APRILE 2026

Cyber Magazine

IN QUESTO NUMERO
INTERVISTA A

Milena Antonella Rizzi

Capo del Servizio Regolazione
dell'Agenzia per la Cybersicurezza Nazionale

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

CYBER
Think Tank
ASSINTEL

CYBER
Think Tank
ASSINTEL

COORDINATORE CYBER THINK TANK

ANTONIO ASSANDRI

COMITATO SCIENTIFICO

ANTONIO ASSANDRI, GIANPIERO COZZOLINO,
PAOLO MONTALI, VITTORIO OREFICE, RANIERI RAZZANTE

REDAZIONE

A CURA DI ASSINTEL

SEGRETERIA@ASSINTEL.IT
WWW.ASSINTEL.IT

CYBER Think Tank ASSINTEL

Indice

CYBER Think Tank ASSINTEL

Indice

CYBER Think Tank ASSINTEL

Indice

L’editoriale del Coordinatore del Cyber Think Tank Antonio Assandri

APRILE 2026

Carissimi lettori,

benvenuti in questa nuova edizione del Cyber Magazine.

Apriamo questo numero con un’intervista al Prefetto Milena Antonella Rizzi, Capo del Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale, che ci accompagna in una riflessione sul ruolo della cybersecurity nel contesto attuale, tra sicurezza nazionale, protezione delle infrastrutture critiche e crescente attenzione al quadro normativo europeo, a partire dalla direttiva NIS2. Un contributo che aiuta a inquadrare con chiarezza le sfide che imprese, soprattutto le PMI, e istituzioni sono chiamate ad affrontare.

Proseguiamo con una serie di articoli che raccolgono punti di vista diversi ma complementari, offrendo uno sguardo ampio su un panorama in continua evoluzione. L’ormai imprescindibile intelligenza artificiale, la gestione del rischio lungo la supply chain, la resilienza operativa, il tema della governance della sicurezza e quello della sovranità digitale sono solo alcuni degli ambiti che emergono con forza in questo numero. Insieme a sempre utili approfondimenti su NIS2 e DORA.

Questa edizione rappresenta anche un momento di evoluzione per il nostro Magazine: abbiamo lavorato su un aggiornamento del formato grafico e dell’impaginazione, con l’obiettivo di rendere la lettura più fluida e valorizzare ulteriormente i contenuti. Un cambiamento che accompagna la crescita del progetto e della community che lo rende possibile.

Per me, questo è il primo numero in qualità di Coordinatore del Cyber Think Tank. Raccolgo questo ruolo con senso di responsabilità e con la volontà di dare continuità a un percorso costruito in questi ultimi anni da Pierguido Iezzi, che ringrazio per il lavoro svolto e per aver contribuito a far crescere il Cyber Magazine fino a renderlo uno spazio riconosciuto di confronto e approfondimento.

Il nostro obiettivo resta quello di continuare a promuovere una cultura della cybersecurity sempre più diffusa e consapevole, capace di accompagnare imprese e organizzazioni in un contesto che richiede attenzione, competenze e visione.

Buona lettura!

CYBER Think Tank ASSINTEL

INTERVISTA

A colloquio con il Prefetto Milena Antonella Rizzi Capo del Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale

Laurea in Giurisprudenza con lode, Università degli studi di Genova e abilitazione all'esercizio della professione forense. Master in "Cittadinanza europea e amministrazioni pubbliche", SSAI/Terza Università di Roma. Master in "Sicurezza economica, geopolitica ed intelligence", SIOI. First Certificate in English, Università di Cambridge e Diploma Superiorde Español, Università di Salamanca. Dottore di ricerca in Studi Giuspubblicistici, Università di Roma Tor Vergata.
Carriera oltre trentennale presso il Ministero dell'interno, molteplici incarichi a livello periferico, centrale ed in ambito europeo (Commissione Europea, DG HOME e Rappresentanza Permanente d'Italia presso l'Unione Europea). Dal 2016 al 2021 Capo Staff di diversi uffici del Gabinetto del Ministro dell'interno, tra cui dal 1° agosto 2020 Capo della Segreteria Tecnica del Ministro. Cdm 12/01/2022 nominata Prefetto. Cdm 31/10/2022 collocata fuori ruolo presso l'Agenzia per la cybersicurezza nazionale; dal 7/11/2022 Capo del Servizio Regolazione (già Autorità e sanzioni).
Molteplici incarichi di docenza in materia di prevenzione antimafia, di governo locale della sicurezza, di normazione anche tecnica nel settore della cybersicurezza (Università Luiss e Università Sapienza di Roma). Autrice di pubblicazioni in materia di prevenzione antimafia per le case editrici Dike e Giappichelli nonché in materia di cybersicurezza e cyberresilienza per la Rivista Italiana di Informatica e Diritto.

Al fine di agevolare le imprese nel comprendere meglio la NIS2 (dubbi interpretativi, quesiti e incertezze), quali azioni ha sviluppato ACN e quali ha in programma, anche attraverso la collaborazione con le associazioni?

La Direttiva UE 2022/2555, meglio nota come NIS2, ha rafforzato l'approccio alla sicurezza informatica per le Istituzioni e le aziende che rientrano nel suo rinnovato ambito di applicazione che risponde all'evoluzione della minaccia cyber, ormai interessata a soggetti diversi dalle classiche "infrastrutture critiche".
Sono direttamente impattati dalla nuova disciplina, recepita con il decreto legislativo 4 settembre 2024, n. 138, c.d. decreto NIS, oltre 80 tipologie di soggetti operanti in almeno uno dei 18 settori, di cui 11 altamente critici (originariamente erano 8) e 7 critici (che non erano contemplati dalla precedente Direttiva 2016/1148, alla quale va comunque riconosciuto il merito di essere stata la prima normativa europea orizzontale in materia di sicurezza informatica.).
Stiamo parlando di oltre 20.000 soggetti che sono tenuti ad applicare le misure di sicurezza su tutta la loro infrastruttura digitale e quindi anche a protezione degli assetti ritenuti meno rilevanti, che spesso sono la porta di accesso sfruttata dagli attaccanti per avvicinarsi, tramite i c.d. movimenti laterali, al tesoro digitale dell'impresa presa di mira.
In questo contesto, per favorire concretamente il progressivo rafforzamento della postura di cybersicurezza dei soggetti NIS – molti dei quali operanti in settori precedentemente non attinti dalla

normativa cyber – l'Agenzia per la cybersicurezza nazionale, nella sua qualità di Autorità nazionale competente NIS, ha adottato un approccio innovativo, capace di coniugare le esigenze della regolazione con la definizione di un percorso sostenibile per tutti i soggetti coinvolti, in cui le iniziative a sostegno della costituency NIS hanno svolto un ruolo fondamentale.
In particolare, al fine di fornire supporto ai soggetti NIS, il sito istituzionale dell'Agenzia per la cybersicurezza è stato arricchito con una sezione dedicata alla nuova disciplina, nonché un ampio catalogo di risposte a domande frequenti.
Inizialmente pubblicata nel mese di dicembre 2024 con chiarimenti di carattere generale, con il progressivo sviluppo dell'attività regolamentare sono state pubblicate ulteriori sezioni inerenti alle specifiche di base in materia di misure di sicurezza, alle notifiche di incidente e all'uso dei servizi NIS resi disponibili tramite il Portale dei Servizi.
Il patrimonio informativo messo a disposizione degli utenti risiede oggi in 150 risposte a domande frequenti, suddivise per argomento tematico in 4 sezioni e 30 sottosezioni costantemente aggiornate.
Inoltre, per accompagnare i soggetti NIS nella comprensione e interpretazione del testo delle "Specifiche tecniche di base", adottate, in via definitiva, con la determinazione del Direttore generale di ACN, n. 379907 del 19 dicembre 2025, sono state pubblicate due Linee guida, recanti, rispettivamente, la "Guida alla lettura" e la "Definizione del processo di gestione degli incidenti di sicurezza informatica". In particolare, tale documento suggerisce un modello per il processo di gestione degli incidenti e descrive la relazione tra le fasi del processo e le misure di sicurezza di base.
A complemento del supporto documentale, l'Agenzia ha inoltre attivato un c.d. service desk tramite il quale i soggetti possono porre quesiti e richiedere assistenza per difficoltà di carattere tecnico-procedurale. Nel corso del 2025, sono state evase oltre 45.000 richieste, di cui circa il 60% relative a chiarimenti tecnico-procedurali per l'interazione con il Portale dei Servizi che, nell'ottica della semplificazione dei procedimenti amministrativi, rappresenta lo strumento tramite il quale i soggetti NIS assolvono agli obblighi di comunicazione con l'Autorità nazionale competente NIS.
Una particolare menzione, per il valore aggiunto apportato all'interazione con i soggetti NIS, a complemento delle attività istituzionali condotte nel contesto dei Tavoli settoriali, va effettuata con riferimento alla collaborazione con le associazioni di categoria e le realtà istituzionali e locali, con le quali, nel corso del 2025, è stato organizzato il 25% delle 60 iniziative realizzate nel corso dell'anno.
Tali attività si sono concretizzate, tra l'altro, in eventi informativi e formativi, incontri di approfondimento tematico, momenti di confronto tecnico e iniziative di assistenza e chiarimento, di cui l'85% è stato realizzato in presenza e il restante 15% videoconferenza.
La sinergia con le associazioni rappresentative di categoria ha favorito il rafforzamento della conoscenza del quadro regolatorio applicabile, un'interpretazione uniforme delle disposizioni vigenti contribuendo a promuovere elevati livelli di conformità e responsabilità operativa.
Questo proficuo e strutturato dialogo con gli stakeholder, mediato dalle associazioni di categoria, proseguirà nel 2026 con ulteriori iniziative di confronto, in un'ottica di sinergico scambio di informazioni e buone pratiche capace di favorire l'emersione di potenziali elementi da valutare nelle successive fasi dell'attività legislativa e regolamentare di attuazione.

La NIS2 riguarda anche le PMI, soprattutto quali parte di una supply chain. Il rischio è che si scarichi su di loro un onere di compliance sproporzionato, rispetto alle loro capacità sia economiche che organizzative. Assintel più volte ha lanciato questo allarme. A suo avviso ACN, insieme alle associazioni di categorie e al Governo, come potrebbe collaborare per supportare tali difficoltà?

Innanzitutto, va evidenziato che le PMI, in quanto (potenziali) parti di una supply chain, non sono automaticamente attratte nell'ambito di applicazione della nuova disciplina NIS, fatta eccezione per i fornitori c.d. sistemici che saranno individuati nel corso del 2026.

In merito al paventato rischio di un onere sproporzionato di compliance a carico dei fornitori va premesso che, in continuità con quanto fatto nel percorso di attuazione della direttiva NIS1 e in coerenza con quanto previsto dall'attuale quadro normativo nazionale in materia di cybersicurezza, anche le misure di sicurezza NIS2, rientranti nei 10 ambiti di sicurezza fissati dalla direttiva europea stessa, sono state definite nel contesto del framework nazionale per la cybersecurity e la data protection.
Ciò ha consentito di valorizzare gli esiti delle interlocuzioni avviate con le Autorità di settore nell'ambito dei tavoli settoriali e con le associazioni di categoria resesi disponibili a realizzare concrete forme di partenariato pubblico privato, attraverso il coinvolgimento degli operatori ad esse associati, i cui contributi sono stati presi in considerazione nel processo di elaborazione delle cennate misure.
Va poi osservato che nella declinazione degli obblighi sono stati tenuti in considerazione i principi di proporzionalità e di gradualità, l'ampiezza della platea dei soggetti cui si indirizzano (la maggior parte dei quali senza alcuna pregressa esperienza in materia o competenza interna), il periodo di riferimento per la loro attuazione e il severo impianto sanzionatorio.
Nell'elaborazione dei citati obblighi, è stato fatto uno sforzo di calibrazione e chiarimento che, con particolare riferimento alle previsioni concernenti la catena di approvvigionamento – considerata la sua rilevanza per le ripercussioni sistemiche che possono essere causate da un incidente subìto da un fornitore – si è giovato del contributo di un gruppo di lavoro ristretto, composto da rappresentanti del tessuto imprenditoriale e di alcune organizzazioni rappresentative di categoria.
In particolare, per la definizione delle misure di sicurezza a protezione della catena di approvvigionamento, è stato delineato un processo che prevede 4 fasi:

- valutazione del rischio associato alla fornitura, ogni fornitura è infatti caratterizzata da un proprio rischio, non solo per via della sua tipologia (servizio ICT, fornitura Cloud, consulenza, etc.) ma anche in base al sistema informativo e di rete sul quale verrà impiegata;
- definizione dei requisiti di sicurezza, la sicurezza della fornitura è realizzata tramite la previsione di requisiti di sicurezza definiti sulla base del rischio associato alla fornitura;
- enforcement dei requisiti di sicurezza, ovvero garantire che i requisiti definiti siano applicati, prevedendo l'inserimento dei requisiti nei bandi di gara, nei contratti e in generale negli accordi con i fornitori;
- verifica dei requisiti di sicurezza, per validare che le specifiche indicate dai requisiti siano effettivamente soddisfatte, attraverso la verifica della conformità delle forniture ai requisiti di sicurezza definiti.

In accordo con tale processo sono state quindi definite 5 misure di sicurezza per la supply chain nelle quali i requisiti specificano cosa è richiesto ai soggetti ai fini dell'implementazione della misura, favorendo così una più omogenea applicazione della disciplina che si traduce in una riduzione degli oneri amministrativi di compliance.

La NIS2 introduce responsabilità dirette per gli organi di gestione delle imprese. Come si coordina questo principio con il sistema di responsabilità previsto dal diritto societario italiano e quali saranno i criteri con cui ACN valuterà l'adeguatezza delle misure adottate dai board?

Anche in questo caso va preliminarmente evidenziato che il principio di responsabilità, stabilito dall'articolo 23 del decreto NIS, non è un "aliquid novi" ma si inserisce nel solco tracciato dalla disciplina della responsabilità amministrativa degli enti, operata con il decreto legislativo n.231/2001, dalla riforma del diritto societario del 2003 e dalla riforma del Codice della Crisi d'impresa e dell'insolvenza, entrata in vigore il 15 luglio 2022.
In sostanza, l'adozione dell'approccio basato sul rischio, nel rispetto di quanto stabilito dagli articoli 2381 e 2392 del codice civile, postula l'esigenza della definizione, da un lato, di ruoli, responsabilità, procedure, attribuzione di compiti e poteri, e dall'altro, di una politica di gestione del rischio cyber che sia coerente con gli esiti della ricognizione della robustezza delle difese informatiche già poste in essere dal soggetto, il contesto operativo e la strategia generale dell'organizzazione.
In quest'ottica, vale la pena di ricordare che spetta quindi al plenum consiliare, titolare dei poteri di indirizzo strategico dell'ente, procedere all'approvazione di tutte le pianificazioni per la gestione del rischio cyber, elencate nell'appendice C della "Guida alla lettura" sopra citata, supervisionarne la corretta implementazione, seguire una formazione in materia di sicurezza informatica e promuovere la formazione periodica dei loro dipendenti.
Questo impianto si pone in linea con l'evoluzione dei sistemi di amministrazione e controllo societari e con la moderna concezione del rischio "interno" dell'impresa. Ne deriva la necessità che i componenti del plenum consiliare sviluppino adeguate capacità di valutare l'idoneità delle pianificazioni di mitigazione del rischio cyber sottoposte alla loro approvazione, in modo da poter altresì esercitare una supervisione efficace.
Pertanto, nel rispetto del principio di responsabilità sopra citato, in questa fase, nelle more della pubblicazione di specifiche Linee guida, sarà possibile valutare l'adeguatezza delle misure di gestione del rischio cyber adottate dal soggetto NIS attraverso la verifica del rispetto del contenuto minimo obbligatorio predefinito dalla determinazione

del Direttore generale di ACN che ha approvato in via definitiva le Specifiche tecniche di base, tenendo in debito conto, naturalmente, le dimensioni e il grado di esposizione al rischio del soggetto stesso.

Alcune aziende italiane, anche molto piccole, fanno parte di gruppi internazionali europei. L'Italia è una tra le poche nazioni europee che hanno recepito la direttiva comunitaria NIS2. Quando NIS2 verrà recepita anche dagli altri paesi europei, le aziende italiane già NIS2-compliant ma che hanno la capogruppo estera che opera presso altre nazioni quale modello di gestione dovrebbero adottare a livello di Gruppo per evitare incoerenze e duplicazioni?

Questo tema, spesso sollevato dai soggetti NIS aventi sede in Italia e facenti parte di gruppi la cui holding è situata in un altro Stato membro, temo tragga origine da una lettura della Direttiva NIS2 focalizzata sulla struttura societaria del gruppo anziché su quella delle singole "legal entities" che ne fanno parte.
In proposito, l'Agenzia per la cybersicurezza nazionale ha già avuto modo di chiarire che gli obblighi si applicano alle singole "legal entities" secondo la giurisdizione del Paese ove sono ubicate, con la conseguenza che spetta a tali legal entities definire ed approvare le pianificazioni delle misure di gestione del rischio cyber, adottando un modello che, attraverso la mappatura dei singoli requisiti di sicurezza richiesti dai vari Stati membri in cui opera il gruppo societario, assicuri la coerenza con l'impianto regolatorio complessivamente considerato.

Le aziende ed in particolare le PMI sono preoccupate per le sanzioni che ACN potrà applicare in caso di mancato adempimento NIS2, ci può raccontare il processo sanzionatorio?

I poteri di esecuzione, che comprendono l'esercizio della leva sanzionatoria, sono disciplinati nell'ambito del Capo V del decreto NIS che rimette all'adozione di un decreto del Presidente del Consiglio dei ministri la definizione dei criteri, delle procedure e delle modalità per lo svolgimento delle attività, l'esercizio dei poteri e l'adozione dei provvedimenti ivi previsti.
Inoltre, il comma 15 dell'articolo 38, la cui rubrica recita "Sanzioni amministrative", affida anch'esso all'adozione di un decreto del Presidente del Consiglio dei ministri la definizione delle modalità di applicazione, nell'ambito del procedimento sanzionatorio, degli strumenti deflattivi del contenzioso ivi contemplati.
Nelle more dell'adozione di tali decreti, vale la pena di evidenziare che l'articolo 35, nel disciplinare le attività di monitoraggio, analisi e supporto dell'Autorità nazionale competente NIS, al fine di evitare che possano concretizzarsi i presupposti della violazione, espressamente prevede che nello svolgimento delle suddette attività la predetta Autorità possa "emanare raccomandazioni e avvertimenti relativi a presunte violazioni del presente decreto da parte dei soggetti interessati", implementando altresì interventi di supporto per i soggetti medesimi, qualora ciò non costituisca un onere sproporzionato o eccessivo.
Non solo. Laddove tali raccomandazioni e avvertimenti non dovessero sortire il risultato atteso, l'articolo 37, la cui rubrica recita "Misure di

esecuzione", prevede che l'Autorità nazionale competente NIS – previa notifica ai soggetti interessati delle conclusioni preliminari sulle attività di monitoraggio e verifica, con la quale deve essere concesso a questi ultimi un termine ragionevole, comunque non inferiore a quindici giorni, per presentare osservazioni – possa rivolgere al soggetto inadempiente specifiche intimazioni, quali quelle indicate dalle lettere d), e) e f) del cennato articolo, indicando modalità e termini ragionevoli e proporzionati per adempiere nonché per riferire circa lo stato di attuazione degli adempimenti.
In caso di inerzia del soggetto, e previa notifica anche in questo caso delle conclusioni preliminari, sarà possibile emettere una formale diffida ad adempiere ai sensi dell'articolo 37, comma 6, del decreto NIS, recante modalità e termini ragionevoli e proporzionati per adempiere nonché per riferire circa lo stato di attuazione degli adempimenti.
Va evidenziato, al riguardo, che ai sensi dell'articolo 38, comma 4, del decreto NIS, l'esercizio dei poteri di cui all'articolo 37 (i.e. intimazione/diffida) non impedisce la contestazione delle violazioni di cui ai commi 8 e 10 del predetto articolo, nonché la relativa irrogazione delle sanzioni amministrative previste dal cennato articolo 38 che, come noto, sono di elevato importo (10 milioni di euro o 2% del fatturato per i soggetti essenziali e 7 milioni di euro o 1,4% del fatturato per i soggetti importanti) cui si affiancano, in taluni casi, specifiche sanzioni accessorie.

In conclusione, è evidente che adempiere agli obblighi proporzionati e graduali imposti dalla nuova disciplina NIS non è solo una questione di compliance ma consente all'organizzazione, dotata di una governance proattiva fondata sulla cultura della resilienza, di conseguire un vantaggio competitivo e proteggere i propri dati, le proprie attività, i propri servizi e la continuità operativa.

Ci può brevemente raccontare il cronoprogramma di ACN in ambito NIS2 e quindi quali saranno i prossimi step che le aziende dovranno svolgere per essere compliant?

Innanzitutto merita di essere ricordato che per i soggetti NIS inseriti nell'elenco 2025, lo scorso gennaio è entrato in vigore l'obbligo di procedere alla notifica degli incidenti significativi di cui agli allegati 3 e 4 alla Determinazione ACN n. 379907/2025, che si è sommato a quello di aggiornare la bozza di Dichiarazione precompilata che è stata resa loro disponibile, tramite la piattaforma digitale NIS, sulla base delle informazioni trasmesse in occasione della registrazione 2025.
Come noto, infatti, dal 1° gennaio ed entro il 28 febbraio di ogni anno i soggetti sono chiamati a registrarsi sulla piattaforma NIS o ad aggiornare la propria dichiarazione di registrazione effettuata nell'annualità precedente.
Entro il mese di aprile 2026, verrà quindi elaborato l'elenco dei soggetti NIS 2026 ai quali verrà inviata formale comunicazione di inserimento e/o permanenza e/o espunzione, al fine di favorire l'attuazione dei successivi adempimenti.
Conseguentemente, dal 15 aprile ed entro il 31 maggio 2026, i soggetti che riceveranno la comunicazione di inserimento/permanenza nell'elenco dei soggetti NIS dovranno effettuare l'aggiornamento annuale delle informazioni di cui all'articolo 7, commi 4 e 5, del decreto NIS, tramite il Servizio NIS/Aggiornamento annuale informazioni.
Inoltre, i medesimi soggetti, dal 1° maggio ed entro il 30 giugno 2026, dovranno comunicare, tramite la piattaforma digitale NIS, l'elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e alla relativa attribuzione di una categoria di rilevanza, secondo quanto previsto dall'articolo 30 del decreto NIS.
Infine, entro ottobre 2026 i soggetti NIS inseriti per la prima volta in elenco nel 2025, dovranno assicurare la completa implementazione delle misure di sicurezza di base di cui agli allegati 1 e 2 alla Determinazione ACN n. 379907/2025, mentre per i soggetti NIS inseriti per la prima volta in elenco nel 2026 l'obbligo di notifica e quello di implementazione delle misure di sicurezza diverrà cogente a partire, rispettivamente, da gennaio 2027 e luglio 2027.

Profili e retribuzioni nella Cybersecurity: analisi di 5 ruoli chiave

A cura di Luca Balbo

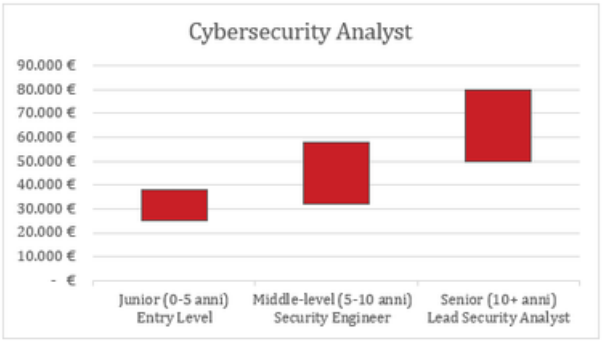
Il settore della cybersecurity è in rapida espansione a livello globale: si prevede che il mercato raggiungerà i 351,9 miliardi di dollari entro il 2030. Nonostante la sua rilevanza strategica, l'Italia investe solo lo 0,12% del proprio PIL nazionale nella cybersecurity, un dato destinato a cambiare nel breve periodo, soprattutto alla luce degli ultimi dati: oltre 3.500 incidenti informatici registrati a livello mondiale hanno collocato l'Italia tra i principali bersagli, confermando l'urgenza di un rafforzamento del settore.

In questo contesto, la cybersecurity si conferma una leva competitiva imprescindibile per imprese pubbliche e private di ogni dimensione, richiedendo professionisti con competenze specializzate in aree come intelligenza artificiale (AI), cloud e conformità normativa, in grado di collaborare in team strutturati e di affrontare le minacce con solide capacità comunicative e di problem solving.
Riteniamo siano 5 le figure chiave, che ci consentono una fotografia completa e aggiornata del mercato: Cybersecurity Analyst, Penetration Tester, Security Architect, Specialista Governance e Risk & Compliance (GRC).

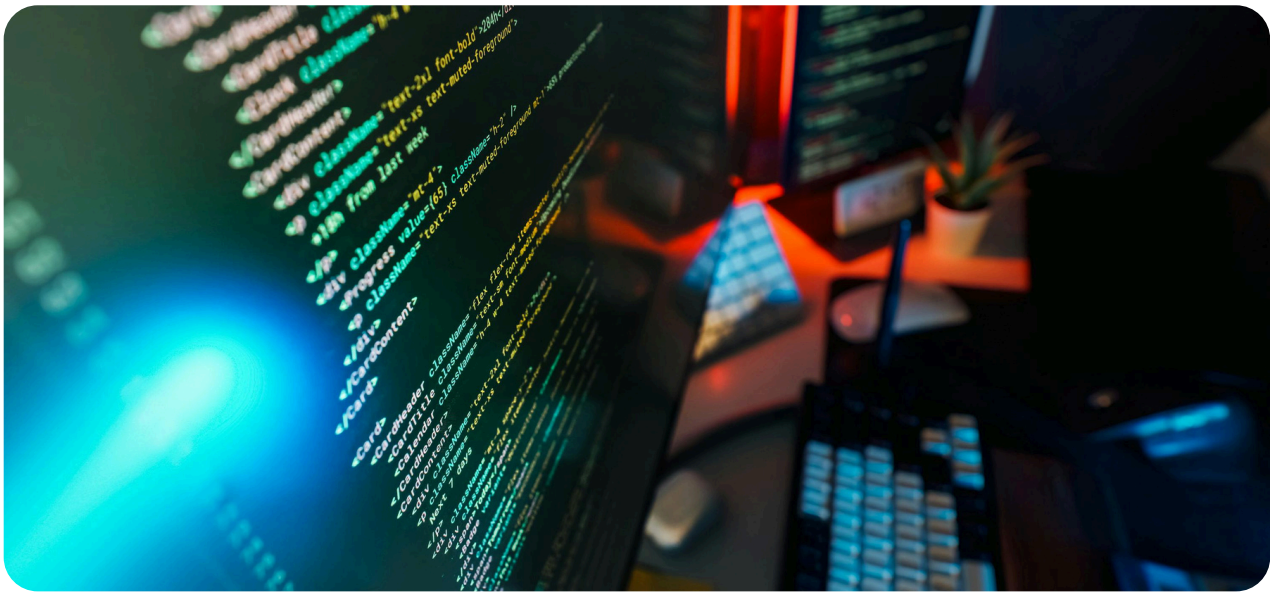
CYBERSECURITY ANALYST

Il Cybersecurity Analyst ha il compito di proteggere sistemi, reti e dati di un'organizzazione da minacce e attacchi informatici. Il suo ruolo è fondamentale per prevenire, rilevare e gestire incidenti, garantendo l'integrità, la riservatezza e la disponibilità delle informazioni. In Italia, la domanda per questa figura è cresciuta del 18% rispetto all'anno precedente, con particolare richiesta da parte di società di consulenza, istituti bancari, aziende del settore aerospaziale e della difesa.

Il ruolo offre interessanti prospettive di crescita retributiva: si parte da posizioni Junior con stipendi compresi tra €25.000 e €38.000, si passa a ruoli come Security Engineer e, con almeno dieci anni di esperienza, è possibile raggiungere posizioni manageriali, come quella di Lead Security Analyst.



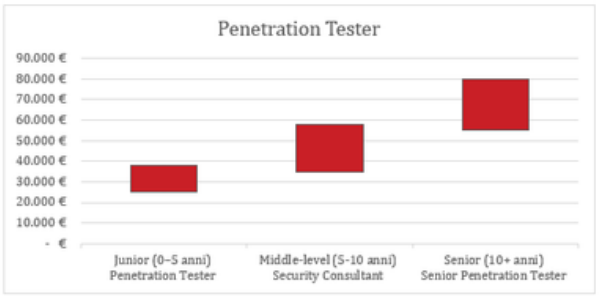
Fonte: Hunters Group



PENETRATION TESTER

Un Penetration Tester, o Ethical Hacker, è un esperto di cybersecurity che simula attacchi informatici autorizzati contro sistemi, reti, applicazioni web e mobile, o altre infrastrutture IT di un'organizzazione. L'obiettivo è identificare e sfruttare le vulnerabilità prima che possano essere sfruttate da attaccanti malevoli, fornendo successivamente raccomandazioni e soluzioni correttive. Negli ultimi dodici mesi, la domanda per questa figura è cresciuta del 7%, con particolare richiesta nei settori dei servizi, della sicurezza informatica e dello sviluppo software.

La carriera del Penetration Tester inizia con la posizione Junior (fino ai 3 anni di esperienza), che richiede competenze tecniche di base e capacità operative standard. Con l'acquisizione di competenze avanzate, è possibile progredire verso ruoli come Security Consultant, operando all'interno di team strutturati, fino ad arrivare a posizioni che prevedono il lavoro in un Security Operation Center (SOC).

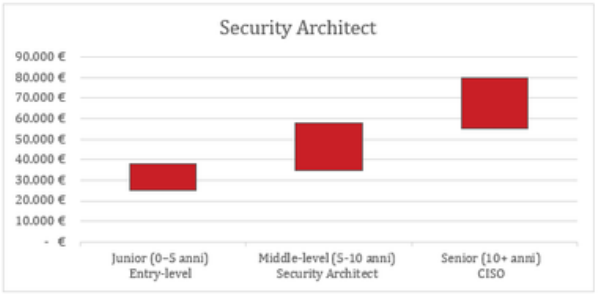


Fonte: Hunters Group

SECURITY ARCHITECT

Il Security Architect progetta, costruisce e supervisiona l'intera architettura di sicurezza informatica di un'organizzazione. A differenza di chi si occupa di singoli componenti o del monitoraggio quotidiano, l'Architect ha una visione strategica e olistica, garantendo coerenza e robustezza nelle difese.

La carriera di un Security Architect inizia con la posizione Junior (0-3 anni di esperienza), caratterizzata da solide competenze tecniche. Grazie alla dimensione strategica del ruolo, le prospettive di crescita sono significative e spesso conducono alla posizione di Chief Information Security Officer (CISO), un ruolo di responsabilità esecutiva e coordinamento, con una RAL (Retribuzione Annua Lorda) che può raggiungere €80.000.

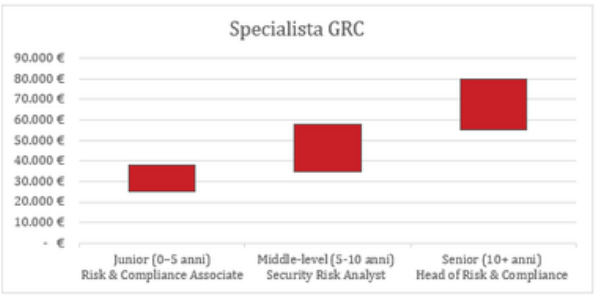


Fonte: Hunters Group

SPECIALISTA GOVERNANCE, RISK E COMPLIANCE (GRC)

Lo Specialista in Governance, Risk e Compliance (GRC) è un professionista che si occupa di allineare la strategia aziendale alla gestione del rischio e al rispetto delle normative. Il suo obiettivo è garantire che l'organizzazione operi in modo etico, legale e conforme, minimizzando i rischi e preservando la fiducia degli stakeholder.

Si tratta di una figura trasversale, che combina competenze tecniche e legali, offrendo opportunità di crescita anche a chi non possiede conoscenze tecnologiche altamente specializzate. Il percorso tipico va da Risk & Compliance Associate, a GRC Specialist o Security Risk Analyst, fino a Head of Risk & Compliance o Head of Internal Audit, con crescenti responsabilità operative e manageriali, dalla gestione di processi e audit alla supervisione strategica dei team.



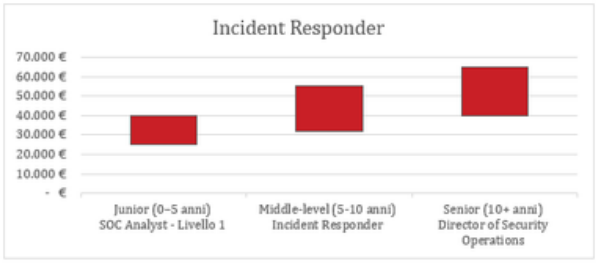
Fonte: Hunters Group

INCIDENT RESPONDER

L'Incident Responder gestisce e mitiga gli incidenti di sicurezza informatica, minimizzando i danni e ripristinando rapidamente le normali operazioni. Agisce come prima linea di difesa reattiva, combinando competenze tecniche e capacità di gestione dello stress.

Il percorso di carriera inizia con una figura junior che

si occupa prevalentemente della gestione degli incidenti informatici e dei rischi ad essi connessi, il SOC Analyst (Livello 1). Successivamente, la figura si evolve nel ruolo di Incident Responder, fino al Director of Security Operations, con responsabilità crescenti dalla gestione operativa degli incidenti alla leadership strategica del team e del centro operativo di sicurezza.



Fonte: Hunters Group

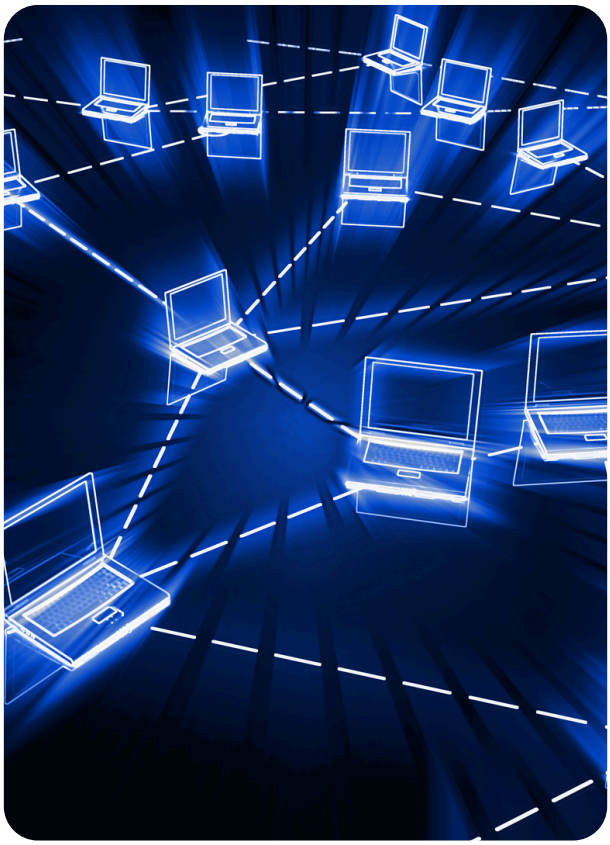
Gender Gap nel settore Cybersecurity

La domanda di figure specializzate in cybersecurity è in costante crescita, con un incremento medio annuo del **15%**, spinta dalla maggiore frequenza di attacchi informatici e dall'impatto di normative come la NIS2.

Il settore, tuttavia, presenta forti disparità di genere: la presenza femminile nel settore si aggira **mediamente tra il 15% e il 20%**, raggiungendo il 23% tra i Cybersecurity Analyst e scendendo al 14% tra i Penetration Tester, con una disparità che si accentua nei ruoli senior. Tra questi, il Security Architect è uno dei più sbilanciati, con solo l'8% di donne. Questa disparità emerge già a livello di studi universitari nei percorsi STEM, dove le studentesse rappresentano solo il 18,7% del totale, con una presenza particolarmente ridotta in corsi come Informatica e Ingegneria informatica.

La cybersecurity, quindi, si conferma un settore in forte espansione, con una domanda crescente di professionisti qualificati e percorsi di carriera ben definiti, che offrono opportunità di crescita tecnica e manageriale. Allo stesso tempo, permangono sfide significative, a partire dalle barriere di genere, che limitano la partecipazione femminile soprattutto nei ruoli più strategici e senior.

Per le aziende, investire nella formazione, nella valorizzazione del talento e nella creazione di percorsi inclusivi diventa quindi non solo un imperativo etico, ma anche un fattore competitivo per costruire team di cybersecurity più efficaci e resilienti.



NIS2 e supply chain security: la sicurezza come leva strategica per l'ecosistema europeo

A cura di Jim Biniyaz

NIS2 e supply chain security: la sicurezza come leva strategica per l'ecosistema europeo

Negli ultimi anni gli incidenti legati alla supply chain hanno evidenziato con chiarezza una dinamica ormai consolidata: una vulnerabilità in un componente ampiamente utilizzato, come nel caso di Log4j, o una compromissione a carico di un fornitore IT, è in grado di propagare i propri effetti a migliaia di organizzazioni in tempi estremamente rapidi.

Questo tipo di eventi ha reso evidente come il rischio non sia più confinato al perimetro della singola azienda, ma si sviluppi lungo l'intera filiera digitale.

La trasformazione digitale ha ulteriormente amplificato questa condizione. L'adozione di servizi cloud, l'integrazione di piattaforme SaaS, l'esternalizzazione di componenti infrastrutturali e in particolare l'intelligenza artificiale hanno aumentato il livello di interdipendenza tra organizzazioni. In molti casi, la continuità operativa dipende direttamente da soggetti terzi.

La Direttiva NIS2 (Direttiva (UE) 2022/2555), recepita in Italia con il D.Lgs. 138/2024, si colloca esattamente in questo contesto. Non introduce il tema della supply chain, ma ne riconosce formalmente la centralità, qualificandolo come elemento essenziale della resilienza complessiva.

Dalla protezione dell'organizzazione alla gestione dell'ecosistema

Per lungo tempo, la cybersecurity è stata interpretata come un ambito prevalentemente interno, focalizzato sulla protezione di asset, infrastrutture e sistemi aziendali. Oggi questo approccio risulta inevitabilmente incompleto.

Le organizzazioni operano all'interno di ecosistemi articolati, in cui fornitori cloud, piattaforme SaaS, MSP e operatori OT contribuiscono in modo diretto al funzionamento dei processi critici. In questo scenario, il rischio non resta confinato, ma si distribuisce lungo l'intera catena del valore.

L'articolo 21 della NIS2 – ripreso nel D.Lgs. 138/2024 – introduce esplicitamente la sicurezza della supply chain tra le misure richieste, con particolare attenzione ai rapporti con fornitori e service provider.

Questo implica, in termini operativi:

- la definizione di una politica di sicurezza della supply chain
- l'identificazione dei fornitori critici
- l'integrazione di requisiti di sicurezza e obblighi di notifica nei contratti
- il monitoraggio continuo della postura di sicurezza dei partner

Si tratta di un passaggio rilevante, ovvero la sicurezza non è più limitata all'organizzazione, ma diventa una responsabilità distribuita.

Supply chain: da funzione operativa a leva strategica

La supply chain non può più essere considerata esclusivamente come un ambito operativo. Le dipendenze tecnologiche, le integrazioni applicative e l'esternalizzazione dei servizi rendono ogni organizzazione parte di una rete interconnessa, in cui il livello di sicurezza complessivo è determinato dalla solidità dell'intera filiera.

Questo comporta un cambio di prospettiva:
- il rischio assume una dimensione sistemica
- la sicurezza diventa prerequisito di partecipazione alle filiere
- la fiducia deve essere supportata da evidenze, processi e capacità di controllo

Per molte realtà italiane questo cambiamento è già tangibile. Sempre più frequentemente, nei processi di selezione e nei rinnovi contrattuali, viene richiesto di dimostrare come viene gestito il rischio lungo la supply chain. In diversi contesti, si tratta già di un requisito di accesso.

L'Europa e la costruzione di resilienza

La NIS2 si inserisce in una strategia più ampia dell'Unione Europea, orientata al rafforzamento della resilienza e dell'autonomia digitale. L'obiettivo non è limitato alla riduzione degli incidenti, ma riguarda la capacità del sistema nel suo complesso di assorbire eventi critici, garantire continuità operativa e mantenere la fiducia nei servizi essenziali.

In questo quadro, la supply chain assume anche una dimensione economica e geopolitica. Ridurre le dipendenze critiche, aumentare la trasparenza lungo le filiere e rafforzare la sicurezza dei fornitori strategici significa intervenire direttamente sulla stabilità e sulla competitività dell'ecosistema europeo. La gestione delle terze parti si configura quindi come un elemento strutturale, non più come una scelta discrezionale.

Intelligenza artificiale e supply chain: una complessità crescente

L'adozione dell'intelligenza artificiale introduce un ulteriore livello di complessità nella gestione della supply chain.
Modelli, servizi AI-as-a-service e sistemi di decisione automatizzata vengono progressivamente integrati in processi critici, spesso attraverso fornitori terzi. Questo genera nuove dipendenze, caratterizzate da minore trasparenza e maggiore difficoltà di controllo.

Non si tratta più soltanto di infrastrutture o applicazioni, ma di modelli, dati e logiche decisionali distribuite lungo la filiera.

Le principali criticità riguardano:
- la visibilità sui dati e sui flussi informativi
- la comprensione del comportamento dei modelli
- il controllo su processi automatizzati ad alto impatto

In questo contesto, i fornitori di servizi AI devono essere considerati a tutti gli effetti fornitori critici della supply chain, con requisiti specifici in termini di governance dei dati, trasparenza, localizzazione e auditing.

La NIS2, pur non essendo una normativa specifica sull'AI, introduce un principio fondamentale: la necessità di comprendere e governare le dipendenze tecnologiche.

Oltre la compliance: competitività e posizionamento

Interpretare la NIS2 esclusivamente come un obbligo normativo rischia di limitarne il potenziale. Per molte organizzazioni, in particolare per quelle che operano come fornitori, la capacità di gestire la supply chain rappresenta un elemento di differenziazione.
Dimostrare affidabilità, trasparenza e capacità di controllo diventa sempre più rilevante nei processi di selezione e nelle relazioni di lungo periodo.

Per le PMI italiane, questo passaggio può rappresentare anche un'opportunità: evolvere il proprio modello operativo e posizionarsi all'interno di filiere più strutturate, in cui la fiducia è un requisito esplicito.

La sicurezza come scelta strategica di sistema

La NIS2 segna un cambiamento significativo nell'approccio alla cybersecurity, spostando l'attenzione dalla protezione del singolo perimetro alla resilienza dell'intero sistema.

La centralità della supply chain evidenzia come la sicurezza richieda una visione sistemica, fondata sulla gestione delle relazioni tra organizzazioni. Per le imprese, questo implica un'evoluzione che va oltre la tecnologia: strutturare la gestione del rischio di terze parti, superare una logica di compliance formale e sviluppare la capacità di dimostrare affidabilità nel tempo.

In un contesto sempre più interconnesso, la sicurezza si configura come una scelta strategica: un elemento che incide direttamente sulla fiducia, sulla continuità operativa e sulla possibilità di operare stabilmente all'interno delle filiere di riferimento.

AI – DOMANDE E RISPOSTE FACILI FACILI: fidarsi o non fidarsi dell'AI

A cura di Gianpiero Cozzolino

L'AI come strumento di frode o controllo

Come tutti gli strumenti, anche l'AI può essere utilizzata a fini legittimi e che portano benefici, ma anche a scopi illeciti e malevoli. In particolare, essa aumenta la capacità di generare frodi credibili (perché ha a disposizione praticamente tutte le informazioni disponibili su un dato oggetto, o soggetto...) eliminando gli errori o le imprecisioni che in passato rendevano i tentativi riconoscibili (si pensi alle mail di phishing sgrammaticate e generiche, oggi sostituite da messaggi personalizzati e scritti in modo ineccepibile). Nei casi più gravi le stesse metodologie permettono il "furto d'identità", la capacità quindi di impersonare credibilmente qualcuno che non si è, facendo ricorso alla già citata disponibilità di informazioni ma soprattutto alla estrazione e sostituzione degli elementi caratteristici di una persona (cambiando la foto su un documento d'identità; con le tecniche di deepfake, sia in video che in audio; fornendo risposte/informazioni corrette ai sistemi di verifica).

Un altro campo di applicazione è il controllo sociale, attraverso l'aumento sia in termini di volume che di qualità dei contenuti usati a fini propagandistici, i quali contenuti vengono sia generati meglio, ma anche filtrati peggio (l'IA stessa va sostituendo il lavoro di moderazione finora gestito da umani: da una parte è inevitabile l'automazione visti i volumi di cui stiamo parlando, dall'altra parte in questo modo si elimina il problema della sensibilità etica).

Ma quindi l'AI favorisce la disinformazione?

Certamente le tecniche generative di testi, immagini e suoni facilitano parecchio la creazione di contenuti non reali ma verosimili, sempre più difficili da distinguere da quelli veri; ciò corrisponde all'aumento della disinformazione, sia essa l'obiettivo (a fini di propaganda) o un semplice effetto collaterale. Il rischio più concreto e attuale è che ci sia un aumento esponenziale dei contenuti, così da rendere di fatto impossibile o estremamente faticoso (e costoso) il poter discernere le notizie false da quelle vere.

Facciamo un esempio concreto: fino a poco tempo fa, se i giornali riportavano le dichiarazioni di un personaggio, era possibile riconoscerne la veridicità se esisteva un video o anche solo un audio che permettesse il controllo della correttezza della trascrizione ma anche la comprensione del contesto in cui la dichiarazione ha avuto luogo; invece è ormai una realtà il fatto che i video o gli audio a supporto della (presunta) veridicità possono essere creati nel giro di minuti, con un'accuratezza e verosimiglianza impressionante.

L'IA Act dell'UE è intervenuto su questo problema imponendo che i contenuti generati tramite strumenti IA riportino un "sigillo" che evidenzi l'origine artificiale; tuttavia, il divieto rimane aggirabile da chiunque voglia diffondere consapevolmente la disinformazione, ed è, ancora, poco usato dai più per valutare il peso della fonte.

Cosa ne penso?

La vera sfida del futuro presente è quella di saper distinguere il reale dal verosimile. Ciò riguarda tutti: i media, almeno quelli onesti, che devono evitare di diventare inconsapevolmente veicolo di disinformazione; e noi cittadini, che dobbiamo evitare di assorbire la disinformazione facendoci condizionare nelle nostre scelte quotidiane.

Un altro aspetto estremamente preoccupante è il fatto che i nuovi contenuti generati tramite IA, veri o falsi che siano, spesso entrano nell'addestramento, che viene fatto continuamente, delle edizioni successive dei modelli utilizzati da tali strumenti; è facilmente comprensibile (peraltro ciò è anche oggetto di studi scientifici che sembrano confermarlo) come questo inquini il modello stesso, con il serio rischio che i contenuti futuri abbiano "qualità",progressivamente, inferiore.

Infine, ora più che mai è necessaria una certa "continenza" nella circolazione delle informazioni personali; se ciò è ormai da decenni un obbligo legale per il mondo professionale, è necessario che anche le persone, singolarmente ed autonomamente, capiscano che tutto ciò che condividono può essere utilizzato contro di loro nei modi più vari ed imprevedibili.

CYBER
Think Tank
ASSINTEL

Unisciti alla nostra community!

Scrivi a segreteria@assintel.it per avere maggiori info

Il rapporto duale tra cybersicurezza e intelligenza artificiale

A cura di Stefano da Empoli e Alessandro D'Amato

Con crescente evidenza negli ultimi anni abbiamo potuto osservare la natura del rapporto duale tra intelligenza artificiale (IA) e cybersicurezza. Da un lato, la prima apre le porte a nuove sfide e rischi, poiché i sistemi di IA possono essere sfruttati dai diversi attori del cyberspazio per scansionare le vulnerabilità di reti e sistemi del bersaglio, oltre che per automatizzare e perfezionare tecniche e procedure di attacco; dall'altro, essa offre strumenti avanzati per rilevare minacce, analizzare vulnerabilità e rispondere rapidamente ad attacchi nel dominio cibernetico.

Ebbene, partendo dalle opportunità, le imprese stanno già registrando da tempo diversi benefici connessi all'integrazione di tali sistemi nelle attività di cybersicurezza, come emerge ad esempio da un'indagine svolta da Cybersecurity Insiders, secondo la quale il 58% dei rispondenti ritiene che l'ottimizzazione del rilevamento delle minacce sia il principale beneficio in tema, a cui segue la gestione delle vulnerabilità (57%) e la riduzione delle tempistiche di *incident response* (56%).
È interessante notare come più di un terzo degli intervistati (37%) sia d'accordo sul fatto che l'automazione abilitata dall'IA in cybersecurity sia un modo per mitigare la carenza di talenti nel settore.
Posto che in cybersicurezza non è possibile raggiungere il rischio zero, per cui anche l'organizzazione meglio attrezzata – pubblica o privata che sia – avrà sempre una parte più o meno ampia di superficie attaccabile, l'integrazione dell'IA e dell'automazione può ridurre i costi che si rendono necessari per affrontare una violazione di dati (*data breach*). E infatti, dati recentemente pubblicati da IBM su un campione internazionale di imprese rendono esplicito che le organizzazioni che non hanno utilizzato l'IA hanno dovuto sostenere un danno di $5,52 milioni in media per una singola violazione di dati, che scendono a $3,62 milioni per quelle che ne hanno fatto un uso esteso, risparmiando in tal modo mediamente $1,9 milioni rispetto alle prime. Ciò è dipeso anche dal tempo necessario a identificare e gestire una violazione di dati, in quanto le imprese che non hanno utilizzato soluzioni di IA in ambito cybersecurity all'interno della loro organizzazione hanno speso mediamente 284 giorni per risolvere un evento di questo tipo, contro i 204 di coloro che le hanno implementate in maniera estesa.

Dato che il *cybercrime* si evolve di pari passo con il progresso tecnologico e il contesto socio-economico di riferimento, è necessario che l'IA sia adottata in maniera adeguata e consapevole nelle organizzazioni, al fine di sostenere una più efficace e tempestiva attività di prevenzione e protezione in termini di rilevazione delle minacce e di risposta agli incidenti in maniera proattiva, consentendo alle stesse di ridurre i tempi di reazione e minimizzare gli impatti. In particolare, i sistemi avanzati di IA possono essere d'aiuto, fra l'altro, ad approcciarsi al rischio cibernetico secondo un modello "*zero-trust*" e ciò a

maggior ragione, se si considera che tra le metodologie di attacco più utilizzate in ambito *cybercrime* vi è l'ingegneria sociale (*social engineering*), che solitamente ha come agente scatenante (o aggravante) lo *human factor*, ovverosia l'essere umano, poiché la sicurezza informatica in senso lato non è legata solamente a contromisure tecnologiche, ma anche alla persona, indipendentemente dal suo ruolo e dalla sua funzione in un determinato ente pubblico o azienda privata.
In questo senso, l'IA permette agli attaccanti di automatizzare simili tecniche ed estenderne la portata (es. miglioramento della qualità del testo, della grafica, del contesto, ovvero della voce o delle immagini utilizzate in un attacco, ma anche di assistere e supportare la resilienza dei soggetti bersaglio secondo il paradigma "*Human-as-a-Security-Sensor*", che si sostanzia nell'utilizzo della capacità umana di individuare elementi ingannevoli, soprattutto di tipo semantico.

Tuttavia, simili evidenze si collocano in un contesto europeo e nazionale che, mediamente, non eccelle nell'utilizzo dell'IA in ambito cybersecurity. Infatti, secondo gli ultimi dati Eurostat (2025), la quota di imprese italiane – tra quelle che hanno adottato almeno una tecnologia di IA – che ricorre a soluzioni di intelligenza artificiale in questo campo si è attestata al 12,1% nel 2025, oltre 7 punti percentuali al di sotto del valore medio nell'UE, molto distante dai primi della classe, ossia Grecia (53,4%), Slovenia (39,6%) e Cipro (29,2%). E' opportuno specificare che anche le altre principali economie europee si collocano al di sotto della media europea, fatta eccezione per la Germania (20,6%). Se si differenziano le imprese italiane per dimensione, il gap rispetto al valore medio europeo risulta essenzialmente riconducibile alla minore penetrazione delle tecnologie di IA associate alla cybersicurezza nelle PMI. In particolare, le piccole imprese fanno registrare oltre 7 punti percentuali in meno rispetto alla media UE (7,3% vs 14,5%), mentre il distacco tra quelle di medie dimensioni è più contenuto, ma comunque piuttosto rilevante (21,7% vs 27%).

Se, come già accennato, l'IA può arrecare notevoli vantaggi al panorama della cybersicurezza – e lo farà ancor di più in futuro – è pur vero che richiede competenze elevate per poter produrre un significativo valore aggiunto. Ebbene, secondo uno studio di ISC2 con riferimento alle principali competenze mancanti o insufficienti all'interno dei team di cybersecurity a livello globale, dietro alle skill in ambito *cloud computing security*, si collocano quelle associate all'IA e al *machine learning*. A ulteriore riprova di quanto detto, una survey condotta da McKinsey riporta che tra i rischi considerati più rilevanti rispetto all'utilizzo dell'IA nelle imprese spicca la cybersecurity (51% dei rispondenti nel 2025), preceduta solo dall'inaccuratezza di tali sistemi (54%). Altro esempio del rapporto duale tra IA e cybersicurezza è costituito dai tentativi di generazione automatica di richieste avversarie (*adversarial attacks*). Ad esempio, un recente paper scientifico – che comprende fra gli autori diversi informatici della Carnegie Mellon University – propone un metodo di attacco che induce modelli linguistici allineati con valori e obiettivi corretti a generare comportamenti discutibili. Nello specifico, l'approccio in questione trova un suffisso che, quando associato a una vasta gamma di query, punta a massimizzare la probabilità che il modello produca una risposta affermativa, anziché rifiutarsi di rispondere. In particolare, gli autori hanno scoperto che le richieste avversarie generate da questo approccio sono piuttosto trasferibili da un modello all'altro, inclusi i *Large Language Models* (LLM) pubblicamente rilasciati. Il paper solleva dunque domande importanti su come si possa prevenire che tali sistemi, che sono stati preliminarmente allineati dai loro creatori proprio per impedire tale tipo di manipolazioni, producano informazioni discutibili. La domanda naturale che si pongono gli autori, in conclusione, è se i modelli di IA generativa possano essere esplicitamente affinati per evitare questo tipo di attacchi. Questa è precisamente la strategia dell'addestramento avversario (*adversarial machine learning*), il mezzo empiricamente più efficace per rendere più robusti i modelli di apprendimento automatico a questo tipo di pericoli, in quanto durante questa fase o quella di ottimizzazione i modelli di apprendimento vengono attaccati con uno di questi metodi per poi essere addestrati iterativamente sulla risposta "corretta" alla query potenzialmente dannosa (e preferibilmente, per aumentare ulteriormente la robustezza, anche su ulteriori richieste non potenzialmente dannose ma in qualche modo correlate).

In definitiva, l'intelligenza artificiale – e in particolare quella generativa – non porta con sé rischi del tutto nuovi in termini di cybersicurezza, bensì amplifica quelli esistenti e, al tempo stesso, genera gli anticorpi necessari per rispondervi con maggiore efficacia che in passato. Purché si disponga delle tecnologie e soprattutto delle competenze necessarie per farlo.

COME TI CREO UNA PASSWORD "INVIOLABILE"

www.assintel.it
info@assintel.it

Gestione degli incidenti di sicurezza informatica: framework, obblighi e continuità operativa

A cura di Davide Giribaldi

La prevenzione è condizione necessaria, ma non sufficiente e quando una minaccia cyber si trasforma in incidente, la capacità di rispondere con efficacia ed efficienza scorre costantemente sul sottile equilibrio tra il requisito strategico e l'obbligo normativo che non sempre è facile da garantire, soprattutto nelle condizioni più critiche. Costruire un programma maturo di Incident Management significa integrare governance, tecnologia, processi e cultura organizzativa in un sistema coerente, capace di reggere la pressione del momento critico per garantire la continuità operativa dell'organizzazione con il minore impatto possibile e su questo non ci sono dubbi, ma come è possibile crearlo?

Il primo passo per gestire un incidente è riconoscerlo. La distinzione tra evento e incidente non è meramente tassonomica e la capacità d'individuarla determina le procedure da attivare, le risorse da allocare e gli obblighi da rispettare. Un evento di sicurezza, sia esso a basso impatto, significativo o critico, è qualsiasi occorrenza identificabile nello stato di un sistema, servizio o infrastruttura di rete, che indichi una possibile violazione delle policy di sicurezza o una situazione anomala potenzialmente rilevante. Un incidente di sicurezza si manifesta invece per tramite di uno o più eventi che hanno - o hanno ragionevole probabilità di avere - un impatto effettivo sulla confidenzialità, integrità o disponibilità delle informazioni, o sulla capacità dell'organizzazione di operare.

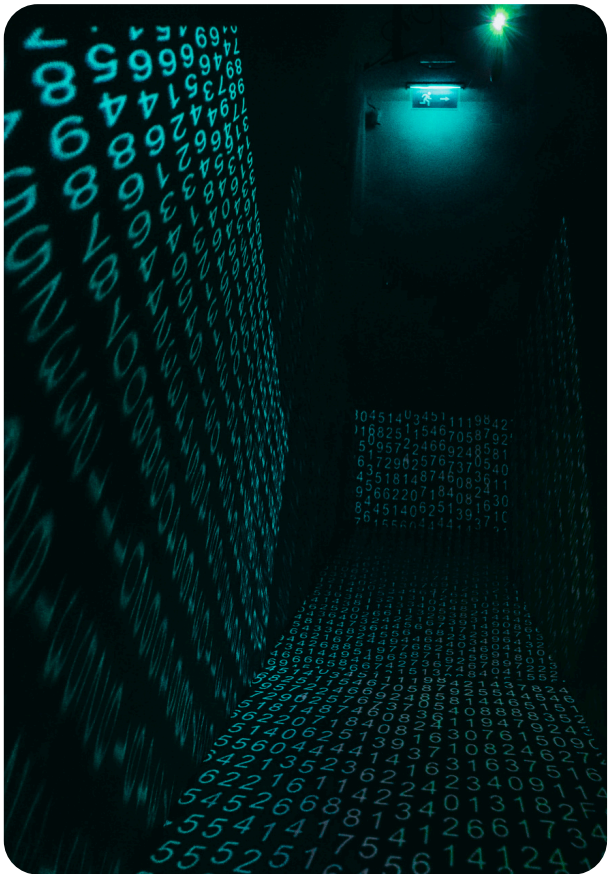
E' opportuno però ricordare che gli incidenti raramente hanno un'unica causa, ma sono quasi sempre il risultato di una convergenza di vulnerabilità tecniche, che di solito includono configurazioni errate, mancanza di patch, infrastrutture non segmentate o componenti obsoleti, lacune organizzative come processi e procedure di sicurezza formalmente definite ma sistematicamente disattese e il fattore umano, erroneamente considerato l'unico anello debole della catena, ma che senza dubbio contribuisce all'amplificazione degli effetti delle prime due cause.

Prima di approfondire alcuni approcci operativi che possono aiutare le nostre organizzazioni a definire un modello di gestione degli incidenti di sicurezza informatica davvero efficace, è necessario fare un piccolo riepilogo sui requisiti della Direttiva NIS2, recepita in Italia con il Decreto Legislativo 4 settembre 2024, n. 138, che di fatto ha (ri)definito in modo sostanziale gli obblighi di gestione degli incidenti per i soggetti rientranti in perimetro e per la loro intera catena di fornitura e sub fornitura.

La norma impone alle organizzazioni in scopo di disporre di capacità strutturate di gestione degli incidenti come team dedicati, procedure documentate e regolarmente testate, tecnologie adeguate, e soprattutto richiede capacità di coordinamento con le autorità competenti - in primis il CSIRT Italia e l'Agenzia per la Cybersicurezza Nazionale (ACN).

Sul fronte della notifica di un incidente, la normativa è chiara e stringente: un incidente è considerato "significativo" e quindi soggetto a notifica obbligatoria, quando causa o può causare una grave perturbazione operativa, perdite finanziarie, o ripercussioni sulle parti interessate come mercato, utenti finali e terze parti. Le tipologie codificate sono quattro: perdita di riservatezza o integrità dei dati (IS-1), disservizio (IS-2), rischio per la vita o la salute (IS-3), e accesso non autorizzato ad alto impatto, quest'ultima riservata ai soli soggetti essenziali (IS-4). Anche le tempistiche di notifica sono rigide e articolate in tre fasi: pre-notifica entro 24 ore dall'identificazione dell'incidente, notifica completa entro 72 ore con valutazione iniziale e indicatori di compromissione, relazione finale entro un mese con la descrizione dettagliata di cause, misure adottate e lezioni apprese. La mancata notifica espone di fatto l'organizzazione a sanzioni amministrative e a responsabilità dirette degli organi di amministrazione, ma non è su questo che vorrei soffermarmi, ma piuttosto sulle opportunità che l'adozione di alcuni framework, possano dare alle nostre organizzazioni per costruire un sistema efficace, efficiente e maturo per la gestione degli incidenti.

Ve ne propongo 6, tra quelli che più spesso ho incontrato durante gli ultimi anni, ma con la doverosa premessa di fondo che nessuno esclude gli altri e ciascuno presidia una dimensione specifica di governance, operatività, service management e conformità, lasciando a noi la vera sfida di comprendere se e come integrarli in modo coerente, evitando ridondanze e colmando i gap.



Credo che il più famoso di tutti sia lo standard **ISO/IEC 27001:2022** che fornisce la base certificabile per un sistema di gestione della sicurezza delle informazioni attraverso un approccio "risk-based" scalabile a qualsiasi tipo di organizzazione, con un ciclo Plan-Do-Check-Act integrato che garantisce il miglioramento continuo. Può essere supportato dalle 4 linee guida **ISO/IEC 27035** che entrano nel dettaglio operativo del ciclo di vita degli incidenti attraverso un'impostazione "process-based". Il framework **ITIL** (ancora per poco nella versione 4.0) porta invece la prospettiva del "Service Management", orientando la risposta agli incidenti al ripristino del valore per il business. **COBIT 2019** presidia poi la dimensione della governance IT, allineando la gestione degli incidenti agli obiettivi aziendali. Ultimi, ma non ultimi, i due framework più vicini alle esigenze delle organizzazioni italiane: il **NIST Cybersecurity Framework 2.0** che offre una visione "outcome-based" organizzata nelle 6 funzioni Govern, Identify, Protect, Detect, Respond, Recover e ripreso dal Framework Nazionale di Cybersecurity e la **UNI PdR 174:2025** che di fatto rappresenta un'armonizzazione pragmatica tra ISO 27001 e NIST CSF 2.0, offrendo una chiave di lettura unificata particolarmente utile per chi deve navigare tra requisiti sovrapposti.

Ci sarebbe poi un ulteriore framework da tenere in considerazione, il **NIST SP 800-61** alla revisione 3 che di fatto è il documento più citato nei runbook delle organizzazioni più strutturate.

Se, infatti, il NIST CSF 2.0 fornisce la visione strategica e le 4 ISO 27035 la struttura processuale, la Special Publication 800-61r3 è la guida tecnica operativa di riferimento per CSIRT, SOC e per i team di risposta agli incidenti incident response e il suo valore aggiunto è la praticità immediata, attraverso la proposta di decision tree concreti, procedure step-by-step, orientamento specifico per categorie di incidenti con indicazione degli errori comuni da evitare e delle considerazioni speciali per ciascuna categoria.
Credo sia utile almeno dal punto di vista della cultura generale sulla gestione degli incidenti.

NIST Cybersecurity Framework 2.0 - Il Linguaggio Strategico

Rilasciato nel febbraio 2024, il **NIST CSF 2.0** evolve la versione originale del 2014 con una novità sostanziale: l'aggiunta della funzione **GOVERN**, assente nel framework precedente. Come già

anticipato, l'approccio è “outcome-based”, quindi ideale per comunicare con il board e il senior management e definisce i risultati desiderati lasciando libertà implementativa all’organizzazione che lo applica, rendendolo particolarmente adatto a contesti eterogenei. La prima delle sei funzioni è quella di “*Governo*” e fornisce il contesto organizzativo senza il quale anche i migliori processi operativi fallirebbero, definendo obiettivi di strategia di cybersecurity, allocazione delle risorse, accountability, integrazione con il risk management aziendale. Segue la funzione di “*Identificazione*” che determina i prerequisiti per la risposta come la mappatura degli asset e dei dati sensibili, le dipendenze dalle terze parti e la valutazione delle vulnerabilità.
La funzione “*Protezione*” copre invece i cosiddetti controlli preventivi tra cui, IAM, security awareness, data protection, hardening dell’infrastruttura, con il duplice obiettivo di ridurre la probabilità degli incidenti e mitigarne la severità. Segue poi la funzione “*Rilevazione*” per tramite della quale è possibile determinare il Mean Time To Detect (MTTD), metrica critica di maturità per la gestione degli incidenti e tra le altre cose, gli indicatori di compromissione e le anomalie comportamentali.
La fase di “*Risposta*” è invece il vero nucleo operativo del framework, perché è qui che avvengono la classificazione, il triage, il contenimento e tutto ciò che è utile tanto al coordinamento interno ed esterno, quanto alla gestione delle comunicazioni. In fine, la fase di “*Recupero*” integra l'Incident Management con la Business Continuity, assicurando non solo la capacità di risposta ma il ripristino efficace, efficiente e rapido dei servizi critici.
Il framework include poi 4 livelli di maturità - *Partial, Risk Informed, Repeatable, Adaptive*, espressi come Tier, con distinzione tra Profilo attuale e obiettivo per identificare gap e prioritizzare investimenti.

UNI PdR 174:2025 - L'Armonizzazione Pragmatica (per le organizzazioni italiane)

Nata da un tavolo multidisciplinare che ha riunito Accredia, CINI e organismi di certificazione, la UNI PdR 174:2025 risponde a una domanda concreta: come evitare duplicazioni quando si adottano contemporaneamente ISO 27001 e NIST CSF?
La prassi fornisce un mapping dettagliato tra la High Level Structure (HLS) di ISO 27001 e le sottocategorie del NIST CSF, armonizzando il Framework Nazionale per la Cybersecurity con i requisiti ISO e gli outcome NIST. Il risultato è una riduzione significativa di ridondanze in termini di processi, documentazione e attività di audit.
È uno strumento particolarmente utile per le organizzazioni meno strutturate, che possono prendere decisioni consapevoli sui gap accettabili nel contesto della propria propensione al rischio. Riduce anche la variabilità negli audit interni, spesso generate da interpretazioni divergenti di come i due framework si relazionano.

Il Ciclo di Vita nella gestione degli incidenti: Cinque Fasi, una Sola Strategia

Qualunque sia il framework che deciderete di adottare, è importante ricordare che la migliore gestione degli incidenti è quella che prevede cinque fasi fondamentali: Pianificazione e Preparazione, Rilevamento e Segnalazione, Valutazione e Decisione, Risposta e Lezioni Apprese.

La fase di **preparazione** è determinante: un'organizzazione che non ha pianificato, addestrato il proprio team, e testato le procedure con esercitazioni periodiche si troverà impreparata nel momento più delicato. La capacità di **rilevamento** dipende dalla qualità degli strumenti, dalle competenze interne ma soprattutto dall’attitudine a correlare segnali deboli. La **valutazione** richiede invece processi di triage rapidi e criteri di prioritizzazione chiari. La **risposta** deve essere coordinata, documentata e tracciabile, anche per soddisfare gli obblighi di notifica. Infine, la fase di **lezioni apprese**, la più delicata e spesso la più trascurata, che non solo chiude il ciclo di gestione dell’incidente, ma ha il delicato compito di migliorare la postura di sicurezza dell’organizzazione, evitando o contenendo eventuali episodi analoghi in futuro.

Gestire un incidente non significa solo agire nell’immediatezza, ma comprendere perché si sia sviluppato, come si sia propagato e cosa cambiare per ridurre la probabilità che si ripeta. È questione di attuare una visione sistemica, tecnica, organizzativa e culturale che aiuti l’organizzazione durante possibili situazioni di crisi.

C’è solo un’ultima considerazione da fare: il ciclo di vita della gestione di un incidente informatico non è una sequenza rigida a senso unico. L’esperienza, ad esempio, mi ha insegnato che durante la fase di “Risposta”, possano emergere nuove evidenze, sistemi coinvolti in modo inatteso, vettori di attacco non identificati nel triage iniziale, impatti latenti che richiedono di tornare alla fase precedente di “Valutazione” sia per classificare diversamente l’evento che per aggiornare le misure di contenimento. Questo tipo di iteratività non va considerato come un fallimento del processo, ma una delle sue caratteristiche più importanti, perché sapersi adattare alle evidenze emergenti è segnale di maturità organizzativa, di processi e tecnologica, soprattutto in situazioni in cui il tempo è il fattore determinante non solo per la notifica di un incidente, ma per la continuità operativa della nostra organizzazione.

La cybersicurezza come precondizione per la sovranità digitale: la revisione del Cyber Security Act è sulla strada giusta, ma serve più ambizione

A cura di Davide Iaccarino

PUNTI CHIAVE

- La proposta CSA 2.0 fa passi avanti sulla sicurezza della supply chain e sulla semplificazione degli adempimenti, spostando la valutazione del rischio a livello dell'UE e riducendo gli oneri per le PMI vincolate dalla Direttiva NIS2 e dal Cyber Resilience Act.

- Nonostante il cambiamento introdotto dal CSA 2.0, la certificazione di cybersicurezza rimane circoscritta a criteri tecnici, dopo che il dibattito sull'EUCS ha sancito la separazione formale tra certificazione e valutazione dei rischi non tecnici.

- Questo disallineamento priva le PMI digitali europee di uno strumento per competere sul piano della fiducia e della sovranità tecnologica, in un contesto in cui clienti e regolatori considerano ormai in modo inscindibile sicurezza tecnica, dipendenza e controllo.

Come osserva l'European DIGITAL SME Alliance - il principale network europeo di PMI digitali, con oltre 45.000 imprese rappresentate in tutta l'Unione - la revisione del Cyber Security Act (CSA) segna un cambio di prospettiva nell'approccio dell'UE: la cybersicurezza smette di essere una questione puramente tecnica, e diventa anche un elemento strategico di sovranità, fiducia e controllo delle infrastrutture digitali critiche.

Con l'entrata in vigore della Direttiva NIS2, del Cyber Resilience Act (CRA) e delle norme settoriali, la proposta della Commissione riconosce tanto lanecessità di alleggerire il carico della compliance, soprattutto per le PMI, quanto l'urgenza di affrontare i rischi non tecnici nelle catene di fornitura. La revisione del CSA mira a rispondere a queste sfide attraverso la semplificazione, l'armonizzazione e un approccio più strategico alla sicurezza della supply chain.

La certificazione diventa un abilitatore di compliance

Uno degli aspetti più rilevanti della revisione riguarda il riposizionamento della certificazione di cybersicurezza, che passa da essere uno strumento volontario di mercato a essere un meccanismo abilitante per la compliance normativa. Ancorando esplicitamente gli schemi di certificazione alla legislazione UE, la proposta fa sì che la certificazione possa valere come dimostrazione di conformità ai requisiti di NIS2 e del CRA.

In concreto, questo significa che le imprese potranno:

- Affidarsi a certificazioni basate su standard per dimostrare la conformità a più atti legislativi in modo simultaneo;
- Ridurre la ripetizione di audit, questionari e richieste di documentazione;

- Operare all'interno di un unico framework riconosciuto invece di gestire processi paralleli di conformità.

L'introduzione della certificazione a livello di entità, con un focus iniziale sulle entità NIS2, consente alle aziende di attestare la propria postura di sicurezza in modo unitario e strutturato. Si tratta di un cambiamento importante, che European DIGITAL SME Alliance ha a lungo sostenuto nelle proprie posizioni di policy: semplificare senza abbassare il livello di sicurezza richiesto.

Un approccio più coerente alla sicurezza della supply chain ICT

La revisione del CSA introduce anche un quadro orizzontale a livello UE per la sicurezza della supply chain ICT. La proposta ha l'obiettivo di superare la frammentazione del modello precedente basato sulle norme nazionali, istituendo criteri comuni di valutazione dei rischi sia tecnici che non tecnici con coordinamento a livello europeo.

Per le PMI digitali europee, si tratta di un passo avanti significativo. Valutazioni del rischio condotte a livello UE possono ridurre la frammentazione, aumentare la prevedibilità e consentire ai fornitori europei di competere oltre i confini nazionali senza doversi adeguare a requisiti di sicurezza differenti in ogni Stato Membro.

Attraverso valutazioni del rischio coordinate e l'identificazione dei fornitori ad alto rischio, la revisione del CSA può migliorare la capacità dell'Europa di gestire le dipendenze tecnologiche in modo più coerente, rafforzando la sua sovranità tecnologica e definendo condizioni più chiare per le PMI ICT che operano come fornitori affidabili nel Mercato Unico.

Perché questo conta per le PMI digitali

Per le PMI digitali, la revisione del CSA incide direttamente su come vengono valutate come fornitori in mercati sempre più strategici e geopoliticamente sensibili. La sicurezza della supply chain non è più una questione puramente tecnica: dipendenza, fiducia e controllo sulle infrastrutture digitali critiche sono diventati criteri di valutazione a tutti gli effetti.

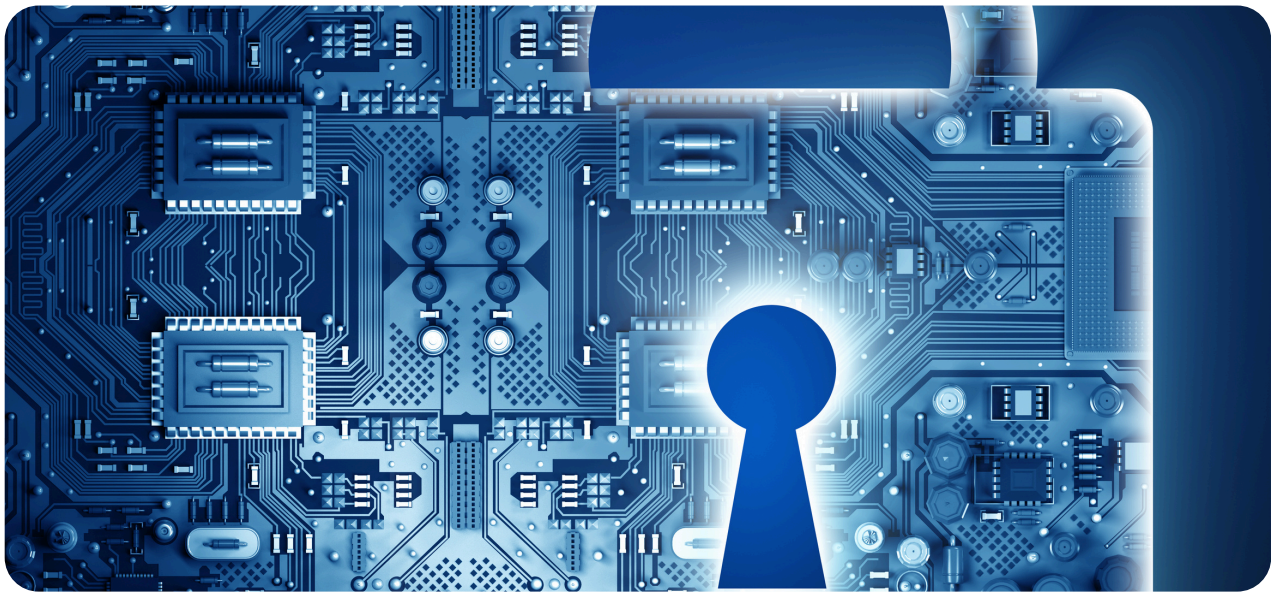
In concreto, la revisione del CSA può consentire alle PMI di:

- Ridurre la duplicazione degli adempimenti grazie alla presunzione di conformità e alle certificazioni basate su standard;
- Semplificare la dimostrazione della maturità in cybersicurezza attraverso la certificazione a livello di entità;
- Diminuire la pressione operativa durante gli incidenti tramite la segnalazione con punto di accesso unico;
- Disporre di requisiti più chiari e uniformi a livello UE rispetto alle operazioni transfrontaliere.

Come sottolinea la guida di DIGITAL SME sulla Direttiva NIS2, diventare un fornitore affidabile per entità critiche significa oggi saper dimostrare una postura di sicurezza coerente e credibile su più livelli: quello normativo, quello di mercato e quello geopolitico.

Il collegamento mancante: cybersicurezza e sovranità

Allo stesso tempo, la revisione compie una scelta deliberata: mantenere la certificazione di cybersicurezza focalizzata principalmente su criteri



tecnici, nonostante le disposizioni sulla supply chain affrontino esplicitamente rischi non tecnici e legati alle dipendenze.

Questo crea un disallineamento strutturale, particolarmente penalizzante per le PMI digitali che operano in mercati strategici:

- I clienti valutano sempre più congiuntamente fiducia, resilienza e dipendenze;
- Gli schemi di certificazione non riflettono ancora queste dimensioni;
- La differenziazione dei fornitori europei affidabili su questi criteri rimane limitata.

Dopo anni di dibattito senza esito sull'integrazione dei rischi non tecnici negli schemi di certificazione UE - di cui il caso dello schema EUCS per i servizi cloud è l'esempio più noto - la Commissione ha scelto di tenere separati certificazione e valutazione dei rischi della supply chain.

Si tratta di una scelta pragmatica, ma che lascia aperto un problema strutturale: le regole sulla supply chain incorporano ormai considerazioni su sovranità, dipendenza e rischi strategici, mentre la certificazione rimane confinata ai soli criteri tecnici.

Per le piccole e medie imprese del settore digitale il risultato è che non esisterà ancora uno strumento europeo che consenta di differenziarsi dai concorrenti sulla base del livello di sovranità, nonostante quest'ultimo pesi sempre più nelle decisioni di acquisto dei clienti pubblici e privati.

Conclusioni: la strada è giusta, serve più ambizione

Guardando al futuro, il successo della revisione del CSA dipenderà dalla capacità dell'Europa di colmare il divario tra le modalità di valutazione del rischio e le capacità di dimostrare sovranità e attrarre fiducia. L'European DIGITAL SME Alliance continua ad impegnarsi per colmare questo divario, anche attraverso iniziative come il Catalogo della Sovranità Tecnologica.

La revisione del CSA rappresenta un passo avanti reale. L'Europa ha capito che cybersicurezza e sovranità tecnologica non si possono più separare.

Ma se si vuole davvero ridurre le dipendenze tecnologiche e permettere alle imprese europee, a partire dalle PMI, di competere come fornitori affidabili e sovrani, gli schemi di certificazione dovranno riflettere anche queste dimensioni.

Sarà inoltre fondamentale garantire che i meccanismi di semplificazione rimangano concretamente accessibili alle PMI: una semplificazione formale che non si traduce in un vantaggio operativo reale rischia di avere effetti anche peggiori dell'assenza di semplificazione.

Cybersecurity e PMI: una priorità concreta per la continuità del business

A cura di Federica Maria Rita Livelli

Ransomware, phishing e violazioni dei dati non sono più eventi eccezionali, ma rischi quotidiani anche per le PMI. Investire in cybersecurity, a fronte di uno scenario di minacce in continua evoluzione e di obblighi normativi sempre più stringenti, significa proteggere il business, la supply chain e il futuro dell'impresa.

Introduzione

Molte PMI continuano a ritenersi "troppo piccole" per attirare l'attenzione dei cybercriminali: una percezione diffusa, ma profondamente fuorviante. In realtà, proprio perché spesso meno strutturate, con risorse e competenze limitate, oggi sono loro i bersagli più esposti. Inoltre, in un sistema economico in cui le PMI rappresentano oltre il 99% delle imprese, la cybersecurity non è più una questione meramente tecnica, ma una priorità strategica per garantire continuità operativa e competitività.

Perché le PMI sono particolarmente esposte

Le PMI costituiscono il tessuto portante dell'economia italiana, con milioni di occupati e un contributo essenziale al PIL nazionale. Proprio questa centralità, tuttavia, le rende particolarmente attrattive per il cybercrime: colpire una PMI significa spesso generare effetti a catena su clienti, fornitori e intere filiere produttive.

I fattori che aumentano l'esposizione delle PMI agli attacchi informatici sono molteplici e strutturali e, precisamente:

- **Limitate risorse dedicate alla sicurezza.** Nelle realtà di dimensioni ridotte la cybersecurity è spesso gestita in modo reattivo e non strutturato, con carenza di competenze specialistiche, budget contenuti e assenza di procedure formalizzate di prevenzione e risposta agli incidenti.

- **Ruolo critico nella supply chain.** Le PMI operano sempre più frequentemente come fornitori, partner tecnologici o subfornitori all'interno di ecosistemi complessi. In questo contesto, rappresentano spesso l'anello più vulnerabile della catena, sfruttato dai cybercriminali come punto di ingresso per colpire organizzazioni più grandi e meglio protette.

- **Aumento della superficie di attacco.** La digitalizzazione accelerata degli ultimi anni, l'adozione di servizi cloud, il lavoro da remoto e l'uso diffuso di dispositivi connessi hanno ampliato in modo significativo il numero di asset, accessi e interfacce esposte, incrementando le potenziali vulnerabilità sfruttabili da un attaccante.

Le minacce che mettono a rischio le PMI

Comprendere le principali tipologie di attacco informatico è il primo passo per costruire una strategia di difesa efficace. Non ci si può proteggere, infatti, da ciò che non si conosce. Di seguito sono riportate le minacce più diffuse che oggi colpiscono con maggiore frequenza le PMI.

Ransomware - Rappresenta una delle minacce più gravi e impattanti per le PMI. In assenza di backup adeguati e verificati, un attacco ransomware può determinare la paralisi totale delle attività aziendali, con effetti economici e operativi che si protraggono nel tempo e mettono a rischio la sopravvivenza stessa dell'impresa.

Phishing – Attraverso e-mail, messaggi o comunicazioni digitali apparentemente legittime, i cybercriminali inducono dipendenti e collaboratori a: rivelare credenziali di accesso; fornire informazioni sensibili; scaricare contenuti malevoli.
Di fatto, il phishing rappresenta, oggi, la principale porta di ingresso degli attacchi informatici, poiché sfrutta il fattore umano, spesso il punto più vulnerabile di qualsiasi sistema di sicurezza. Inoltre, la sua efficacia è ulteriormente amplificata dalla diffusione dello shadow IT, ovvero dall'utilizzo non autorizzato o non governato di applicazioni, servizi cloud e strumenti digitali, che riducono la visibilità e il controllo da parte dell'organizzazione. Ancora, le tecniche di phishing stanno diventando sempre più sofisticate e mirate - anche attraverso l'uso dell'intelligenza artificiale e del social engineering avanzato - rendendo più difficile per gli utenti distinguere comunicazioni fraudolente da quelle legittime.

Attacchi alla supply chain – I criminali informatici compromettono un fornitore o un partner tecnologico per accedere, a cascata, ai sistemi dei suoi clienti. Per le PMI inserite in filiere produttive complesse, tale tipologia di attacco è particolarmente insidiosa, poiché consente di colpire indirettamente organizzazioni anche ben protette.

Violazioni dei dati – Il furto o la compromissione di informazioni sensibili – i.e.: dati personali di clienti e dipendenti, informazioni finanziarie, know-how e segreti industriali - può generare conseguenze rilevanti sul piano economico, reputazionale e legale, includendo potenziali sanzioni previste dal GDPR.

Il costo dell'inazione

Le PMI tendono, spesso, a rimandare gli investimenti in cybersecurity, percependo la sicurezza informatica come un costo da contenere, anziché come un fattore abilitante.

Tale visione, tuttavia, non tiene conto dei costi ben più elevati che derivano da un incidente informatico. Di fatto, una violazione dei dati comporta non solo perdite dirette (i.e. il ripristino dei sistemi, il pagamento di riscatti o il fermo delle attività), ma anche conseguenze indirette spesso difficili da quantificare, tra cui: la perdita di clienti, il danno reputazionale e l'insorgere di contenziosi legali.

Le evidenze internazionali più recenti mostrano come l'impatto di un attacco informatico possa essere fatale per le realtà di dimensioni ridotte: circa il 60% delle PMI colpite da un incidente significativo è costretto a cessare definitivamente l'attività entro sei mesi. Inoltre, anche le aziende che riescono a sopravvivere affrontano tempi di recupero lunghi, impiegando spesso dai 12 ai 18 mesi per tornare ai livelli di fatturato precedenti all'attacco.

Ancora, dal punto di vista economico, il costo medio di una violazione dei dati per una PMI, nel 2025, è stato stimato in circa 120.000 dollari, includendo le perdite di fatturato, le spese legali e le attività di recupero. A ciò si devono aggiungere i costi specifici delle principali minacce: un attacco ransomware comporta in media una perdita di circa 35.000 dollari per incidente; mentre le truffe di phishing generano danni medi pari a 70.000 dollari, considerando il calo di produttività e la perdita di fiducia da parte dei clienti.

Come costruire una difesa efficace

Una PMI può avvalersi del supporto di MSSP (Managed Security Service Provider) e MSP (Managed Service Provider) in grado di offrire misure di sicurezza di base sostenibili ed accessibili, anche alle realtà più piccole, che consentono di ridurre in modo significativo il livello di rischio cyber. Tuttavia, è fondamentale impostare un approccio strutturato e proporzionato alla cybersecurity.

Di seguito i principali fattori da considerare per costruire una strategia di sicurezza informatica efficace ed efficiente.

Formare le persone - Il primo livello di difesa è rappresentato dal capitale umano. Dipendenti e collaboratori devono essere messi nelle condizioni di: riconoscere un'e-mail di phishing; gestire correttamente le credenziali di accesso; sapere come comportarsi in presenza di un sospetto incidente. Di fatto, la formazione continua non è un'attività accessoria, ma una misura essenziale per ridurre il rischio legato al fattore umano.

Adottare l'autenticazione a più fattori (Multi-factor authentication - MFA) - L'introduzione di un secondo livello di verifica per l'accesso ai sistemi aziendali è una delle misure con il miglior rapporto costo-beneficio. Anche in caso di compromissione delle password, l'MFA rende significativamente più difficile l'accesso non autorizzato agli account.

Mantenere i sistemi aggiornati - Molti attacchi informatici sfruttano vulnerabilità presenti in software non aggiornati. Pertanto, una politica rigorosa di aggiornamento regolare di sistemi operativi, applicazioni e firmware dei dispositivi riduce significativamente la superficie di attacco.

Eseguire backup regolari - L'adozione della regola del 3-2-1 rappresenta una best practice consolidata: mantenere tre copie dei dati, archiviate su due supporti differenti, di cui almeno una conservata off-site o in cloud. Ciò è fondamentale dato che, in caso di attacco ransomware, la disponibilità di backup recenti e integri può determinare la differenza tra la continuità operativa e una crisi aziendale irreversibile. È altrettanto importante testare periodicamente i backup - attraverso prove di ripristino - per assicurarsi che siano effettivamente utilizzabili nel momento del bisogno.

Limitare i privilegi di accesso - Il principio del "minimo privilegio" prevede che ogni utente abbia accesso solo alle risorse strettamente necessarie al suo ruolo, in modo da ridurre l'impatto potenziale di una compromissione, oltre a limitare la propagazione dell'attacco all'interno dei sistemi aziendali.

Proteggere endpoint, reti e servizi cloud – L'adozione di misure di sicurezza di base per la protezione degli endpoint, delle reti e degli ambienti cloud (i.e. anti-malware, firewall, monitoraggio degli accessi) consente di intercettare tempestivamente comportamenti anomali e tentativi di intrusione, migliorando la capacità di rilevamento degli incidenti.

Gestire i fornitori ICT e strumenti digitali – È fondamentale valutare il livello di sicurezza dei fornitori IT e dei servizi utilizzati, nonché limitare l'uso di applicazioni e strumenti non autorizzati (shadow IT), che possono introdurre vulnerabilità difficili da controllare, soprattutto nelle PMI inserite in supply chain complesse.

Dotarsi di piani di risposta agli incidenti, di business continuity, di disaster recovery e crisis management - La capacità di sapere come reagire nei primi minuti dopo un attacco informatico è un elemento chiave della resilienza informatica. Disporre di piani documentati - anche essenziali e proporzionati alla dimensione dell'impresa - che definiscano ruoli, responsabilità, procedure operative e contatti di emergenza consente all'organizzazione di contenere l'incidente, assorbire l'impatto e ripristinare rapidamente le attività, riducendo in modo significativo i tempi di recovery e i danni complessivi. Ciò permette altresì di dimostrare la conformità ai requisiti del quadro normativo europeo che adotta sempre più un approccio risk-based e resilience-based.

Il quadro normativo europeo: opportunità e obblighi

L'UE ha progressivamente rafforzato l'attenzione verso la cybersecurity attraverso un quadro normativo sempre più articolato e stringente che adotta un approccio risk-based e resilience-based.

La Direttiva NIS2, recepita nell'ordinamento italiano, amplia in modo significativo l'ambito di applicazione degli obblighi di sicurezza informatica, estendendoli a un numero molto più ampio di settori e organizzazioni rispetto alla normativa precedente, con un impatto rilevante anche sulle catene di fornitura. Per le PMI, ciò significa che la conformità normativa non è più un tema riservato alle sole grandi imprese o ai soggetti direttamente qualificati come essenziali o importanti. Anche le aziende di dimensioni minori, quando operano come fornitori, partner tecnologici o subfornitori all'interno di supply chain complesse, sono sempre più chiamate a dimostrare adeguati livelli di sicurezza informatica.

Pertanto, diventa fondamentale, nella gestione aziendale, conoscere gli obblighi applicabili, valutare i rischi in modo strutturato e documentare le misure tecniche e organizzative adottate, anche in risposta alle richieste di clienti e di committenti.

A ciò si affiancano gli obblighi previsti dal GDPR che impone requisiti stringenti in materia di sicurezza dei dati personali e prevede sanzioni significative in caso di violazione. Per le PMI che trattano dati di clienti, fornitori o dipendenti all'interno di ecosistemi interconnessi, la cybersecurity, la protezione dei dati e l'affidabilità della supply chain non rappresentano più ambiti distinti, ma elementi integrati di un unico sistema di responsabilità, fiducia e resilienza operativa.

Inoltre, le PMI dovranno altresì considerare la propria conformità ai vari standard e regolamentazioni relative al settore di appartenenza.

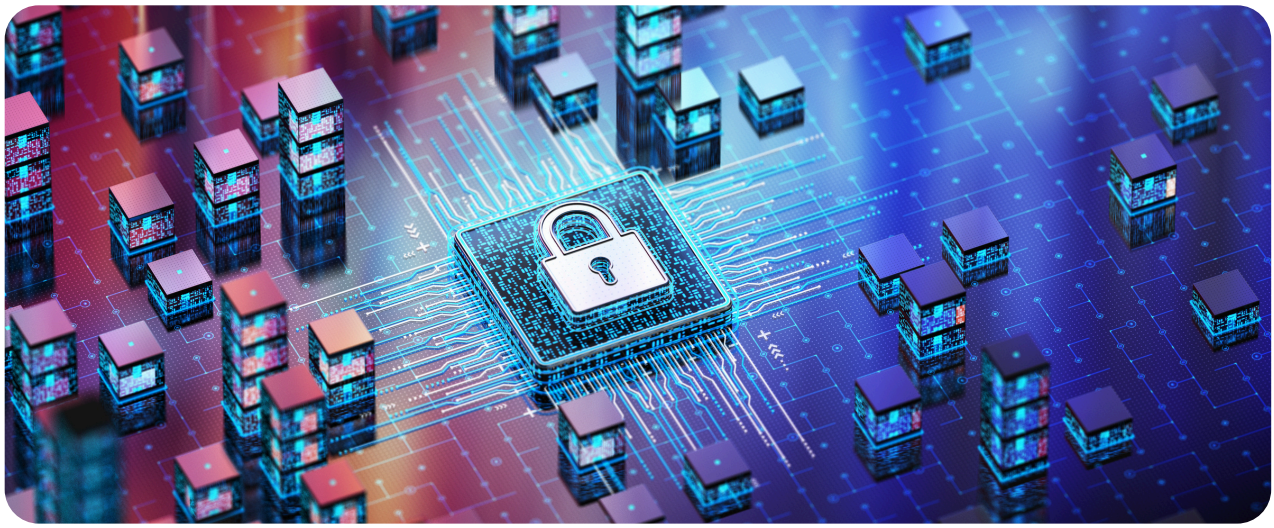
Conclusioni: la cybersecurity come investimento strategico

La sicurezza informatica non può più essere considerata un costo, ma un investimento strategico nella continuità operativa, nella competitività e nella fiducia che clienti, partner e stakeholder ripongono nelle PMI.

Inoltre, in un contesto economico sempre più digitale e interconnesso, la capacità di gestire in modo consapevole e strutturato i rischi informatici rappresenta un fattore distintivo e abilitante per la crescita aziendale e la salvaguardia dei nostri ecosistemi di cui le PMI fanno parte.

Per le PMI italiane, il momento di agire è ora: investire in cybersecurity non è più un'opzione, ma una condizione necessaria per operare in modo sostenibile, tutelare il proprio patrimonio informativo e garantire la continuità del business. È tuttavia essenziale considerare la cybersecurity come un percorso evolutivo: un processo continuo di apprendimento, adattamento e miglioramento, in risposta a un panorama di minacce in costante trasformazione.

Inoltre, è doveroso evidenziare che la cybersecurity è una responsabilità condivisa che coinvolge persone, processi e tecnologie. Solo attraverso un approccio proattivo e un impegno diffuso è possibile costruire una cyber resilienza solida e duratura, intesa come calibrata sintesi dei principi di risk management, business continuity e cybersecurity. Ovvero, una resilienza che consenta alle organizzazioni di affrontare il cambiamento digitale con maggiore consapevolezza, ridurre l'impatto degli incidenti e cogliere con fiducia le opportunità offerte dall'innovazione tecnologica.



Cybersecurity, prova digitale e responsabilità: perché le imprese devono imparare a pensare come un tribunale

A cura di Daniela Mainenti

Nel dibattito pubblico la cybersecurity viene ancora rappresentata prevalentemente come una questione tecnologica: firewall, antivirus, segmentazione di rete, backup, sistemi di rilevazione delle intrusioni. Questa rappresentazione è parziale e rischia di essere fuorviante, perché l'attacco informatico non è soltanto un incidente tecnico ma sempre più spesso l'inizio di una vicenda giuridica complessa che coinvolge responsabilità, obblighi di notifica, contenziosi civili, procedimenti amministrativi e, nei casi più gravi, indagini penali.

Il punto critico non è dunque soltanto impedire che un attacco avvenga, ma essere in grado, dopo un incidente, di dimostrare cosa sia realmente accaduto. È qui che emerge una dimensione della cybersecurity che molte organizzazioni non hanno ancora pienamente interiorizzato: la dimensione probatoria.

Quando un sistema informativo viene compromesso, l'impresa si trova immediatamente immersa in un contesto nel quale ogni decisione ha implicazioni giuridiche. Bisogna comprendere la dinamica dell'intrusione, ricostruire la sequenza degli eventi, dimostrare se vi sia stata sottrazione o alterazione di dati, valutare se siano coinvolti dati personali e quindi attivare gli obblighi previsti dal quadro normativo europeo. In parallelo occorre considerare i possibili profili di responsabilità verso clienti, fornitori o partner commerciali e, sempre più spesso, prepararsi alla possibilità che l'incidente diventi oggetto di accertamento giudiziario.

In questo scenario i log di sistema, le tracce digitali, le configurazioni delle piattaforme e le registrazioni delle attività degli utenti assumono un valore che non è più soltanto tecnico ma giuridico. Essi diventano, a tutti gli effetti, elementi di prova. Il problema è che molte infrastrutture informatiche aziendali non sono progettate per produrre prova. I sistemi raccolgono dati tecnici utili alla gestione operativa della sicurezza, ma non necessariamente garantiscono tracciabilità completa, integrità delle registrazioni, conservazione affidabile delle evidenze digitali e ricostruibilità delle decisioni. Ciò significa che, nel momento in cui un incidente si trasforma in contenzioso, l'impresa può trovarsi nella posizione paradossale di non riuscire a dimostrare di aver adottato tutte le misure necessarie o di non essere in grado di ricostruire con precisione ciò che è accaduto.

La cybersecurity, in altri termini, non si esaurisce nella protezione dei sistemi ma implica la capacità di documentare e dimostrare le scelte compiute. Questa prospettiva sta diventando sempre più centrale nel contesto normativo europeo. Le nuove politiche di sicurezza digitale, dalle direttive sulla resilienza delle infrastrutture critiche alle strategie di regolazione dell'intelligenza artificiale, si fondano infatti su un principio che può essere sintetizzato in

una parola: accountability.

Non basta dichiarare di essere sicuri; bisogna poterlo dimostrare.

Per le imprese ciò significa integrare la sicurezza informatica con modelli di governance che tengano conto anche delle esigenze probatorie e della gestione delle evidenze digitali. In altre parole, progettare sistemi e procedure come se ogni incidente potesse essere un giorno analizzato in un'aula di tribunale.

Pensare come un tribunale, però, non significa trasformare l'azienda in un'organizzazione giudiziaria, ma assumere un approccio metodologico più rigoroso alla gestione del rischio digitale. Significa costruire infrastrutture che registrino in modo affidabile le attività rilevanti, definire procedure di conservazione delle evidenze digitali, integrare competenze giuridiche e tecniche nella gestione degli incidenti e sviluppare una cultura organizzativa nella quale sicurezza, trasparenza e responsabilità siano elementi inseparabili. Le imprese che adotteranno questo approccio non solo saranno più preparate ad affrontare attacchi informatici sempre più sofisticati, ma saranno anche in grado di dimostrare in modo credibile la propria affidabilità a clienti, partner e autorità di controllo.

La cybersecurity, infatti, non è soltanto una questione di difesa tecnologica ma un'infrastruttura di fiducia economica.

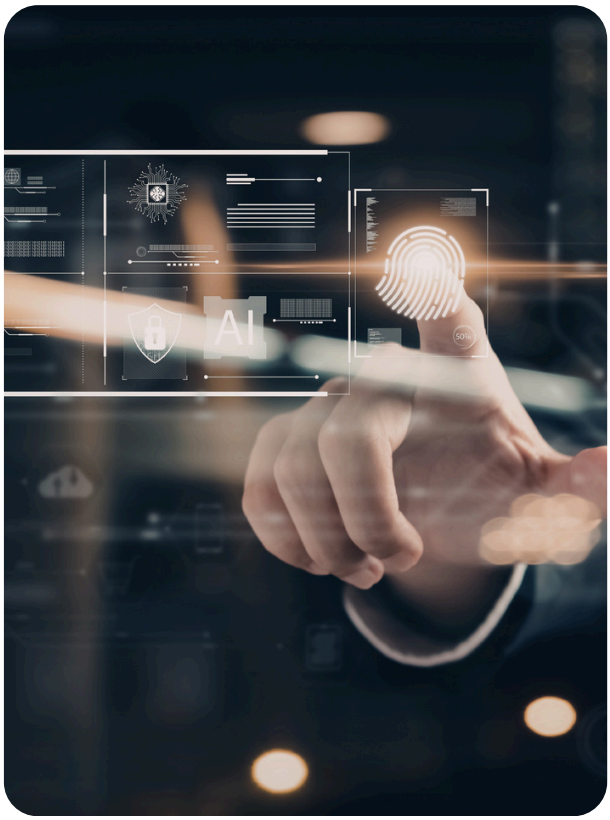
In un ecosistema digitale nel quale dati, piattaforme e algoritmi determinano gran parte delle relazioni economiche, la capacità di garantire sicurezza, e allo stesso tempo di dimostrarla, diventa un fattore competitivo decisivo. Questa prospettiva non è meramente teorica ma trova conferma in numerosi casi concreti nei quali l'incidente informatico ha assunto immediatamente una dimensione probatoria, istituzionale e, sempre più spesso, reputazionale.

Si pensi in Italia all'attacco ransomware subito nel 2023 dalla Regione Lazio, che ha coinvolto sistemi sanitari e piattaforme amministrative regionali. L'evento non ha generato soltanto una crisi operativa legata all'indisponibilità dei servizi digitali, ma ha immediatamente attivato un complesso circuito istituzionale che ha visto coinvolti il CSIRT nazionale, l'Agenzia per la Cybersicurezza Nazionale e l'autorità giudiziaria. In quel contesto l'analisi delle evidenze digitali è stata essenziale non solo per ricostruire la dinamica dell'intrusione ma anche per valutare eventuali profili di responsabilità organizzativa e per comprendere se vi fossero state carenze nella gestione degli accessi o nella segmentazione delle infrastrutture informatiche.

Il caso ha mostrato con chiarezza come un attacco informatico possa rapidamente trasformarsi in un problema di accountability istituzionale e come la capacità di documentare le scelte tecniche e organizzative assuma un ruolo centrale nella valutazione delle responsabilità.

Per non dire delle numerose indagini penali relative a frodi informatiche e attacchi ransomware che negli ultimi anni hanno coinvolto imprese private e pubbliche amministrazioni. Quando le infrastrutture aziendali non conservano in modo adeguato le registrazioni delle attività di sistema o non dispongono di procedure di conservazione dei log sufficientemente robuste, la ricostruzione degli eventi diventa più complessa e talvolta impossibile. Ne deriva che la capacità di collaborare efficacemente con le autorità investigative dipende in larga misura dalla qualità dei propri sistemi di tracciamento e dalla capacità di preservare le evidenze digitali senza comprometterne il valore probatorio.

Analoghe dinamiche emergono con ancora maggiore evidenza nel contesto internazionale, dove gli incidenti informatici tendono a produrre non solo conseguenze tecniche e investigative ma anche rilevanti effetti economici e reputazionali. L'attacco ransomware che nel 2021 colpì Colonial Pipeline negli Stati Uniti, per esempio, provocò la sospensione temporanea di una delle principali infrastrutture energetiche del Paese.



Allo stesso modo, il caso SolarWinds ha mostrato come la compromissione della supply chain del software possa essere ricostruita solo attraverso un'analisi forense estremamente accurata delle tracce lasciate nei sistemi di sviluppo e aggiornamento. Oppure l'attacco ransomware che nel 2023 ha colpito MGM Resorts International che ha provocato gravi disservizi nelle strutture di Las Vegas ha avuto un forte impatto mediatico globale, mentre l'incidente che ha coinvolto nello stesso anno il gruppo Clorox ha inciso direttamente sui risultati economici e sulla percezione degli investitori. Ancora più significativo è il caso dell'attacco del 2024 alla piattaforma sanitaria Change Healthcare, che ha interrotto servizi utilizzati da ospedali e farmacie negli Stati Uniti generando un ampio dibattito sulla sicurezza delle infrastrutture digitali sanitarie.

Anche in Europa non mancano esempi analoghi. L'attacco informatico che nel 2024 ha colpito la British Library ha determinato il blocco prolungato dei servizi digitali e la diffusione online dei dati sottratti, con un impatto reputazionale rilevante per l'istituzione.

Nel loro insieme questi episodi dimostrano come gli incidenti informatici non producano soltanto conseguenze tecniche o economiche, ma incidano direttamente sulla credibilità delle organizzazioni coinvolte.

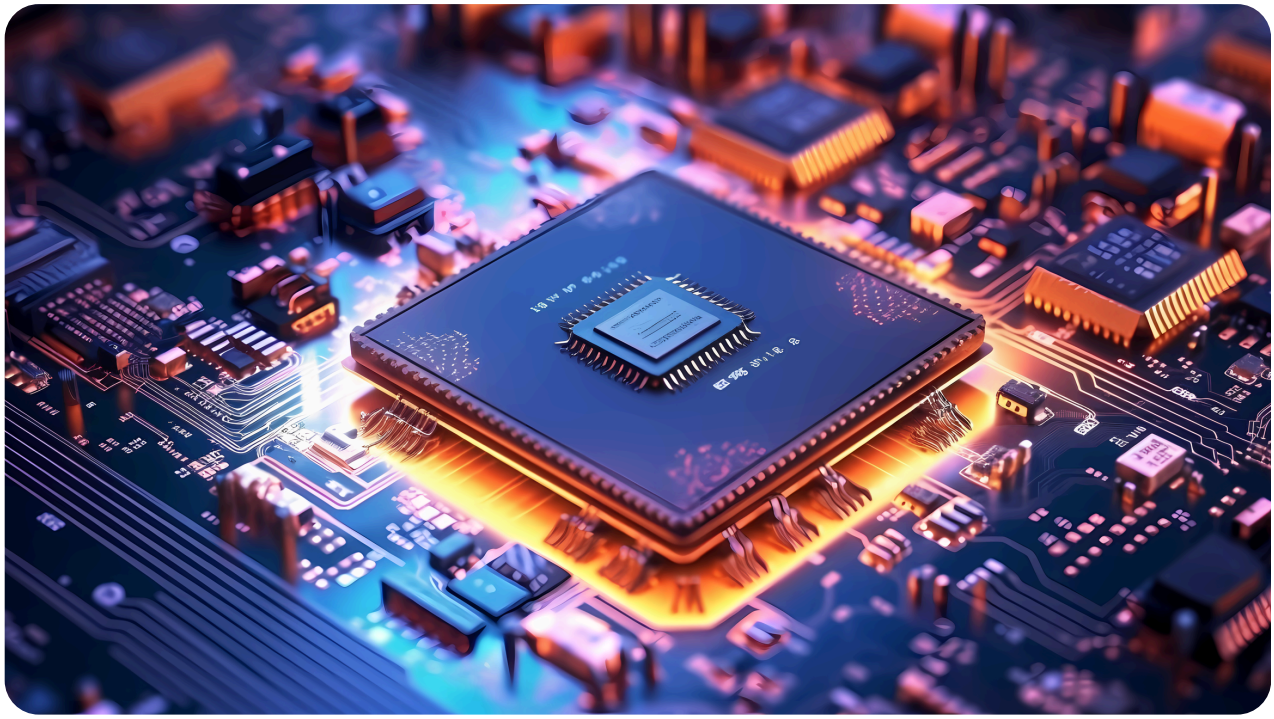
Questo perché, in un ecosistema informativo caratterizzato da una forte interconnessione tra media, mercati finanziari e opinione pubblica, l'incidente informatico tende a trasformarsi rapidamente in un evento che va ben oltre il momento investigativo e, nel contesto europeo che è caratterizzato da un quadro regolatorio sempre più attento alla responsabilità delle organizzazioni nella gestione del rischio digitale, l'aspetto reputazionale tende a intrecciarsi con la dimensione della conformità normativa.

In questo senso la cybersecurity diventa uno strumento essenziale di costruzione della fiducia istituzionale e di tutela della immagine aziendale.

La gestione della prova digitale e delle evidenze informatiche non rappresenta dunque soltanto una esigenza tecnica o processuale, ma costituisce un elemento strategico nella governance della reputazione.

In un ambiente economico nel quale le informazioni circolano con estrema rapidità e gli incidenti informatici assumono immediatamente una dimensione pubblica, la capacità di dimostrare, con chiarezza giuridica, cosa sia accaduto, quali misure siano state adottate e quali azioni siano state intraprese diventa un fattore essenziale per preservare la credibilità dell'organizzazione.

Pertanto, le imprese che, oltre a integrare sicurezza informatica e comunicazione responsabile, saranno affiancate da giuristi esperti saranno quelle meglio attrezzate per affrontare non solo la dimensione tecnica degli attacchi ma anche il loro inevitabile impatto reputazionale.



La discrasia necessaria: comunicare la segretezza nell'era dell'IA

A cura di Vittorio Orefice

La Discrasia Necessaria: Comunicare la Segretezza nell'era dell'IA

Le recenti riflessioni emerse all'interno del nostro Cybersecurity Think Tank hanno messo in luce un paradosso fondamentale dei nostri tempi: la profonda discrepanza tra la potenza disponibile dei mezzi di divulgazione e la natura di informazioni, saperi e dati che spesso non vorremmo vedere divulgati. Ci troviamo nella condizione di dover utilizzare i canali più capillari e performanti per trasmettere un messaggio che esorta, al contrario, alla massima attenzione verso la riservatezza e la protezione dei dati.

Questa discrasia non è un limite, ma il segnale di un nuovo paradigma operativo in cui l'Intelligenza Artificiale (IA) assume un ruolo ancipite, diventando uno strumento essenziale in due modalità diametralmente opposte, entrambe vitali per il bene delle aziende.

L'IA come motore di diffusione: la funzione "Marketing"

Il primo ambito è quello della sensibilizzazione e della creazione di cultura. In questa veste, il Think Tank opera con una logica simile a quella del marketing aziendale: l'obiettivo è la massima risonanza. L'IA viene qui impiegata come un moltiplicatore di potenza informativa, capace di generare report, sintesi di riunioni e materiali formativi per raggiungere il maggior numero possibile di stakeholder.

In questo contesto, l'IA è uno strumento di efficienza che trasforma i contenuti tecnici in messaggi accessibili, accelerando la diffusione di buone pratiche di difesa collettiva. L'uso di IA per la presa di note o la redazione di minute è accolto positivamente proprio perché facilita la circolazione delle idee laddove la sensibilità dei dati lo permette.

L'IA come scudo della riservatezza: la funzione "Protezione"

Il secondo ambito, speculare e opposto, riguarda la protezione seria del patrimonio di saperi e asset intangibili. Qui l'IA non deve diffondere, ma blindare. In questa modalità, l'IA viene utilizzata per monitorare le minacce, gestire sistemi di crittografia avanzata o analizzare i metadati per ridurre la superficie di attacco.

Mentre nella fase divulgativa cerchiamo la massima visibilità, nella protezione degli asset critici applichiamo il modello **Zero Trust**, presupponendo un ambiente intrinsecamente ostile. In questo dominio, l'IA deve operare entro i confini della sovranità digitale, preferendo giurisdizioni protette (come UE o Svizzera) e tecnologie che impediscano ai fornitori di accedere ai dati cifrati.

L'analogia aziendale: una scelta strategica

Ogni azienda deve oggi imparare a gestire questa doppia velocità, distinguendo nettamente tra:

- **Marketing e Comunicazione**: Dove l'IA serve a espandere il raggio d'azione, utilizzando piattaforme agili e trasversali per coinvolgere il mercato.
- **Protezione dei Saperi**: Dove l'IA serve a restringere l'accesso, proteggendo brevetti, segreti industriali e strategie attraverso una segregazione rigorosa dei canali.

Confondere questi due ambiti significa esporre il patrimonio dell'organizzazione a rischi finanziari e legali insostenibili. La responsabilità del management consiste nel decidere, caso per caso, quale delle due facce dell'IA attivare.

Per queste ragioni stiamo preparando un webinar che approfondirà l'aspetto protettivo poiché di quello "marketing" è piena la rete. Nel webinar insisteremo sui metodi per proteggere le informazioni durante eventi on line e scambi di messaggi.

Gli eventi infatti debbono essere vissuti con in mente il concetto che si sta, potenzialmente, condividendo dati con "tutti" ivi compresi proprio coloro cui non vorremmo fare questo regalo mentre i messaggi possono essere scambiati in modalità più protette a patto di prestare attenzione ai sistemi utilizzati.

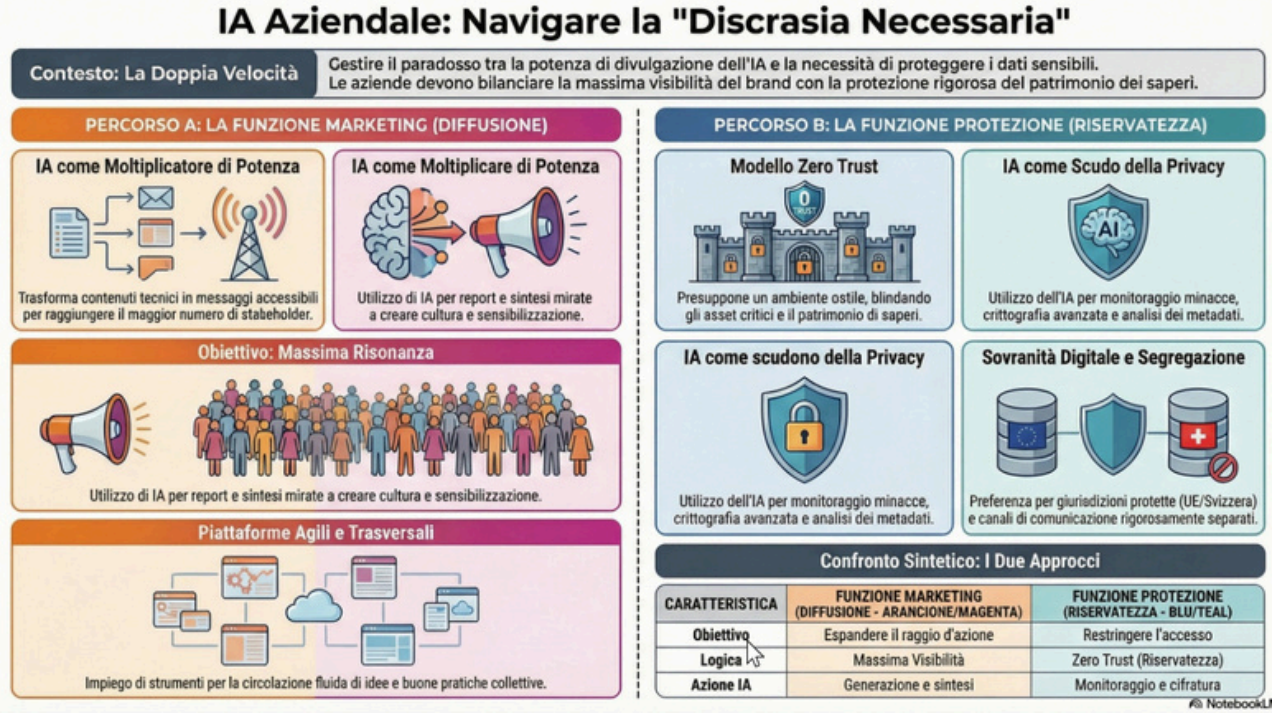
Qualche anno fa si usava dire " di certe cose si parla solo di persona non al telefono...".

Anticipiamo con la figura seguente i temi che tratteremo.

Conclusioni

Imparare a sfruttare l'IA in questi due modi opposti è la competenza distintiva del futuro.

Il Cyber Think Tank continuerà a utilizzare i mezzi più potenti per predicare la segretezza, consapevole che la vera sicurezza non nasce dall'isolamento, ma dalla capacità strategica di governare la discrasia tra la forza della parola e la sacralità del dato.



Cyberspazio: finzione o realtà?

A cura di Ranieri Razzante

Una cosa è certa: i confini tra legalità e crimine risultano sempre più sfumati nel cyberspazio.

Ed occorre ancora tornare sulla sua definizione, proprio per comprendere quali siano le sue caratteristiche strutturali e le dinamiche – oggi persino "geopolitiche" - più rilevanti.

Il concetto di *cyberspace* ha conosciuto un'evoluzione significativa: da metafora letteraria degli anni Ottanta si è trasformato in categoria analitica del diritto e della sicurezza, quale ambiente operativo multidimensionale che integra reti, dispositivi, software e interazioni umane, imponendo al giurista la qualificazione di diritti e obblighi in un contesto privo di confini fisici.

È utile ad esempio distinguere il cyberspazio dall'"infosfera", intesa come spazio semantico in cui i dati assumono valore informativo e giuridico: distinzione che mostra come la regolazione non possa limitarsi alle infrastrutture tecniche, ma debba estendersi alla *governance* dell'informazione.

Il cyberspazio non è un luogo fisico, è chiaro, bensì un concetto socio-tecnico che designa spazi di comunicazione, elaborazione e conservazione dell'informazione mediati da tecnologie digitali. È un ecosistema stratificato composto sostanzialmente da tre livelli – infrastrutture materiali, artefatti logici e attori umani – che insieme consentono generazione, trasporto, elaborazione e conservazione dei dati.

Tale ecosistema è caratterizzato però (da quello che si può ricavare da studi maggiormente tecnici) da territorialità incerta, velocità e scalabilità degli attacchi, asimmetria di costi tra offensore e difensore, pervasività degli *endpoint* e dipendenza da servizi essenziali erogati tramite terze parti e *supply chain* complesse. Ne deriva una lettura del rischio che integri analisi tecnica, valutazione organizzativa e controllo contrattuale, ridefinendo processi decisionali, modelli di *governance* e assetti di responsabilità. Ce n'è per i giuristi, per i risk manager, gli economisti, oltre a sociologi, strateghi del marketing e psicologi comportamentali.

Accanto a ciò si collocano questioni (sempre più presenti ed insopprimibili) di ordine pubblico e sovranazionale (che vanno dalla sovranità digitale alla cooperazione investigativa) che richiedono strumenti normativi multilivello compatibili con diritti fondamentali e proporzionalità delle conseguenze.

L'evoluzione normativa europea amplia l'ambito soggettivo di ricaduta delle protezioni, rafforza la gestione del *cyber risk*, con rilevanti conseguenze operative per le aziende. La NIS2 distingue, come noto, tra "entità essenziali" e "importanti", estendendo obblighi di *governance* e segnalazione degli incidenti a numerosi settori. Una "cyber governance" si affianca a quella amministrativa, contabile, legale e operativa delle imprese, con le conseguenze in termini di costi, ma pure di ricavi (o meglio, di mitigazione delle perdite), fino a cinque

anni fa probabilmente non allocabili e nemmeno calcolate.

A tale ultimo fine è centrale il ruolo della certificazione europea prevista dal *Cybersecurity Act*, che introduce tre livelli di garanzia – base, sostanziale, alto – e tende a rendere l'asseverazione fattore d'ordine nel mercato digitale, incidendo su *procurement*, diligenza e criteri di equivalenza. Se integrata nei processi contrattuali, essa contribuisce a ridurre le asimmetrie informative e le conseguenze della (oggi forse ancora eccessiva) frammentazione regolatoria.

Il *Cyber Resilience Act* estende detti obblighi lungo l'intero il ciclo di vita dei prodotti digitali, ridefinendo, come noto, le responsabilità di fabbricanti e distributori, prevedendo inoltre un quadro sanzionatorio rilevante. Il Regolamento DORA rappresenta invece un paradigma di auspicata convergenza tra sicurezza informatica e *governance* del rischio finanziario, imponendo una gestione integrata del rischio ICT, specifiche metriche operative, piani di continuità e coinvolgimento attivo degli organi di vertice, con specifica attenzione alla gestione del rischio di terze parti e dei *provider cloud* (ai quali banche e intermediari finanziari hanno sempre più affidato l'archiviazione della documentazione della clientela).

La *supply chain* digitale emerge allora sempre più quale elemento di rischio sistemico: la *governance* della sicurezza deve estendersi all'intera rete contrattuale, commerciale e delle infrastrutture produttive. Ciò richiede coordinamento anche tra Autorità nazionali e sovranazionali, evitando frammentazioni e sovrapposizioni nelle policy normative ed operative che si stanno approntando soprattutto a livello euro unitario.

Sul piano penale, l'evoluzione dei reati informatici, l'uso del *Dark Web*, il pericolo *Ransomware* e le insidie derivanti dall'ingegneria sociale ridefiniscono problemi di attribuzione delle responsabilità nel mondo virtuale e di cooperazione giudiziaria. Accanto alla sicurezza penale, assume rilievo poi quella *extra*-penale: come già accennato, standard tecnici, gestione del rischio, protezione dei dati. L'interazione tra sicurezza e GDPR, poi, impone misure tecniche e organizzative adeguate, specie rispetto ad IoT, 5G e *cloud*, valorizzando i principi di sicurezza *by design e by default*.

Analoghe opportunità e rischi emergono con l'intelligenza artificiale: sistemi capaci di apprendimento e adattamento incrementano efficienza, ma possono potenziare il cybercrime, abbassando la soglia tecnica per condotte malevole. Occorrono ancora riflessioni giuridiche sull'uso improprio dell'IA e un coordinamento tra *AI Act*, *Cyber Resilience Act*, DORA e altri apparati normativi dedicati.

Nel contesto *Cyber* multirischio, l'IA può supportare *detection* e risposta, ma anche essere strumentalizzata per attacchi sofisticati, imponendo validazione dei modelli e *audit* periodici. La responsabilità assume natura multidimensionale, intrecciando profili civili, amministrativi e penali. Si stanno infatti aggiornando le categorie penali, col rischio però di estendere indebitamente la responsabilità individuale, a fronte della quale bisognerà sempre mantenere equità e proporzionalità.

Ma la madre di tutte le questioni continua ad essere, a mio avviso, il *matching tra Cyber Security* e protezione dei dati: si impongono sempre più, solo guardando alla cronaca, soluzioni che concilino

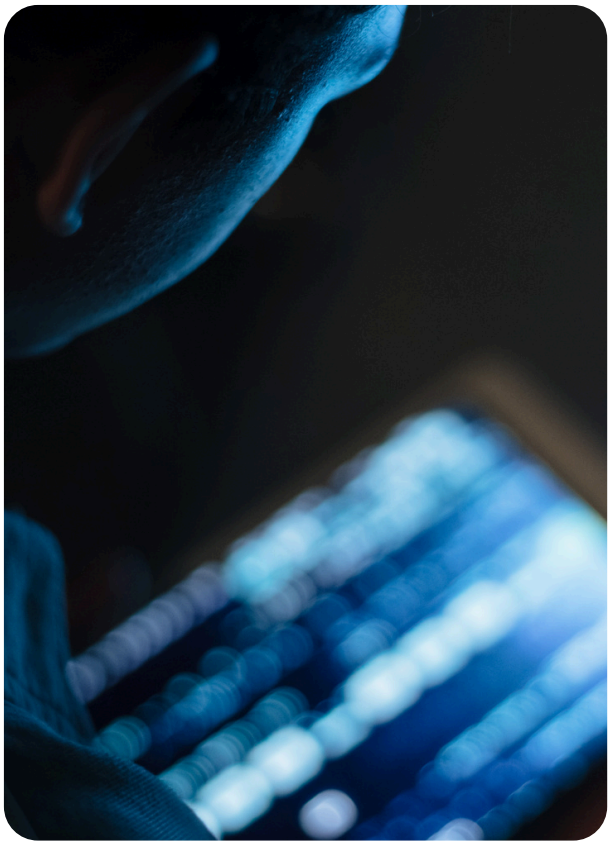
monitoring e principi del GDPR, attraverso, ad esempio, sistemi con pseudonimizzazione e cifratura.

In prospettiva, risultano assai utili ed auspicabili delle *community of practice*, con una condivisione volontaria di *threat intelligence*, *standard* tecnici aperti e sicurezza nella progettazione. Un modello operativo su tre livelli – prevenzione tecnica, gestione organizzativa, reazione coordinata – può ad esempio integrare clausole contrattuali tipo, formazione specialistica ed esercitazioni congiunte pubblico-privato. È necessario armonizzare adempimenti tra NIS2, DORA e CRA, investire in ricerca e prepararsi agli scenari del *quantum computing*.

Sul piano dei diritti fondamentali, occorre bilanciare sicurezza e libertà mediante l'applicazione rigorosa dei già noti - a dire il vero - concetti di proporzionalità, minimizzazione e trasparenza. Prioritaria risulta – giova ricordarlo ancora una volta - una chiara allocazione delle responsabilità negli organi di vertice e nei ruoli tecnici, con KPI di sicurezza, *audit* periodici e soglie di *escalation*. In ambito contrattuale, clausole modulari per il *procurement* ICT devono prevedere ambiti precisi di responsabilità della sicurezza, *disclosure* delle vulnerabilità, diritti di ispezione e rimedi graduati.

Nel pubblico, sono auspicabili strumenti interpretativi condivisi tra Autorità e coordinamento transfrontaliero, per ridurre duplicazioni di norme e frammentazione degli ordinamenti. La formazione continua di magistrati, forze di polizia, auditors, giuristi d'impresa e cittadini rappresenta leva sistemica e strategica per una cultura della resilienza.

L'obiettivo, non solo teorico, è un equilibrio dinamico tra prevenzione, responsabilità e risposta coordinata, a tutela di interessi economici, diritti fondamentali e interessi pubblici strategici. La cybersicurezza è dimensione trasversale della modernità giuridica. Il compito del giurista e del decisore pubblico, ricordiamolo, è, in questo frangente, tradurre la complessità tecnologica in regole chiare e di *governance* coerenti, attraverso cooperazione multilivello e linguaggio comune tra discipline.



Solo così si potrà garantire che l'era digitale resti spazio di libertà, sviluppo e tutela dei valori democratici. Il cyberspazio non è una finzione, quindi, ma una realtà fenomenologica e un nuovo dominio da normare e governare senza perdere le opportunità che offre alla scienza e alla quotidianità.

DORA come architettura di resilienza sistemica: specialità normativa, integrazione tecnologica e governo contrattuale della filiera ICT

A cura di Matteo Rocchi

Il Regolamento (UE) 2022/2554, noto come Digital Operational Resilience Act (DORA), non si limita a costituire un ulteriore tassello nel mosaico delle discipline europee in materia di cybersicurezza, bensì si impone quale vero e proprio dispositivo di riequilibrio sistemico del rapporto tra stabilità finanziaria e dipendenza tecnologica. Esso interviene in un contesto caratterizzato da un'evoluzione strutturale dell'ecosistema finanziario, nel quale la trasformazione digitale ha progressivamente dissolto i confini tra infrastruttura tecnica e funzione economica, rendendo l'operatività digitale non più subalterna, ma preminente all'erogazione dei servizi finanziari.

In tale scenario, la vulnerabilità informatica non rappresenta soltanto un rischio operativo, bensì un fattore potenzialmente idoneo a compromettere l'integrità del mercato, la continuità dei servizi essenziali e, in ultima analisi, la fiducia sistemica degli investitori e dei consumatori. DORA si inserisce in questo orizzonte come norma settoriale di specialità, la cui funzione non è quella di replicare obblighi già presenti nella disciplina orizzontale della cybersicurezza, ma di declinarli secondo la logica prudenziale propria del diritto finanziario europeo.

La qualificazione di DORA quale lex specialis rispetto alla normativa generale in materia di sicurezza delle reti e dei sistemi informativi non costituisce un mero tecnicismo. Nel linguaggio giuridico, la lex specialis è infatti la norma che, disciplinando in modo puntuale e specifico un determinato ambito materiale, prevale sulla norma generale in caso di sovrapposizione o conflitto. Trasposta sul piano della resilienza operativa digitale, tale qualificazione implica che gli obblighi, le soglie, le procedure di reporting, i requisiti di testing e le disposizioni in materia di gestione del rischio ICT da terzi previsti da DORA assumano carattere primario e prevalente per il settore finanziario, anche laddove esistano discipline di carattere generale applicabili ad altri settori critici, quale ad esempio la normativa NIS2 di più ampio respiro.

Ne deriva una conseguenza di non secondaria importanza: la conformità a standard generici di sicurezza informatica, a framework volontari o a best practice di mercato non è, di per sé, sufficiente a soddisfare l'impianto regolatorio di DORA, il quale esige una declinazione specifica, documentata e verificabile della resilienza digitale in funzione della stabilità del sistema finanziario.
L'oggetto della disciplina non è semplicemente la sicurezza tecnica del sistema informativo, bensì la capacità dell'entità finanziaria di costruire, mantenere, riesaminare e dimostrare la propria integrità e affidabilità operativa lungo l'intero ciclo di vita dei sistemi ICT.

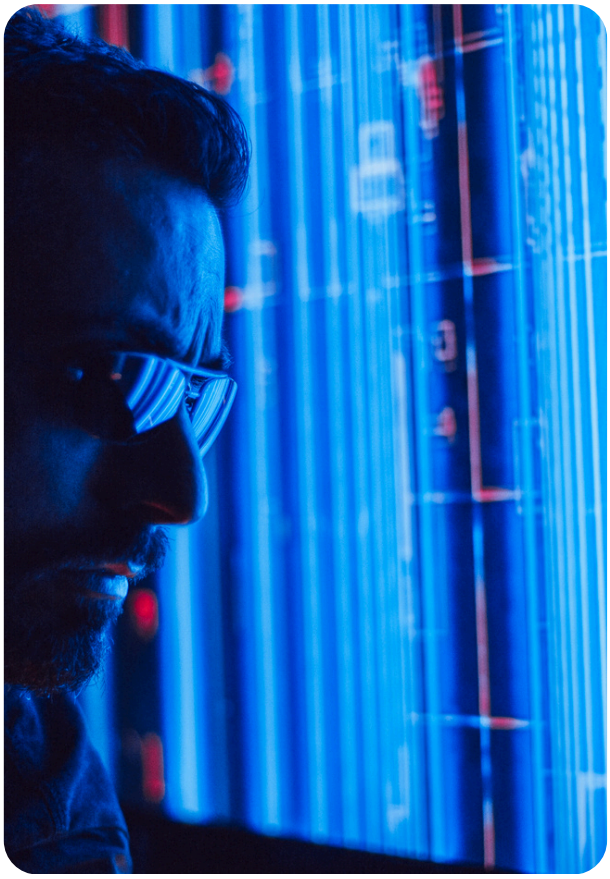
Responsabilità e framework ICT

L'elemento forse più incisivo del Regolamento è rappresentato dalla centralità attribuita all'organo di

gestione, al quale viene riconosciuta una responsabilità piena e non delegabile nella definizione e supervisione del framework di gestione del rischio ICT. La resilienza digitale non è più, in questa prospettiva, materia riservata alla funzione IT o alla sicurezza informatica, ma diviene componente strutturale della governance societaria. L'organo di amministrazione è chiamato ad approvare politiche, soglie di tolleranza al rischio, allocazioni di budget e piani di remediation, nonché a dimostrare, in sede ispettiva, la coerenza tra scelte allocative e profilo di rischio.

La codificazione del principio secondo cui l'esternalizzazione non comporta trasferimento di responsabilità regolatoria rappresenta un ulteriore snodo di rilievo. L'entità finanziaria resta pienamente responsabile nei confronti delle autorità di vigilanza anche quando la funzione tecnologica sia affidata a un provider esterno, ivi inclusi hyperscaler cloud, vendor software o fornitori di servizi di sicurezza. In tal modo, il Regolamento trasforma il rapporto tra ente vigilato e fornitore ICT in una relazione strutturalmente integrata, nella quale la conformità non può essere confinata al perimetro del cliente, ma deve essere incorporata nell'intera filiera tecnologica.

L'ICT Risk Management Framework previsto da DORA si articola come processo ciclico e continuo, che muove dall'identificazione completa e aggiornata degli asset tecnologici e delle relative dipendenze, per giungere alla protezione, alla rilevazione delle anomalie, alla risposta agli incidenti, al ripristino e, infine, al miglioramento continuo attraverso analisi post-evento e piani di remediation formalizzati. La prima fase, spesso trascurata in contesti non regolati, assume qui una dimensione determinante: non è possibile proteggere, né tantomeno ripristinare, ciò che non è stato censito e classificato.



L'inventario degli asset non può limitarsi ai server fisici o virtuali, ma deve comprendere applicazioni, componenti open source, interfacce API, flussi dati, ambienti cloud, database, sistemi legacy, integrazioni con terze parti e catene di subfornitura. Tale mappatura costituisce la base per la classificazione delle funzioni essenziali o importanti, la cui interruzione potrebbe generare impatti significativi sulla continuità operativa o sulla tutela dei clienti. È in funzione di tale classificazione che si determinano i livelli di controllo richiesti, la frequenza dei test, la severità delle soglie di incident reporting e l'intensità dei requisiti contrattuali nei confronti dei fornitori coinvolti.

In questo contesto, concetti quali Recovery Time Objective e Recovery Point Objective cessano di essere indicatori meramente tecnici per assumere la natura di parametri normativi vincolanti. Il tempo massimo tollerabile di interruzione e la perdita massima accettabile di dati devono essere formalmente definiti, coerenti con la criticità della funzione e oggetto di test periodici documentati. La continuità operativa non può essere dichiarata in astratto: deve essere dimostrata attraverso evidenze verificabili, simulazioni e reportistica strutturata.

L'eterogeneità tecnologica nell'era DORA

È proprio su questo terreno che emergono le complessità legate all'eterogeneità tecnologica di molte organizzazioni finanziarie e dei loro fornitori. Il tessuto infrastrutturale reale è raramente omogeneo: accanto a piattaforme cloud-native e ambienti virtualizzati di ultima generazione coesistono sistemi legacy, architetture IBM Power, partizioni IBMi, database DB2, soluzioni proprietarie sviluppate in epoche precedenti e integrate nel tempo. Tali sistemi, pur rappresentando spesso il cuore storico e business-critical dell'organizzazione, non sono nativamente progettati per interfacciarsi con moderni sistemi di logging centralizzato, SIEM, dashboard di compliance o motori di correlazione eventi.

L'esigenza regolatoria di disporre di flussi informativi tempestivi, tracciabili e normalizzati impone dunque l'adozione di strumenti software capaci di estendere le funzionalità di auditing, reporting e monitoraggio anche agli ambienti meno recenti.

Non si tratta soltanto di integrare log tecnici, ma di renderli intellegibili ai fini della classificazione dell'incidente, della valutazione delle soglie di materialità e della predisposizione delle notifiche obbligatorie. Il flusso informativo richiesto da DORA non può prescindere dalla sinergia tra il mondo legacy e quello delle moderne infrastrutture cyber: la resilienza, per essere tale, deve essere sistemica e non settoriale.

L'obbligo armonizzato di segnalazione degli incidenti ICT gravi, articolato in notifiche iniziali, relazioni intermedie e report finali, impone tempistiche stringenti che mal si conciliano con sistemi incapaci di fornire rapidamente dati strutturati sull'impatto, sulla durata e sulla portata dell'evento. In uno scenario di outsourcing, la qualità e la tempestività delle informazioni fornite dal provider determinano la capacità del cliente vigilato di adempiere ai propri obblighi regolatori. Un'infrastruttura incapace di generare report auditabili o di garantire la conservazione immutabile dei log espone non soltanto a rischi tecnici, ma a responsabilità regolatorie.

Parallelamente, il programma di testing proporzionato alla resilienza digitale, richiede che l'intera architettura, inclusi i fornitori ICT critici, sia predisposta a essere sottoposta a verifica empirica. Il testing non si limita, infatti, a sondare la robustezza perimetrale, ma valuta anche la capacità di rilevazione, contenimento, escalation e ripristino; l'assenza di integrazione tra ambienti tradizionali e piattaforme moderne può tradursi in una frammentazione della difesa e in una perdita di visibilità sistemica.

L'opportunità di nuovi paradigmi contrattuali

La disciplina del rischio ICT da terzi costituisce, probabilmente, il segmento più innovativo e incisivo del Regolamento. DORA non vieta l'esternalizzazione, ma la incardina in una struttura di governo formalizzata, che comprende l'adozione di una strategia approvata dall'organo di gestione, la tenuta di un registro dettagliato dei contratti ICT e l'inserimento di clausole minime obbligatorie. Tali clausole non hanno carattere meramente dichiarativo, ma devono garantire diritti effettivi di audit, accesso alle informazioni, cooperazione in caso di incidente, standard di sicurezza verificabili, gestione dei subfornitori e predisposizione di strategie di uscita praticabili.

È in questo ambito che il ruolo di partner specializzati in compliance assume rilievo determinante. La redazione di contratti che siano al contempo tecnicamente efficaci e "DORA-friendly" non rappresenta un esercizio di stile, bensì un presidio di equilibrio negoziale e di sostenibilità operativa. Predisporre sin dall'origine schemi contrattuali che incorporino in modo equilibrato i diritti di audit previsti dal Regolamento, le modalità di accesso ai log, le procedure di notifica degli incidenti e le condizioni di cooperazione con le autorità consente al fornitore di proporsi come controparte matura e consapevole delle esigenze regolatorie del cliente.

In assenza di tale preparazione, il rischio concreto è che il cliente soggetto a DORA, nel tentativo di tutelarsi rispetto alla propria esposizione regolatoria, imponga addenda contrattuali standardizzati e potenzialmente sbilanciati, con clausole invasive, obblighi informativi sproporzionati e responsabilità amplificate. Una contrattualistica predisposta con criteri di compliance preventiva non solo facilita il dialogo con il cliente, ma preserva l'equilibrio reciproco del rapporto, evitando che la conformità si traduca in un trasferimento eccessivo del rischio.

La capacità di offrire soluzioni tecnologiche integrate da un impianto contrattuale coerente con DORA costituisce, pertanto, un autentico vantaggio competitivo. Essa consente di superare con maggiore agilità le procedure di vendor assessment, di ridurre i tempi di negoziazione e di consolidare una reputazione di affidabilità nel mercato finanziario europeo. In un contesto nel quale la resilienza digitale è divenuta requisito prudenziale, la preparazione preventiva sul piano legale e organizzativo è elemento distintivo tanto quanto l'innovazione tecnica.

Un cammino da affrontare preparati

Alla luce di tali considerazioni, il percorso di adeguamento a DORA non può essere affrontato in modo frammentario. Esso richiede una visione integrata che coniughi governance, architettura tecnologica, strumenti software di estensione e normalizzazione dei flussi informativi, nonché presidio contrattuale della filiera ICT. I partner chiamati ad accompagnare le organizzazioni in tale processo devono essere in grado di comprendere e orchestrare la complessità di ambienti ibridi, nei quali sistemi legacy e infrastrutture moderne convivono e devono dialogare in modo coerente ai fini della resilienza. DORA, in definitiva, non è una checklist di adempimenti, ma un paradigma di responsabilità sistemica. Essa impone trasparenza, controllabilità, tracciabilità e continuità come condizioni strutturali dell'operatività finanziaria digitale. Le organizzazioni che sapranno interpretare tale impianto non come vincolo, ma come architettura di fiducia, potranno trasformare la compliance in leva di posizionamento strategico, rafforzando la propria credibilità in un mercato nel quale la stabilità operativa coincide, ormai, con la legittimazione stessa dell'attività economica.

Cos'è il phishing?

Una truffa online che cerca di carpire le tue informazioni personali (password, numeri di carta di credito, ecc.) fingendosi qualcuno di fidato (banca, social network, ecc.).

Come Funziona?

Email
Messaggi che sembrano provenire da enti affidabili, ma contengono link dannosi.

Siti Web falsi
Pagine che imitano perfettamente quelle originali per indurti a inserire i tuoi dati.

Messaggi
SMS o notifiche push che ti invitano a cliccare su link pericolosi.

Chiamata
furto di informazioni personali tramite telefono.

Perché lo fanno?

I cyber criminali utilizzano il phishing per:

- Rubare informazioni personali.
- Spiare le aziende.
- Crittografare i dati e chiedere un riscatto.
- Diffondere malware.

Cosa sfruttano?

Le loro armi sono:

La paura:
Ti minacciano di conseguenze negative.

L'avidità:
Ti promettono ricompense incredibili.

L'urgenza:
Ti spingono ad agire subito.

L'inganno:
Ti fanno credere di essere qualcuno di fidato.

Come difendersi?

Verifica l'indirizzo e-mail:
Controlla attentamente l'indirizzo del mittente.

Non cliccare su link sospetti:
Evita di cliccare su link presenti in e-mail o messaggi non richiesti.

Controlla l'URL:
Assicurati che l'indirizzo del sito web inizi con "https://" e abbia un certificato di sicurezza.

Non fornire mai informazioni personali:
Non comunicare mai password, codici di sicurezza o dati sensibili tramite e-mail o messaggi.

Utilizza un antivirus e un firewall:
Proteggi il tuo dispositivo con software di sicurezza aggiornati.

Tieniti aggiornato:
Informati sulle ultime truffe online.

Credits by: Tinexta Cyber

Quando i dati sopravvivono alle persone. La nuova frontiera della sovranità digitale

A cura di Giulia Salis Nioi

C'è stato un tempo in cui lasciare qualcosa dopo la morte significava case, libri, forse qualche fotografia in una scatola. Oggi lasciamo dietro di noi un ecosistema intero: e-mail, documenti nel cloud, account professionali, archivi aziendali, wallet digitali, accessi a piattaforme, cronologie, metadati. Una vita intera tradotta in credenziali.

Il punto è che Internet non ha mai imparato a gestire la fine delle persone.

Ogni giorno milioni di identità continuano a esistere online anche quando il loro proprietario non c'è più. Non sono solo profili social dimenticati. Sono caselle e-mail che contengono contratti, repository di codice, account amministrativi, cartelle condivise con colleghi, archivi di clienti, sistemi aziendali. La morte biologica è un evento chiaro. Quella digitale è lenta, confusa, spesso invisibile. E soprattutto: per la cybersecurity è un problema enorme.

Uno degli studi più citati sull'argomento, condotto dall'Oxford Internet Institute, stima che gli account di persone decedute su Facebook potrebbero arrivare a circa 4,9 miliardi entro la fine del secolo. Se la crescita della piattaforma rallentasse, i morti potrebbero addirittura superare i vivi già in questo secolo. Non è solo una curiosità sociologica. È la prova che stiamo accumulando identità digitali che non hanno più un proprietario attivo.

Quando una persona smette improvvisamente di gestire i propri accessi, succede qualcosa di molto semplice: la superficie di attacco aumenta. Password che non vengono mai cambiate, sistemi che restano collegati ad altri account, e-mail che continuano a ricevere reset di sicurezza, archivi che nessuno controlla più. Nel mondo fisico chiudiamo la casa di chi non c'è più. Nel mondo digitale spesso lasciamo tutto acceso.

Una ricerca internazionale commissionata da Kaspersky ha rilevato che oltre il 60% delle persone teme che l'identità online dei defunti possa essere sfruttata per furti di identità o frodi, proprio perché nessuno la gestisce più. Non serve immaginare scenari da fantascienza. Basta pensare a cosa contiene oggi una singola casella e-mail: banche, servizi pubblici, accessi aziendali, autenticazioni a due fattori: in pratica, il vero "master key" della nostra vita digitale.

Il problema è che quasi nessuno pianifica cosa succederà dopo. Studi sulla digital legacy mostrano che solo una minoranza delle persone lascia istruzioni per i propri account, e pochissimi inseriscono indicazioni nel testamento. Non è negligenza: è che il concetto stesso è nuovo. Per secoli l'eredità è stata materiale. Ora è fatta di dati, e i dati non hanno ancora un rituale sociale.

Ma la questione non riguarda solo la sfera privata. In molte organizzazioni esistono identità professionali che diventano critiche nel tempo: account amministrativi creati anni prima, accessi condivisi tra team, sistemi collegati a singole persone. Quando qualcuno scompare, la sua identità digitale spesso rimane incastrata nei processi. Non è raro che aziende scoprano troppo tardi che un servizio fondamentale dipendeva da una casella e-mail o da un accesso personale che nessuno può più recuperare.

Nel linguaggio della sicurezza informatica si parla molto di identity management. Ma quasi sempre lo si immagina mentre le persone sono vive, presenti, operative. In realtà l'identità digitale ha un ciclo di vita molto più lungo della persona che l'ha creata. E qui emerge una domanda che tocca la sovranità dei dati. Finché siamo vivi possiamo cambiare password, revocare accessi, cancellare contenuti, migrare archivi. Dopo la morte, invece, il controllo passa a procedure delle piattaforme, politiche aziendali, o semplicemente all'inerzia tecnologica. Molte famiglie scoprono che recuperare foto o documenti è più complicato che gestire un conto bancario. In alcuni casi è impossibile. Il paradosso è che la nostra epoca produce più memoria di qualsiasi altra nella storia, ma molto meno controllo su di essa.

Ogni attività digitale genera tracce persistenti: log, copie, backup, cache, archivi distribuiti. Anche quando un account viene chiuso, i dati spesso continuano a esistere altrove. Internet è progettato per conservare, replicare, sincronizzare. Non per morire. Questo crea una nuova categoria di rischio che le aziende stanno appena iniziando a vedere: identità senza proprietario. Non sono compromesse, non sono violate, non sono rubate. Sono semplicemente rimaste senza qualcuno che le governi. Eppure, continuano ad avere privilegi, accessi, relazioni con altri sistemi.

Se guardiamo alla storia della cybersecurity, ogni grande evoluzione è nata da un cambio di prospettiva. Prima abbiamo protetto i computer, poi le reti, poi i dati, poi le identità. Il prossimo passaggio potrebbe essere proteggere le identità nel tempo. Perché la domanda non è più solo chi può accedere a un sistema oggi, ma chi potrà farlo quando il proprietario dell'account non esisterà più.

Questo significa ripensare molte cose: governance degli accessi, gestione degli archivi, eredità digitale, responsabilità delle piattaforme, continuità operativa delle identità professionali. Significa anche riconoscere che la sicurezza non finisce con il logout finale.

Finora abbiamo progettato Internet come se tutti restassero sempre presenti. Ma nessuna infrastruttura umana funziona davvero così.

Prima o poi qualcuno smette di rispondere alle e-mail.

La cybersecurity è nata per difendere i sistemi dai cyber criminali. Il prossimo passo sarà difenderli dall'assenza dei loro proprietari.

Cyber War e conflitti geopolitici tra minacce e rischi per le aziende

A cura di Sofia Scozzari

I conflitti contemporanei non si sviluppano più soltanto sul piano militare o diplomatico, ma si estendono anche al dominio digitale. In questi contesti, nel cyberspazio convivono attività malevole molto visibili, come gli attacchi DDoS, la propaganda, la disinformazione, e operazioni più silenziose, come il cyber espionage, i sabotaggi e l'intelligence.

La dimensione cyber non è più un elemento accessorio del conflitto, ma una delle sue estensioni operative, e l'attuale escalation USA-Iran ne è una conferma. Per le aziende dell'area, e non solo, questo scenario impone una riflessione più ampia sul rischio cyber e di business.

Le minacce cyber tipiche nei contesti di conflitto

Nei contesti di tensione geopolitica o guerra aperta, il panorama cyber tende a concentrarsi attorno a poche categorie ricorrenti:

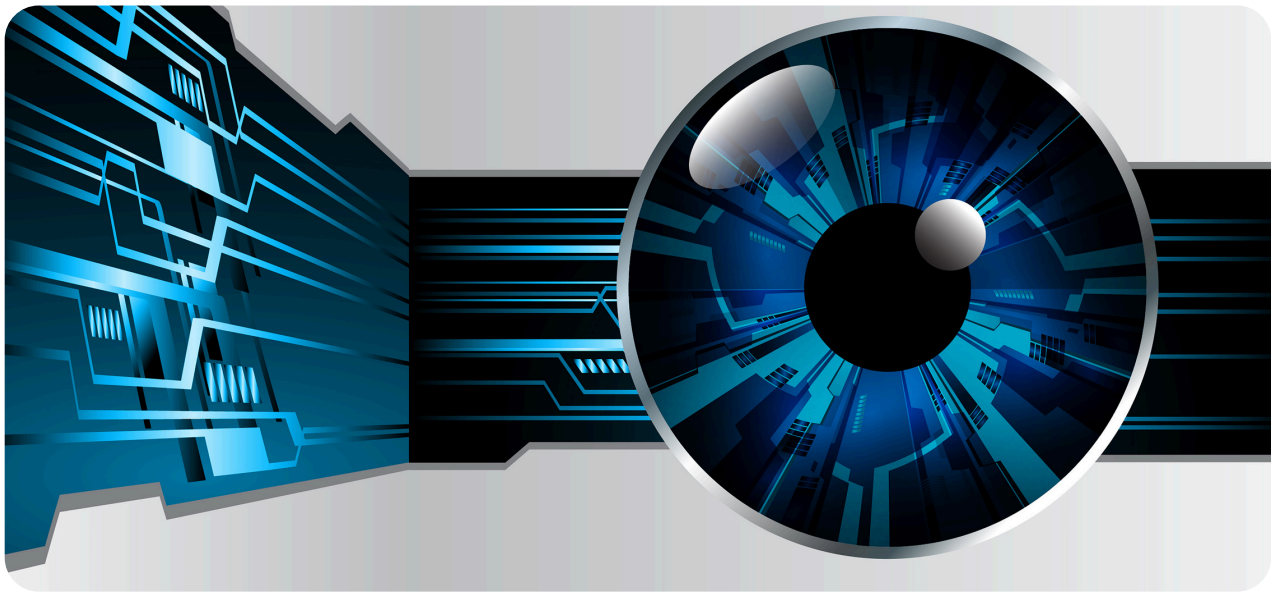
- **Attività pubbliche e dimostrative**, che comprendono attacchi DDoS, defacement, propaganda digitale, fake news e rivendicazioni ideologiche da parte di gruppi hacktivisti. Queste azioni, spesso più simboliche che distruttive, possono comunque generare interruzioni, perdita di fiducia e pressione reputazionale.
- **Operazioni di influenza e manipolazione dell'informazione**, finalizzate a orientare la percezione degli eventi, amplificare il senso di instabilità e colpire indirettamente istituzioni ed economia.
- **Operazioni di cyber spionaggio**, che includono raccolta di informazioni, persistenza occulta e preposizionamento su infrastrutture governative, critiche e grandi aziende, in vista di possibili evoluzioni del conflitto.
- **Operazioni di sabotaggio o disruption**, volte a compromettere direttamente la continuità operativa di servizi, supply chain e infrastrutture, attraverso malware particolarmente distruttivi (ad esempio i wiper), ransomware o interruzioni mirate su nodi critici.

Cosa stiamo osservando nel corso del recente conflitto in Middle East

Nel contesto mediorientale attuale, la dimensione più evidente del conflitto cyber è quella più esposta e pubblica. In particolare, esattamente come già successo per il conflitto Russia-Ucraina, l'hacktivism è il fenomeno più presente.

Gli attacchi DDoS rappresentano una delle manifestazioni più frequenti in questi scenari, poiché consentono di colpire in modo rapido target istituzionali, mediatici o aziendali. Allo stesso tempo, fake news, propaganda e narrazioni manipolate contribuiscono a generare confusione, amplificare il senso di crisi e polarizzare il dibattito pubblico.

A questa dimensione *alla luce del sole* si affiancano



attività più discrete e meno visibili, come operazioni di intelligence, cyber spionaggio e tentativi di compromissione finalizzati a ottenere accesso a sistemi da sfruttare in successive operazioni di sabotaggio.

I rischi per le aziende

Per le aziende, il problema non consiste soltanto nell'aumento degli attacchi, ma nella crescente complessità della valutazione del rischio in un contesto geopolitico sempre più instabile.

Durante i conflitti, infatti, le minacce cyber possono produrre effetti che vanno ben oltre il danno tecnico immediato incidendo su continuità operativa, reputazione, governance e capacità decisionale.

I principali rischi per le aziende possono includere:

- interruzioni di servizi e rallentamenti operativi;
- compromissione di supply chain e fornitori critici;
- esposizione a campagne di disinformazione o pressione reputazionale;
- maggiore efficacia di phishing, truffe e social engineering legati al contesto geopolitico;
- pressione crescente sul management, chiamato a decidere in condizioni di forte incertezza.

Per il settore ICT questo tema è ancora più rilevante, perché molte aziende rappresentano anche nodi tecnologici essenziali per altri settori e la loro esposizione può avere impatti sistemici.

Rischi che si propagano oltre l'area di crisi

Uno degli errori più comuni consiste nel ritenere che le minacce cyber legate a un conflitto regionale riguardino solo gli attori localizzati nell'area. In realtà, per un'azienda europea o americana il rischio può materializzarsi anche in assenza di una presenza diretta nel teatro di crisi.

Le imprese sono oggi collegate da catene di fornitura, relazioni commerciali, infrastrutture cloud, partner logistici, operatori finanziari e reti di telecomunicazione che rendono il rischio fortemente interdipendente.

A rendere il quadro ancora più delicato vi è la forte dipendenza, nel Middle East come in Europa, da tecnologie, piattaforme e infrastrutture sviluppate o gestite da grandi operatori statunitensi. Sistemi operativi, software enterprise, servizi cloud, datacenter, piattaforme AI e strumenti di collaboration costituiscono oggi l'ossatura digitale di sostanzialmente tutte le organizzazioni. Nell'attuale scenario di conflitto tra Stati Uniti e Iran, questa concentrazione introduce una vulnerabilità aggiuntiva: se le infrastrutture tecnologiche americane presenti nell'area GCC dovessero essere colpite o anche solo temporaneamente rese indisponibili, gli effetti potrebbero propagarsi ben oltre l'area locale.

Le conseguenze possono includere:

- ritardi o interruzioni nella filiera;
- indisponibilità di servizi forniti da partner regionali o da grandi provider tecnologici;
- degrado di servizi cloud, applicativi critici e ambienti di lavoro digitali;
- difficoltà di accesso a dati, piattaforme e comunicazioni;
- maggiore esposizione a campagne di phishing o social engineering costruite sul contesto di crisi;
- impatti reputazionali derivanti da narrazioni manipolate, contenuti falsi o attribuzioni fuorvianti;
- effetti a catena su clienti, fornitori, filiali e partner internazionali.

Conclusioni

La cyber war non riguarda soltanto governi e infrastrutture critiche nazionali, ma può avere ripercussioni dirette anche sulle aziende.

Il conflitto digitale, inoltre, non ha confini geografici netti e, anche aziende geograficamente lontane dalla guerra, possono essere colpite o coinvolte, sia come bersagli opportunistici, sia come parte di filiere, infrastrutture o ecosistemi digitali interdipendenti.

Per il tessuto imprenditoriale italiano, europeo e internazionale, la lezione è chiara: il rischio geopolitico non è più un fattore esterno alla sicurezza aziendale, ma una sua componente strutturale.

In questo scenario, la capacità di interpretare il contesto, comprenderne le dipendenze critiche ed essere pronti a gestire effetti indiretti e sistemici, assume un ruolo critico nella strategia cyber e di business.

Nel 2026 torna l'iperammortamento anche per il software industriale. Vantaggi fino al 52%

A cura di Francesco Tieghi

Il disegno di legge di bilancio 2026 segna un netto cambio di strategia nelle politiche governative di supporto all'innovazione per l'industria. Si chiude la stagione dei crediti d'imposta previsti dai piani Transizione 4.0 e 5.0 e tornano superammortamento e iperammortamento che avevamo imparato a conoscere con il primo piano Industria 4.0. Il nuovo piano presentato dal Governo prevede un nuovo strumento unificato a supporto della duplice transizione digitale e green, fondato su coperture nazionali e reso appetibile da aliquote particolarmente generose.

Il ritorno del software

L'incentivo per il 2026, oltre a replicare il "format" della maggiorazione degli ammortamenti, recupera dalle vecchie normative anche le merceologie dei beni incentivati. In particolare, si potranno acquistare i beni materiali e immateriali tecnologicamente avanzati elencati negli allegati A e B. Ricordiamo infatti che nel 2025 i software dell'allegato B erano stati eliminati dal piano Transizione 4.0.

In più accedono all'incentivo anche i beni strumentali destinati all'autoproduzione energetica per autoconsumo da fonti rinnovabili: in pratica pannelli solari, pale eoliche, ma anche sistemi per lo storage dell'energia.

Su questo punto vale la pena anticipare che Governo e Imprese stanno discutendo l'opportunità di ampliare ulteriormente le merceologie attualmente presenti negli allegati A (beni materiali) e B (software). Appena avremo notizie in tal senso non mancheremo di aggiornarvi.

Quali sono i software industriali inclusi nell'allegato B? La lista è lunga e la trovate qui. Per quanto ci riguarda, vale la pena sottolineare che sono inclusi SCADA, MES, sistemi Industrial IoT, sistemi per la gestione della qualità a livello di sistema produttivo e dei relativi processi, sistemi per l'industrial analytics e soluzioni per la cybersecurity.

Iperammortamento OK anche per gli energivori

Un elemento molto importante della nuova misura riguarda la fonte di finanziamento. Mentre l'attuale piano Transizione 5.0 è coperto da fondi PNRR, con tutti i vincoli del caso, la nuova misura è sostenuta interamente da risorse statali e sarà quindi svincolata dai complessi obblighi europei legati al principio "Do No Significant Harm" (DNSH). Questo significa che anche le imprese hard-to-abate o energivore, come ad esempio acciaierie o produttori di ceramica, che finora non potevano accedere agli incentivi PNRR, potranno invece sfruttare i benefici offerti dalla nuova misura unica per Transizione 4.0 - 5.0 2026.

Aliquote super

Le aliquote sono notevolmente vantaggiose. Il testo del DDL di Bilancio (che, è bene ricordarlo, deve

completare l'iter parlamentare e potrebbe subire modifiche prima della promulgazione, attesa entro fine anno) stabilisce maggiorazioni che variano in base alle fasce di investimento e al raggiungimento o meno di un obiettivo di efficientamento energetico.

Vediamo tutto in dettaglio. Per i beni 4.0, le aliquote che si applicano a tutti i beni, indipendentemente dal fatto che siano hardware, software o pannelli solari, sono le seguenti:

- +180% per la quota di investimenti fino a 2,5 milioni di euro;
- +100% per gli investimenti tra 2,5 e 10 milioni di euro;
- +50% per la fascia tra 10 e 20 milioni di euro.

Per ognuna di queste aliquote è prevista poi una maggiorazione ulteriore del 40% nel caso in cui, grazie all'investimento in quei beni, si possa dimostrare un beneficio in termini di risparmio energetico (3% dei consumi dell'unità produttiva o 5% dei consumi del processo interessato dall'investimento). È la formula che conosciamo per il piano Transizione 5.0 ancora in vigore, ma senza gli ulteriori scaglioni attualmente previsti in base al livello di risparmio conseguito.

Le aliquote potenziate, come dicevamo, sono più alte del 40% rispetto a quelle standard. Lo schema delle maggiorazioni diventa quindi il seguente:

- +220% per la quota di investimenti fino a 2,5 milioni di euro;
- +140% per gli investimenti tra 2,5 e 10 milioni di euro;
- +90% per la fascia tra 10 e 20 milioni di euro.

Il Governo ha poi stabilito che alcune tipologie di investimento hanno accesso diretto alle aliquote potenziate del 40% senza dover dimostrare il risparmio energetico. Si tratta dei seguenti casi:

- Investimenti in sostituzione di beni il cui ammortamento è concluso da almeno 24 mesi.
- Investimenti nell'ambito di progetti gestiti tramite ESCo con contratto EPC che garantisca il raggiungimento dei target di efficienza del 3% sulla struttura produttiva o del 5% sul processo interessato.
- Pannelli solari bifacciali con efficienza di cella non inferiore al 24%.

Ora però facciamo un passo indietro e vediamo qual è il vantaggio concreto offerto da queste aliquote rispetto a quelle offerte oggi dai crediti d'imposta di Transizione 4.0 e 5.0.

Come funziona il sistema dell'iperammortamento

Vediamo quindi come funziona il sistema della maggiorazione degli ammortamenti e in che cosa differisce dal credito d'imposta. Partiamo proprio da quest'ultimo, che è il sistema presente nei piani Transizione 4.0 e 5.0 che scadono quest'anno. Il credito d'imposta offre un'aliquota che determina direttamente il vantaggio fiscale. Per esempio il 20% previsto dal vecchio piano Transizione 4.0 significa che se investo 100.000 euro posso recuperarne 20.000 scalando questo credito dai prossimi versamenti in F24.
Il meccanismo del super e iperammortamento funziona con una variazione in diminuzione dell'imponibile fiscale, distribuita su più esercizi in base alla durata dell'ammortamento del bene (solitamente dai 3 ai 10 anni).

Per fare un esempio, acquistando anche in questo caso un bene che costa 100.000 euro, con una maggiorazione degli ammortamenti del 180% si potranno dedurre dall'imponibile (oltre ai 100.000 euro che si deducono sempre come costi) altri 180.000 euro. Il che, considerando che l'IRES è al 24%, corrisponde a un risparmio sulle imposte di 43.200 euro. Volendo semplificare, possiamo quindi dire che una maggiorazione del 180% dell'ammortamento "equivale" a un credito d'imposta del 43,2%.

Il vantaggio economico può arrivare fino al 52,8%

Lo schema delle maggiorazioni, come abbiamo visto, è strutturato per tre fasce di investimento: fino a 2,5 milioni, da 2,5 a 10 milioni e da 10 a 20 milioni.

Per un investimento 4.0 da 15 milioni, a titolo esemplificativo, si applicherà una maggiorazione del 180% sui primi 2,5 milioni, una maggiorazione del 100% sui 7,5 milioni (cioè la parte 2,5-10 milioni) e il 50% sugli ultimi 5 milioni che ricadono nella fascia superiore a 10 milioni.

Per semplificare la comprensione del beneficio che si può ottenere con un investimento, qui di seguito vi riportiamo uno schema che mostra, in base all'ammontare dell'investimento (in prima colonna), il beneficio in euro con le maggiorazioni spettanti per i beni hardware e software 4.0 (in seconda colonna), a quanto equivale quel beneficio in percentuale sull'investimento iniziale (terza colonna).

Il beneficio massimo è quindi pari al 43,2% del costo dell'acquisto per gli investimenti fino a 2,5 milioni. Vale qui la pena ricordare si tratta di un vantaggio di oltre il doppio rispetto all'attuale piano Transizione 4.0 che offre un vantaggio del 20%.

Investimento (€)	Beneficio 4.0 (€)	Beneficio % 4.0
1.000.000	432.000	43,20%
2.500.000	1.080.000	43,20%
5.000.000	1.680.000	33,60%
10.000.000	2.880.000	28,80%
15.000.000	3.480.000	23,20%
20.000.000	4.080.000	20,40%

Qui di seguito lo stesso schema con le aliquote maggiorate spettanti agli investimenti 5.0 (cioè quelli che conseguono anche un beneficio in termini di risparmio energetico).

Investimento (€)	Beneficio 5.0 (€)	Beneficio % 5.0
1.000.000	528.000	52,80%
2.500.000	1.320.000	52,80%
5.000.000	2.160.000	43,20%
10.000.000	3.840.000	38,40%
15.000.000	4.920.000	32,80%
20.000.000	6.000.000	30,00%

Anche in questo caso il vantaggio è superiore a quello offerto da piano Transizione 5.0 attuale, la cui aliquota massima è del 45% (qui siamo al 52,8% di vantaggio massimo conseguibile).

Pro e contro del sistema della maggiorazione degli ammortamenti

Fin qui tutto relativamente semplice. In realtà la transizione dal sistema basato sui crediti d'imposta alla maggiorazione degli ammortamenti non è priva di conseguenze.

Il credito d'imposta è utilizzabile in F24 in tempi rapidi (spesso 3 anni, o anche 1 anno come è stato finora per Transizione 5.0) e, fattore determinante, è fruibile anche da aziende che non hanno utili d'esercizio (o ne hanno pochi) perché si usano, come accennato, per compensare altri versamenti dovuti allo stato.

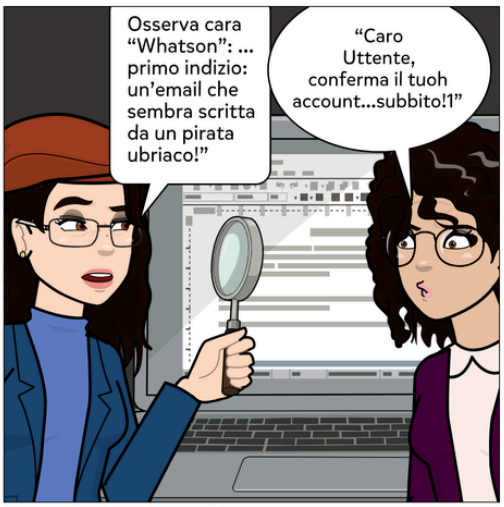
Proprio su questo vale però la pena sottolineare che, sempre nel DDL di Bilancio, il governo sta operando una forte stretta proprio sulle compensazioni, ma questo è un discorso che esula dallo scopo di questo articolo.

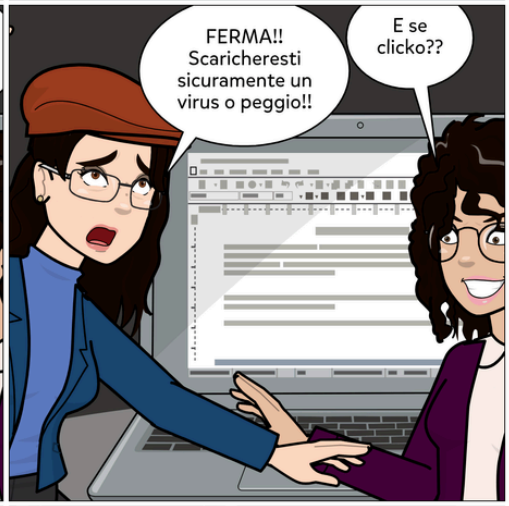
Per quanto riguarda l'iperammortamento i vantaggi risiedono nella relativa semplicità burocratica (per l'accesso all'aliquota base) e nelle "aliquote" decisamente più elevate. Lo svantaggio principale, di contro, è la necessità di avere "capienza" IRES per monetizzarlo: essendo una deduzione, se l'azienda non produce utili imponibili, si trasforma semplicemente in una perdita fiscale da riportare negli esercizi successivi. Il vantaggio fiscale, inoltre, anche in presenza di utili, si distribuisce sull'intero periodo di ammortamento del bene che può essere anche molto lungo, dilatando i tempi di recupero del beneficio.

MARY HOLMES E LO STRANO CASO DEL PESCIOLINO ROSSO!

COME NON CADERE VITTIMA DEL PHISHING

www.assintel.it
info@assintel.it





Non cadere nei tranelli del phishing! Verifica sempre l'autenticità delle email e proteggi i tuoi dati.
Credits: NWN solutions Bologna

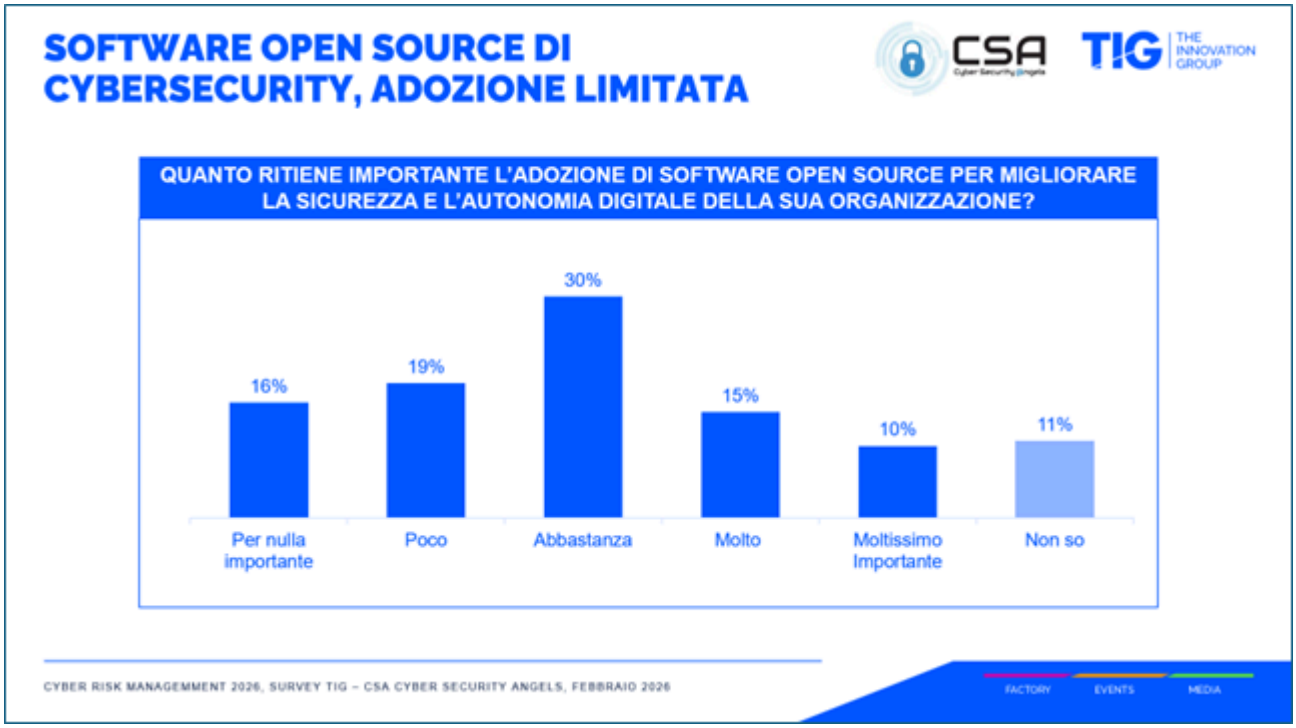
Open source in cybersecurity: alternativa per l'autonomia tecnologica

A cura di Elena Vaciago

La sovranità digitale sta diventando un requisito essenziale, per assicurare sicurezza, indipendenza e competitività in un mondo instabile. Da più parti viene indicata la soluzione dell'open source, una scelta per aumentare autonomia tecnologica che potrebbe trovare applicazione anche in un ambito critico come quello della cybersecurity. Ma qual è l'indirizzo delle aziende? Per rispondere a questa domanda, ci affidiamo a quanto risulta da una recente indagine.

L'analisi restituisce un quadro ancora in divenire con riferimento all'adozione dell'open source in cybersecurity. L'importanza riconosciuta al codice aperto è significativa ma non dominante: una parte rilevante del campione considera l'adozione di open source in cybersecurity "abbastanza importante", mentre solo una minoranza la ritiene centrale. L'open source è presente, ma non si posiziona tra le scelte strategiche.

Quando si approfondiscono i **benefici legati all'adozione**, emerge che l'indipendenza dal vendor e la riduzione del lock-in (67% delle risposte) rappresentano i driver più forti dell'open source, seguiti dalla riduzione dei costi (49%). Solo in seconda battuta compaiono elementi tipicamente associati alla sicurezza, come la trasparenza del codice (38%) o il contributo delle community globali (33%). L'open source è dunque letto soprattutto come leva di autonomia e flessibilità, più che come



garanzia di maggiore protezione.

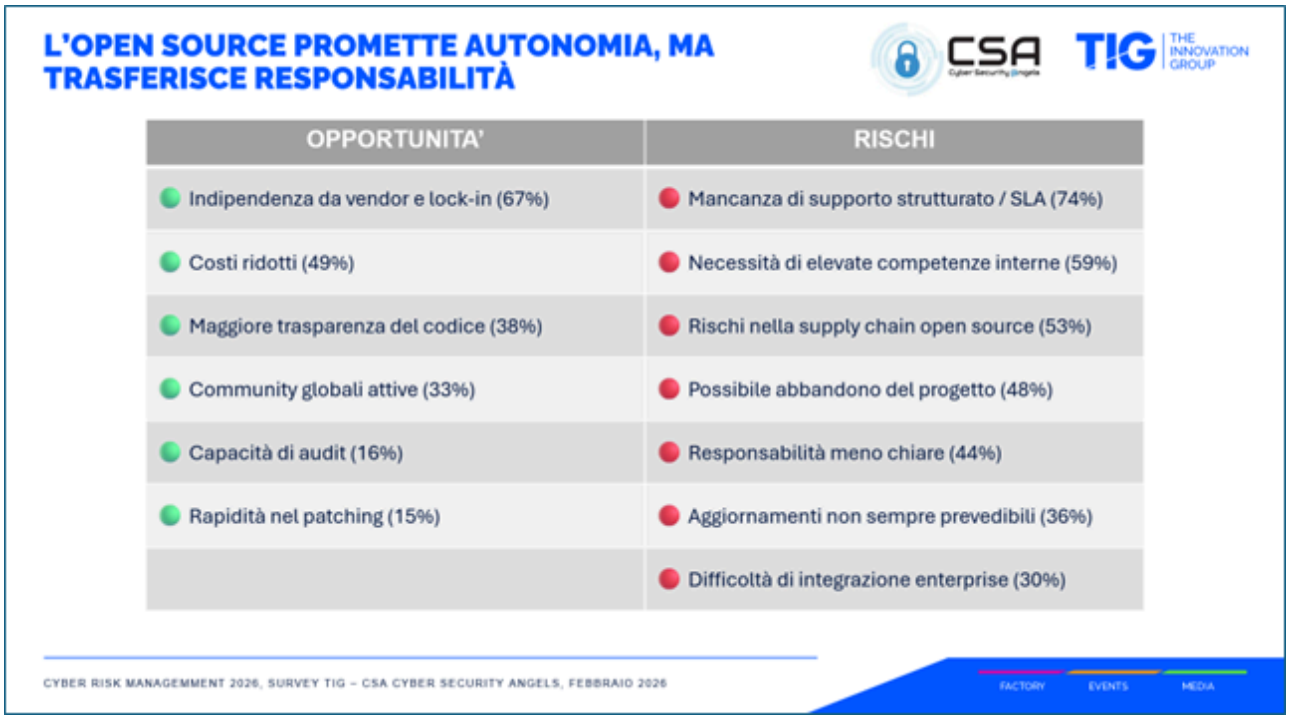
Sul fronte dei **rischi**, però, si osserva un approccio molto prudente. Un gran numero di organizzazioni evidenzia come limite di questa scelta la mancanza di supporto strutturato e SLA garantiti (74% delle risposte), la necessità di competenze interne elevate (59%), i rischi legati alla supply chain del software open source (53%) e la possibilità che non sia garantito il proseguimento della soluzione per abbandono del progetto (48%), oltre che la mancanza di accountability chiara (44%).

In altri termini, l'autonomia promessa comporta un **trasferimento di responsabilità** verso la stessa organizzazione, che a fronte di una minore dipendenza dal vendor, deve assumersi maggiori oneri di governo e controllo.

Questo equilibrio tra opportunità e rischi si riflette nei dati di adozione. Solo il 12% delle organizzazioni dichiara di utilizzare ampiamente soluzioni open

source in ambito cybersecurity, mentre il 24% le impiega in ambiti molto specifici. Complessivamente, quindi, circa un terzo del campione ha già integrato strumenti open source nel proprio stack di sicurezza. Viceversa, il 46% afferma di non utilizzarli e di non prevederne l'adozione, mentre un ulteriore 11% non si sbilancia. Anche le intenzioni di breve-medio periodo appaiono contenute: solo l'8% prevede di adottare soluzioni open source nei prossimi 12–24 mesi.

Il dato relativo all'adozione, attuale e prevista, conferma una tensione già emersa nell'analisi benefici / rischi. Se l'open source è riconosciuto come leva di indipendenza dal vendor e di riduzione dei costi, al tempo stesso le organizzazioni mostrano cautela operativa, probabilmente influenzata da timori legati a supporto, competenze interne, supply chain e accountability. **L'adozione è limitata a una minoranza,** prevale un approccio selettivo e circoscritto: l'open source in cybersecurity rimane uno strumento valutato caso per caso, integrato dove esistono competenze adeguate e governance



solida. Questo ci insegna qualcosa sul senso da dare a concetti ampi come quello della "sovranità digitale", un principio che viene spesso richiamato nel dibattito pubblico, ma che non si traduce automaticamente in scelte tecnologiche radicali: per la maggioranza delle organizzazioni, dovendo bilanciare autonomia e cautele legate alle proprie responsabilità, si continua a favorire le decisioni pragmatiche piuttosto che posizioni ideologiche.

Analizzando gli ambiti concreti di utilizzo dell'open source in cybersecurity emergono la Threat Intelligence (52%) e il Vulnerability Assessment/Scanning (50%), seguiti da SIEM/Log Management (36%): sono risposte elevate ma parliamo solo di aziende che già utilizzano o prevedono l'open source. In misura intermedia compaiono IDS/IPS e Container & Cloud Security (24%), Application Security/DevSecOps e Network Security (21%).

Il dato suggerisce una logica pragmatica: l'open source è preferito nelle aree di analisi, monitoraggio e arricchimento informativo, dove la flessibilità, l'integrazione e l'accesso a community tecniche rappresentano un valore. Al contrario, nelle funzioni più direttamente legate alla protezione attiva, alla gestione dell'identità o alla risposta automatizzata – ambiti dove SLA, supporto strutturato e responsabilità contrattuale sono cruciali – prevale un maggiore orientamento verso soluzioni commerciali. Questo pattern riflette un CISO che utilizza l'open source come **leva tattica di arricchimento tecnologico.**
La sfida futura sarà comprendere se questa adozione rimarrà complementare o se, con l'aumento della maturità organizzativa, potrà estendersi anche ai domini più centrali della cybersecurity. Se la sovranità digitale è un obiettivo crescente, la sua realizzazione concreta passerà meno da scelte ideologiche e più da investimenti in competenze, standardizzazione e processi di controllo. L'open source può rappresentare una leva potente, ma solo per organizzazioni in grado di trasformare l'indipendenza in responsabilità e governance interna.

CISO, Risk Manager, DPO: un team vincente per l'adeguamento alla NIS2

A cura di Enzo Veiluva

I ruoli standard nella gestione dei rischi e della sicurezza delle informazioni stanno acquisendo nuove responsabilità o maggior interazione, in particolare nei confronti del ruolo di punti di contatto NIS2 e referenti CSIRT, secondo quanto richiesto dalla normativa NIS2.

Il nuovo quadro normativo stabilito dal decreto di recepimento della Direttiva NIS2 impone alle organizzazioni di rafforzare e ridefinire le proprie strutture di governance. Di conseguenza, si assiste a una crescente centralità di figure chiave come il Data Protection Officer (DPO), il Chief Information Security Officer (CISO) e, sempre più spesso, il Risk Manager (RM). Se in passato questi ruoli operavano in modo indipendente, la NIS2 li spinge verso una collaborazione più stretta, ridefinendo compiti, responsabilità e strategie condivise.

La NIS2 impone alle organizzazioni di designare figure come il punto di contatto ed il referente CSIRT, oltre a loro sostituti. Spesso questo incarico viene affidato a chi gestisce prevalentemente la sicurezza all'interno dell'azienda, come il responsabile dei sistemi informativi o, quando presente, il CISO, soggetti tecnici che solitamente mantengono rapporti diretti con l'Agenzia per la Cybersicurezza Nazionale (ACN).
Tuttavia, secondo le indicazioni riportate nella FAQ 3.8 "Registrazioni" sul sito ACN alla voce NIS2, il ruolo di punto di contatto non richiede necessariamente competenze tecniche o specifiche in ambito cybersecurity, ma piuttosto capacità gestionali, comunicative e una conoscenza approfondita della realtà aziendale. Mentre il referente CSIRT deve essere un interlocutore con forte competenza tecnica e conoscenza della sicurezza dei sistemi informativi e delle reti aziendali.

Indubbiamente, nell'ambito di questo nuovi ruoli, il CISO — in seguito all'applicazione della normativa — è chiamato a presidiare l'intero ciclo di vita della sicurezza informatica: dalla fase di prevenzione, passando per la risposta agli incidenti, fino alla ripresa e alla resilienza operativa, sia per le infrastrutture che per le applicazioni aziendali.

Il CISO, inoltre, si trova sempre più a svolgere un ruolo fondamentale, insieme al Responsabile del Rischio (RM) ove presente, nella mappatura e nella mitigazione dei rischi non solo legati all'IT, ma anche di natura organizzativa e lungo tutta la filiera produttiva, coinvolgendo attivamente fornitori e partner che necessitano di un monitoraggio ancora più attento. Al CISO viene affidato il compito di coordinare processi che siano rapidi, accurati e trasversali, coinvolgendo diverse funzioni aziendali. Rientra inoltre tra le sue responsabilità la promozione di programmi di formazione continua sulla sicurezza, destinati a tutto il personale.

La figura del DPO, introdotto dal Regolamento Europeo sulla protezione dei dati (GDPR), garantisce il rispetto delle norme sulla privacy, mentre il CISO ha da sempre il compito di tutelare la sicurezza delle informazioni aziendali. Con la NIS2, la linea di demarcazione tra privacy e sicurezza si fa meno netta, e le due funzioni sono chiamate a lavorare fianco a fianco su tematiche comuni come la gestione dei rischi informatici, la compliance integrata e la risposta agli incidenti. Parallelamente, il Risk Manager – figura ancora poco diffusa nelle aziende – analizza e gestisce i rischi che possono compromettere tutti gli obiettivi aziendali, sviluppando strategie volte a minimizzare gli impatti negativi e a garantire la continuità operativa.

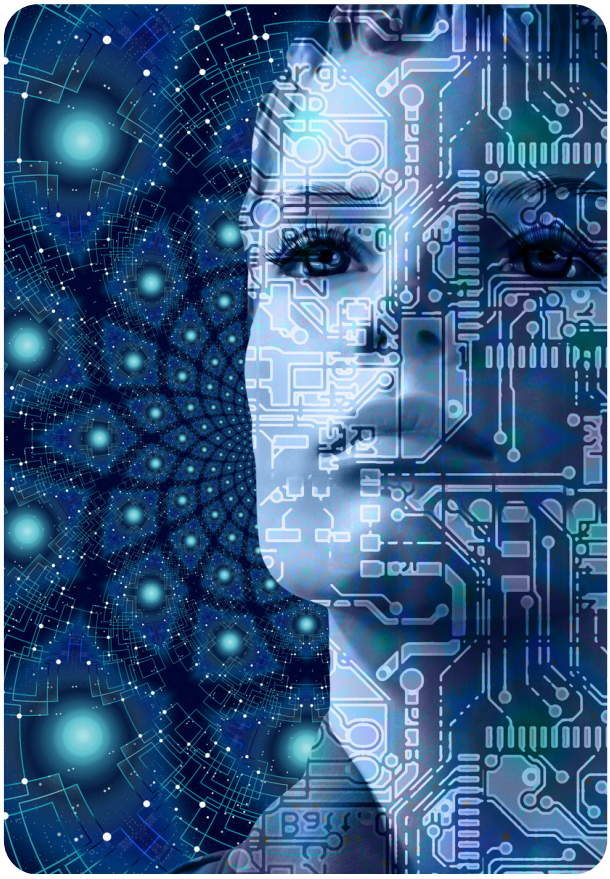
La partecipazione sempre più significativa di queste professionalità emerge chiaramente dall'intento espresso dalla normativa, che mira a innalzare il livello globale di sicurezza delle reti e dei sistemi informativi su scala europea. L'espansione del perimetro di applicazione — sia per quanto riguarda i settori coinvolti sia le tipologie di attività richieste, come la gestione del rischio, la segnalazione degli incidenti e la governance della sicurezza — influisce notevolmente sulle dinamiche di collaborazione tra DPO, CISO e RM.

Dall'altra parte, il Data Protection Officer – figura resa obbligatoria dal GDPR per molte organizzazioni – si trova a vedere il proprio ruolo evolversi con l'introduzione della NIS2. La protezione dei dati personali, infatti, non può più essere considerata isolata rispetto alla sicurezza informatica.
Partendo dai suoi compiti fondamentali, che comprendono informare e consigliare il titolare, il responsabile e i soggetti autorizzati al trattamento, vigilare sull'osservanza del GDPR e delle politiche interne, nonché fungere da punto di contatto per gli interessati, il DPO sarà sempre più coinvolto in una stretta collaborazione con il CISO. L'obiettivo sarà assicurare che i principi di privacy by design e by default vengano integrati efficacemente nei processi di sicurezza informatica, promuovendo così una reale sinergia con i concetti di security by design e by default.

È fondamentale che venga compresa l'importanza, nell'ambito del supporto all'analisi delle valutazioni d'impatto sulla protezione dei dati, del fatto che queste ultime includono anche i nuovi rischi informatici introdotti dalla NIS2. Ciò richiede un potenziamento delle competenze trasversali, ampliando così la propria capacità di affrontare scenari in continua evoluzione.

Sarà necessario collaborare in modo diretto e costante con il CISO, al fine di assicurare una segnalazione corretta e separata alle autorità competenti, rispettando rigorosamente le tempistiche stringenti previste sia dal GDPR (72 ore) sia dalla NIS2 (24 ore). In questo contesto, il ruolo diventa sempre più quello di consulente, focalizzato sulla prevenzione e sul supporto strategico a tutte le funzioni aziendali coinvolte nella gestione dei dati.

Nel panorama delineato dalla NIS2, dove la sicurezza deve essere integrata a ogni livello e sapersi adattare a contesti digitali sempre più complessi e interconnessi, DPO, CISO e RM si trasformano quindi in veri architetti della resilienza. Non sono più solamente figure dedite al controllo, bensì leader del cambiamento: collaborazione, proattività, resilienza e supporto al top management diventano i cardini della loro azione quotidiana. La loro sinergia non rappresenta più solo un valore aggiunto, ma una condizione imprescindibile per assicurare competitività, conformità normativa e la fiducia di chi ogni giorno affida dati e servizi alle tecnologie digitali.



Basta carta, vogliamo sicurezza (quella vera)

A cura di Fabio Zanoli

Udite, udite la lieta novella: l'Europa non ha prodotto norme su dati e cybersecurity per torturare dirigenti e addetti, per impedire lo sviluppo economico, no.
Nascono per spingere le organizzazioni a costruire un vero ecosistema di sicurezza: dei dati, delle strutture, dei sistemi informatici.
Considero GDPR, NIS2, DORA, AI Act – i "Fantastici 4" del panorama regolatorio – come tasselli di un unico disegno: far smettere di considerare la sicurezza come un faldone polveroso in un armadio, un balzello normativo, l'ennesima fonte di spesa, la solita palla al piede, per trasformarla in pratica quotidiana all'interno delle nostre attività e un vantaggio competitivo.
Uno scudo contro le enormi perdite di tempo e risorse, che costano le esfiltrazioni dei dati, causate da imperizia o attacchi esterni poco importa, ma sempre causate dalla mancata attitudine a considerare la protezione dei dati come una parte fondamentale delle attività aziendali. Che, se ben applicate, creano reddito, non spesa.

Per anni molte organizzazioni si sono accontentate, anche spinte dall'atteggiamento, a volte compiacente di alcuni professionisti del settore, di quella che molti di noi definiscono "Paper Compliance": policy copiate da internet, mansionari che nessuno legge, informative privacy in linguaggio da antico codice notarile e, soprattutto, procedure mai davvero applicate, perché scritte come se si stesse scrivendo "Il dizionario delle cose impossibili".

L'importante era poter dire "ce l'abbiamo", in caso di ispezione o di audit, di fronte alla dirigenza, o al proprio capo. Peccato che gli attaccanti non chiedano prima di vedere la documentazione e che i cittadini, i clienti e la stessa PA inizino a giudicare un'organizzazione non da quante carte produce, ma da quanto è affidabile nel custodire dati e servizi. NIS2 e supply chain vi dicono qualcosa?

La "Real Compliance" è un'altra storia. Significa fare ciò che sulla carta si è promesso, farlo in modo ripetibile e dimostrabile, e soprattutto farlo comprendere a chi lavora in prima linea. Renderlo un'attitudine, un tassello del nostro modo di lavorare, applicabile, comprensibile, trasparente. Sia all'interno che all'esterno.

Un regolamento scritto benissimo ma ignorato in reception, in ufficio amministrativo o nel CED vale meno di una procedura semplice, chiara ed effettivamente adottata. Non è un caso se le norme europee insistono su accountability, documentazione delle scelte, formazione continua, gestione dei rischi e degli incidenti: non chiedono solo di scrivere, chiedono di fare. E a ben pensare da "vecchio informatico" ricordo a me stesso che la base per "scrivere ottimo codice è sempre il "Bacio" K.I.S.S, ovvero Keep It Simple, Stupid.
Possiamo, anzi perdonate lo scivolone nel buonismo evidentemente lo spirito Natalizio mi sta pervadendo, non possiamo ma DOBBIAMO applicare questo concetto, da "vecchi smanettoni", anche a livello

manageriale.

Quando pensiamo a procedure, misure di sicurezza e via dicendo facciamola semplice, deve funzionare, deve essere applicabile, capibile, replicabile, dimostrabile. Poi, se avremo tempo, soddisferemo il nostro ego di far vedere “quanto siamo bravi” e la renderemo, magari, elegante.

Passare dalla compliance di facciata alla conformità sostanziale richiede alcune scelte coraggiose. La prima è smettere di nascondere tutto dietro lunghe policy incomprensibili: le persone non applicano ciò che non capiscono. Procedure operative brevi, istruzioni passo-passo, esempi concreti di cosa fare (e cosa non fare) in situazioni tipiche – dall’email sospetta al fascicolo cartaceo dimenticato in sala riunioni – hanno un impatto infinitamente maggiore di dieci pagine di legalese (non me ne vogliano i colleghi avvocati) .

La seconda scelta è accettare che la sicurezza è trasversale. Non riguarda solo il responsabile IT o il DPO, ma coinvolge il management, le risorse umane, il procurement, fino all’ultimo tirocinante. Una gestione reale della conformità fa emergere queste interdipendenze: se il fornitore non è sicuro, lo diventa anche l’organizzazione; se la procedura di onboarding non prevede la formazione minima, ogni nuovo assunto è una potenziale vulnerabilità; se nessuno sa cosa fare in caso di data breach, la norma diventa un boomerang.

La terza scelta è misurare. La Paper Compliance ama i documenti; la Real Compliance ama gli indicatori. Quanti incidenti sono stati registrati, in quanto tempo vengono gestiti, quante persone sono state formate, quali controlli vengono eseguiti sulle infrastrutture fisiche e digitali. È su questi numeri che si misura la maturità di un’organizzazione, non sul numero di firme raccolte sotto l’ennesimo regolamento interno.

Certo, è più facile dichiarare che “siamo a posto col GDPR” perché esiste un manuale di 200 pagine in intranet, che mettere in discussione processi, ruoli e abitudini. Ma continuare a vedere le norme come un fastidio burocratico significa non cogliere il punto: oggi compliance e competitività vanno insieme. Chi dimostra di saper proteggere dati e servizi diventa un partner affidabile nella filiera, accede a bandi e gare, riduce l’impatto economico ed economico-reputazionale degli incidenti. Chi resta alla Paper Compliance rischia di scoprirlo nel modo più sgradevole: dopo una violazione, un’ispezione o una domanda imbarazzante del cliente.

Un buon modo per iniziare è scegliere un ambito concreto – per esempio la gestione degli accessi – e rifare il percorso completo: quali dati raccolgo, chi decide, chi controlla, cosa succede se qualcosa va storto. Se alla fine i documenti cambiano poco ma i comportamenti cambiano molto, siete sulla strada giusta. Se invece avete solo aggiunto un allegato alla policy, indovinate? È ancora Paper Compliance, solo con più carta.

La transizione chiesta dalle norme europee è soprattutto culturale: passare dal “compiliamo il modulo e speriamo” al “sappiamo cosa stiamo facendo e perché”. È un salto che richiede impegno, ma segna la differenza tra subire le regole e usarle come leva per un’organizzazione più robusta e credibile.

Ecco perché non è più tempo di farraginose e oscure politiche di privacy o cybersecurity. È tempo di manuali che si leggono, procedure che si applicano, controlli che si fanno davvero. In fondo, per citare (quasi) un grande poeta, non siamo fatti per memorizzar le norme, ma per farne pratica d’impresa. Il resto è solo burocrazia travestita da sicurezza.

Abbandonate il lato oscuro della forza. Se c’è riuscito Darth Vader, lo potete fare anche voi.

Disclaimer

Gentile lettore,

ti informiamo che il contenuto pubblicato su questo magazine è fornito a scopo puramente informativo e di intrattenimento. Tutte le opinioni, idee e punti di vista espressi negli articoli sono esclusivamente quelli degli autori e non riflettono necessariamente l'opinione di Assintel o dei suoi redattori.

Tutte le informazioni fornite sono basate sulle conoscenze e le fonti disponibili al momento della pubblicazione. Tuttavia, non possiamo garantire l'accuratezza, l'integralità o l'aggiornamento delle informazioni fornite. Pertanto, l'utilizzo delle informazioni presenti su questo magazine avviene a proprio rischio e discrezione.

Si prega di tenere presente che il contenuto potrebbe evolvere nel tempo e potrebbe non essere più aggiornato o rilevante al momento della lettura. Pertanto, consigliamo di verificare sempre l'attualità delle informazioni fornite e di consultare professionisti qualificati per eventuali questioni specifiche o decisioni importanti.

Inoltre, il Cyber Think Tank di Assintel declina ogni responsabilità per eventuali errori, omissioni o danni derivanti dall'uso delle informazioni contenute nel presente magazine. Non siamo responsabili per qualsiasi rivendicazione, perdita o danno di qualsiasi tipo che possa sorgere direttamente o indirettamente dall'utilizzo delle informazioni qui presentate.

Ti invitiamo a fare affidamento su più fonti di informazione per ottenere una visione più completa e a considerare che i punti di vista espressi possono variare in base all'esperienza e alle opinioni personali degli autori.

Infine, vorremmo sottolineare che il magazine non fornisce consulenza legale, finanziaria, medica o professionale di alcun genere. Si consiglia di consultare sempre un professionista qualificato per risolvere eventuali questioni specifiche che riguardano la tua situazione personale.

Cordialmente

La redazione

CYBER
Think Tank
ASSINTEL

Assintel è l'associazione nazionale delle imprese ICT e rappresenta le aziende dell'ecosistema tecnologico e digitale italiano. Aderisce a Confcommercio – Imprese per l'Italia, entro cui è punto di riferimento per la valorizzazione del Digitale, sia a livello di mercato sia di politiche istituzionali. L'associazione è un vero business network per l'ecosistema ICT, capace di creare relazioni, sinergie e opportunità concrete per le aziende socie su tutto il territorio nazionale, negli ambiti tecnologici più innovativi e nei diversi settori economici, dagli operatori globali alle PMI e alle startup.

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

CYBER
Think Tank
ASSINTEL