oggi la vera sfida non è soltanto adottare nuove tecnologie, ma sviluppare la capacità di governarle. Come SMI crediamo che il nostro ruolo vada oltre la progettazione di infrastrutture e soluzioni digitali: vogliamo contribuire a costruire una comunità educante, capace di generare conoscenza, consapevolezza e fiducia. *Le tecnologie proteggono il dato, ma noi abbiamo la responsabilità di proteggere il futuro*".

Sul tema della **fiducia** si è focalizzato l'intervento di **Stefano Tiburzi**, COO e Co-Founder di SMI Group: «*Camminando in montagna, si impara una lezione fondamentale: non ci si affida alla persona più equipaggiata, ma a quella che di fronte a un bivio sa indicare la direzione giusta. Per conquistare la fiducia dei nostri clienti non dobbiamo essere solo i più competenti, ma aiutarli a prendere decisioni che garantiscano continuità e crescita nel tempo».*

Proteggere, garantire continuità, ripartire: il valore della Cyber Resilience

Il confronto è proseguito con **due panel** moderati da Marco Maria Lorusso, che hanno coinvolto alcuni dei principali **Vendor Partner** dell'ecosistema SMI.

Il primo, dedicato al tema *"**Proteggere, garantire continuità, ripartire: il valore della Cyber Resilience**"*, ha visto la partecipazione dei partner **Rubrik, WatchGuard, OPSWAT e MongoDB**. Sono intervenuti: **Mario Noioso**, EMEA Public Sector Advisory Solutions Architect di MongoDB; **Emilio Tonelli**, Solution Engineer di Opswat; **Fabio Zambon**, Regional Director di Rubrik; **Gioacchino D'Amore**, Channel Account Manager di WatchGuard.

Il confronto ha messo in luce come la resilienza informatica sia oggi un elemento strategico per assicurare la continuità operativa delle organizzazioni. Dal confronto è emersa la **necessità di superare un approccio esclusivamente orientato alla rilevazione delle minacce** per adottare modelli sempre più preventivi. Al centro del dibattito anche **il ruolo del dato**: **un asset fondamentale da proteggere e rendere sempre disponibile** attraverso infrastrutture flessibili e progettate per favorire il recupero rapido delle attività.

I relatori hanno poi evidenziato **come la cyber resilience non si esaurisca nelle tecnologie di backup o recovery**, ma richieda processi, cultura e capacità di risposta in tempo reale. In questo scenario, assume un ruolo chiave l'evoluzione verso ecosistemi di sicurezza integrati e modelli **Zero Trust**, basati sulla verifica continua di utenti, dispositivi e accessi, in un contesto in cui la protezione deve estendersi all'intero ecosistema digitale.

Identità, governance e disponibilità: i pilastri della sicurezza del dato

Il secondo panel si è focalizzato sul tema *"**Identità, governance e disponibilità: i pilastri della sicurezza del dato"***. Sono intervenuti: **Oronzo Ungaro**, Territory Account Manager di **CheckPoint**; **Luca Galloni**, Strategic Partner Sales Manager di **Dynatrace**; **Massimiliano Moschini**, Presales Manager di **Veeam**.

Nel corso del panel è emerso come la protezione delle informazioni richieda oggi **un approccio sempre più integrato, capace di coniugare tecnologia, processi e consapevolezza organizzativa**. La crescente complessità degli ecosistemi digitali, amplificata dall'intelligenza artificiale, rende necessario adottare strumenti avanzati in grado di correlare dati provenienti da fonti diverse, monitorare in modo continuo infrastrutture e applicazioni e individuare tempestivamente potenziali criticità.

Centrale resta inoltre il **fattore umano**: la formazione e la consapevolezza degli utenti continuano a rappresentare elementi decisivi per ridurre l'esposizione alle minacce e definire strategie di sicurezza efficaci.

Ampio spazio è stato dedicato anche al tema della **continuità operativa**, con un cambio di paradigma che sposta l'attenzione dal semplice backup alla capacità di garantire una ripartenza rapida e sicura in caso di incidente. In quest'ottica, assumono un ruolo fondamentale la **definizione di procedure documentate e testate**, la **protezione dei sistemi di backup** e **l'immutabilità del dato**.

Trend, criticità e prospettive della Cyber Resilience: gli interventi dei Platinum Partner

La sessione plenaria è stata completata dagli interventi dei **Platinum Partner**: **F5**, **OpenText** e **Oracle**. Sono intervenuti: **Paolo Pambianco**, Sr Principal Solutions Engineer di **F5**; **Vito Volpini**, CISSP – CISM – CEH Security Solution Achitect di **OpenText**; e **Stefano Bucci**, Country Leader Account Cloud Engineering for Data Platform di **Oracle**.

I relatori hanno approfondito **l'evoluzione delle strategie di protezione del dato** nell'era dell'intelligenza artificiale, evidenziando **la necessità di un approccio alla sicurezza sempre più integrato e proattivo**. Al centro del confronto, la protezione dell'intero ciclo di vita di applicazioni e dati, per individuare vulnerabilità, governare gli accessi e monitorare le minacce in tempo reale.

È stato inoltre sottolineato come la diffusione di modelli generativi e agenti AI renda **fondamentale conoscere dove risiedono i dati, garantirne l'integrità e controllarne l'utilizzo nelle nuove pipeline applicative**. In questo scenario assumono un ruolo sempre più rilevante la **cifratura avanzata**, la **protezione dei dati sensibili**, i **modelli Zero Trust** e gli strumenti di osservabilità e correlazione degli eventi. È infine emersa l'importanza di **prepararsi ai futuri scenari tecnologici**, adottando misure capaci di garantire continuità operativa e resilienza di fronte alle **sfide dell'intelligenza artificiale e del quantum computing**.

Incontri One to One: aziende, partner tecnologici e specialisti a confronto

A conclusione della prima parte della giornata, hanno preso il via le attività di approfondimento previste dal format dell'Open Day: gli **incontri One to One** tra partecipanti, partner tecnologici ed esperti SMI, pensati per favorire un **confronto diretto sulle esigenze specifiche delle organizzazioni e sulle possibili strategie di evoluzione** in ambito cybersecurity e data protection.

L'Open Day di SMI Group si configura infatti anche come **epicentro di connessioni e opportunità**, come ricorda **Stefano Novelli**, General Manager di SMI Group: «*È un evento per noi importantissimo perché il nostro ecosistema si fonda sui Vendor, che sono il veicolo attraverso cui raggiungiamo il cliente finale. Un evento come questo crea opportunità, poiché unisce gli operatori del mercato*».

Una visione condivisa da **Marco Valenti**, Chief Revenue Officer di SMI Group, che ha enfatizzato «*il ruolo fondamentale della costruzione dell'ecosistema tra partner, tecnologia e system integrator. Tre realtà che insieme possono costruire l'identità di una proposizione che risolve i problemi delle imprese e pubbliche amministrazioni a cui diamo un supporto operativo*».

Le novità dell'edizione 2026: la Executive Round Table

Tra le principali novità dell'edizione 2026, la **Executive Round Table** dal titolo "***Oltre la sicurezza del dato: le giuste domande che guidano la resilienza del business***", che ha riunito il top management di SMI Group, i Platinum Partner F5, OpenText e Oracle e un gruppo selezionato di manager. Un momento di dialogo particolarmente apprezzato dai partecipanti: «*Una giornata molto interessante insieme a clienti e attori del mercato, focalizzata su resilienza e continuità operativa*», ha commentato **Paolo Capomasi**, Country Manager di **F5**.

Anche **Mario Nicosia**, Vice President Technology Country Leader Italy di **Oracle**, ha evidenziato il valore del confronto, sottolineando come l'Open Day sia stato «*uno dei pochissimi eventi in cui nel titolo non compariva l'Intelligenza Artificiale. Abbiamo parlato di resilienza e di protezione dei dati, raccogliendo spunti molto interessanti dalle aziende e dagli operatori*».

Un aspetto richiamato anche da **Pierpaolo Alì**, Director Southern Europe, CIS, CEE & Israel di **Open Text**, che ha definito l'iniziativa «*un confronto tecnologico su quanto sia importante la protezione dell' hardware e la cyber resilience in ottica di governance e continuità operativa*».

La quarta edizione dell'Open Day si conferma quindi **un punto di incontro tra competenze, innovazione e visione strategica**, consolidando il percorso avviato da SMI Group per promuovere una cultura della sicurezza orientata alla protezione del dato e alla resilienza del business.

* * *

SMI Group

SMI Group, nato nel 2015 come SMI, è un ecosistema di aziende tecnologiche fondato e guidato da SMI Technologies and Consulting, che comprende Younified, Wyl e SM Innovation Polska. Con oltre 300 professionisti e una presenza consolidata in Italia e in Polonia, il Gruppo supporta aziende e istituzioni nei processi di trasformazione digitale attraverso competenze integrate nell'Information Technology, nell'automazione industriale e nella consulenza strategica. Opera in diversi settori, tra cui alimentare, metalmeccanico, tessile, ICT, manifatturiero, siderurgico, farmaceutico e chimico. www.smi-group.it

Ufficio Stampa SMI Group