NOVEMBRE 2026

Cyber Magazine



IN QUESTO NUMERO INTERVISTA A

Marco Barbieri

Segretario Generale
Confcommercio

Confcom

Assintel

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

8 **INTERVISTA**
A colloquio con Marco Barbieri
Segretario Generale Confcommercio

11 **GUIDA PER LE PMI - IMPLEMENTAZIONE DELLA ISO/IEC 27001:2022 SULLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI**
Scarica la Guida in italiano

13 **NIS2 & DORA – IL FORNITORE CRITICO E LE EVIDENZE DIMOSTRABILI**
A cura di Mark Alan Barlow

15 **IL RICATTO DIGITALE ESCE DAL DARK WEB**
A cura di Mohammed Bellala

18 **CYBERSECURITY IN BORSA: DAL BOOM POST-PANDEMICO FINO ALL'INGRESSO DI ANTHROPIC E OPENAI NEL 2026**
A cura di Matteo Biagini

21 **IL FORNITORE DEL FORNITORE: IL RISCHIO CHE LA NORMA NON VEDE**
A cura di Jim Biniyaz

CYBER Think Tank ASSINTEL

Indice

23 **PMI ITALIANE, GENAI E AGENTIC AI: INNOVARE SENZA PERDERE IL CONTROLLO**
A cura di Andrea Ceiner

25 **LE PMI E I RISCHI CYBER: LA SICUREZZA DELLA FILIERA PARTE DA CHI SA COSA PROTEGGERE**
A cura di Marco Cortinovis

27 **AI – DOMANDE E RISPOSTE FACILI FACILI IO AGO IN UN PAGLIAIO MA CON IL NUMERO DI MATRICOLA**
A cura di Gianpiero Cozzolino

29 **LE SFIDE DELLA TRANSIZIONE POST-QUANTISTICA TRA CYBERSECURITY E CAPACITÀ INDUSTRIALE**
A cura di Stefano da Empoli e Alessandro D'Amato

31 **VULNERABILITÀ NOTE E RESPONSABILITÀ DEGLI AMMINISTRATORI: QUANDO IL MANCATO AGGIORNAMENTO DIVENTA COLPA**
A cura di Armando De Lucia

34 **QUANDO L'AI DIVENTA UNA NUOVA SUPERFICIE DI RISCHIO**
A cura di Francesco Iarlori

CYBER Think Tank ASSINTEL

Indice

39 **CHI È COMPETENTE PER USARE L'AI? FORMAZIONE, STANDARD ISO E ASSICURABILITÀ DEL RISCHIO NEL NUOVO QUADRO ITALIANO**

A cura di Daniela Mainenti

42 **AI ACT IN ITALIA: LA SFIDA NON È SOLO REGOLARE L'INNOVAZIONE, MA FARLA ACCADERE**

A cura di Fabrizio Milano D'Aragona

45 **IL DIGITALE NON È ETEREO**

A cura di Mauro Munzi

53 **GUERRA IBRIDA: QUANDO LE RETI DIGITALI DIVENTANO IL NUOVO CAMPO DI BATTAGLIA**

A cura di William Nonnis

55 **OCCTET RILASCIA UN KIT DI STRUMENTI GRATUITO A SUPPORTO DELLE PMI NELL'ADEGUAMENTO AL CYBER RESILIENCE ACT**

A cura di James Philpot

58 **I DANNI DELLA "MANCATA" CYBERSICUREZZA**

A cura di Ranieri Razzante

CYBER Think Tank ASSINTEL

Indice

61 **DALLA COMPLIANCE ALLA RESILIENZA: PERCHÉ LA CONVERGENZA NORMATIVA RICHIEDE UN SISTEMA DI GESTIONE INTEGRATO**
A cura di Marco Scognamiglio

64 **LA MINACCIA SILENZIOSA: COMPRENDERE IL CYBER ESPIONAGE IN ITALIA**
A cura di Sofia Scozzari

67 **OLTRE I QUESTIONARI: LA RESILIENZA SISTEMICA COMINCIA DALLA MAPPA DEL SOFTWARE**
A cura di Michele Slocovich

69 **QUANDO UN ESTRANEO RUBA I TUOI COOKIE: IL PUNTO IN CUI PRIVACY E CYBERSECURITY SI INCONTRANO**
A cura di Laura Valentini

72 **NIS2: LA SICUREZZA SI COSTRUISCE NEL BUDGET 2027**
A cura di Enzo Veiluva



L’editoriale di Antonio Assandri

Coordinatore del Cyber Think Tank

NOVEMBRE 2026

“Gli imprenditori chiedono innanzitutto di essere accompagnati in una trasformazione che sta cambiando profondamente il modo di fare impresa”.

Prendo spunto da questa frase, con cui si apre l’intervista a Marco Barbieri, Segretario Generale di Confcommercio, perché mi sembra racchiudere una parte essenziale della missione di Confcommercio e Assintel.

Intelligenza artificiale e cybersicurezza, osserva poi Barbieri, sono due facce della stessa sfida. Ciò che le imprese chiedono, soprattutto le più piccole, è prima di tutto un supporto concreto: formazione, competenze accessibili, regole comprensibili. Affiancarle significa aiutarle a portare AI e cyber security dentro la gestione quotidiana, con investimenti commisurati alle loro dimensioni e senza che diventino solo l’ennesimo adempimento.

Gli articoli che seguono affrontano il tema da più parti. L’intelligenza artificiale è, ancora una volta, protagonista. Guardiamo a come cambia il rischio quando i sistemi non si limitano a eseguire istruzioni ma interpretano e agiscono, a come le nostre PMI possono adottare l’AI senza perderne il controllo e all’attuazione italiana dell’AI Act, che fa della formazione un elemento fondamentale della valutazione dei rischi.

Ci occupiamo, poi, di filiera: il fornitore del fornitore, la conoscenza effettiva del software che si acquista e le PMI che, nelle supply chain, sono spesso l’anello più esposto. A questo si collega il tema della responsabilità: lasciare aperta una vulnerabilità nota è oggi una questione di governance, non solo tecnica. Inoltre, il sovrapporsi di NIS2, DORA, AI Act e Cyber Resilience Act spinge verso sistemi di gestione integrati, più che verso adempimenti separati. Non mancano contributi su cyberspionaggio, guerra ibrida e ransomware, insieme ad alcuni sguardi più ampi: dalla crittografia post-quantistica al costo, tutt’altro che immateriale, del digitale.

Questo è l’ultimo numero del 2026, un anno che ci ha confermato due cose: la cyber security riguarda tutti, e tutti dobbiamo tenerci costantemente aggiornati. Durante le Olimpiadi di Milano Cortina sono stati bloccati attacchi contro sedi diplomatiche, siti olimpici ed alberghi. Con il caso PHP2Shell l’intelligenza artificiale ha permesso di scoprire falle critiche, presenti da oltre dieci anni, nel linguaggio su cui gira gran parte dei siti web. Infine, i recenti attacchi ai sistemi che gestiscono la catena del freddo nella grande distribuzione europea hanno portato la minaccia cyber direttamente nel mondo fisico. Sono episodi molto diversi tra loro, ma rispondono bene a chi, come ricorda Barbieri, pensa ancora che, siccome non gli è mai successo niente, il problema non lo riguardi.

Per questo, anche nel 2027, continueremo a tenere aggiornate le imprese e ad affiancarle con strumenti concreti. Uno lo trovate già in questo numero: il link per scaricare la Guida per le PMI all’implementazione della ISO/IEC 27001:2022, tradotta in italiano dal Cyber Think Tank. È un punto di partenza pratico per chi vuole organizzare la sicurezza delle informazioni in modo proporzionato alle proprie dimensioni.

CYBER Think Tank ASSINTEL

Buona lettura e buone feste.

INTERVISTA

A colloquio con Marco Barbieri
Segretario Generale Confcommercio



Nato a Vizzolo Predabissi il 2 Settembre 1975.

Laureato in Giurisprudenza presso l'Università Cattolica del Sacro Cuore di Milano con Master di specializzazione in diritto del lavoro.

Dal 2016 è Segretario Generale di Confcommercio Milano Lodi Monza e Brianza.

Dal 2025 Segretario Generale di Confcommercio Imprese per l'Italia.

Cybersicurezza e AI sono temi centrali per Confcommercio. In particolare, le imprese associate cosa richiedono?

Gli imprenditori chiedono innanzitutto di essere accompagnati in una trasformazione che sta cambiando profondamente il modo di fare impresa. Intelligenza artificiale e cybersicurezza rappresentano due facce della stessa sfida. Da una parte le opportunità offerte dall'innovazione, dall'altra la necessità di proteggersi dai rischi che ne derivano.

La priorità è rendere queste tecnologie accessibili anche alle realtà più piccole, che costituiscono l'ossatura del nostro sistema economico. Non possiamo permetterci una trasformazione digitale a due velocità, nella quale soltanto le grandi imprese dispongano delle risorse e delle competenze necessarie per coglierne i benefici.

Un'indagine condotta nel 2025 da Confcommercio Milano, Lodi, Monza e Brianza evidenzia che il 91% delle imprese chiede una maggiore regolamentazione dell'intelligenza artificiale, il 90% ritiene indispensabile la supervisione umana e l'87% individua nella mancanza di competenze un ostacolo alla sua introduzione.

La richiesta che emerge con maggiore forza è quindi quella di un supporto concreto: formazione, consulenza, accesso alle competenze, soluzioni tecnologiche sostenibili e un quadro normativo comprensibile. Il nostro compito, anche attraverso il contributo specialistico di Assintel, è trasformare una sfida complessa in un'opportunità di crescita per tutto il terziario.

Sapere che esiste un rischio è una cosa, attrezzarsi concretamente per affrontarlo e mitigarlo è un'altra. Ed è noto che le micro e PMI investono ancora poco nella digitalizzazione. Qual è l'ostacolo principale per le imprese: mancanza di risorse, di competenze, o semplicemente di tempo?

Credo che il principale ostacolo sia proprio la combinazione di questi tre fattori.

Per una microimpresa, investire nella sicurezza informatica significa spesso sottrarre risorse economiche, organizzative e umane alla gestione quotidiana dell'attività. E quando si è impegnati ogni giorno a far funzionare un negozio, un ristorante, un albergo o un'impresa di servizi, diventa difficile dedicare tempo a rischi che possono apparire lontani.

Esiste poi un problema di consapevolezza. La cybersicurezza viene percepita ancora come un costo aggiuntivo, anziché un investimento nella continuità e nella reputazione della propria attività. Eppure, oggi anche una piccola impresa gestisce pagamenti elettronici, informazioni sui clienti, piattaforme digitali e rapporti con fornitori attraverso sistemi informatici.

Il punto, quindi, non è soltanto aumentare gli investimenti, ma renderli possibili e proporzionati. Servono incentivi, strumenti semplici, formazione mirata e soprattutto competenze accessibili, anche attraverso servizi condivisi e soluzioni sviluppate specificamente per le PMI.

È qui che il sistema associativo può fare la differenza, mettendo in relazione le imprese che hanno bisogno di innovare con quelle che producono tecnologie e servizi digitali.

Dobbiamo aiutare gli imprenditori a comprendere che il digitale, così come la sicurezza digitale, non sono un'attività straordinaria, ma una componente ordinaria della gestione d'impresa.

NIS 2, AI Act, perimetro di sicurezza nazionale: le imprese associate si trovano davanti a un quadro normativo sempre più complesso. Confcommercio e Assintel siedono a diversi tavoli istituzionali su questi temi. Cosa chiedete concretamente al legislatore?

Rafforzare la sicurezza, la resilienza e l'affidabilità del sistema economico è una necessità. Ma dobbiamo evitare che gli strumenti individuati per raggiungere questi obiettivi producano effetti sproporzionati sulle imprese di minori dimensioni.

Attraverso Assintel intratteniamo un confronto costante e costruttivo con l'Agenzia per la Cybersicurezza Nazionale e con il Ministero delle Imprese e del Made in Italy, partecipando ai tavoli istituzionali, in particolare su NIS 2. Un dialogo nel quale portiamo non soltanto competenze e osservazioni tecniche, ma soprattutto la prospettiva concreta delle PMI, sia dal lato dell'offerta tecnologica, rappresentata dalle imprese Assintel, sia da quello della domanda, costituita dalla vasta platea delle imprese associate a Confcommercio.

Servono proporzionalità, chiarezza e gradualità. Gli obblighi devono tenere conto delle differenti capacità organizzative ed economiche delle imprese. Adeguarsi alle normative significa investire in tecnologie, procedure, formazione e nuove competenze. Uno sforzo che, in termini relativi, pesa molto di più su una piccola impresa rispetto a una grande organizzazione.

Un secondo elemento riguarda la coerenza degli standard tecnici. Abbiamo evidenziato come il riferimento a standard non aggiornati possa generare duplicazioni operative e costi aggiuntivi, costringendo le imprese a successivi adeguamenti.

La conformità normativa non deve diventare un ostacolo alla competitività. Le regole devono aumentare la sicurezza dell'intero sistema produttivo, senza lasciare indietro proprio le imprese che hanno maggiore bisogno di essere accompagnate.

Sportelli, formazione, tavoli istituzionali, c'è un ecosistema che si sta costruendo. Ma alla fine come si misura se sta funzionando? Quali sarebbero per lei i segnali concreti che le imprese associate stanno davvero cambiando approccio?

Il vero indicatore di successo non è il numero di convegni organizzati o di iniziative realizzate, ma la capacità di tradurre la sensibilizzazione in comportamenti concreti.

Misureremo l'efficacia del nostro lavoro quando vedremo crescere il numero di imprese che



investono stabilmente nella protezione dei propri sistemi, formano i collaboratori, adottano procedure di prevenzione e aggiornano periodicamente i propri strumenti digitali. Il cambiamento più importante sarà il passaggio da un approccio reattivo a uno preventivo, nel quale la gestione del rischio diventi parte integrante delle decisioni quotidiane dell'impresa.

Ma c'è un altro aspetto che considero fondamentale e che riguarda direttamente il futuro della nostra rappresentanza. Le imprese cambiano, i mercati evolvono e nascono continuamente nuovi modelli di business. L'intelligenza artificiale, l'automazione e la digitalizzazione stanno trasformando profondamente anche il settore dei servizi, che rappresenta una componente sempre più strategica dell'economia e un ambito nel quale Confcommercio sta rafforzando ulteriormente la propria presenza.

Non possiamo limitarci a rappresentare meglio ciò che già esiste. Dobbiamo essere capaci di intercettare ciò che sta nascendo, allargando il perimetro della nostra rappresentanza alle imprese che sviluppano tecnologie, offrono servizi avanzati e generano nuove competenze.

Quando cambia il vento, non dobbiamo cambiare destinazione, ma modificare l'assetto per raggiungerla.

La destinazione non cambia: rappresentare e tutelare gli interessi delle imprese. Ma per continuare a farlo efficacemente dobbiamo evolvere, innovare i servizi, integrare competenze e ampliare la nostra capacità di rappresentanza verso nuovi mercati e nuove attività. Perché i nuovi modelli di business non vanno contrastati o subiti: vanno compresi, accompagnati e rappresentati.

Quando saremo capaci di trasformare questa evoluzione in maggiore competitività per le imprese e in una rappresentanza più ampia, moderna e autorevole, potremo dire che il nostro ecosistema sta davvero funzionando in modo efficiente ed efficace.

C'è ancora chi pensa: “Tanto a me non è mai capitato niente e, in fondo, non è un problema mio”. Quale messaggio vorrebbe rivolgere a questi imprenditori?

Il fatto di non aver mai subito un attacco informatico non significa essere al sicuro. La cybersicurezza riguarda tutti, indipendentemente dalla dimensione dell'impresa o dal settore nel quale opera. Non occorre essere una multinazionale per subire un tentativo di frode, perdere dati importanti o ritrovarsi con i sistemi bloccati. Basta pensare a quanto dipendiamo quotidianamente dagli strumenti digitali: dai pagamenti alle prenotazioni, dalla gestione del magazzino ai rapporti con clienti e fornitori. La sicurezza non deve, però, essere percepita come un costo ulteriore o un nuovo adempimento, ma come un elemento di qualità dell'impresa, di affidabilità verso i clienti e di tutela del lavoro. Non serve diventare esperti informatici. Serve comprendere il rischio e iniziare dalle misure essenziali, con investimenti proporzionati alla propria attività. È esattamente per questo che esiste il sistema associativo, per accompagnare le imprese, soprattutto quelle più piccole, in sfide che difficilmente potrebbero affrontare da sole.

La trasformazione digitale e l’intelligenza artificiale sono già parte del nostro presente. E la sicurezza è la condizione necessaria per viverle come un'opportunità, non come rischi.





GUIDA PER LE PMI:

IMPLEMENTAZIONE DELLA ISO/IEC 27001:2022 SULLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

GIUGNO 2026

GUIDA PER LE PMI

IMPLEMENTAZIONE DELLA ISO/IEC 27001:2022 SULLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Nell'ambito delle azioni finanziate dall'UE, promosse dalla Small Business Standards (SBS) - associazione europea che rappresenta gli interessi delle piccole e medie imprese (PMI) nel processo di normazione, la European DIGITAL SME Alliance ha sviluppato e aggiornato una Guida per le PMI per l'implementazione della ISO/IEC 27001 sulla gestione della sicurezza delle informazioni.

L'obiettivo principale della Guida è supportare le PMI nella comprensione e nell'applicazione della ISO/IEC 27001 per la gestione dei sistemi di sicurezza delle informazioni. Con la pubblicazione della revisione del 2022 della norma, si è reso necessario un aggiornamento per recepire i nuovi requisiti e adattare i contenuti al panorama europeo della cybersecurity. La nuova edizione della Guida continua a fornire alle PMI uno strumento pratico e accessibile per rafforzare la gestione della sicurezza delle informazioni in linea con gli standard internazionali.

Questa pubblicazione è il risultato del lavoro del gruppo di lavoro DIGITAL SME "WG27K", che ha riunito esperti con esperienza nelle problematiche di standardizzazione relative ai sistemi di gestione della sicurezza delle informazioni.

La Guida, elaborata nella sua versione originale in inglese dalla European DIGITAL SME Alliance e Small Business Standards, è stata tradotta in italiano dal Cyber Think Tank di Assintel, con il contributo di Mark Alan Barlow, Jim Biniyaz, Vittorio Orefice, Marco Scognamiglio e Sofia Scozzari, con la supervisione di Antonio Assandri e di Davide Giribaldi.

Scarica la Guida in italiano!

NIS2 & DORA – Il fornitore critico e le evidenze dimostrabili



A cura di Mark Alan Barlow

Due anni fa, in un precedente numero di Cyber Magazine, avevamo proposto di leggere NIS2 e DORA come una mappa per misurare la propria **Postura di Sicurezza**: studiare i requisiti, confrontarli con le mitigazioni in essere e pianificare la chiusura dei gap. Nel webinar del Cyber Think Tank Assintel del 30 gennaio 2026 abbiamo poi raccontato come quella mappa possa diventare una roadmap. Oggi la domanda è un'altra: come si dimostra?

DORA si applica dal 17 gennaio 2025 alle entità finanziarie e, attraverso i contratti, ai loro fornitori ICT.

In Italia la NIS2, recepita con il D.lgs. 138/2024, ha reso obbligatoria dal 1° gennaio 2026 la notifica degli incidenti significativi al CSIRT Italia e ha fissato a ottobre 2026 il termine per le misure di sicurezza di base.

Da qui in avanti l'ACN passa dall'accompagnamento alla verifica: più controlli, più ispezioni, meno tolleranza.

Per molte imprese ICT la sfida arriva anche per via indiretta.

Chi fornisce servizi a banche, intermediari finanziari o altri soggetti regolati è spesso un **fornitore critico**, con a sua volta una catena di sub-fornitori: non basta essere sicuri, bisogna saperlo provare, ai clienti come alle autorità.

Nella mia esperienza professionale, la risposta è trasformare la roadmap in un programma continuo di resilienza, con una reportistica periodica condivisa con la Direzione e con i clienti. Di seguito le aree dell'articolo 21 della Direttiva NIS2 e le evidenze che fanno la differenza.

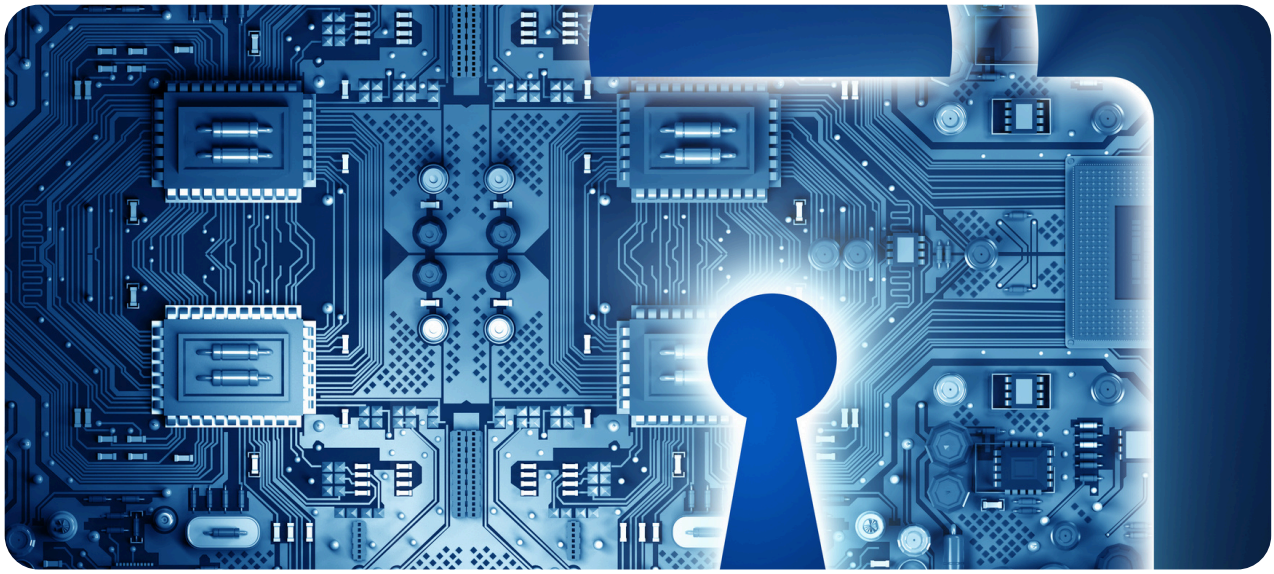
(a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi

Il rischio si governa dall'alto, con strumenti che la Direzione vede ogni mese.

- Un **Comitato Rischi** che valuti mensilmente stato e andamento dei rischi prioritari e ne segua la riduzione nel tempo.
- Un cruscotto di **una cinquantina di indicatori** di sicurezza e resilienza: alert del SOC, disponibilità dei sistemi, esito dei backup, incidenti, fornitori qualificati.
- Un'**autovalutazione della postura** su ogni area NIS2 e su ogni pilastro DORA, validata da una revisione esterna indipendente e inserita in un ISMS certificato **ISO/IEC 27001**.

(b) gestione degli incidenti

Le tempistiche sono stringenti: preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro un mese.



- Una **piattaforma dedicata**, che raccolga anche lo storico: chiunque deve poter segnalare un incidente, da qualsiasi luogo, con un controllo centralizzato.
- Un **SOC** che filtri il rumore: su centinaia di alert al mese, solo una piccola percentuale dovrebbe richiedere l'intervento del team interno.
- Un **test periodico** del processo, che misuri i tempi reali rispetto alle scadenze.

(c) continuità operativa, backup, disaster recovery e gestione delle crisi

Un piano di continuità vale quanto il suo ultimo test.

- **Politica di backup**, **BCP**, Contingency Plan e **DRP** integrati, con un indicatore mensile sugli esiti dei backup.
- **Decine di test di Disaster Recovery** ogni anno, applicazione per applicazione, aperti alla partecipazione dei clienti.
- Una strategia di data center che collochi produzione e disaster recovery presso provider specializzati.

(d) sicurezza della catena di approvvigionamento

Per un fornitore critico la catena di fornitura va presidiata in entrambe le direzioni: verso i clienti, che lo valutano, e verso i sub-fornitori, che valuta lui.

- Piena collaborazione agli **audit dei clienti**, con evidenze già raccolte e centralizzate.
- Un **questionario di Security Posture** strutturato per aree, dalla governance alla continuità, dalle terze parti alla privacy, da applicare prima a sé stessi e poi ai fornitori, con lo stesso metro.
- L'analisi completa concentrata sui **fornitori critici**, individuati per sensibilità dei dati, supporto a funzioni critiche o importanti e sostituibilità, con un assessment di dettaglio per chi resta sotto soglia.
- Gli adempimenti sul **portale ACN**, dalla registrazione dei fornitori alla categorizzazione di attività e servizi, gestiti come un processo vivo e non come una scadenza.

(e) sicurezza dei sistemi e gestione delle vulnerabilità
(h) crittografia

Le vulnerabilità vanno cercate attivamente, con un calendario preciso.

- Un **piano annuale di sicurezza offensiva**: penetration test, re-test, network scan e cicli di cyber threat intelligence.
- Un trend misurabile: con remediation e re-test sistematici, in due anni le vulnerabilità aperte possono ridursi di **oltre il 90%**.
- **Crittografia** dei dati in transito e a riposo, e **WAF** a protezione delle applicazioni esposte.

(f) valutazione dell'efficacia delle misure di gestione del rischio

- Una misura non verificata è solo un'intenzione.
- Una metodologia come la **FMEA** per i rischi di processo e di progetto e per le analisi di scenario.
- Lo stesso ciclo per ogni test: **pianificazione, esecuzione, analisi dei risultati, risoluzione delle criticità, nuova esecuzione.**

(g) igiene informatica e formazione

Ogni iniziativa di formazione ha un indicatore, e ogni indicatore va seguito nel tempo.

- Una piattaforma di e-learning con **centinaia di contenuti**, percorsi per ruolo e tassi di completamento monitorati mese per mese.
- **Campagne di phishing simulato** regolari e sempre più realistiche: se i clic aumentano non è un fallimento, ma un segnale prezioso per azioni mirate per ruolo.
- Un processo di **intelligence sharing** che raccolga ogni giorno notizie, alert ed eventi esterni e li condivida, perché un evento esterno non diventi un incidente interno.
- Formazione specifica per il **top management** e partecipazione attiva alle associazioni di settore.

(i) gestione degli accessi e degli asset
(j) autenticazione multifattore

Ogni accesso deve essere autorizzato, verificato e tracciato.

- **MFA** su accessi remoti, utenze amministrative e applicazioni critiche, e una soluzione **PAM** per gli accessi privilegiati.
- L'estensione della MFA anche ai servizi offerti ai clienti, con un piano a fasi e una copertura misurabile.

Per il 2026 la parola d'ordine è: consolidare, migliorare, collaudare.

Il consiglio che mi sento di dare alle imprese ICT che servono soggetti regolati è semplice: preparare oggi le evidenze che domani verranno chieste, in un audit di un cliente o in un'ispezione mirata.

Ogni test, ogni campagna, ogni questionario lascia una traccia documentata, ed è proprio quella traccia a trasformare una roadmap in resilienza.

Il ricatto digitale esce dal dark web

A cura di Mohammed Bellala



Come i gruppi ransomware usano il clearnet per esporre le vittime e aumentare la pressione fino al pagamento

Per molto tempo, quando si parlava di siti di estorsione ransomware, l'immagine era quasi sempre la stessa: un portale nascosto nella rete Tor, accessibile soltanto con un browser dedicato. Lì i gruppi criminali pubblicavano i nomi delle aziende colpite e una parte dei dati sottratti, quando queste non pagavano il riscatto. Per il resto del mondo quel materiale rimaneva relativamente lontano: bisognava sapere dove cercare e come arrivarci.

Questa distanza si sta riducendo. Alcune operazioni affiancano al sito tor-onion una pagina raggiungibile con un normale browser, ospitata sul cosiddetto clearnet, la parte pubblica di Internet. L'obiettivo non è soltanto rendere disponibili i file: è fare in modo che la minaccia sia visibile a clienti, fornitori, dipendenti, giornalisti e potenziali partner della vittima. L'estorsione digitale smette così di essere una trattativa riservata e diventa una campagna di pressione pubblica.

Non è una novità assoluta. Già nel 2023 il gruppo Cl0p aveva creato siti pubblici dedicati alle aziende coinvolte nella campagna MOVEit, per rendere più semplice la consultazione e la diffusione dei dati rubati.

La ragione è pratica: un sito sul clearnet non richiede strumenti particolari, può essere condiviso con un link e, in alcuni casi, i contenuti possono finire nei motori di ricerca. Per chi estorce, significa allargare il pubblico che può vedere la minaccia.[1]

Il punto, quindi, non è che il cybercrime abbia abbandonato il dark web. È più corretto dire che sta ampliando il palcoscenico. Il caso Titan è indicativo: nel 2026 il dominio pubblico titanblog.org è comparso nelle raccolte di threat intelligence accanto a un servizio onion associato al gruppo. Il 20 agosto una ricerca indipendente ha registrato sul blog rivendicazioni relative a nove imprese italiane in una sola giornata. Alla data di quel resoconto nessuna delle nove aveva confermato pubblicamente un incidente: si tratta di affermazioni dei criminali, non di prove definitive di compromissione.[2]

Il clearnet come strumento di pressione

I siti di pubblicazione delle vittime, spesso chiamati Data Leak Site (DLS), fanno parte da anni del modello della doppia estorsione: prima vengono sottratti i dati e, sempre più spesso, cifrati tutti i sistemi; poi l'organizzazione viene minacciata di divulgazione se non paga. La pagina pubblica è il megafono di questo meccanismo. La sua utilità non dipende solo dalla quantità di informazioni esposte, ma anche da quanto è facile raggiungerla e da chi può imbattersi



nella notizia.

Nel giugno 2026 ZeroFox ha documentato un sito clearnet associato all'operazione DeadLock, che riportava circa ottanta vittime dichiarate. Il rapporto precisava che le pagine contenevano nomi e rivendicazioni, ma non prove sufficienti a dimostrare tutte le intrusioni. È una distinzione essenziale: la pubblicazione può essere parte dell'estorsione anche prima che il gruppo renda disponibili i file, ma non certifica da sola che ogni affermazione sia vera.[3]

Anche le infrastrutture possono essere miste. Il rapporto pubblicato il 28 ottobre 2026 da SOCRadar su n0n descrive portali sia Tor sia clearnet e un'attività di pressione che non si ferma alla pagina pubblica: il gruppo avrebbe contattato clienti, MSP, sindacati e media delle organizzazioni prese di mira. Qui la lista delle vittime è solo un elemento di una strategia più ampia, in cui il rischio di divulgazione viene portato direttamente a chi può amplificarne le conseguenze.[4]

Quattro leve che rendono più efficace il ricatto

Per capire perché un gruppo criminale scelga di esporsi sul web aperto, conviene osservare le leve che mette in movimento. La tecnologia non cambia necessariamente il modo in cui entra in una rete; cambia il modo in cui trasforma l'accesso ottenuto in una pressione economica e reputazionale.

1. La vetrina: il nome della vittima diventa pubblico

Un elenco consultabile senza Tor abbassa la soglia di accesso per chiunque voglia controllare se un'azienda sia stata nominata. Clienti e fornitori non devono conoscere forum clandestini né seguire canali specializzati: basta un link, a volte condiviso anche tramite messaggi diretti. Per il criminale è una forma di pubblicità gratuita; per l'azienda, un danno reputazione enorme, ovvero un problema che può diventare visibile prima ancora che sia stata completata la verifica tecnica dell'incidente.

2. Il campione: la minaccia deve sembrare credibile

Il solo nome può non bastare. Per convincere la vittima che i criminali possiedano davvero informazioni utili, vengono talvolta pubblicati estratti, schermate, directory o link a porzioni di archivio. In altri casi compare un conto alla rovescia o la promessa di divulgare tutto a una certa ora. Il gruppo Medusa, ad esempio, ha affiancato al proprio sito onion un canale Telegram pubblico e ha previsto opzioni a pagamento per estendere i termini o gestire la pubblicazione dei dati.[5]

Il risultato è una trattativa costruita come un conto alla rovescia: pagare per fermare la diffusione, oppure affrontare la possibilità che informazioni aziendali e personali circolino senza controllo. Anche quando il materiale mostrato è limitato, la vittima deve decidere sotto pressione e senza sapere con certezza quanto altro sia stato sottratto.

3. La pressione laterale: coinvolgere chi sta intorno all'azienda

La comunicazione può essere indirizzata anche a soggetti esterni: clienti, partner commerciali, fornitori IT, assicurazioni, dipendenti o giornalisti. È una leva particolarmente delicata per le aziende che gestiscono dati per conto terzi o dipendono da una catena di fornitura. Se il gruppo riesce a far percepire l'incidente come un problema che riguarda più organizzazioni, la pressione non resta confinata al responsabile IT e arriva al management, all'ufficio legale e alle relazioni commerciali.

L'episodio del portale clearnet BreachForums.hn, usato nell'ottobre 2025 per minacciare aziende coinvolte in furti di dati Salesforce, mostra anche l'altro lato della scelta. Le autorità statunitensi e francesi hanno sequestrato il dominio pubblico mentre la controparte Tor è rimasta disponibile e ha poi ripreso a funzionare. Il clearnet amplia la visibilità, ma può rendere più semplice intervenire sul dominio e interrompere una parte della campagna.[6]

4. La reputazione: la minaccia diventa parte della ricerca online

Un sito pubblico può essere citato in una mail, condiviso sui social o trovato da chi cerca il nome dell'azienda. Non significa che ogni pagina venga indicizzata o resti online a lungo: questi domini possono essere rimossi, spostati o bloccati. Ma la possibilità che la rivendicazione riaffiori, venga copiata o ripresa da altri canali aumenta la durata della crisi. È questo il valore aggiunto per l'estorsore: non solo minacciare una fuga di dati, ma far pesare in anticipo le conseguenze della sua eventuale pubblicazione.

Non tutto ciò che compare online è una prova

C'è un rischio che riguarda direttamente chi deve gestire l'incidente: prendere l'elenco pubblicato dal gruppo come conferma automatica della violazione. Non è così. Nel primo trimestre del 2025 Check Point Research ha osservato 2.289 rivendicazioni di vittime su siti di leak attribuite a 74 gruppi, segnalando anche casi in cui nomi e vecchie rivendicazioni erano stati riciclati o inventati per gonfiare l'attività apparente. Il dato descrive ciò che i criminali dichiarano, non il numero di intrusioni verificate.[7]

Questo non significa che un post possa essere

ignorato. Significa che va trattato come un indicatore da verificare rapidamente, insieme a log, alert EDR, evidenze di esfiltrazione, accessi anomali e informazioni raccolte dal team di risposta. Comunicare troppo presto che l'azienda è stata violata può amplificare una falsa notizia; minimizzare una rivendicazione reale può invece concedere agli aggressori altro tempo. La prima risposta deve essere una verifica disciplinata, non una reazione istintiva.

Cosa cambia per chi decide

Quando il ricatto è pubblicamente visibile, la gestione non può restare solo tecnica. Occorre prepararsi a un incidente in cui la risposta informatica e quella comunicativa procedono insieme. ENISA ha rilevato che gli operatori ransomware hanno adottato tattiche di estorsione più aggressive e fanno leva anche sui timori legati agli obblighi normativi: il sito pubblico si inserisce bene in questa logica, perché porta la minaccia fuori dai sistemi e dentro le decisioni dell'organizzazione.[8]

Non servono procedure irrealistiche o costosi progetti da avviare dopo l'incidente. Servono alcune decisioni già prese:

- **Una regia unica.** Definire chi coordina SOC o MSP, incident response, direzione, legale, DPO e comunicazione. Le dichiarazioni esterne devono essere coerenti e basate su evidenze, non sulle affermazioni degli aggressori.

- **Una verifica rapida, senza dare per certa la rivendicazione.** Conservare screenshot, URL, data e ora, messaggi di estorsione e ogni indicazione utile. Le verifiche sui dati esposti vanno condotte in modo controllato, senza scaricare archivi sospetti su postazioni ordinarie o diffondere ulteriormente materiale potenzialmente riservato

- **Monitoraggio anche sul web aperto**. La ricerca di nomi aziendali, domini, marchi e dati esposti deve includere clearnet, siti onion, forum e canali pubblici. Limitarsi al dark web significa lasciare fuori una parte della superficie usata per fare pressione.

- **Piano per clienti e fornitori.** Stabilire in anticipo chi informa le controparti e con quali criteri. Un messaggio tempestivo e verificato può ridurre voci e richieste incontrollate; una comunicazione improvvisata rischia invece di aumentare il danno reputazionale.

- **Decisioni legali e di continuità già definite.** Coinvolgere presto chi valuta gli obblighi di notifica, il rapporto con le autorità e le condizioni contrattuali. In parallelo, mantenere verificabili i backup e le procedure di ripristino: pagare non garantisce né la cancellazione dei dati né il silenzio dei criminali.

Conclusione: il palcoscenico è cambiato, il ricatto no

Il clearnet non ha inventato la doppia estorsione e non ha sostituito Tor. Ha però reso più semplice portare la minaccia davanti a un pubblico che prima restava fuori dalla trattativa. Titanblog.org, i domini pubblici osservati per DeadLock e l'infrastruttura mista descritta nel caso non sono esempi differenti della stessa direzione: il criminale sceglie il canale che gli permette di aumentare la pressione sulla vittima.

Per chi difende, il punto non è inseguire ogni nuovo dominio né trasformare ogni rivendicazione in un'emergenza comunicativa. È avere un processo per verificare, contenere, ripristinare e comunicare, sapendo che i dati sottratti possono diventare uno strumento di pressione anche quando i sistemi sono di nuovo operativi. La sicurezza informatica deve quindi includere la gestione della pubblicazione e delle sue conseguenze, non soltanto il blocco dell'attacco.

Il messaggio per chi guida l'impresa è semplice: un attacco non finisce quando il criminale perde l'accesso alla rete, e non comincia quando il nome dell'azienda appare su un sito pubblico. La risposta più efficace è quella preparata prima, con responsabilità chiare, evidenze verificabili e un piano che tenga insieme tecnologia, persone e reputazione.

Note:
[1] BleepingComputer, "Clop now leaks data stolen in MOVEit attacks on clearweb sites" (23 luglio 2023).
[2] IntelFusions, "Small ransomware crew Titan turns its aim on Italy" (22 agosto 2026); Breach House, scheda del gruppo Titan e infrastrutture di leak, consultata il 28 ottobre 2026.
[3] ZeroFox Intelligence, "Flash Report: DeadLock's Ransomware Leak Site Lists over 80 Victims" (29 giugno 2026).
[4] SOCRadar Threat Research Unit, "n0n Ransomware: Inside an AI-Assisted Extortion Operation" (28 ottobre 2026).
[5] Palo Alto Networks Unit 42, "Medusa Ransomware Turning Your Files into Stone" (11 gennaio 2024).
[6] BleepingComputer, "FBI takes down BreachForums portal used for Salesforce extortion" (10 ottobre 2025).
[7] Check Point Research, "The State of Ransomware in the First Quarter of 2025" (22 aprile 2025).
[8] ENISA, "Threat Landscape 2025" (ottobre 2025), Executive Summary.

Cybersecurity in borsa: dal boom post-pandemico fino all'ingresso di Anthropic e OpenAI nel 2026



A cura di Matteo Biagini

Come il settore ha vissuto hype, correzione e nuove paure dettate dall'AI negli ultimi 6 anni.

Negli anni successivi alla pandemia, il settore della cybersecurity ha vissuto una crescita senza precedenti spinto dalla necessità globale di proteggere infrastrutture digitali sempre più complesse e interconnesse.

Tale periodo è stato segnato da una forte accelerazione della digitalizzazione che, combinata ad una crescita di perimetri target (e quindi di attacchi informatici), ha portato ad un ingente aumento degli investimenti da parte delle aziende.

L'iniziale narrativa per la quale le imprese venivano a conoscenza della sicurezza informatica solo a posteriori di un attacco, ha lasciato spazio ad una crescente consapevolezza del fatto che è solo una questione di tempo: la preparazione della propria difesa, prima o poi verrà testata.

Un attacco riuscito impatta economicamente una realtà non solo nel periodo nel quale avviene, ma anche nella fase successiva in cui il marchio può subire delle forti perdite a livello di reputazione. Questo genera una reazione a catena che causa una possibile perdita di fiducia degli investitori o fuoriuscite di dati strategici (*data leak*) accessibili dai competitor.

Da qui la nascita di normative con lo scopo di dare una direzione generale in tal senso e alzare in modo uniforme il livello di protezione per infrastrutture ritenute critiche.

Il nuovo approccio alla materia si è riflettuto anche sui mercati finanziari che, negli anni 2020 e 2021, hanno visto moltiplicare la crescita dei principali indici di riferimento del settore con i relativi player, con percentuali che hanno toccato anche il +300%.

Azienda	Performance titolo 2020	Crescita ricavi 2020	Performance titolo 2021	Crescita ricavi 2021
Palo Alto Networks (PANW)	+54%	+18%	+57%	+25%
CrowdStrike (CRWD)	+323%	+93%	-3%	+81%
Fortinet (FTNT)	+39%	+20%	+142%	+29%
Zscaler (ZS)	+322%	+42%	-64%	+56%
Check Point (CHKP)	+19%	+4%	-12%	+43%
Okta (OKTA)	+120%	+47%	-12%	+43%
CyberArk (CYBR)	+36%	+7%	+7%	+8%
SentinelOne (S)	n.a.	+100%	-32% (post-IPO)	+120%

Fonti: Marketscreener, Yahoo Finance, Investing.com, Seeking Alpha, Tradingview, Slickcharts, 1stock1, TotalRealReturns



Nel 2022, l'esponenziale ondata rialzista vista negli anni precedenti, ha fatto spazio ad un importante ribasso dando inizio al primo processo di *re-rating*:

Azienda (anno 2022)	Performance titolo	Crescita ricavi
Palo Alto Networks (PANW)	-25%	+29%
CrowdStrike (CRWD)	-49%	+54%
Fortinet (FTNT)	-31%	+32%
Zscaler (ZS)	-65%	+62%
Check Point (CHKP)	+8%	+7%
Okta (OKTA)	-69%	+56%
CyberArk (CYBR)	-25%	+18%
SentinelOne (S)	-72%	+120%

Fonti: Marketscreener, Yahoo Finance, Investing.com, Seeking Alpha, Tradingview, Slickcharts, 1stock1, TotalRealReturns

È interessante notare come, nonostante l'ottima crescita dei ricavi e l'affermazione comprovata del settore Cyber a livello globale, i titoli in borsa hanno registrato una forte correzione a ribasso dei titoli e relativi indici.

Quindi quali sono i fattori che hanno causato questi valori così negativi?

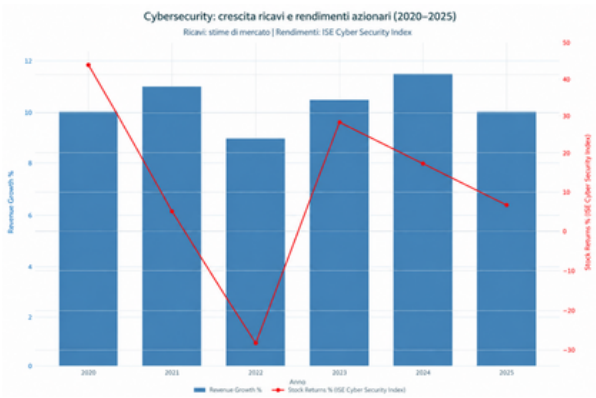
Da una profonda analisi del periodo, i fattori che hanno influenzato tali risultati sono stati: da un lato un ritracciamento fisiologico che avviene sempre a seguito di accelerazioni del genere sommato ad un contesto geopolitico non favorevole ai mercati (inizio guerra Russia-Ucraina) e, dall'altro, la caduta di aspettative irrealistiche nonostante il costante aumento degli attacchi: è molto comune che l'emotività generata da un tema così nuovo ma concreto, generi un *hype* molto importante, soprattutto sui mercati finanziari, portando le persone ad investire a causa della cosiddetta *FOMO* (Fear Of Missing Out) e a pensare che non ci sarà mai un punto di flessione.

Una storia diversa è avvenuta nel 2023, un anno che ha invece visto un forte rimbalzo generato dal recupero post-crash: in modo selettivo sono state premiate le aziende che hanno saputo resistere meglio alla caduta dell'anno precedente e sono state lasciate indietro piccole realtà che non avevano basi solide per proseguire la loro evoluzione.

Tuttavia, il medesimo anno ha visto l'inizio dello sviluppo della tecnologia che sta più segnando e segnerà la nostra epoca: l'intelligenza artificiale.

Come sempre avviene, l'avvento di una tecnologia dalla portata così rivoluzionaria, ha comportato lo spostamento conseguente della stragrande maggioranza degli investimenti da parte delle Big Tech verso quest'ultima e tutto ciò che ruota intorno ad essa (es. chip e semiconduttori). Questo fenomeno ha generato una riduzione dei multipli delle maggiori realtà del settore Cyber (e della sua narrativa) per i successivi anni 2024 e 2025, riducendo la percezione degli investitori in merito all'ascesa dell'industria.

È possibile notare dal grafico come, in questi due anni, il comparto Cyber è passato da un recupero esplosivo ad una crescita matura e selettiva, con un rallentamento graduale dei ricavi che si sono assestati gradualmente attorno ad un +15-18% medio.



Proprio nel momento in cui la crescita sembrava aver trovato una stabilità duratura, l'inizio del 2026 è stato caratterizzato da due eventi chiave firmati da una delle aziende più in auge dell'ambito intelligenza artificiale: Anthropic.

Il primo evento è relativo alla pubblicazione di Claude Code Security nel febbraio 2026, uno strumento che permette di fare revisione automatizzata del codice con lo scopo di cercare vulnerabilità presenti al suo interno, proponendo possibili remediation.

Il secondo fa riferimento invece al leak di Claude Mythos di fine marzo, un modello di intelligenza artificiale che, da quanto emerso, consente di agire da agente autonomo per fare discovery di vulnerabilità in un'infrastruttura (anche zero-day) provando a sfruttarle.

Il mercato, all'uscita ravvicinata delle due notizie, ha reagito prezzando i timori della possibile obsolescenza delle tecnologie di alcuni vendor generando un sell-off immediato dei maggiori titoli del comparto (-5/10%) e dell'indice cyber principale (-3/5%) tra l'8 e il 10 aprile.

Come spesso accade, l'emotività del momento ha incentivato gli investitori a pensare che la prospettiva

imminente da parte di Anthropic, fosse quella di "pensionare" tutti gli strumenti di sicurezza diffusi sul mercato quali EDR, NDR, XDR, tools di Vulnerability assessment ecc.

Tuttavia, non si è tenuto conto del quadro globale nel quale operano queste soluzioni, coordinate e utilizzate dai gruppi specializzati come SOC (Security Operation Center) e CSIRT (Computer Security Incident Response Team).

La risposta e l'analisi agli incidenti infatti potrà essere, e in parte già lo è, automatizzata dall'intelligenza artificiale, ma la gestione della situazione di emergenza non può essere demandata completamente; né, tantomeno, quello che è il rapporto con chi gestisce l'infrastruttura di rete nel tempo: la sicurezza è un processo che si basa anche sulle interazioni umane, non un risultato certo a priori.

La capacità decisionale e la visione di insieme di un gruppo specializzato non può essere al momento sostituita da strumenti che automatizzano esecuzioni specifiche. Ciò è avvalorato anche da un contesto che intravede l'inizio dell'introduzione degli agenti AI nei perimetri infrastrutturali, un'operazione che richiederà nuovi modelli di governance e gestione per limitare il potenziale dirompente che possono avere in cooperazione (vedi il caso OpenAI – Hugging Face).

Nei giorni successivi, questo tipo di considerazioni e l'inizio della nuova narrativa più moderata, ha portato gli investitori ad acquistare i titoli a sconto post ritracciamento, generando un rimbalzo delle azioni dei principali vendor quotati in borsa (CrowdStrike, Cisco e Palo Alto Networks tra tutti). Quest'ultimi, hanno goduto della partnership iniziata in aprile proprio con Anthropic grazie al lancio del "*Project Glasswing*", un'iniziativa nata per usare Claude Mythos nella difesa al fine di trovare e correggere vulnerabilità prima che lo facciano gli attaccanti.

L'azienda l'ha descritto come un tentativo urgente di mettere la propria soluzione al servizio della sicurezza difensiva e la mossa è stata quindi letta dal mercato come un tentativo di inserirsi nel settore al fianco dei principali attori (almeno in un primo periodo).

È doveroso evidenziare la forza del segnale che comunque ha ricevuto il settore a causa di tale vicenda: l'integrazione dell'AI sarà cruciale da parte dei grandi vendor per continuare a mantenere la solidità di un comparto che gode e, con tutta probabilità godrà nel lungo termine, di alta domanda viste le nuove implicazioni analizzate in precedenza.

A conferma di ciò, i maggiori titoli quotati hanno avuto un forte rialzo nell'indice azionario che è proseguito fino al periodo estivo, trainati da due fattori principali che si sono aggiunti: l'uscita di trimestrali molto positive per quasi tutte le realtà e l'inizio della rincorsa all'integrazione dell'AI più vincente nelle proprie soluzioni. Questo secondo passaggio ha visto l'inserimento di un nuovo attore chiamato "Daybreak", una piattaforma sviluppata da OpenAI come risposta alle proposte di Anthropic, che vuole provare a primeggiare nella costruzione di nuovi strumenti di difesa.

In questo caso la soluzione si pone come obiettivo quello includere l'analisi delle vulnerabilità nel ciclo di sviluppo del software, andandosi ad allargare successivamente in altre aree tecniche come *threat modeling* e *risk analysis*.

È cambiato quindi il campo di battaglia che si è spostato sul terreno Cyber ma la sfida rimane sempre tra due delle più importanti realtà nell'ambito dell'intelligenza artificiale.

Come in altri comparti ormai pienamente maturati, sarà interessante vedere come e chi dagli scenari attuali riuscirà a ritagliarsi il proprio spazio di mercato che vedrà alla lunga presumibilmente pochi vincitori che si prenderanno la scena, staccando tutti gli altri.



Il fornitore del fornitore: il rischio che la norma non vede



A cura di Jim Biniyaz

Nel 2023 il gruppo criminale Cl0p ha sfruttato una vulnerabilità zero-day di MOVEit, un software di trasferimento file adottato da un gran numero di organizzazioni. Il Rapporto Clusit 2026 stima oltre 2.700 organizzazioni colpite e 93 milioni di record personali esposti.

Il caso mostra come avviene oggi una violazione indiretta. Il Data Breach Investigations Report 2026 di Verizon distingue tre scenari in cui il rischio arriva da un fornitore: un suo prodotto che contiene una vulnerabilità, anche quando gira nei sistemi dell'azienda stessa; un fornitore che conserva i dati dell'azienda nel proprio ambiente; un fornitore collegato alla rete dell'azienda. Nel secondo caso all'attaccante basta violare l'infrastruttura del fornitore: il perimetro del cliente resta intatto, i suoi dati no.

Un rischio che si sposta a monte

I numeri dicono che non si tratta di casi isolati. Secondo il DBIR 2026, le violazioni che coinvolgono terze parti sono arrivate al 48% del totale, il 60% in più rispetto all'anno precedente. Per il Cost of a Data Breach Report 2026 di IBM, la compromissione della supply chain è il secondo vettore di attacco iniziale più frequente, dopo il phishing, ed è tra i più lenti da gestire: in media 258 giorni tra identificazione e contenimento. Tra i fattori analizzati da IBM, è quello che aumenta di più il costo medio di un data breach: 227.250 dollari in più.

ENISA aveva descritto la dinamica già nel 2021. Un attacco alla supply chain è la somma di almeno due attacchi: uno contro il fornitore, uno contro il cliente. Nel 66% degli incidenti analizzati dall'agenzia gli attaccanti si sono concentrati sul codice del fornitore. Nel 62% hanno sfruttato la fiducia del cliente nel fornitore. Nel 58% l'obiettivo era l'accesso ai dati, soprattutto quelli dei clienti.

Fin dove arriva la norma

La direttiva (UE) 2022/2555, nota come NIS2, mette la sicurezza della catena di approvvigionamento tra le misure obbligatorie. L'art. 21, par. 2, lett. d) parla però delle relazioni tra ciascun soggetto e i suoi fornitori diretti. Il par. 3 chiede di valutare le vulnerabilità di ciascun fornitore diretto e la qualità delle sue pratiche di sicurezza, comprese quelle di sviluppo sicuro. Sui livelli successivi il considerando 85 si limita a dire che i soggetti potrebbero tenerne conto.

Il regolamento di esecuzione (UE) 2024/2690, che si applica a una parte dei soggetti digitali, fa un passo in più. I contratti devono regolare il subappalto e, quando è consentito, imporre ai subappaltatori



requisiti di sicurezza allineati a quelli del fornitore principale (allegato, punto 5.1.4, lett. g). Il registro dei fornitori che le entità devono tenere comprende però solo quelli diretti.

In Italia l'ACN, con una determinazione aggiornata da ultimo a ottobre 2026, chiede ai soggetti NIS di comunicare ogni anno, dal 15 aprile al 31 maggio, l'elenco dei propri «fornitori rilevanti». Sono rilevanti i fornitori di servizi ICT e quelli non fungibili, la cui interruzione avrebbe un impatto significativo sui servizi del soggetto. Di norma si indica il fornitore con cui esiste il contratto. Le FAQ pubblicate dall'ACN il 18 maggio 2026 chiedono però di indicare anche il subfornitore quando il suo contributo alla fornitura è palese: un primo passo oltre il fornitore diretto.

Il settore finanziario mostra fin dove può arrivare la regolazione. Il regolamento delegato (UE) 2025/532, che integra il regolamento DORA, chiede alle entità finanziarie di identificare l'intera catena dei subappaltatori che supportano funzioni essenziali o importanti. Della catena vanno valutati lunghezza, complessità, localizzazione e rischio di concentrazione. Il fornitore deve notificare in anticipo le modifiche sostanziali al subappalto, e l'entità può recedere dal contratto se il fornitore subappalta senza autorizzazione. La responsabilità finale resta comunque all'organo di gestione.

Perché una verifica una tantum non basta

Anche dove il primo livello è sotto controllo, il controllo è spesso una fotografia. Le Good Practices di ENISA del 2023 osservano che gli operatori valutano i rischi della supply chain in modo ad hoc e che le certificazioni non sostituiscono una valutazione costante. Il DBIR 2026 dà la misura del problema. Per due tipi di debolezze rilevate presso terze parti, password deboli e permessi configurati male, servono quasi otto mesi per correggerne la metà. E solo il 23% delle organizzazioni terze risolve del tutto i problemi di autenticazione a più fattori mancante o configurata male. Una verifica annuale fotografa un momento e lascia scoperto il resto dell'anno.

E più si scende lungo la filiera, più le difese si assottigliano. Il Rapporto Clusit 2026 lo documenta nei sistemi industriali italiani. Meno del 10% dei system integrator verifica in modo sistematico le vulnerabilità note dei componenti che fornisce. Nessuno dei produttori analizzati applica un threat modeling strutturato.

Come estendere la visibilità oltre il primo livello

Ispezionare ogni subfornitore non è possibile, sapere dove guardare sì. Dalle fonti di riferimento, da ENISA al NIST Cybersecurity Framework 2.0 fino al DORA, emergono sei pratiche.

1. **Mappare le dipendenze critiche**. Censire servizi, software e flussi verso terzi; per il software più sensibile, fino a librerie e pacchetti.
2. **Classificare per criticità**. Dare la precedenza ai fornitori con accessi privilegiati, funzioni di sicurezza o dati sensibili e individuare i singoli punti di guasto (single point of failure) per la continuità operativa.
3. **Portare i requisiti a cascata**. Inserire clausole che regolino il subappalto, estendano ai subfornitori gli stessi requisiti di sicurezza e prevedano diritto di audit e notifica degli incidenti.
4. **Monitorare in modo continuo**. Passare dalle revisioni periodiche a informazioni in tempo reale o quasi reale, come descrive il Tier 4 (Adaptive) del NIST CSF 2.0, con verifiche straordinarie a ogni incidente o cambiamento rilevante.
5. **Misurare la concentrazione**. Capire quanti servizi critici dipendono dallo stesso fornitore, diretto o indiretto, e quanto sarebbe difficile sostituirlo.
6. **Preparare l'uscita**. Definire in anticipo cosa succede alla fine del contratto: recupero dei dati, transizione verso un altro fornitore, continuità del servizio.

Oltre il primo anello

La NIS2 si concentra sul primo anello della catena, gli attaccanti no. Per le aziende fuori dal settore finanziario, l'impostazione del DORA è il riferimento più concreto per colmare questa distanza: non un obbligo, ma un metodo. Conoscere il fornitore del proprio fornitore non significa controllarlo. Significa sapere in anticipo da dove può arrivare la prossima crisi.



PMI Italiane, GenAI e Agentic AI: innovare senza perdere il controllo



A cura di Andrea Ceiner

Le piccole e medie imprese italiane stanno vivendo una delle trasformazioni più rapide degli ultimi decenni.

Strumenti di Generative AI come Microsoft Copilot, ChatGPT e Claude, insieme ai nuovi sistemi di Agentic AI capaci di svolgere attività in autonomia, stanno entrando anche nelle aziende con meno di un milione di euro di fatturato.

L'adozione avviene spesso in modo spontaneo: un impiegato utilizza un assistente AI per scrivere offerte commerciali, il responsabile marketing genera contenuti in pochi minuti, il supporto clienti automatizza le risposte e l'ufficio tecnico accelera la produzione di documentazione.

I benefici sono evidenti. La produttività aumenta, molte attività ripetitive vengono automatizzate e competenze che prima richiedevano conoscenze specialistiche diventano accessibili a un numero maggiore di persone.

L'AI non sostituisce necessariamente i lavoratori: molto spesso valorizza l'esperienza dei dipendenti, colma lacune formative e consente alle persone di concentrarsi su attività a maggior valore aggiunto.

Le PMI vedono inoltre opportunità concrete per innovare prodotti e servizi, differenziarsi dai concorrenti e offrire ai clienti esperienze più rapide e personalizzate.

Accanto alle opportunità, però, crescono rischi spesso sottovalutati.

Secondo il Rapporto Clusit 2025, nel 2024 sono stati registrati 3.541 incidenti cyber gravi a livello mondiale, con una crescita del 27% rispetto all'anno precedente, mentre l'Italia continua a essere uno dei paesi più colpiti e ha registrato un aumento degli attacchi del 15%.

Il phishing e le tecniche di social engineering sono aumentati del 33%. Questi numeri mostrano come il contesto digitale sia sempre più ostile.

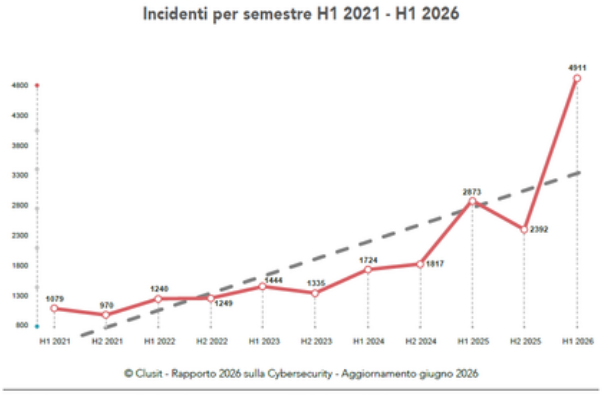


Fig. 1 - Andamento degli incidenti cyber nel periodo 2021 - I sem. 2026



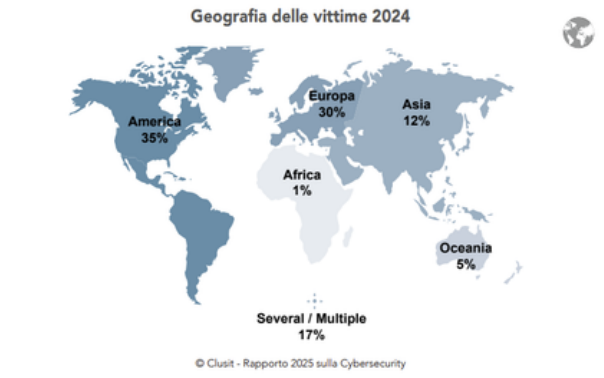


Fig. 7 - Distribuzione geografica delle vittime in percentuale per il 2024

L'intelligenza artificiale amplia ulteriormente la superficie di rischio.

Un dipendente potrebbe caricare informazioni riservate su una piattaforma AI pubblica. Un agente AI potrebbe accedere a dati sensibili senza adeguati controlli. Un attaccante potrebbe sfruttare tecniche di prompt injection per manipolare il comportamento di un assistente aziendale oppure utilizzare l'AI per generare campagne di phishing altamente credibili.

Esistono anche minacce specifiche ai modelli AI, come data poisoning, model extraction e attacchi adversarial.

È qui che entrano in gioco **ISO/IEC 27001 e ISO/IEC 42001**. Molti imprenditori ritengono erroneamente che questi standard siano adatti soltanto a grandi organizzazioni.

In realtà possono essere implementati anche in realtà molto piccole, purché con un approccio proporzionato.

La ISO 27001 aiuta a governare la sicurezza delle informazioni attraverso processi semplici ma efficaci: analisi del rischio, gestione degli accessi, formazione, backup, controllo dei fornitori e risposta agli incidenti. La ISO 42001, primo standard internazionale dedicato ai sistemi di gestione dell'intelligenza artificiale, introduce invece principi di governance, trasparenza, valutazione degli impatti, supervisione umana e gestione dei rischi dell'AI.

Immaginiamo una PMI manifatturiera che utilizzi un agente AI per consultare documentazione tecnica, dati di produzione e informazioni sui clienti.

Un attacco di prompt injection potrebbe indurre l'agente a divulgare dati riservati. I controlli della ISO 27001 impongono classificazione delle informazioni, gestione degli accessi e monitoraggio degli eventi. La ISO 42001 richiede invece la valutazione dei rischi AI, la definizione dei ruoli e la supervisione dei risultati generati dal sistema. L'effetto combinato è una forte riduzione della probabilità e dell'impatto dell'incidente.

Dal punto di vista pratico, una PMI può seguire una **roadmap semplice:**

1. **Primo trimestre**: censire dati, processi e soluzioni AI utilizzate.
2. **Secondo trimestre**: eseguire una valutazione integrata dei rischi cyber e AI, definendo policy e responsabilità.
3. **Terzo trimestre**: implementare i controlli prioritari, formazione del personale, gestione dei fornitori, procedure di incident response e registro dei sistemi AI.
4. **Quarto trimestre**: condurre audit interni e preparare la certificazione integrata ISO 27001 e ISO 42001. Grazie alla struttura comune degli standard ISO, gran parte della documentazione e dei processi può essere condivisa.

Per una piccola impresa, certificarsi non significa fare burocrazia. Significa creare un metodo di governo dell'innovazione.

Nei prossimi anni sopravvivranno le aziende capaci di adottare rapidamente l'intelligenza artificiale mantenendo però il controllo sui propri dati, sui processi e sui rischi. ISO 27001 e ISO 42001 rappresentano una guida concreta per trasformare l'AI da possibile fonte di problemi a reale vantaggio competitivo e strategico.



Le PMI e i rischi cyber: la sicurezza della filiera parte da chi sa cosa proteggere



A cura di Marco Cortinovis

“Prima di difendersi, un’organizzazione deve conoscere sé stessa”.

Il principio può sembrare scontato, ma nella realtà delle piccole e medie imprese è tutt’altro che consolidato. Alla domanda su quali siano i dati da cui dipende l’attività quotidiana, dove siano conservati e chi possa accedervi, molte aziende non sono in grado di rispondere con precisione.

Non si tratta di mancanza di competenze e conoscenze: spesso nessuno, all’interno delle organizzazioni, ha mai avuto il compito di ricostruire il quadro generale. Ed è proprio da questa lacuna che dipende l’efficacia di qualsiasi investimento in sicurezza.

Le piccole-medie imprese sono l’anello esposto delle filiere di fornitura

Le piccole e medie imprese sono la struttura portante delle filiere italiane, ed è per questa ragione che stanno diventando sempre più l’obiettivo di attacchi cyber. Attaccare un fornitore di piccole dimensioni è spesso il modo più semplice per arrivare a un’azienda più grande e meglio protetta. Il Rapporto Clusit 2026 registra per l’Italia 507 incidenti gravi nel 2025, contro i 357 del 2024: una crescita del 42%, con il manifatturiero ancora tra i settori più colpiti.

Secondo il Cyber Index PMI 2025, il 24% delle piccole e medie imprese italiane dichiara di aver subito almeno una violazione negli ultimi tre anni, un dato triplicato rispetto alla rilevazione precedente.

Questo cambia anche il modo in cui va letta la sicurezza di un’impresa di piccole dimensioni. Non è più soltanto un tema di tutela del singolo patrimonio aziendale, ma un fattore che incide sulla solidità dell’intera catena del valore. Un incidente presso un subfornitore può bloccare una linea di produzione a centinaia di chilometri di distanza, con effetti che vanno ben oltre il perimetro dell’azienda colpita.

La NIS2 ha trasformato questa dinamica in un obbligo. Anche le imprese che non rientrano direttamente nel perimetro della norma ricevono dai propri clienti richieste di garanzie, questionari e documentazione sulla sicurezza. Per molte PMI la protezione dei propri sistemi è diventata, di fatto, un requisito per continuare a lavorare in filiera.

La consapevolezza arriva prima degli strumenti

I dati sulla maturità delle imprese confermano il quadro. Il Cyber Index PMI 2025, promosso da Confindustria e Generali con il Politecnico di Milano e la partnership dell’ACN su un campione di oltre 1.500 aziende, registra un livello medio di consapevolezza di 55 punti su 100, ancora sotto la soglia di



sufficienza fissata a 60. Solo il 16% delle PMI ha una postura di sicurezza adeguata. Il rapporto individua il nodo principale non tanto nella percezione del rischio, che cresce, quanto nella capacità di tradurla in governance, gestione del rischio e competenze.

Sotto la pressione di clienti e normative, la risposta istintiva è acquistare qualcosa: una soluzione più avanzata, un servizio di monitoraggio, un nuovo sistema di backup. Sono investimenti utili, ma se arrivano prima di un'analisi dell'organizzazione rischiano di fare investimenti che non necessariamente aumentino il livello di sicurezza.

Nelle attività di audit emergono con regolarità utenze di ex collaboratori ancora attive, accessi remoti concessi a un fornitore e mai revocati, copie di dati personali conservate su dispositivi privati. Nessuna di queste situazioni si risolve con un prodotto; si risolve sapendo che esiste.

Gli standard lo dicono da tempo. La ISO/IEC 27001 chiede di definire il contesto dell'organizzazione prima di scegliere qualsiasi controllo, e la NIS2 impone misure proporzionate, cosa possibile solo se si conosce il valore di ciò che si vuole proteggere. Conoscersi, in questo senso, è già una misura di sicurezza. Probabilmente la più importante.

In pratica, il lavoro da cui partire consiste nel ricostruire tre cose: un inventario delle informazioni e dei sistemi che contano, una mappa dei fornitori, una valutazione oggettiva di quali processi non si possono fermare.

Non serve che il risultato sia perfetto al primo tentativo: serve che il processo si avvii, che qualcuno ne sia responsabile e che venga migliorato nel tempo.

Il Sistema ha bisogno che ogni singola impresa si assuma le sue responsabilità

La maggior parte delle PMI non ha una figura dedicata alla sicurezza, affida l'informatica a una persona o a un fornitore esterno e deve confrontarsi con norme scritte in un linguaggio lontano da quello dell'impresa. Se non accompagnate e supportate, il rischio concreto per queste imprese è che la conformità si riduca a una mera serie di documenti compilati per superare una verifica.

Per questo la sicurezza delle PMI va considerata una responsabilità condivisa. L'ACN ha già messo a disposizione guide e canali di assistenza per orientare i soggetti NIS, e le associazioni come Assintel svolgono un ruolo prezioso nel portare campagne di sensibilizzazione con le imprese. Agli operatori che lavorano ogni giorno con le aziende spetta il compito di rendere gli standard praticabili e accessibili: costruire l'analisi insieme alle persone che conoscono i processi, scrivere procedure che descrivono il modo in cui l'azienda lavora davvero, restare accanto all'impresa nel tempo, perché ogni cambiamento organizzativo modifica il profilo di rischio.

La NIS2 lo mette nero su bianco e pretende un coinvolgimento della direzione, attribuendo responsabilità dirette agli organi di gestione. Per esercitare quella responsabilità chi guida un'azienda deve avere sotto controllo il perimetro, i propri processi, i fornitori e tutti gli asset critici. Il tutto con la consapevolezza di aver preso coscienza delle conseguenze che avrebbe avuto nel perderli.

È un passaggio che riguarda l'intero sistema produttivo, e su cui ciascun attore dell'ecosistema è chiamato a fare la propria parte.



AI – DOMANDE E RISPOSTE FACILI FACILI
Io ago in un pagliaio ma con il numero di matricola



A cura di Gianpiero Cozzolino

L'AI per la profilazione

La "profilazione" è una pratica che permette di associare agli individui (con la doverosa precisazione che, contrariamente a quanto si creda, i dati anagrafici sono spesso ignorati perché non indispensabili agli scopi perseguiti) una serie di caratteristiche utili per comprendere la personalità e prevedere comportamenti, con la conseguenza che è possibile personalizzare ciò che si offre ad ogni individuo. Anche in questo caso, le tecniche di intelligenza artificiale, che grazie all'addestramento hanno la possibilità di riconoscere in modo più preciso tali caratteristiche, hanno portato grandi miglioramenti nei risultati.

Finché si rimane nell'ambito del marketing, al di là delle questioni legate all'invadenza nella vita privata delle persone, non ci sono grandi problemi.

Invece, spesso la profilazione è il risultato di attività di monitoraggio sia sociale che comportamentale (le quali attività, sia chiaro, non sono nate con l'IA: esistevano anche precedentemente, ma erano basate su algoritmi deterministici); l'effetto, quando non proprio lo scopo, è la possibilità di monitorare il contesto sociale per individuare i soggetti da considerare pericolosi, problematici, non allineati, ecc., con tutti i rischi di discriminazione o limitazione dei diritti (non a caso l'UE, con l'AI Act, ha tassativamente proibito tali sistemi, anche a fini di sicurezza pubblica).

La profilazione "sociale"

Questo genere di minaccia non è limitato ai soliti e noti soggetti, per lo più privati e americani, su cui normalmente ci concentriamo: la tentazione prende spesso anche i soggetti pubblici.

Più volte sono state avanzate proposte (in maniera totalmente bipartisan) di adottare "facilitazioni" nell'ambito della vita politica e sociale basandosi su valutazioni di tipo comportamentale e di aderenza ai valori di riferimento (pratica che prende il nome di "social scoring", ossia punteggio sociale).

Come spesso accade, il problema non è tecnologico: l'abbondanza di dati e le tecniche di elaborazione sempre più sopraffine, tra cui appunto le metodologie basate su intelligenza artificiale, permettono di stilare classifiche decisamente affidabili; ma l'utilizzo per diversificare opportunità e servizi pubblici a seconda della "classifica" diventa incompatibile con i principi di uguaglianza propri delle nostre democrazie.

Ricordiamo anche che la profilazione è sempre



considerata (per es. nel GDPR) come un rischio: infatti, la sola esistenza di profili accurati (a prescindere dalla motivazione per cui sono stati creati) espone alle minacce legate al riutilizzo di tali profili per finalità malevole.

Cosa ne penso?

Non è possibile scindere totalmente le opportunità date dalle nuove tecnologie dagli impatti che esse possono avere nelle vite concrete dei cittadini.

Gli interessi pur legittimi, privati e pubblici che siano, vanno sempre bilanciati con i principi fondanti e con i diritti riconosciuti nelle nostre società.

Il tema dell'introduzione dell'etica nell'ambito delle applicazioni dell'IA viene portato avanti già da alcuni anni da diversi attori (tra cui vale la pena citare l'ONU e il Vaticano), tuttavia esso appare, nella pratica, troppo spesso sopravanzato dagli interessi economici e politici.

Di conseguenza, è un bene che la profilazione, soprattutto se realizzata con tecniche di IA, venga molto limitata a livello giuridico, e costituisca una delle principali attenzioni di "igiene digitale" che ognuno di noi deve avere.





CYBER
Think Tank
ASSINTEL

Unisciti alla nostra community!

Scrivi a segreteria@assintel.it
per avere maggiori info

Le sfide della transizione post-quantistica tra cybersecurity e capacità industriale

A cura di Stefano da Empoli e Alessandro D'Amato





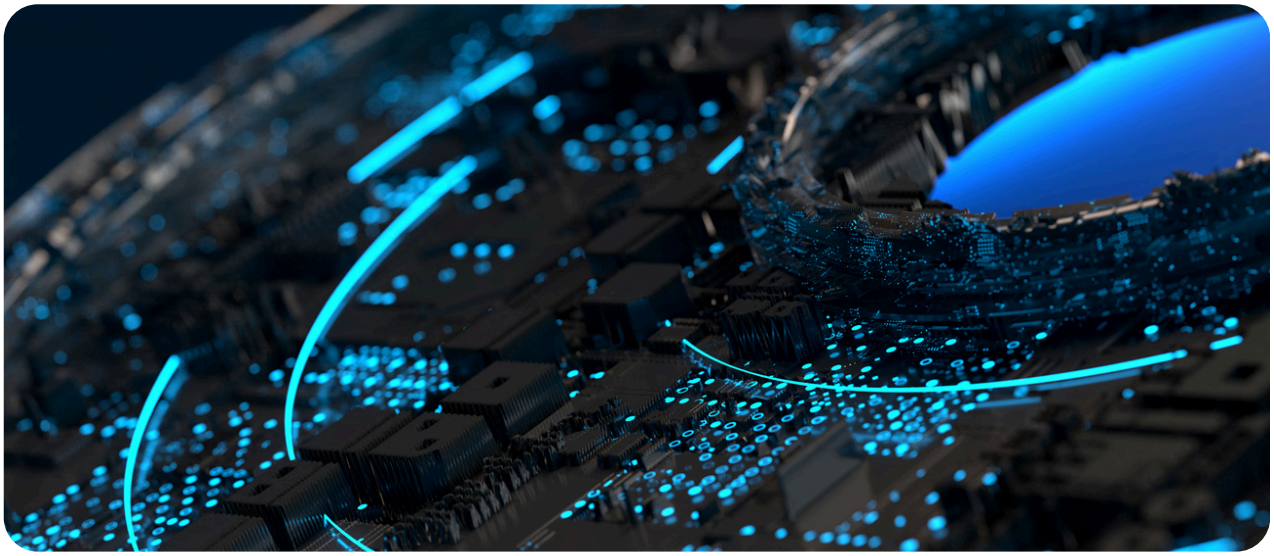
In Europa e nel nostro Paese le tecnologie quantistiche stanno progressivamente uscendo dalla sola dimensione della ricerca per entrare nelle strategie industriali e di sicurezza. La Commissione europea, nella *Quantum Europe Strategy* (luglio 2025), stima che UE e Stati membri abbiano investito circa 11 miliardi di euro nel settore negli ultimi cinque anni e che, entro il 2040, il mercato globale possa superare i 155 miliardi. Sul fronte cyber, il *Global Cybersecurity Outlook* 2026 del *World Economic Forum* rileva, sulla base di una survey, che il 37% dei rispondenti si aspetta un impatto delle tecnologie quantistiche sulla cybersecurity già entro i successivi dodici mesi. La conseguenza più concreta è quindi già attuale: la necessità di preparare la transizione verso sistemi crittografici capaci di resistere alla futura minaccia quantistica.

Il punto, utile per evitare allarmismi, non è che i computer quantistici siano già oggi in grado di compromettere su larga scala gli schemi di crittografia a chiave pubblica utilizzati nelle comunicazioni digitali; tuttavia, l'incertezza sui tempi del cosiddetto Q-Day non riduce il problema: al contrario, rende rischioso attendere che tale capacità sia disponibile prima di iniziare a intervenire. A rendere la minaccia quanto mai attuale nel dibattito è soprattutto lo scenario *harvest now, decrypt later*: un attore ostile può raccogliere oggi informazioni cifrate e conservarle con l'obiettivo di decifrarle in futuro. Il rischio è maggiore per dati governativi, sanitari o finanziari che devono necessariamente restare riservati nel lungo periodo.

Non a caso, lo scorso 3 settembre il *Cyber Security Working Group* del G7, con il contributo dell'Agenzia per la Cybersicurezza Nazionale (ACN), ha invitato governi e soggetti privati ad accelerare la transizione alla crittografia post-quantistica, qualificando il quantum non soltanto come rischio tecnologico, ma anche economico e di sicurezza nazionale.

In questo scenario, la principale risposta tecnologica è rappresentata dalla *post-quantum cryptography* (PQC), ossia da un insieme di algoritmi progettati per funzionare sugli attuali sistemi informatici e resistere anche ad attacchi condotti con futuri computer quantistici crittograficamente rilevanti. Nell'agosto 2024, il *National Institute of Standards and Technology* (NIST) statunitense ha finalizzato i primi tre standard post-quantum (FIPS 203, 204 e 205), mentre nel marzo 2025 ha selezionato l'*Hamming Quasi-Cyclic* (HQC) come ulteriore algoritmo da standardizzare. La disponibilità di standard ormai divenuti un riferimento a livello internazionale riduce una parte dell'incertezza tecnica, ma non rende semplice e automatica la migrazione: sostituire la crittografia significa intervenire su certificati, *Public Key Infrastructure* (PKI), protocolli, *firmware*, applicazioni e servizi distribuiti lungo supply chain spesso articolate.

Per tali ragioni, la parola chiave non è soltanto *quantum-safe*, ma anche *crypto-agility*, vale a dire la capacità di individuare dove viene utilizzata la crittografia e di sostituirne i componenti senza riprogettare ogni volta l'intera architettura.



Il primo passo è costruire un inventario degli asset crittografici, mappare le dipendenze da fornitori terzi, classificare i sistemi sulla base del rischio e pianificare una migrazione graduale. La distanza tra consapevolezza e preparazione è già misurabile: una recente indagine FINMA – l'autorità di vigilanza svizzera sui mercati finanziari – su 60 istituzioni finanziarie ha rilevato una diffusa consapevolezza del rischio e al contempo l'assenza di roadmap chiare e di una pianificazione sufficientemente lungimirante nella maggior parte dei casi.

Sul piano europeo, il passaggio dalla strategia all'attuazione è già iniziato. La roadmap coordinata pubblicata dal *NIS Cooperation Group* a giugno 2025 indica che tutti gli Stati membri dovrebbero avviare la transizione entro la fine del 2026, mentre i casi d'uso ad alto rischio dovrebbero essere migrati il prima possibile e comunque non oltre il 2030. Non a caso, nei risultati della consultazione sulla roadmap pubblicati lo scorso 2 settembre, sulla base di 97 contributi, scadenze chiare, approccio basato sul rischio, schemi ibridi e *crypto-agility* figurano tra gli elementi giudicati più utili dagli stakeholder.

Accanto alla PQC, l'Europa sta investendo anche nella *quantum communication*. L'EuroQCI, cui partecipano tutti i 27 Stati membri insieme alla Commissione e all'Agenzia Spaziale Europea, sta costruendo un'infrastruttura composta da un segmento terrestre in fibra e da uno spaziale basato su satelliti, parte integrante del sistema europeo di connettività sicura IRIS².

Anche le politiche nazionali iniziano a incidere sul mercato: negli Stati Uniti, l'Executive Order 14412 del 22 giugno 2026 ha previsto che le agenzie federali migrino gli "*high-value assets*" e gli "*high-impact systems*" alla PQC entro il 31 dicembre 2030 e per le firme digitali entro la fine del 2031, intervenendo anche sul procurement federale. Ad agosto, il Tesoro statunitense ha poi lanciato una *Quantum-Readiness Task Force* per il settore finanziario. Il segnale è quindi chiaro: la quantum *readiness* sta passando dalle strategie pubbliche alle condizioni di acquisto e, a cascata, alle supply chain.

In Europa, l'ANSSI – l'autorità cyber francese – punta a introdurre requisiti PQC per l'accesso alla qualificazione dei prodotti dal 2027 e ritiene non ragionevole acquistare dopo il 2030 prodotti che non integrino tali soluzioni. Anche l'Italia ha iniziato a strutturare la propria risposta tramite la Strategia italiana per le tecnologie quantistiche, approvata dal Comitato interministeriale per la transizione digitale a luglio 2025, che inserisce sicurezza, infrastrutture, ricerca, competenze e trasferimento tecnologico in un quadro unitario.

Sul fronte imprenditoriale, tuttavia, permangono evidenti limiti nella possibilità concreta di trasformare le competenze scientifiche nazionali in capacità industriale e attrarre capitali.

Qualche recente segnale in questa direzione appare comunque incoraggiante. Telsy, ad esempio, sta lavorando insieme a QTI – spin off del CNR attivo nella *Quantum Key Distribution* (QKD) – all'integrazione tra crittografia tradizionale, PQC e tecnologie quantistiche. Ad aprile 2026, insieme a TIM Enterprise e altri partner, le due società hanno contribuito alla realizzazione di un collegamento *quantum-safe* di lunga distanza tra Roma e Napoli, basato su un'architettura ibrida che combina QKD e crittografia post-quantistica. Parallelamente, il progetto QuRE punta allo sviluppo di *quantum repeater* per reti quantistiche più estese e scalabili. A settembre 2026, IonQ Italia e Lutech hanno annunciato una collaborazione di 24 mesi per accompagnare imprese, PA e infrastrutture critiche dalla quantum *readiness* alla sperimentazione e all'adozione.

Sul piano concorrenziale, l'AGCM ha avviato a marzo un'indagine conoscitiva sul quantum computing (che proseguirà fino alla fine di dicembre), concentrandosi anche su *lock-in*, barriere all'ingresso, *Quantum-as-a-Service* e dipendenze strategiche. Sicurezza, concorrenza e sovranità tecnologica iniziano così a convergere nelle priorità di policy.

Il passaggio decisivo sarà tradurre strategie, standard e sperimentazioni in un percorso di migrazione effettivo. La Banca centrale europea (BCE), in una lettera del 7 luglio indirizzata alle istituzioni significative sottoposte alla sua vigilanza, ha sottolineato che l'adozione della PQC richiederà tempi lunghi, ma deve iniziare ora e necessita di investimenti strategici continuativi.

In definitiva, per l'Italia la sfida sarà anche industriale: accanto al coordinamento tra ACN, amministrazioni, operatori critici e ricerca, sarà necessario consolidare una filiera nazionale capace di integrare competenze scientifiche, crittografia, componentistica e infrastrutture di comunicazione. È un tema destinato ad assumere ancora maggiore rilevanza con il futuro Quantum Act europeo, inizialmente previsto per il secondo trimestre 2026 e, sebbene in ritardo rispetto alla tabella di marcia, atteso ancora entro la fine dell'anno, che dovrebbe intervenire proprio su ricerca e innovazione, capacità industriale e resilienza delle *supply chain*. La capacità degli attori italiani di inserirsi in queste catene del valore sarà quindi parte integrante della stessa *quantum readiness*: una transizione che non comincia quando arriverà un computer capace di rompere la crittografia odierna, ma quando esiste ancora il tempo per prepararsi senza trasformare una vulnerabilità futura in una crisi sistemica.

Vulnerabilità note e responsabilità degli amministratori: quando il mancato aggiornamento diventa colpa

A cura di Armando De Lucia



Quando una vulnerabilità diventa pubblica e la correzione è disponibile, il rischio cambia natura: da evento imprevedibile a evento prevedibile ed evitabile, cioè il terreno su cui il diritto misura la diligenza. L'articolo esamina come i principali riferimenti normativi europei e nazionali – lo "stato dell'arte" del GDPR e della Direttiva NIS2, i doveri degli organi di amministrazione, il dovere generale di adeguati assetti del codice civile – trasformino il mancato aggiornamento da questione tecnica a questione di governance. La tesi è che il vero fattore di esposizione non sia la vulnerabilità in sé, ma l'assenza di una decisione documentata su di essa: aggiornare, mitigare o accettare il rischio sono scelte difendibili; non scegliere non lo è. Il contributo si chiude su una tensione ancora aperta – chi debba provare cosa, e davanti a chi – che ogni consiglio di amministrazione farebbe bene a porsi prima che sia qualcun altro a farlo.

Nel contemporaneo contesto sociale ed economico la sicurezza e la resilienza dei sistemi informatici hanno assunto una rilevanza prioritaria nella gestione degli asset aziendali. Infatti, la sussistenza di una falla informatica, definibile come vulnerabilità, può esporre le imprese ad attacchi informatici e a rischi concreti per la continuità aziendale e la relativa stabilità economica.

In tale prospettiva, per inquadrare i suddetti profili di pericolosità per l'ecosistema aziendale, appare necessario fare un preliminare riferimento alla nozione di vulnerabilità.

Ai sensi della Direttiva (UE) 2022/2555 (NIS2), emanata nel contesto giuridico europeo, ma recepita anche dall'ordinamento italiano, la vulnerabilità è un punto debole, una suscettibilità o un difetto che può essere sfruttato da una minaccia informatica. In altri termini, la vulnerabilità è una debolezza presente nella progettazione, nella configurazione o nello sviluppo di un sistema software, hardware o di rete.

Invero, sul fronte temporale, allorquando la vulnerabilità diviene pubblica la criticità non è più confinata al reparto IT: diventa un rischio di business che minaccia la reputazione, la stabilità finanziaria e la protezione dei dati personali dei clienti e dipendenti. *La presa di coscienza pubblica circa la presenza della vulnerabilità ha rilevanti effetti anche sul piano giuridico, in virtù del fatto che muta la natura del rischio, considerato prevedibile ed evitabile, e dunque, anche la misura di diligenza richiesta dalle imprese e da chi le amministra.*

Perché una vulnerabilità nota cambia la natura del rischio?

Quando la vulnerabilità diviene pubblica possono sorgere rischi sistemici per l'intero patrimonio informativo dell'azienda, legati a possibili responsabilità sul fronte giuridico.

Tali responsabilità promanano anche da alcune fonti di riferimento nel contesto europeo, direttamente applicabili o recepite, e comunque vincolanti.



In particolare, l'articolo 32 del Regolamento europeo per la protezione dei dati personali (GDPR) dispone che coloro i quali trattano i dati personali debbano mettere in atto misure tecniche e organizzative adeguate rispetto al livello di rischio, in un'ottica proporzionata ai costi di attuazione e alla natura del trattamento nonché tenendo conto dello stato dell'arte. Un approccio analogo, basato sul rischio, caratterizza anche l'articolo 21 della citata Direttiva europea NIS2, vincolante in tema di cybersecurity, stante il recepimento nazionale, che impone di proteggere i sistemi di reti di informazione e l'ambiente fisico dagli incidenti informatici, adottando politiche su rischio e garantendo una continuità operativa. *In particolare, l'art. 21, par. 2, lett. e), NIS2, parla proprio della manutenzione dei sistemi, compresa la gestione e la divulgazione delle vulnerabilità.*

Invero, la trasposizione di tali coordinate normative al caso di specie (la vulnerabilità diviene di dominio pubblico) induce ad affermare che la perdita di controllo sui dati personali in seguito a una vulnerabilità nota e non gestita può integrare una violazione dell'obbligo di adottare misure adeguate, misurabile in termini di prevedibilità ed evitabilità dello sfruttamento della falla tecnica. In particolare, per non incorrere in responsabilità l'azienda dovrebbe dimostrare di aver adottato misure tecniche adeguate per gestire la rilevata vulnerabilità.

In tal senso, sul piano operativo per governare tali criticità in modo conforme alle prescrizioni normative individuate, sarebbe necessario adottare un approccio proattivo, che consenta di gestire i software e di effettuare aggiornamenti critici in tempi utili rispetto alla pubblicazione delle patch correttive.

Chi risponde se l'aggiornamento non viene installato?

Ai sensi del GDPR, il responsabile per le condotte negligenti in merito alla gestione della vulnerabilità pubblica è in primo luogo il titolare del trattamento, così come chiarito anche dal Garante per la protezione dei dati personali quando ha sanzionato un titolare del trattamento (caso Postel S.p.A. – Registro dei provvedimenti n. 572 del 4 luglio 2024), che aveva procrastinato per quasi un anno l'intervento su una vulnerabilità informatica già nota e segnalata.

Al contempo, nell'ordinamento italiano l'articolo 24 del D.lgs. 4 settembre 2024, n. 138, che ha recepito la Direttiva NIS2, impone l'adozione di misure tecniche, operative ed organizzative adeguate e proporzionate alla gestione dei rischi informatici.

Sul fronte della responsabilità, questa norma, strettamente correlata all'articolo 23 del medesimo D.lgs., fa sorgere particolari profili di interesse, sostanzialmente legati al riconoscimento della responsabilità diretta degli organi di amministrazione.

Segnatamente, per i soggetti sottoposti alla NIS2, *gli organi di amministrazione sono responsabili delle violazioni del decreto* se non approvano e non supervisionano queste misure e, nei casi più gravi, possono anche essere destinatari di misure



personali, fino all'incapacità temporanea a svolgere funzioni dirigenziali.

In questi termini, nel quadro normativo nazionale odierno, una falla informatica non gestita può essere indice di un assetto organizzativo non adeguato, valutabile ai sensi dell'art. 2086 c.c. Tale norma impone all'imprenditore che operi in forma societaria o collettiva l'obbligo inderogabile di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa.

In questo quadro, foriero di responsabilità per gli amministratori, si inserisce anche l'articolo 2392 c.c., che dispone come gli amministratori rispondano solidalmente dei danni causati alla società se non adempiono i doveri ad essi imposti dalla legge e dallo statuto.

Da quanto esposto emerge come la condotta negligente degli amministratori nel contesto aziendale assuma assoluta rilevanza.

Al contempo, però, appare opportuno fare dei chiarimenti in merito allo *standard di diligenza richiesto per non essere riconosciuti responsabili*.

In tale prospettiva, da taluni precedenti giurisprudenziali è desumibile che la business judgment rule protegge il merito delle scelte gestionali (nei limiti della ragionevolezza e della cautela preventiva) assunte in modo informato, ma non copre le omissioni o le condotte negligenti prive di un preventivo processo decisionale.

Aggiornare, mitigare o accettare: chi decide?

Più un'impresa dipende da sistemi digitali, più la gestione delle vulnerabilità diventa una questione di cultura organizzativa: proteggere gli asset digitali significa curarne la manutenzione in modo continuo e proattivo, e sapere chi ne risponde.

Questo non significa che ogni vulnerabilità debba essere corretta immediatamente e a ogni costo. Un aggiornamento può compromettere la continuità di un servizio critico, richiedere verifiche preventive o dipendere dai tempi di un fornitore. Esistono alternative legittime: mitigare il rischio con misure compensative, isolare il sistema, accettare consapevolmente un rischio residuo. Ciò che il diritto valuta non è l'esito, ma il percorso.

Su questo punto convergono due regole diverse. In materia di dati personali è il titolare a dover dimostrare l'adeguatezza delle misure adottate. In sede societaria, invece, chi agisce contro gli amministratori deve indicare le specifiche condotte contestate. In entrambi i casi l'elemento decisivo è lo stesso: la traccia della decisione assunta, o la sua assenza.

Il vero fattore di esposizione, dunque, non è la vulnerabilità in sé, ma la mancanza di una decisione documentata su di essa. Ne discende una domanda che ogni organo di amministrazione dovrebbe porsi: *se oggi qualcuno chiedesse perché quella vulnerabilità era ancora aperta, esisterebbe una risposta scritta, datata e attribuibile?*



Quando l'AI diventa una nuova superficie di rischio

A cura di Francesco Iarlori



Dalla protezione dei sistemi alla governance dell'autonomia: come quarant'anni di evoluzione digitale stanno cambiando ancora una volta la cybersecurity.

Ho iniziato ad interagire con i sistemi informatici quando Unix era uno degli ambienti nei quali si costruiva il futuro dell'informatica. Negli anni Ottanta e nei primi anni Novanta la sicurezza aveva un significato relativamente chiaro: proteggere sistemi, utenti, dati e privilegi, stabilendo chi potesse accedere a una determinata risorsa e quali operazioni fosse autorizzato a compiere.

Con Internet abbiamo dovuto proteggere le reti; con il Web e i servizi digitali abbiamo iniziato a proteggere identità e transazioni; con il cloud abbiamo imparato a governare infrastrutture distribuite che non coincidevano più con un luogo fisico. Ogni trasformazione ha ampliato la superficie di attacco e richiesto nuovi strumenti, nuove competenze e, progressivamente, nuovi modelli organizzativi.

L'Intelligenza Artificiale introduce però qualcosa di diverso. Per la prima volta stiamo inserendo nelle organizzazioni sistemi che non si limitano a conservare informazioni o eseguire istruzioni, ma interpretano il contesto, producono conoscenza, suggeriscono decisioni e, sempre più spesso, possono trasformare queste decisioni in azioni.

Il problema della cybersecurity diventa quindi inevitabilmente anche un problema manageriale. Non dobbiamo più chiederci soltanto chi possa accedere ai nostri sistemi, ma quali decisioni siamo disposti a delegare a sistemi che, una volta ottenuto quell'accesso, possiedono una crescente capacità di interpretare autonomamente ciò che devono fare.

La superficie di attacco diventa organizzativa

Per decenni la cybersecurity è stata considerata prevalentemente una responsabilità delle funzioni IT e Security. Questo modello diventa insufficiente quando l'AI entra direttamente nei processi aziendali e partecipa, ad esempio, alla selezione di un candidato, alla sintesi di un contratto, all'analisi di una richiesta di credito, alla preparazione di una risposta a un cliente o al supporto di una decisione amministrativa.

La sicurezza non riguarda quindi più soltanto l'infrastruttura, ma il processo organizzativo nel quale l'AI viene inserita. Il management deve sapere dove questi sistemi vengono utilizzati, quali informazioni possono consultare, quali decisioni possono influenzare e, soprattutto, dove debba terminare la loro autonomia. In questa prospettiva, la nuova superficie di attacco tende progressivamente a coincidere con l'organizzazione stessa.

Dal punto di vista tecnico, nel software tradizionale



possiamo semplificare il processo attraverso una sequenza relativamente deterministica:
Input → Programma → Output

Con un sistema AI la catena diventa
Input → Contesto → Modello → Interpretazione → Output

e, con l'introduzione degli agenti, può estendersi fino a
Input → Contesto → Interpretazione → Decisione → Azione.

Ogni passaggio aggiunge nuove possibilità di manipolazione. Non dobbiamo quindi proteggere soltanto codice e infrastruttura, ma anche prompt, contesto, fonti informative, modelli, strumenti collegati e output, considerando soprattutto le relazioni che si creano tra questi elementi.

Dal controllo degli accessi al controllo dell'autonomia

Uno dei principi fondamentali della sicurezza informatica è sempre stato il controllo dei privilegi. Negli ambienti Unix degli anni Ottanta e Novanta era immediatamente comprensibile: un utente normale poteva compiere determinate operazioni, mentre un utente privilegiato disponeva di possibilità molto più ampie.

Oggi questo principio assume una dimensione differente. Un agente AI può avere accesso alla posta elettronica, al calendario, al CRM, ai documenti aziendali, ai sistemi ERP e progressivamente anche a workflow operativi. Possiamo aver configurato correttamente ogni singolo permesso e avere comunque creato un rischio, perché il vero problema non riguarda soltanto ciò a cui l'agente può accedere, ma il modo in cui può combinare autonomamente risorse e autorizzazioni differenti.

Per il management questo significa passare dalla governance dei privilegi alla **governance dell'autonomia.**

Dal punto di vista tecnico, un agente può essere perfettamente autenticato, utilizzare API correttamente autorizzate, comunicare attraverso connessioni cifrate e produrre log completi delle proprie attività, generando comunque un comportamento indesiderato attraverso la combinazione legittima di una serie di autorizzazioni.

Potremmo considerarla una nuova forma di **escalation dell'autonomia**: il sistema non acquisisce necessariamente nuovi privilegi, ma utilizza quelli esistenti per raggiungere un risultato che nessuno aveva previsto quando quei privilegi erano stati assegnati.

La conoscenza diventa infrastruttura critica

Per anni abbiamo considerato database, applicazioni e reti come infrastrutture critiche. Con l'AI dobbiamo aggiungere la conoscenza, perché sempre più organizzazioni stanno costruendo sistemi nei quali i modelli interrogano documenti interni, knowledge base, procedure, e-mail, database e architetture RAG per produrre informazioni e supportare decisioni.

Questi strumenti stanno diventando una sorta di memoria operativa dell'organizzazione. Se quella memoria viene alterata, il problema non consiste necessariamente nella perdita o nell'indisponibilità dei dati: le informazioni possono essere perfettamente accessibili e i sistemi tecnicamente funzionanti, mentre l'organizzazione inizia a prendere decisioni sulla base di una rappresentazione distorta della realtà.

Per un CEO, un CIO o un board emerge quindi una nuova domanda di governance: chi garantisce l'integrità della conoscenza utilizzata dall'AI e attraverso quali meccanismi questa integrità viene verificata nel tempo?

A livello tecnico entra in gioco il rischio del data poisoning e, in senso più ampio, di quello che potremmo definire **knowledge poisoning**. Un attaccante potrebbe non aver bisogno di compromettere direttamente il modello, ma potrebbe intervenire sui documenti, sulle informazioni o sulle fonti che alimentano il suo contesto.



Il sistema continuerebbe in questo caso a funzionare normalmente, senza necessariamente produrre anomalie infrastrutturali rilevabili dagli strumenti tradizionali di sicurezza, ma potrebbe arrivare sistematicamente a conclusioni errate. Nel mondo dell'AI, all'integrità del dato dobbiamo quindi aggiungere una dimensione ulteriore: **l'integrità semantica.**

Il linguaggio diventa una superficie di attacco

Esiste un altro cambiamento meno intuitivo, ma particolarmente significativo. Per quarant'anni abbiamo insegnato alle organizzazioni a non aprire allegati sospetti, verificare i link e proteggere password e credenziali; con l'AI, anche un documento apparentemente innocuo può diventare parte di un attacco.

Documenti, e-mail, siti Web e contenuti esterni non devono quindi essere considerati soltanto informazioni da acquisire, perché possono influenzare direttamente il comportamento di un sistema intelligente. Il confine tra comunicazione e comando diventa molto più sottile.

La **prompt injection** rappresenta uno degli esempi più evidenti di questo fenomeno. Nel software tradizionale abbiamo imparato, anche attraverso vulnerabilità come la SQL injection, quanto sia importante mantenere una separazione tra istruzioni e dati. Con i Large Language Model il problema ritorna sotto una forma diversa, perché una frase contenuta in un documento può essere contemporaneamente un dato da analizzare e un'istruzione interpretabile dal modello.

Il linguaggio naturale entra così a far parte della superficie di attacco, estendendo il problema della sicurezza a un territorio nel quale sintassi, semantica e contesto diventano elementi tecnicamente rilevanti.

L'AI industrializza l'ingegneria sociale

Esiste poi il lato offensivo dell'AI. Negli anni Novanta molte truffe digitali erano relativamente facili da riconoscere: e-mail scritte male, siti approssimativi, errori linguistici e richieste improbabili costituivano segnali che permettevano anche a un utente non particolarmente esperto di percepire il rischio.

L'AI sta progressivamente eliminando questi segnali e, soprattutto, sta modificando l'economia dell'attacco. Un cybercriminale non deve necessariamente essere un eccellente programmatore, perché può diventare soprattutto un efficace **orchestratore di strumenti intelligenti**, utilizzando l'AI per creare comunicazioni personalizzate, traduzioni, identità sintetiche, phishing mirato, voce artificiale e deepfake.

Il problema manageriale non è quindi soltanto l'aumento quantitativo degli attacchi, ma la crescita della loro qualità e della loro credibilità. Tecnologie di generazione linguistica, voice cloning, immagini e video sintetici possono essere combinate con informazioni pubblicamente disponibili o precedentemente sottratte all'organizzazione, rendendo scalabile una personalizzazione che in passato richiedeva un significativo lavoro manuale.

In termini economici, l'AI sta riducendo il costo marginale della sofisticazione dell'attacco, permettendo di portare tecniche precedentemente riservate a operazioni mirate verso una scala molto più ampia.

Il nuovo malware potrebbe essere una decisione

Questa è probabilmente una delle trasformazioni più importanti. Per decenni abbiamo cercato software malevolo, identificando virus, worm, trojan e ransomware attraverso le modifiche che producevano sui sistemi o attraverso comportamenti considerati anomali.

In un'organizzazione sempre più dipendente dall'AI potrebbe però non essere necessario compromettere direttamente un sistema. Potrebbe essere sufficiente influenzare una decisione.

Immaginiamo un sistema AI che supporta acquisti, credito, gestione delle risorse umane, investimenti o pianificazione strategica.

Se qualcuno riesce a modificare sistematicamente il contesto utilizzato dal sistema, può alterare le decisioni dell'organizzazione senza necessariamente violare l'infrastruttura sottostante. Gli utenti rimangono autenticati, i server operativi e le API perfettamente funzionanti, ma le conclusioni sulle quali vengono costruite le decisioni possono essere sbagliate.

Questo rende necessario ampliare il concetto stesso di incidente cyber e introduce quella che potremmo definire una forma di **attacco epistemico**, nella quale l'obiettivo non è compromettere ciò che il sistema fa, ma ciò che il sistema crede di sapere.

Data poisoning, manipolazione del contesto, retrieval poisoning, prompt injection e alterazione delle fonti possono diventare strumenti per modificare il processo decisionale senza necessariamente compromettere l'infrastruttura.

Se il malware tradizionale modifica il comportamento del computer, l'attacco epistemico modifica la rappresentazione della realtà sulla quale il sistema costruisce le proprie decisioni.

Dagli assistenti agli agenti: cambia la responsabilità

La differenza tra assistenti e agenti AI dovrebbe entrare nelle discussioni dei board che stanno valutando l'introduzione di sistemi agentici. Un assistente prevalentemente propone o produce un risultato che un essere umano può verificare, mentre un agente può acquisire informazioni, interpretare una situazione, selezionare uno strumento ed eseguire direttamente un'azione.

Finché un sistema prepara una risposta e una persona decide se inviarla, esiste un punto di controllo umano relativamente evidente. Quando invece il sistema può leggere una richiesta, decidere cosa fare, utilizzare uno strumento ed eseguire autonomamente l'azione, il modello di responsabilità cambia radicalmente.

Dobbiamo quindi definire non soltanto il principio di **human in the loop**, ma stabilire dove, quando e per quali decisioni l'essere umano debba effettivamente rimanere nel processo. Non tutte le decisioni hanno infatti lo stesso livello di rischio e, di conseguenza, non tutta l'autonomia dovrebbe essere governata nello stesso modo.

Dal punto di vista tecnico, possiamo rappresentare intuitivamente il rischio attraverso una relazione:
Autonomia × Accesso × Velocità × Scala = Impatto potenziale.

Un errore umano può produrre un'azione sbagliata, mentre un agente può ripetere la stessa azione migliaia di volte prima che qualcuno rilevi l'anomalia. Diventano quindi necessari limiti operativi, segregazione dei privilegi, monitoring comportamentale, approval gate, audit trail e meccanismi tecnici capaci di interrompere rapidamente l'autonomia quando il comportamento supera determinate soglie.

La cybersecurity diventa una responsabilità manageriale

Per questo considero rischioso trattare l'AI security esclusivamente come un nuovo capitolo della sicurezza informatica. Naturalmente abbiamo bisogno di specialisti di cybersecurity e dobbiamo continuare a proteggere modelli, API, infrastrutture, identità e dati, ma questo livello di protezione non è più sufficiente.

Il management deve definire quanta autonomia sia disposto a concedere, quali decisioni possano essere delegate, quali richiedano una validazione umana, quali fonti siano considerate affidabili e, soprattutto, chi risponda quando una decisione algoritmica produce conseguenze inattese.

Non siamo quindi più soltanto nel territorio dell'IT governance. Stiamo entrando progressivamente nella **governance dell'intelligenza organizzativa**, dove tecnologia, responsabilità, conoscenza e capacità decisionale diventano parti dello stesso problema.

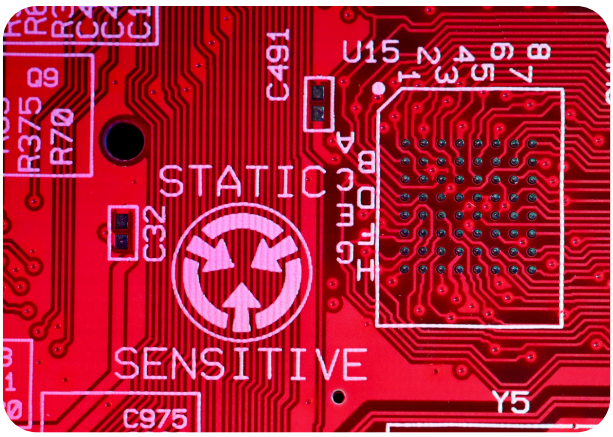
Da Zero Trust a Zero Assumption

Zero Trust ci ha insegnato il principio "**Never trust, always verify**", spostando la sicurezza dalla fiducia implicita alla verifica continua dell'identità e delle condizioni di accesso. L'AI potrebbe richiedere un ulteriore passo, che definirei **Zero Assumption**: non assumere che un output sia corretto perché il modello è sofisticato, che un agente stia operando correttamente perché è autenticato, che un'informazione sia affidabile perché proviene da un sistema interno o che un'azione sia sicura semplicemente perché tecnicamente autorizzata.

Soprattutto, non dovremmo assumere che una maggiore intelligenza del sistema corrisponda automaticamente a un maggiore controllo da parte dell'organizzazione.

Guardando agli ultimi quarant'anni emerge infatti una progressione precisa. Abbiamo iniziato proteggendo le macchine, abbiamo esteso la sicurezza alle reti e successivamente alle identità, ai dati e alle transazioni; oggi dobbiamo includere conoscenza e decisioni e, con la progressiva diffusione degli agenti, dovremo imparare a proteggere anche l'autonomia.

È probabilmente in quest'ultimo passaggio che cybersecurity e management finiranno definitivamente per incontrarsi, perché la domanda fondamentale non sarà più soltanto se un sistema AI sia tecnicamente sicuro, ma **quanto potere decisionale siamo disposti ad affidargli, quali confini intendiamo porre alla sua autonomia e come possiamo riprenderne il controllo quando qualcosa non va.**



AIUTO, È ARRIVATA LA NIS2!

CONSIGLI ZEN PER LE PMI

by NWN SOLUTIONS

CYBER ASSINTEL

www.assintel.it
info@assintel.it

Conf com Assintel



Maria fa ricorso alla sua proverbiale calma per assistere il cliente!



Ecco le risposte ! !!



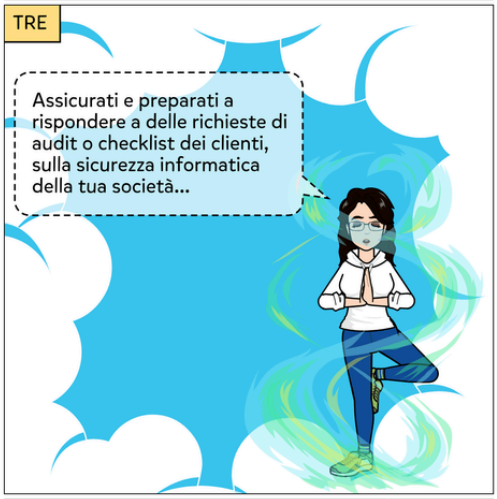
UNO



DUE



TRE







Maria torna in versione Office manager !!!



...è avvenuto il prodigio...





NWN solutions-Cybersecur ity, Privacy & Web Agency www.nwn.solutions

Chi è competente per usare l'AI? Formazione, standard ISO e assicurabilità del rischio nel nuovo quadro italiano



A cura di Daniela Mainenti

Per molto tempo la formazione sull'intelligenza artificiale è stata considerata dalle imprese come un'attività accessoria: un corso introduttivo, qualche ora dedicata al funzionamento degli strumenti generativi, un attestato da conservare nel fascicolo del personale. Il decreto legislativo 7 ottobre 2026, n. 179, pubblicato l'8 ottobre, cambia radicalmente questa prospettiva. Non perché trasformi ogni utilizzatore di un sistema di intelligenza artificiale in un tecnico, né perché introduca un obbligo generalizzato di certificazione ISO, che il decreto non prevede. Il cambiamento è più profondo: la competenza di chi utilizza l'AI entra nella struttura della governance del rischio. Da questo momento la domanda per l'impresa non è più soltanto se i propri lavoratori abbiano "fatto formazione", ma se la formazione sia adeguata rispetto al sistema utilizzato, alle funzioni esercitate e ai rischi che quell'utilizzo può generare.[1]

L'articolo 42 del decreto è, da questo punto di vista, particolarmente significativo. L'impiego di sistemi di intelligenza artificiale che incidono sull'organizzazione del lavoro, sui ritmi produttivi, sulle modalità di esecuzione della prestazione o sui processi decisionali rilevanti per la sicurezza deve essere considerato nell'ambito della valutazione dei rischi prevista dal decreto legislativo n. 81 del 2008. E i datori di lavoro devono assicurare ai lavoratori un'adeguata informazione e formazione sui rischi specifici connessi all'utilizzo dei sistemi di AI e sulle misure di prevenzione e protezione adottate.

Il legislatore compie così un passaggio decisivo: collega l'alfabetizzazione tecnologica alla gestione organizzativa del rischio. Non basta conoscere lo strumento; occorre comprenderne limiti, errori possibili, impatto sul lavoro e condizioni di utilizzo sicuro.[2]

Lo stesso impianto emerge nelle altre disposizioni del decreto. Per le Università e gli ITS Academy la formazione deve comprendere la capacità di interpretare criticamente gli output, conoscere limiti, rischi, distorsioni ed errori, comprendere le implicazioni giuridiche e di responsabilità, il ruolo della sorveglianza umana e i rischi di cybersicurezza. Per le professioni regolamentate, l'articolo 47 impone l'inserimento di percorsi di alfabetizzazione e formazione all'uso dei sistemi di AI nella formazione iniziale e continua, con contenuti tecnici, giuridici e deontologici e con un monte ore minimo. È difficile non cogliere la direzione complessiva: la competenza digitale cessa di essere una qualità genericamente desiderabile e diventa una componente verificabile della corretta organizzazione.[3]

Per le imprese ICT questo passaggio è particolarmente importante. Un *system integrator*, una *software house* o un *provider* non possono più ragionare soltanto in termini di funzionalità del prodotto. L'adozione dell'AI genera una catena di responsabilità che coinvolge chi sviluppa, chi configura, chi integra, chi acquista e chi utilizza il



sistema. La formazione diventa il punto nel quale tecnologia e organizzazione si incontrano. Un sistema perfettamente configurato può produrre un rischio elevato se viene affidato a persone che non ne comprendono i limiti; allo stesso modo, un lavoratore genericamente "formato sull'AI" può non essere competente per utilizzare uno specifico sistema in un contesto ad alto impatto. È quindi necessario passare *dall'AI literacy* alla competence assurance: non soltanto conoscenza generale dell'intelligenza artificiale, ma capacità dimostrabile di utilizzare responsabilmente determinati strumenti nell'ambito di determinati ruoli.

È qui che il nuovo quadro normativo incontra gli standard di gestione. La ISO/IEC 42001:2023, recepita nel 2026 anche nel sistema europeo e nazionale come EN ISO/IEC 42001 e UNI CEI EN ISO/IEC 42001, definisce i requisiti per istituire, attuare, mantenere e migliorare continuamente un Artificial Intelligence Management System. Il suo punto 7.2 sulla competenza è illuminante: l'organizzazione deve determinare le competenze necessarie delle persone il cui lavoro incide sulle prestazioni del sistema di gestione dell'AI, assicurarsi che tali persone siano competenti sulla base di istruzione, formazione o esperienza adeguate, intervenire sui gap e valutare l'efficacia delle azioni intraprese. Soprattutto, deve essere disponibile informazione documentata quale evidenza della competenza. È una differenza sostanziale rispetto alla logica dell'attestato: partecipare a un corso dimostra la presenza; non necessariamente dimostra la competenza.[4]

Il decreto n. 179 e la ISO/IEC 42001 non vanno sovrapposti. Il primo stabilisce obblighi giuridici; la seconda è uno standard volontario di sistema di gestione. Sarebbe quindi inesatto affermare che il decreto imponga alle imprese la certificazione ISO 42001. Ma è altrettanto riduttivo considerarli mondi separati. Il legislatore chiede formazione adeguata ai rischi; lo standard offre un metodo organizzativo per determinare le competenze necessarie, colmare i divari, verificarne l'efficacia e conservarne l'evidenza. La conformità normativa indica il "che cosa"; il sistema di gestione può fornire uno dei possibili metodi per dimostrare il "come".

Questo punto diventa ancora più interessante se lo si osserva dalla prospettiva assicurativa. Anche qui occorre evitare semplificazioni: il decreto n. 179 non introduce un obbligo di assicurazione per l'utilizzo dell'AI e non stabilisce che una polizza debba essere subordinata alla certificazione ISO/IEC 42001. Tuttavia il mercato assicurativo opera attraverso la valutazione del rischio e la qualità della governance è inevitabilmente una delle informazioni che possono incidere sull'underwriting, sulle condizioni contrattuali e, in caso di sinistro, sulla ricostruzione di quanto l'organizzazione aveva dichiarato e concretamente implementato. Nel settore cyber questa relazione tra standard di gestione e assicurazione è già formalizzata dalla ISO/IEC 27102, che considera il sistema di gestione della sicurezza delle informazioni conforme alla ISO/IEC 27001 come una possibile base informativa nei rapporti tra organizzazione e assicuratore, dall'assunzione del rischio al monitoraggio fino alla gestione del claim.[5]

L'intelligenza artificiale potrebbe seguire una traiettoria analoga. Non perché esista oggi un automatismo "ISO 42001 uguale premio assicurativo più basso", che sarebbe scorretto sostenere, ma perché un'organizzazione capace di documentare inventario dei sistemi AI, valutazione dei rischi, responsabilità, supervisione umana, competenze, formazione, controlli e riesami offre all'assicuratore un rischio più leggibile. E nel mercato assicurativo un rischio leggibile è, per definizione, più valutabile di un rischio opaco. La formazione assume allora un valore che supera il rapporto datore-lavoratore: diventa un elemento della rappresentazione del rischio aziendale verso terzi.

Anche il settore assicurativo, del resto, si sta muovendo nella stessa direzione. EIOPA ha chiarito nel 2025 che l'impiego dell'AI nelle assicurazioni deve essere governato secondo un approccio proporzionato al rischio, considerando *data governance, record keeping, fairness, cybersecurity, explainability e human oversight.* È significativo che l'AI governance venga trattata come un insieme di controlli organizzativi e documentali, non come una semplice caratteristica del software. Questo approccio rende sempre meno plausibile una separazione netta tra rischio tecnologico, rischio umano e rischio organizzativo.[6]

La conseguenza pratica per le imprese è importante. Un programma serio di formazione AI dovrebbe partire dalla mappatura dei sistemi effettivamente utilizzati e dei ruoli che interagiscono con essi. Un addetto HR che utilizza un sistema per lo screening delle candidature non ha lo stesso fabbisogno formativo di un programmatore che integra un modello in un prodotto, di un dirigente che convalida decisioni supportate dall'AI o di un operatore che utilizza un sistema in un processo rilevante per la sicurezza. La formazione deve quindi essere proporzionata al ruolo e al rischio, prevedere una verifica dell'apprendimento e lasciare un'evidenza documentale. E deve essere aggiornata quando cambiano il sistema, la sua versione, il contesto di utilizzo o il quadro normativo.

Il vero salto culturale consiste proprio qui. Per anni abbiamo misurato la formazione in ore. Nell'economia dell'intelligenza artificiale dovremo imparare a misurarla anche in competenze. Quattro

ore di corso possono essere sufficienti per un utilizzatore occasionale di uno strumento a basso impatto e del tutto insufficienti per chi esercita la sorveglianza umana su un sistema ad alto rischio. Il parametro non può essere soltanto quantitativo. Deve diventare funzionale: quale capacità deve possedere quella persona per esercitare correttamente il ruolo che l'organizzazione le assegna?

Da questa prospettiva cambia anche il significato della documentazione. Registri, test finali, matrici delle competenze, programmi, aggiornamenti e abilitazioni non dovrebbero essere considerati burocrazia da produrre dopo la formazione. Sono l'infrastruttura attraverso la quale l'impresa può dimostrare di avere governato il rischio umano connesso all'AI. La differenza è decisiva anche quando accade qualcosa. Se un output errato produce un danno, se un lavoratore utilizza impropriamente un sistema o se una decisione assistita dall'AI viene contestata, non basterà esibire un attestato. Bisognerà poter ricostruire quale formazione fosse stata prevista per quel ruolo, quale competenza fosse richiesta, se fosse stata effettivamente verificata e quali istruzioni operative fossero state impartite.

È in questo spazio che conformità normativa, standardizzazione e assicurazione cominciano a convergere. Non perché siano la stessa cosa, ma perché pongono progressivamente la medesima domanda all'organizzazione: il rischio è stato identificato, governato e documentato? Il decreto dell'ottobre 2026 rende la formazione un tassello esplicito della prevenzione dei rischi nell'impiego dell'AI; la ISO/IEC 42001 colloca competenza ed evidenza documentata dentro un sistema di gestione; il mondo assicurativo ha interesse a distinguere tra organizzazioni che dichiarano controlli e organizzazioni capaci di dimostrarne l'effettiva esistenza.

Per il settore ICT questa convergenza rappresenta un'opportunità industriale, non soltanto un nuovo adempimento. Le imprese che sapranno progettare soluzioni accompagnate da modelli di formazione per ruolo, procedure di supervisione, evidenze di competenza e documentazione compatibile con i sistemi di gestione potranno offrire qualcosa di più di una tecnologia: potranno offrire una tecnologia governabile. Ed è probabile che la governabilità diventi progressivamente una delle caratteristiche attraverso cui clienti, auditor, partner e assicuratori valuteranno l'affidabilità di un fornitore.

La sfida, dunque, non è moltiplicare corsi sull'intelligenza artificiale. È evitare che la formazione diventi il nuovo "checkbox" della compliance digitale. L'attestato dimostra che una persona ha partecipato. La conformità richiede di poter dimostrare che l'organizzazione ha compreso quali competenze fossero necessarie, le ha costruite, ne ha verificato l'efficacia e le mantiene nel tempo. È questo il passaggio *dall'AI literacy* alla competenza verificabile. E potrebbe essere uno dei cambiamenti più importanti introdotti, quasi silenziosamente, dal nuovo quadro italiano: nell'era dell'intelligenza artificiale non sarà sufficiente dire che le persone sono state formate. Bisognerà essere in grado di provare che erano davvero preparate a usare il sistema che l'impresa ha deciso di affidare loro.

Note:

[1] D.lgs. 7 ottobre 2026, n. 179, Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2024/1689, pubblicato in G.U. n. 234 dell'8 ottobre 2026, in vigore dal 23 ottobre 2026.

[2] D.lgs. 7 ottobre 2026, n. 179, art. 42, in materia di utilizzo dei sistemi di intelligenza artificiale nei luoghi di lavoro, valutazione dei rischi e adeguata informazione e formazione dei lavoratori.

[3]D.lgs. 7 ottobre 2026, n. 179, Capo III e, per le professioni regolamentate, art. 47: il decreto inserisce l'alfabetizzazione e la formazione all'uso dei sistemi di IA nei percorsi iniziali e di formazione continua, secondo un'impostazione che integra profili tecnici, giuridici e deontologici.

[4]ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system, § 7.2 (Competence): l'organizzazione deve determinare le competenze necessarie, assicurare che le persone siano competenti sulla base di istruzione, formazione o esperienza, valutare l'efficacia delle azioni adottate e rendere disponibile informazione documentata quale evidenza della competenza.

[5]ISO/IEC 27102:2019, Information security, cybersecurity and privacy protection — Guidelines for applying ISO/IEC 27001 and related standards in support of cyber insurance. Lo standard contempla espressamente l'utilizzo dell'ISMS e lo scambio di informazioni tra assicurato e assicuratore a supporto di underwriting, monitoring e claims. È in corso di sviluppo una seconda edizione destinata a sostituire quella del 2019.

[6] EIOPA, Opinion on Artificial Intelligence Governance and Risk Management, 6 agosto 2025. L'Opinion adotta un approccio risk-based e proporzionato e richiama, tra gli elementi della governance dell'IA nel settore assicurativo, data governance, record-keeping, fairness, cybersecurity, explainability e human oversight.



AI Act in Italia: la sfida non è solo regolare l'innovazione, ma farla accadere



A cura di Fabrizio Milano D'Aragona

L'attuazione italiana dell'AI Act rappresenta un passaggio decisivo per trasformare la regolazione dell'intelligenza artificiale in uno strumento di crescita.
La vera sfida consiste nel coniugare tutela, innovazione e proporzionalità, evitando che gli obblighi normativi rallentino PMI e filiera digitale. Regole chiare, formazione e accompagnamento saranno determinanti per rendere l'ecosistema italiano più competitivo.

Con l'approvazione in esame preliminare dei primi due schemi di decreto legislativo in materia di intelligenza artificiale, il Governo ha iniziato a tradurre l'AI Act europeo in un'infrastruttura nazionale fatta di autorità, procedure, formazione, sandbox, vigilanza e sanzioni. È un passaggio importante, perché sposta il tema dell'IA dal piano dei principi a quello dell'organizzazione concreta del mercato.

I decreti indicano che AgID e ACN diventano i due riferimenti principali dell'attuazione nazionale, rispettivamente per la notifica e per la vigilanza del mercato, con un ruolo di raccordo rispetto al sistema europeo e con il coinvolgimento delle autorità settoriali competenti. Allo stesso tempo, vengono introdotti strumenti come lo Spazio di sperimentazione italiano per l'IA, misure sulla formazione, regole per l'uso dell'intelligenza artificiale nel lavoro, un quadro sanzionatorio e alcune tutele connesse a dati, algoritmi e segreti industriali.

Per Assintel, questo è il punto di partenza corretto: una tecnologia così pervasiva richiede una governance riconoscibile e un'applicazione coerente. Ma la vera questione, ora, non è più se regolare l'intelligenza artificiale. È come farlo senza rallentare l'adozione, senza penalizzare le imprese più piccole e senza trasformare la compliance in un nuovo ostacolo burocratico.

L'attuazione italiana dell'AI Act va letta da due prospettive complementari: quella della domanda, cioè delle imprese e delle organizzazioni che useranno sistemi di IA, e quella dell'offerta, cioè dell'ecosistema digitale che quei sistemi li sviluppa, li integra, li adatta e li porta sul mercato.

Dal lato della domanda, la prima distinzione fondamentale è tra grandi aziende e PMI.

Le grandi imprese, soprattutto nei settori regolati o ad alta intensità di dati - finanza, assicurazioni, sanità, energia, telecomunicazioni, industria, pubblica amministrazione - dispongono già di funzioni legali, compliance, risk management, procurement, cybersecurity e audit. Per loro l'AI Act rappresenta certamente un impegno significativo, ma si innesta su processi già esistenti: classificazione del rischio, controllo dei fornitori, valutazione degli impatti, sicurezza, accountability e monitoraggio.

I decreti rafforzano questa direzione. Il tema del controllo umano, ad esempio, diventa



particolarmente rilevante nel lavoro: quando l'IA incide su organizzazione, mansioni, ritmi, sicurezza o valutazioni, la decisione finale non può essere abbandonata a un automatismo. Deve restare in capo a una persona fisica, con potere effettivo e autonomo, e deve essere possibile fornire una motivazione intelligibile. Questo richiede alle grandi organizzazioni di costruire una vera governance interna dell'IA.

Per le PMI, invece, la questione è diversa e più delicata.

La piccola e media impresa italiana non può affrontare l'AI Act con la stessa struttura, gli stessi budget e gli stessi livelli di formalizzazione di una multinazionale. Eppure è proprio nelle PMI che l'intelligenza artificiale può produrre uno degli impatti più significativi: automazione di processi amministrativi, supporto commerciale, analisi dei dati, customer care, manutenzione predittiva, marketing, gestione documentale, cybersecurity, produttività individuale.

Il rischio è che la regolazione venga percepita come qualcosa di distante, complesso, "da grandi aziende". Se questo accadesse, molte PMI finirebbero per rinviare l'adozione dell'IA, oppure per utilizzarla in modo inconsapevole, senza strumenti adeguati di valutazione e controllo. Sarebbe il risultato peggiore: meno innovazione e meno sicurezza.

Per questo il principio di proporzionalità deve essere il criterio guida dell'attuazione. Gli obblighi devono essere commisurati al ruolo effettivo dell'impresa nella catena del valore, al livello di rischio del sistema utilizzato e alla sua capacità reale di incidere sulla tecnologia. Un conto è sviluppare un modello di IA general purpose; un altro è integrare una soluzione di terze parti in un processo aziendale; un altro ancora è usare strumenti già disponibili sul mercato per aumentare la produttività interna.

Alle PMI servono linee guida semplici, checklist operative, esempi concreti, percorsi di autovalutazione, template documentali, formazione accessibile e un'interlocuzione chiara con le autorità.

In questo senso, lo Spazio di sperimentazione italiano per l'IA può diventare uno degli strumenti più importanti previsti dai decreti. Se sarà realmente accessibile a PMI e startup, con procedure leggere, tempi certi e accompagnamento tecnico, potrà aiutare imprese e sviluppatori a testare sistemi innovativi in un ambiente controllato, riducendo l'incertezza regolatoria prima dell'ingresso sul mercato. Se invece resterà uno strumento complesso o riservato di fatto agli operatori più strutturati, rischierà di perdere la sua funzione.

La sandbox deve fungere da acceleratore di mercato e non essere solo una vetrina istituzionale.

C'è poi il lato dell'offerta, che riguarda direttamente il mondo rappresentato da Assintel: software house, system integrator, startup, società di consulenza digitale, provider tecnologici, sviluppatori di soluzioni verticali e imprese innovative.

Per questo ecosistema, l'attuazione dell'AI Act può essere una grande opportunità. La domanda di IA affidabile, sicura, documentata e conforme crescerà. Le aziende avranno bisogno di partner capaci non solo di sviluppare tecnologia, ma di accompagnarle nella scelta, nell'integrazione, nella valutazione del rischio, nella formazione degli utenti e nel monitoraggio delle soluzioni adottate.

La compliance, se interpretata bene, può diventare un mercato che esprime qualità del servizio, differenziazione competitiva e fiducia.

Allo stesso tempo, però, l'offerta digitale italiana non deve essere schiacciata da oneri sproporzionati. Molte imprese innovative costruiscono applicazioni, verticalizzazioni, interfacce, agenti, workflow e servizi basati su tecnologie esistenti. È quindi essenziale che l'attuazione nazionale distingua chiaramente tra i diversi ruoli: provider, deployer, distributori, importatori, integratori, utilizzatori professionali.



Una classificazione incerta genererebbe prudenza eccessiva, costi inutili e rallentamento del mercato. Una classificazione chiara, invece, consentirebbe alle imprese digitali italiane di diventare abilitatrici dell'adozione responsabile dell'IA in tutti i settori produttivi.

Anche il tema delle sanzioni va letto in questa prospettiva. È giusto che esista un sistema di enforcement, soprattutto per pratiche vietate, violazioni gravi, usi discriminatori o mancanza di misure di sicurezza. Ma nella prima fase applicativa sarà decisivo distinguere tra condotte dolose o gravemente negligenti e situazioni in cui imprese, soprattutto di minore dimensione, si trovano davanti a obblighi nuovi, tecnicamente complessi e ancora in evoluzione. L'enforcement deve accompagnare il mercato verso comportamenti corretti ed evitare di generare paura preventiva dell'innovazione.

Un altro punto rilevante dei decreti riguarda la tutela del know-how. Il riferimento a dati, algoritmi e metodi matematici come informazioni potenzialmente tutelabili come segreti commerciali è importante, perché l'ecosistema dell'IA vive anche di investimenti, proprietà intellettuale, modelli, dataset, metodologie e competenze. La trasparenza è essenziale, ma deve convivere con la protezione degli asset industriali, soprattutto per le imprese che innovano.

Infine, la formazione. I decreti dedicano attenzione all'alfabetizzazione e alle competenze, dalla scuola al lavoro, dalla pubblica amministrazione alle professioni. È un passaggio fondamentale. L'AI literacy prevista dal quadro europeo non può limitarsi agli specialisti. Deve arrivare nei consigli di amministrazione, nei team HR, nei reparti marketing e vendite, negli uffici acquisti, nei responsabili IT, nei consulenti e nelle funzioni operative.

Il punto politico e industriale è questo: l'Italia non deve limitarsi ad attuare l'AI Act. Deve usarlo per costruire un ecosistema nazionale dell'intelligenza artificiale più forte, più consapevole e più competitivo.

Per riuscirci servono tre condizioni.

La prima è certezza applicativa: imprese e fornitori devono sapere cosa fare, quando farlo, con quali documenti e davanti a quali autorità.

La seconda è proporzionalità: la tutela dei diritti e della sicurezza non può tradursi in un modello unico di compliance, identico per una big tech, una banca, una PMI manifatturiera o una startup software.



La terza è dialogo strutturato con il mercato: le associazioni dell'ICT devono essere coinvolte stabilmente nella costruzione di linee guida, strumenti operativi e percorsi di accompagnamento.

L'intelligenza artificiale non sarà competitiva se sarà lasciata senza regole. Ma non sarà davvero europea, né italiana, se le regole renderanno troppo difficile innovare.

La sfida dell'attuazione italiana dell'AI Act è tutta qui: trasformare una normativa complessa in un'infrastruttura di fiducia. Una fiducia che protegga cittadini e imprese, ma che allo stesso tempo permetta al tessuto produttivo italiano — grandi aziende, PMI e filiera digitale — di adottare, sviluppare e portare sul mercato soluzioni di IA con responsabilità e ambizione.

Per Assintel, questa è la direzione: regole chiare, applicazione proporzionata, centralità delle PMI e valorizzazione dell'offerta digitale italiana. Non per frenare l'innovazione, ma per renderla possibile su basi più solide.

Il digitale non è etereo

A cura di Mauro Munzi



Settantotto gigawatt di richieste sulla rete elettrica italiana, un mercato del cloud per il 70 per cento in mano a tre imprese, milioni di persone che lavorano per l'intelligenza artificiale senza essere viste: quanto costa davvero il digitale, e che cosa può farci un'impresa.

Per trent'anni la società dell'informazione si è raccontata come una storia di alleggerimento. I bit avrebbero sostituito gli atomi, e il passaggio dall'industria ai servizi, poi all'economia della conoscenza, avrebbe ridotto il peso delle attività umane sul pianeta. Il cloud, la «nuvola» dove finiscono i nostri file e le nostre applicazioni, prometteva fin dal nome un'industria senza zavorra. Accanto alla promessa ecologica ne correva una sociale: la rete avrebbe aperto a tutti l'accesso alla conoscenza, ridotto le disuguaglianze e distribuito il potere fra gli utenti. Sono state smentite tutte e due. Il digitale consuma energia e materia in scala industriale, ha concentrato il potere economico in poche mani come nessuna industria aveva fatto prima, e funziona grazie al lavoro di milioni di persone che nessuno vede.

Nel discorso delle imprese e delle istituzioni la sostenibilità digitale, il nome corrente di questa contraddizione, significa quasi sempre Green IT, cioè l'informatica a basso consumo: data center più efficienti, server che durano più a lungo, rifiuti elettronici smaltiti a norma.

È una parte della questione. L'altra parte riguarda il lavoro che fa funzionare il digitale, la proprietà delle sue infrastrutture, la decisione su che cosa si calcola, per conto di chi e a beneficio di chi. Ridotta all'energia, la sostenibilità digitale lascia alle grandi piattaforme il solo terreno su cui possono esibire progressi misurabili, l'efficienza, e mette fuori discussione tutto il resto.

Giovanna Sissa, in «Le emissioni segrete» (il Mulino, 2024), ha descritto il meccanismo che rende invisibile il costo: la familiarità quotidiana con gli oggetti digitali ci rende insensibili al loro impatto. Usiamo lo smartphone, cerchiamo sul web, interroghiamo un assistente virtuale senza chiederci quale apparato fisico risponda alla domanda. Il costo esiste, si misura e cresce, e lo stesso vale per i costi che non si misurano in chilowattora: quelli sociali, politici, economici.

*

L'intelligenza artificiale si presenta come automatica, autonoma, quasi ineffabile. Dietro ogni modello lavorano persone che etichettano immagini, moderano contenuti, verificano risposte e correggono gli errori del sistema, pagate a compito attraverso piattaforme come Amazon Mechanical Turk, senza contratto stabile, senza tutele e spesso senza sapere per quale committente stiano lavorando. Mary Gray e Siddharth Suri, nel libro che



nel 2019 ha dato a questo lavoro il nome di ghost work (lavoro fantasma), hanno stimato che circa l'8 per cento degli americani lo abbia svolto almeno una volta. Nei paesi del Sud del mondo, dove le piattaforme spostano i micro-compiti perché il lavoro costa meno, la quota è certamente più alta.

Paola Tubaro, Antonio Casilli e Marion Coville, in un articolo del 2020 su «Big Data & Society», hanno distinto tre funzioni del lavoratore di piattaforma nell'industria dell'intelligenza artificiale, il trainer, il verifier e l'imitator: l'addestramento del modello, il controllo dei suoi risultati, l'imitazione del modello stesso. Il lavoro umano non precede il sistema e poi sparisce: lo accompagna in permanenza, e le imprese che vendono il sistema hanno ogni interesse a nasconderlo. Clément Le Ludec, Maxime Cornet e lo stesso Casilli hanno seguito nel 2023 le catene di esternalizzazione dell'annotazione dei dati fra la Francia e il Madagascar, e hanno documentato come riproducano, aggiornate, le strutture del lavoro coloniale. Nel 2024 l'Organizzazione internazionale del lavoro ha dedicato a questi lavoratori un documento di indirizzo, segnalando che la crescita dei sistemi di apprendimento automatico poggia su una forza lavoro globale frammentata, sottopagata e priva di tutele.

I moderatori di contenuti decidono, immagine dopo immagine, se una scena di violenza, di abuso o di morte va rimossa, e sviluppano disturbi da stress post-traumatico con una frequenza allarmante. Lavorano spesso da casa, senza supporto psicologico, per compensi irrisori. La pulizia del feed che scorriamo sullo schermo ha questo prezzo, e non compare in nessun bilancio di sostenibilità.

In Italia l'indagine Inapp-Plus sui lavoratori delle piattaforme digitali, condotta nel 2020 e nel 2021 dall'Istituto nazionale per l'analisi delle politiche pubbliche, ha trovato che il 26 per cento di loro non gestisce direttamente l'account con cui accede al lavoro, e che nel 13 per cento dei casi il compenso passa per un soggetto terzo. È caporalato digitale: un intermediario incassa il pagamento, ne trattiene una parte e subappalta un lavoro che la piattaforma aveva già esternalizzato, oppure cede l'account a un lavoratore che non potrebbe aprirne uno a proprio nome. Un'impresa che adotta un servizio di intelligenza artificiale compra anche questo lavoro, e nella propria contabilità non ne trova traccia.

*

Quattro o cinque imprese, tutte statunitensi o cinesi, controllano oggi i motori di ricerca, i sistemi operativi, i servizi cloud, i social network, il commercio online e le piattaforme di intelligenza artificiale. Il Digital Markets Act, il regolamento europeo del 2022 sui mercati digitali, le chiama gatekeeper, guardiani dell'accesso, perché decidono quali imprese entrano nel mercato e a quali condizioni. Il loro potere si estende lungo tutta la catena: detengono i data center e i cavi sottomarini, i sistemi operativi, i negozi da cui si scaricano le applicazioni, i sistemi di pagamento. Uscire da uno di questi sistemi, per un'impresa, significa ricostruire da capo il proprio modo di lavorare, ed è per questo che le dipendenze durano.

Nel 2024 il mercato europeo dei servizi cloud valeva 61 miliardi di euro. La quota dei fornitori europei è scesa dal 29 per cento del 2017 al 15, e lì si è fermata; Amazon, Microsoft e Google ne detengono insieme il 70 per cento, e in Europa investono intorno ai 10 miliardi a trimestre. Quel mercato non ha selezionato i migliori. Per quindici anni le amministrazioni pubbliche europee hanno comprato servizi dagli hyperscaler (i fornitori che gestiscono data center propri su scala planetaria), e hanno finanziato con la propria domanda lo squilibrio che oggi denunciano. Quando un ente europeo acquista servizi cloud da un fornitore americano privo di certificazioni ambientali e sociali, e la fornitura risulta in regola perché lo è il rivenditore europeo che fa da tramite, la conformità alle norme è una finzione giuridica.

A un parlamentare francese che chiedeva se Microsoft potesse garantire la riservatezza dei dati dei cittadini francesi conservati su server in Francia, l'azienda ha risposto di no: il luogo dei server non conta, finché li controlla un'impresa americana ricadono sotto il Cloud Act, la legge statunitense che obbliga le imprese di quel paese a consegnare alle autorità i dati richiesti, ovunque siano conservati. Ecosia e Qwant, due motori di ricerca europei, hanno scritto ai ventisette capi di governo dell'Unione offrendo di costruire indici di ricerca nazionali per una cifra dell'ordine dei 50 milioni. L'indice esiste, si chiama Staan, funziona dall'agosto 2025 in francese, inglese e tedesco, e per ora Ecosia lo usa per i propri utenti soltanto in Francia.

Nel 2013 il legislatore francese ha stabilito che l'istruzione superiore usa in via prioritaria il software libero, mentre per la scuola dell'obbligo si è limitato a chiedere che si tenga conto dell'offerta libera dove esiste. Due anni dopo il ministero firmava con Microsoft un accordo da 13 milioni che apriva Office 365 a tutti gli istituti del piano nazionale per il digitale. Nel 2022, rispondendo a un'interrogazione parlamentare, lo stesso ministero riconosceva che la gratuità serve a indurre gli utenti abituati a quegli strumenti a sottoscrivere poi la versione a pagamento. Nel marzo 2025 l'accordo è stato rinnovato fino al 2029, per un massimo di 152 milioni. Una scuola che lavora così forma gli studenti all'uso di un prodotto e insieme prepara i clienti di un fornitore.

I trattori John Deere montano un software proprietario che impedisce la riparazione ai meccanici esterni: possono intervenire solo i concessionari autorizzati, e l'agricoltore che ha pagato la macchina ne detiene di fatto una licenza d'uso revocabile. I sistemi di posizionamento satellitare che lo aiutano a programmare semina e raccolto trasmettono intanto al costruttore i dati sull'attività della sua azienda. Pietro Jarre, che dal 1990 ha contribuito a costruire un gruppo di società di ingegneria arrivato a 10.000 dipendenti in 35 paesi, e che nel 2017 ha fondato con altri l'associazione Sloweb, ne ricava una conseguenza che vale per ogni impresa: «La proprietà si trasforma in abbonamento, e l'autonomia in dipendenza permanente». La subordinazione delle imprese manifatturiere e di servizi alle grandi piattaforme ricalca, per Jarre, la struttura feudale: pochi signori detengono gli strumenti che producono i dati, e tutti gli altri, come vassalli, cedono gratis o quasi la merce più preziosa del mercato, i dati dei produttori e dei consumatori.

Yanis Varoufakis, l'economista che è stato ministro delle Finanze greco, porta la stessa analogia fino a sostenere, in «Tecnofeudalesimo» (2023), che il capitalismo sia morto e che la rendita delle piattaforme cloud abbia sostituito il profitto come forma dominante di estrazione del valore. La tesi chiede una verifica empirica che ancora manca, ma coglie un punto: le grandi piattaforme non si comportano come imprese in concorrenza, si comportano come infrastrutture obbligate che dettano le condizioni a tutti gli altri. Un commerciante che vende online passa per Amazon e paga la commissione, un sito che vuole essere trovato passa per Google. Quando OpenAI annuncia investimenti per 1.000 miliardi di dollari in infrastrutture di calcolo, una cifra vicina alla metà del prodotto interno lordo italiano, orienta la direzione tecnologica del pianeta.

Per questo conviene parlare di indipendenza digitale piuttosto che di sovranità digitale, che è il termine più usato nel dibattito europeo. La sovranità evoca la proprietà formale dell'infrastruttura e dei dati. Ma un'impresa può possedere i propri dati, conservati su server altrui e lavorati con applicazioni che girano sul cloud di un terzo, senza poterne fare alcun uso autonomo. L'indipendenza indica la capacità effettiva di elaborare, analizzare e valorizzare il proprio patrimonio digitale senza un intermediario che ne condizioni l'accesso, la portabilità e il funzionamento. Le grandi piattaforme erodono proprio questa capacità, e lo fanno senza toccare la proprietà, con dipendenze funzionali difficili da sciogliere. Per un'impresa la conseguenza è concreta: architetture che si possano smontare, clausole di portabilità nei contratti, standard aperti dove esistono.

*

Il digitale ha un corpo. Ogni bit esiste perché esiste un supporto fisico che lo genera e lo conserva, un chip, una cella di memoria, un cavo in fibra ottica, un satellite, e ogni operazione di calcolo consuma energia. In Italia la potenza elettrica assorbita dai data center è oggi intorno a mezzo gigawatt, su 120 gigawatt installati nel paese. Alla fine di gennaio 2026 Terna, la società che gestisce la rete di trasmissione nazionale, aveva ricevuto 449 richieste di connessione per data center, per un totale di 78,79 gigawatt; erano 30 alla fine del 2024 e 69 un anno dopo. Una richiesta di connessione non è un'autorizzazione e non prova che il terreno sia stato comprato o che il finanziamento esista: è una prenotazione sulla rete che costa quasi niente. Le stime di quanto verrà davvero costruito fra il 2028 e il 2030 stanno fra i 2 e i 3 gigawatt.

Fra la potenza prenotata e quella che verrà costruita corre un fattore trenta, e quella distanza è il fenomeno da spiegare. Un operatore che deposita una domanda di allaccio prenota un posto in coda e scarica sul gestore della rete il costo di pianificare per una domanda che in gran parte non arriverà. Anche alla stima prudente, la potenza dedicata al calcolo si moltiplica fra le quattro e le sei volte in cinque anni, in un paese che negli stessi cinque anni deve decarbonizzare tutto il resto. E le richieste sul tavolo di Terna valgono, sulla carta, quanto l'intero piano italiano per le rinnovabili, che prevede di installare fra i 70 e gli 80 gigawatt entro il 2030. Nessuno costruirà tutti quei data center, ma nelle amministrazioni e nel dibattito pubblico c'è chi ragiona come se dovesse.



Su scala mondiale l'Agenzia internazionale per l'energia colloca i consumi elettrici dei data center a 485 terawattora nel 2025 e a 950 nel 2030, intorno al 3 per cento della domanda elettrica del pianeta. Le stime sull'impronta climatica del digitale nel suo insieme oscillano fra il 2 e il 4 per cento delle emissioni globali, a seconda del perimetro scelto e di come si contano le emissioni incorporate nei dispositivi: la sintesi di Freitag e colleghi, passata al vaglio della revisione paritaria, dà l'1,8-2,8 per cento per il 2020, che sale al 2,1-3,9 se si correggono le filiere troncate nei calcoli. È il peso dell'aviazione civile. L'aviazione però è sottoposta a un controllo pubblico intenso e a una pressione normativa crescente, mentre l'impatto del digitale resta coperto dalla retorica della leggerezza e, da qualche anno, dalla richiesta delle piattaforme di abolire ogni regola in nome del progresso e della libertà d'impresa.

Quando si misura l'impronta carbonica dell'informatica dentro una singola azienda manifatturiera si trovano quote largamente inferiori all'uno per cento, e la differenza con le cifre mondiali è istruttiva. La forbice si spiega con lo Scope 3, la categoria che raccoglie le emissioni indirette della catena di fornitura e dell'uso dei prodotti, fuori dagli impianti dell'impresa: le emissioni incorporate nell'hardware, nei servizi cloud e nell'intera catena digitalizzata sfuggono al calcolo dell'impresa che li ha ordinati. Secondo Axenbeck e colleghi, in uno studio pubblicato nel gennaio 2026 su dati del 2021, il 42 per cento delle emissioni incorporate nella domanda digitale finisce dentro le catene del valore di industrie che digitali non sono, e fra il 77 e l'87 per cento delle emissioni della produzione digitale sta a monte, nello Scope 3. Un'azienda di commercio elettronico che genera emissioni nei dispositivi dei suoi clienti non le contabilizza come proprie.

Patterson e colleghi hanno calcolato che l'addestramento di GPT-3, uno dei grandi modelli linguistici di OpenAI, ha prodotto circa 550 tonnellate di anidride carbonica equivalente, quanto un'automobile media che percorresse più di 3 milioni di chilometri. A pesare di più nel tempo è però l'uso quotidiano, perché ogni domanda posta a ChatGPT consuma molta più energia di una ricerca tradizionale su Google. Kate Crawford, in «Né intelligente né artificiale» (il Mulino, 2021), propone di guardare all'intelligenza artificiale come a un apparato che mette insieme miniere nel Sud del mondo, consumi energetici concentrati in pochi territori, istituzioni e governi, lavoro sottopagato e reso invisibile, e di cercarne i costi dove la retorica li nasconde.

Guillaume Pitron, in «La guerra dei metalli rari» e in «Inferno digitale», ha seguito la catena dell'estrazione che alimenta l'industria digitale: cobalto dalla Repubblica Democratica del Congo, litio dal triangolo andino fra Cile, Argentina e Bolivia, terre rare dalla Cina, con una geografia che ricalca quella dello sfruttamento coloniale. La Cina controlla circa il 69 per cento dell'estrazione mondiale di terre rare e oltre il 90 per cento della separazione e raffinazione dei metalli che servono ai magneti. L'europio, una terra rara usata nei fosfori rossi degli schermi, si produce quasi soltanto lì; nell'ottobre 2025 Pechino ha esteso anche all'europio i controlli all'esportazione, e il 30 dello stesso mese ne ha sospeso l'attuazione per un anno. All'altro capo della catena, secondo le Nazioni Unite, nel 2022 si sono prodotti nel mondo 62 milioni di tonnellate di rifiuti elettronici, e solo il 22,3 per cento è stato raccolto e riciclato in modo documentato; il resto è finito in discarica, spesso nei paesi del Sud del mondo, o è stato trattato in condizioni che mettono a rischio la salute dei lavoratori.

Nel 1865 William Stanley Jevons, studiando il mercato del carbone, osservò che le macchine a vapore più efficienti non riducevano il consumo di carbone ma lo facevano crescere, perché rendevano conveniente usarle in molti più impieghi. Il digitale ripete lo schema. Trasmettere la stessa quantità di informazione richiede oggi molti meno chilowattora di pochi anni fa, ma il volume delle trasmissioni cresce più in fretta del risparmio; server più efficienti permettono di installarne di più, data center meno energivori ne incoraggiano la moltiplicazione. Il consumo complessivo dell'informatica cresce, anche se meno di quanto sarebbe cresciuto senza quei miglioramenti, e per ridurlo davvero all'efficienza tecnica deve accompagnarsi la sobrietà nell'uso: data center migliori e meno dati inutili.

*

Il 2016 è l'anno dell'accordo di Parigi sul clima e di AlphaGo, il programma di intelligenza artificiale che vince a go contro un campione umano, ma è anche l'anno della Brexit e della prima elezione di Donald Trump, due segnali di una crisi del governo multilaterale che si è rivelata strutturale. La Crimea era stata annessa dalla Russia nel 2014, e nel 2022 la Russia ha invaso l'Ucraina: da allora l'energia non è più soltanto una voce di costo, è uno strumento di pressione geopolitica. La Cina ha consolidato il controllo sulle filiere dei semiconduttori e delle terre rare, e gli Stati Uniti hanno risposto con il CHIPS Act, la legge del 2022 che finanzia la produzione nazionale di microprocessori, e con un protezionismo industriale che non si vedeva dal dopoguerra. La pandemia del 2020 ha mostrato quanto fossero fragili le filiere globali, e quanto i data center pesassero ormai sul sistema energetico di interi paesi.

Questi fenomeni non corrono paralleli alla crisi climatica, le sono intrecciati. Chi controlla i minerali rari controlla la transizione energetica, chi controlla i

semiconduttori controlla l'intelligenza artificiale, e chi controlla l'intelligenza artificiale controlla in misura crescente le condizioni della produzione, della comunicazione e del consenso. Una politica per la sostenibilità digitale che ignori questo campo di forze non vede il terreno su cui si muove.

*

Nel 1981 la Convenzione 108 del Consiglio d'Europa è stata il primo strumento internazionale vincolante sulla protezione dei dati personali. Nel 2013, dopo le rivelazioni di Edward Snowden sulla sorveglianza di massa condotta dall'agenzia di sicurezza nazionale statunitense, l'Assemblea generale delle Nazioni Unite ha approvato una risoluzione sul diritto alla privacy nell'era digitale. Nel 2014 la Corte di giustizia dell'Unione europea, con la sentenza Google Spain, ha riconosciuto il diritto all'oblio: i dati personali sono una proiezione della persona, non una risorsa degli operatori che li raccolgono. Nel 2015 la Camera dei deputati ha approvato la Dichiarazione dei diritti in Internet, scritta dalla commissione presieduta da Stefano Rodotà e promossa dalla presidente Laura Boldrini: neutralità della rete, diritto all'accesso, protezione dei dati, libertà di comunicazione, dignità del lavoro nell'economia digitale. Non è una legge, ma riconosce il digitale come spazio in cui si esercitano diritti, oltre che luogo di consumo e di profitto. Su queste fondamenta è nato il regolamento generale sulla protezione dei dati, adottato nel 2016 e applicato dal 2018.

Partire da qui e non dal Green Deal cambia la lettura di tutto il resto. Se la sostenibilità digitale nasce dai diritti, comprende il lavoro, il potere e la democrazia oltre all'ambiente; se nasce dal Green Deal, si restringe ai consumi. Il Green Deal del 2019, con l'obiettivo della neutralità climatica entro il 2050, ha portato con sé strumenti specifici: la direttiva sulla rendicontazione di sostenibilità (CSRD), la tassonomia delle attività economiche sostenibili, i criteri ambientali minimi per gli acquisti pubblici. La CSRD ha introdotto la doppia materialità (l'obbligo di rendicontare sia l'impatto dell'impresa sull'ambiente e sulla società, sia l'effetto delle questioni ambientali e sociali sui conti dell'impresa), ed è stata svuotata in due anni. La direttiva «Stop the clock» dell'aprile 2025 ne ha rinviato l'applicazione di due anni; il pacchetto Omnibus I, in vigore dal 18 marzo 2026, ha alzato la soglia da 250 a 1.000 dipendenti e ha aggiunto il requisito di 450 milioni di euro di ricavi netti. Circa l'80 per cento delle imprese prima obbligate è uscito dal perimetro, e la direttiva che doveva cambiare il modo di fare impresa è diventata un adempimento per poche grandi aziende.

Dario Denni, intervenendo al Digital Ethics Forum di Sloweb, ha descritto il Green Deal con una formula: «pochi l'hanno letto, tutti l'hanno interpretato».

Ha ricordato che san Francesco, prima di morire, lasciò scritto che la sua Regola non andava interpretata, e che subito dopo la sua morte l'ordine si divise fra gli spirituali, fedeli alla lettera, e i conventuali, che la interpretavano. Le interpretazioni del Green Deal vanno tutte nella stessa direzione: obiettivi attenuati, scadenze rinviate, meno soggetti obbligati. L'AI Act, il regolamento europeo sull'intelligenza artificiale, ha seguito una strada simile, perché le pressioni delle grandi imprese tecnologiche hanno ottenuto esenzioni e attenuazioni sul riconoscimento facciale, sulla discriminazione algoritmica e sui sistemi di sorveglianza. Eppure l'AI Act conta per la sostenibilità digitale proprio perché riconosce l'impatto sociale e politico dell'intelligenza artificiale, e non si ferma ai consumi.

I contratti pubblici valgono in Italia 309,7 miliardi, secondo la relazione dell'Autorità nazionale anticorruzione sul 2025, e orientare quella spesa riorganizzerebbe il mercato più di qualunque incentivo. Ma i criteri ambientali minimi per computer e monitor, fissati con un decreto del dicembre 2013, sono stati abrogati con effetto dal marzo 2020, e per sei anni le amministrazioni hanno comprato quei prodotti senza criteri ambientali. Il vuoto si è chiuso il 24 maggio 2026, con l'entrata in vigore del decreto ministeriale dell'11 marzo, che detta i criteri per computer, monitor, tablet e smartphone e impone alle stazioni appaltanti almeno il 10 per cento di prodotti ricondizionati. Restano senza criteri i servizi cloud, i data center e le infrastrutture di rete, e non ci sono istruttorie aperte per darglieli: gli acquisti che pesano meno hanno regole da anni, quelli che pesano di più non ne hanno nessuna. Intanto la Francia si è data una legge sul digitale responsabile, in Germania SAP, Deutsche Telekom, Bosch e Otto



Group aderiscono a un'iniziativa per la responsabilità digitale d'impresa e ne pubblicano ogni anno il rapporto, e i Paesi Bassi hanno reso obbligatori i criteri europei per le forniture informatiche in tutte le gare pubbliche.

*

Le prime pratiche di Green IT, negli anni Novanta, nacquero dalla bolletta elettrica e non da un'illuminazione etica. Furono poi codificate in standard volontari, come il PUE (l'indice che misura quanta parte dell'energia consumata da un data center arriva davvero ai server), nato nel 2007, e solo dopo diventarono obblighi. Il rapporto fra pratiche d'impresa e norme è circolare: le norme nascono dalle pratiche dei pionieri, e una volta scritte tornano sul campo, trasformano il vantaggio dei primi in requisito minimo per tutti e aprono alle imprese che vanno oltre la conformità un nuovo spazio per distinguersi. Una lettura del panorama attuale come sequenza semplice, prima la norma e poi l'adeguamento delle imprese, ne perde la metà.

Una norma performativa fissa un obiettivo e lascia all'impresa la libertà di scegliere come raggiungerlo; una norma prescrittiva stabilisce i requisiti tecnici, ed è efficace finché la tecnologia che descrive resta in uso. Nel digitale quella tecnologia cambia in fretta, e la norma prescrittiva entra in un ciclo di obsolescenza che si chiude in tre-cinque anni: la regola fissa i requisiti, le imprese si adeguano, il mercato passa a una tecnologia nuova, la regola non copre più niente e va riscritta. L'AI Act è stato proposto nel 2021, negoziato per tre anni ed è entrato in vigore nel 2024, e nel frattempo i modelli generativi, appena emergenti quando il testo fu scritto, sono diventati il centro della questione. La norma performativa, definendo obiettivi invece che mezzi, resiste meglio a questi cambiamenti.

Gli standard europei di rendicontazione di sostenibilità sono stati elaborati dall'EFRAG, il gruppo consultivo europeo sull'informativa finanziaria, in circa due anni e con la partecipazione di centinaia di soggetti: grandi imprese, società di revisione, investitori istituzionali, consulenti. Le piccole e medie imprese erano sottorappresentate, i sindacati ai margini, le organizzazioni ambientaliste presenti ma senza peso decisivo. Il risultato riflette quella composizione: standard sofisticati, calibrati sulle capacità delle grandi imprese, che privilegiano gli indicatori quantitativi e l'informazione rilevante per i conti rispetto a quella rilevante per la società. Non c'è stato un complotto. In un processo deliberativo influisce sul risultato il soggetto che ha le risorse per mandare esperti ai gruppi di lavoro e rispondere alle consultazioni, e quello che non le ha ne subisce l'esito.

Le norme sulla sostenibilità digitale spingono verso



data center più efficienti, dispositivi meno energivori, pratiche più circolari, ma non mettono in discussione la crescita complessiva della domanda; rendendo il digitale più verde, o dandone l'impressione, possono anzi ridurre le resistenze alla sua ulteriore espansione. È l'effetto osservato da Jevons, trasferito dalla macchina alla regola. L'efficienza relativa non misura l'impatto assoluto, e una regolazione che premia solo la prima può produrre un settore sempre più efficiente che consuma sempre di più. La norma tecnica non può uscire da questo vicolo, perché è costruita per misurare un rapporto fra grandezze date, e il modello di sviluppo le sta a monte come presupposto. La norma di principio, invece, quel presupposto lo tocca.

L'articolo 3 del Trattato sull'Unione europea impegna l'Unione allo sviluppo sostenibile e a un'economia sociale di mercato; l'articolo 11 del Trattato sul funzionamento dell'Unione impone di integrare la tutela dell'ambiente in tutte le sue politiche, non di bilanciarla con esse. La Costituzione italiana, dopo la riforma del 2022, tutela all'articolo 9 l'ambiente, la biodiversità e gli ecosistemi «anche nell'interesse delle future generazioni», e all'articolo 41 pone alla libertà d'impresa il limite del danno alla salute e all'ambiente. La Dichiarazione europea sui diritti e i principi digitali, proclamata il 15 dicembre 2022, dedica un capitolo intero alla sostenibilità e afferma che ognuno dovrebbe avere accesso a informazioni

accurate e comprensibili sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, sulla loro riparabilità e sulla loro durata. Nessuno di questi testi si può far valere davanti a un giudice come una soglia di PUE, e per questo la letteratura sulla conformità li ignora. Sono però i soli che permettono di chiedere se un data center sia necessario, oltre che efficiente, e vanno difesi proprio mentre vengono svuotati di fatto.

*

Per un'impresa la conseguenza pratica è che la norma va conosciuta e rispettata, ma usata come uno specchio e non come una gabbia: registra che cosa la società è riuscita finora a pretendere, non che cosa sarebbe necessario. Raccogliere i dati richiesti dalla rendicontazione costringe l'impresa a chiedersi dove si generano le emissioni, quali processi pesano di più, quali fornitori sono critici. La conformità è uno stato binario, si rispettano o no certi requisiti; la sostenibilità è un processo che si misura anno dopo anno. Un'impresa può anche intervenire sulle norme mentre si formano. La Commissione europea, le autorità nazionali e gli enti di normazione aprono una consultazione pubblica su quasi ogni atto, i contributi restano pubblici e le risposte sono poche, quasi tutte delle grandi imprese e delle loro associazioni di categoria: è una soglia d'accesso molto più bassa di quanto si creda, e le piccole e medie imprese la usano raramente.

Pietro Jarre, nella sua esperienza di imprenditore, ha visto nascere nelle aziende i responsabili dei sistemi informativi e ha visto la direzione d'impresa ritirarsi, lasciando agli specialisti scelte che ridefiniscono i rapporti di potere e le vulnerabilità dell'organizzazione: quale fornitore cloud adottare, quanto automatizzare, fino a che punto digitalizzare. L'informatica attraversa tutti i processi e tutte le relazioni dell'impresa, e il responsabile dei sistemi informativi deve rispondere all'imprenditore, non sostituirlo nelle scelte strategiche. Gli informatici, osserva Jarre, in Italia lavorano senza un codice deontologico obbligatorio e senza un ordine professionale, ed escono da corsi di studio in cui non ricevono nozioni di etica né di impatto energetico del software.

Nel gruppo di cui Jarre era fra i principali azionisti, con quasi 10.000 dipendenti e la necessità di gestire qualità, sicurezza del personale, sicurezza dei dati, ambiente e diritti umani, il sistema di gestione integrato stava in una dozzina di diagrammi di flusso: venti pagine tradotte in venti lingue, e per ogni politica tre o quattro parametri per verificarne l'attuazione. Ogni nuova politica proposta dai consulenti avrebbe portato con sé un codice, manuali, ruoli, corsi e comunicazioni, con un effetto cumulativo che minacciava di paralizzare l'organizzazione. Per governare un'impresa, sostiene Jarre, bastano un codice etico che comprenda il digitale, un registro dei rischi aggiornato che comprenda i rischi del digitale, e una tabella di parametri da sorvegliare, non più di una dozzina, ordinati secondo le priorità vere: prima le persone, clienti e dipendenti, poi la qualità dei prodotti e l'innovazione, per ultimi i risultati finanziari, guardati sul medio periodo e non sul trimestre. Oltre la dozzina i parametri sfuggono di mano, e l'abbondanza di dati che il digitale produce nasconde le criticità nel rumore.

La sostenibilità digitale non chiede quindi un documento nuovo. In Italia quasi ogni impresa strutturata ha già un codice etico, nella maggior parte dei casi allegato al modello di organizzazione previsto dal decreto legislativo 231 del 2001 sulla responsabilità amministrativa delle imprese per i reati commessi nel loro interesse, e quel codice ha già un organismo che ne vigila l'osservanza: basta aggiungere un capo. Il punto di partenza è il registro dei rischi, dove vanno scritti quelli del digitale: la dipendenza da un fornitore unico, l'obsolescenza indotta dagli aggiornamenti, l'esposizione dei dati, il consumo che nessuno misura, il lavoro lungo la catena di fornitura che nessuno ha mai guardato. Il registro è il posto giusto, perché è l'unico documento aziendale in cui un rischio non registrato è già di per sé un problema.



I principi vanno scritti pochi e specifici. «Ci impegniamo a rispettare l'ambiente» è una frase vuota; «ci impegniamo a portare il PUE dei nostri data center sotto 1,3 entro il 2027» è un principio che si può verificare. Ogni principio deve tradursi in impegni con un indicatore, un obiettivo e una scadenza: un impegno senza indicatore è un desiderio, un indicatore senza obiettivo è una statistica, un obiettivo senza scadenza è un'utopia. Gli impegni vanno messi dove stanno già i numeri dell'impresa, in un capitolo del rapporto di sostenibilità dedicato al digitale, e non in un opuscolo a parte, che nessuno confronta con quello dell'anno precedente. Ogni anno quel capitolo riporta che cosa era stato promesso, che cosa è stato fatto e che cosa no, e l'impresa che pubblica anche i risultati mancati acquista una credibilità che nessuna campagna di comunicazione può comprare.

Gli organi che ne rispondono esistono già: l'organismo di vigilanza sul modello 231, il responsabile del sistema di gestione ambientale o energetica, il comitato che porta i rischi al vertice. La sostenibilità digitale entra nei loro ordini del giorno e usa il canale di segnalazione che l'impresa ha già per le violazioni del codice. La figura che coordina deve però avere un mandato formale, tempo assegnato e accesso diretto alla direzione, e fra un referente che conosce la sostenibilità e ha il potere di decidere e uno che conosce l'informatica e non ne ha, conviene il primo. Le competenze tecniche si comprano o si imparano; l'autorità di fermare un progetto, rifiutare un fornitore o chiedere un dato a un'altra funzione no. Un referente senza potere produce documenti e lascia l'impresa com'era.

Il test della credibilità, prima di pubblicare un codice così, sta in cinque domande: se un dipendente scettico lo leggerebbe senza alzare gli occhi al cielo; se un giornalista potrebbe verificarne le affermazioni; se l'impresa, mancando fra un anno un obiettivo, saprebbe spiegare pubblicamente perché; se fornitori e clienti la riconoscerebbero in quel testo; se il suo critico interno più severo vi troverebbe qualcosa di buono da dire. Basta una risposta negativa perché il lavoro sui principi vada rifatto.

I servizi digitali delle amministrazioni pubbliche, a cominciare dai siti dei comuni, dovrebbero dare l'esempio: sobri e semplici da usare, puliti perché consumano poca energia, giusti perché pienamente accessibili anche ai gruppi più vulnerabili. «Sobria, pulita e giusta» è la formula con cui Sloweb, l'associazione fondata a Torino nel 2017, ha ripreso il «buono, pulito e giusto» di Slow Food, e in otto edizioni del suo Digital Ethics Forum ricercatori, imprenditori, attivisti e consulenti hanno raccolto oltre 100 interventi su queste questioni. Pietro Jarre propone l'immagine di un'impresa bella, libera e forte: bella perché se ne può essere orgogliosi per come tratta i dipendenti e la comunità in cui opera, libera perché non è suddita dei guardiani tecnologici, delle mode manageriali e della pressione del trimestre, forte perché dura e investe in competenze, relazioni e reputazione. La sobrietà, scrive Jarre, «è l'opposto dell'austerità»: è la capacità di dire no a una tecnologia quando non serve gli interessi dell'organizzazione.



Guerra ibrida: quando le reti digitali diventano il nuovo campo di battaglia



A cura di William Nonnis

Dai router alle infrastrutture critiche: sicurezza nazionale, governance e sovranità digitale nei prossimi vent'anni.

La guerra ibrida non nasce con l'intelligenza artificiale. Intelligence, sabotaggio, propaganda e interferenze nelle comunicazioni erano già strumenti di destabilizzazione nel Novecento. Con la digitalizzazione, però, sono cambiate velocità, scala e capacità di colpire infrastrutture interconnesse.

Negli anni Novanta, il cyberspionaggio di Moonlight Maze mostrò la vulnerabilità delle reti governative. Nel 2005 James N. Mattis e Frank G. Hoffman contribuirono a definire il concetto moderno di guerra ibrida. Gli attacchi DDoS contro l'Estonia nel 2007 e le operazioni informatiche durante il conflitto Russia-Georgia del 2008 ne evidenziarono la dimensione digitale.

Oggi il campo di battaglia comprende telecomunicazioni, cloud, sistemi industriali e dispositivi che utilizziamo quotidianamente, spesso senza considerarli parte della sicurezza collettiva.

La minaccia geopolitica si estende sempre più ai dispositivi di uso quotidiano: router domestici, telecamere IP e sistemi domotici possono essere compromessi e trasformati, anche all'insaputa degli utenti, in nodi operativi di attività informatiche ostili.

Il rapporto ENISA Threat Landscape 2025, basato sull'analisi di 4.875 incidenti, evidenzia come criminalità informatica, hacktivismo e attori riconducibili a interessi statali possano impiegare tecniche e strumenti analoghi, rendendo più complessa l'attribuzione delle responsabilità e ampliando i rischi per la sicurezza collettiva.

Un router compromesso può fungere da proxy, occultare l'origine del traffico malevolo o facilitare l'accesso ad altri sistemi. Il caso Volt Typhoon è emblematico: nel gennaio 2024 le autorità statunitensi intervennero contro una botnet di router domestici e di piccoli uffici utilizzata, secondo le attribuzioni ufficiali, da attori collegati alla Cina per mascherare attività contro infrastrutture critiche.

Router, telecamere, videoregistratori di rete, sensori e dispositivi dell'Internet of Things (IoT) e dell'Internet of Everything (IoE) possono essere aggregati in botnet: reti controllate da remoto per attacchi coordinati, anche su larga scala.

Telecomunicazioni e infrastrutture critiche

Le operazioni associate a Salt Typhoon, documentate da autorità statunitensi e partner internazionali, hanno mostrato come apparati delle telecomunicazioni possano essere compromessi per ottenere accessi persistenti, intercettare comunicazioni e raccogliere



informazioni strategiche.

L'integrazione tra Information Technology (IT) e Operational Technology (OT) estende il rischio a reti energetiche, acquedotti, trasporti e sanità. Un incidente digitale può compromettere processi fisici e produrre effetti a cascata. Resilienza significa quindi prevenire, mantenere operativi i servizi essenziali e ripristinarli rapidamente.

La guerra ibrida non si limita a Internet.

Il jamming disturba i segnali satellitari di navigazione; lo spoofing trasmette informazioni ingannevoli su posizione o temporizzazione. Navi, aeromobili e logistica possono così subire interferenze anche senza infezioni malware: basta compromettere l'affidabilità del segnale.

Anche la catena di fornitura è strategica. I cercapersone esplosi in Libano nel settembre 2024 hanno mostrato, in un caso distinto dal comune attacco informatico, le conseguenze della manipolazione fisica degli apparati. La sicurezza deve coprire progettazione, produzione, distribuzione e manutenzione.

L'intelligenza artificiale amplifica la minaccia: phishing personalizzato, imitazioni vocali, video manipolati e campagne informative possono essere prodotti e diffusi più rapidamente. Non ogni automazione equivale a un attacco autonomo, ma la riduzione dei costi aumenta la replicabilità delle operazioni.

In tutto questo la risposta europea si basa su una condizione legislativa (che serve ma non basta); infatti la direttiva NIS2 rafforza la gestione del rischio, la continuità operativa e la sicurezza delle catene di fornitura nei settori interessati. Il Cyber Resilience Act introduce requisiti di cybersecurity per hardware e software con elementi digitali, responsabilizzando produttori e sviluppatori.

Dall'11 settembre 2026 si applicano gli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti gravi relativi alla sicurezza dei prodotti, con un primo avviso entro 24 ore. Le principali disposizioni saranno applicabili dall'11 dicembre 2027.

Governance e sovranità digitale: progettare i prossimi vent'anni

Da anni sostengo che la trasformazione digitale non consista semplicemente nell'acquistare nuove tecnologie. Il punto decisivo è la governance: definire una visione, governare processi, sviluppare competenze e mantenere il controllo delle infrastrutture su cui si fonda lo Stato.

La dipendenza europea da piattaforme, cloud, componenti e servizi extraeuropei non equivale automaticamente a insicurezza, ma pone interrogativi su autonomia operativa, continuità dei servizi e capacità decisionale nelle crisi. Sovranità digitale non significa isolamento né soltanto server sul territorio: significa poter scegliere, verificare, sviluppare e, quando necessario, sostituire le tecnologie da cui dipendiamo.

Oggi dobbiamo andare oltre la gestione dell'emergenza: progettare l'architettura tecnologica e istituzionale dei prossimi vent'anni.

Guardare al 2046 significa chiedersi chi governerà dati strategici, intelligenza artificiale, reti, infrastrutture e processi decisionali automatizzati. Occorre passare da una governance reattiva a una governance anticipatoria, che integri cybersecurity, ricerca, formazione e autonomia industriale.

Anche aggiornare il firmware del router, eliminare password predefinite, disattivare servizi inutilizzati e separare i dispositivi IoT dalle reti sensibili contribuisce alla difesa collettiva. La cybersecurity non è più materia esclusiva degli specialisti: è cittadinanza digitale.

Governare la tecnologia per difendere la democrazia

Nel nuovo equilibrio geopolitico il potere non appartiene soltanto a chi possiede le tecnologie più avanzate, ma a chi sa governarle, proteggerle e garantirne il funzionamento nelle condizioni più critiche.

Da anni, insieme a molti colleghi del settore, richiamo la necessità di governare la trasformazione digitale. Oggi non basta mettere in sicurezza il presente: dobbiamo progettare la sovranità tecnologica dei prossimi vent'anni. Il futuro non si governa inseguendo l'innovazione, ma anticipandone le conseguenze.

In questa prospettiva la scuola è decisiva. Cultura digitale, cybersecurity, intelligenza artificiale e consapevolezza dei rischi devono entrare nei percorsi educativi dalla primaria alle secondarie. Non si costruisce una società sovrana senza formare le generazioni che dovranno governarla.

Senza formazione non esiste competenza; senza competenza non esiste capacità di governo; senza capacità di governo non esiste una reale sovranità digitale. Non è più soltanto una questione informatica. È sicurezza nazionale, autonomia strategica, responsabilità verso le nuove generazioni e futuro della democrazia.

OCCTET rilascia un kit di strumenti gratuito a supporto delle PMI nell'adeguamento al Cyber Resilience Act



A cura di James Philpot

La European DIGITAL SME Alliance ha pubblicato un nuovo toolkit gratuito e open source, finanziato dall'Unione Europea e sviluppato nell'ambito del progetto OCCTET, per supportare le piccole e medie imprese (PMI) e i progetti open source a prepararsi a garantire la conformità al Regolamento dell'Unione Europea sulla resilienza informatica (Cyber Resilience Act, CRA).

Il toolkit trasforma i requisiti normativi in semplici passi pratici che le organizzazioni possono integrare nei propri processi di sviluppo software e di sicurezza. Il kit ha l'obiettivo di aiutare a valutare la propria preparazione, identificare i componenti open source utilizzati nei prodotti, gestire le vulnerabilità e documentare il modo in cui i rischi per la sicurezza vengono affrontati.

In occasione di un recente webinar, il consorzio OCCTET ha presentato il toolkit in una sessione online rivolta a PMI, progetti open source, team di sviluppo del prodotto e altre organizzazioni alla ricerca di modalità pratiche e a basso impatto per prepararsi agli adempimenti previsti dal CRA. Durante il webinar sono stati presentati i diversi componenti del toolkit, spiegando come le aziende possano utilizzarlo e portando la testimonianza di un'azienda sulle modalità con cui intende adottarlo in futuro.

La pubblicazione del toolkit avviene in concomitanza con l'entrata in vigore dei primi obblighi del CRA. A partire dall'11 settembre 2026, infatti, tutti i produttori sono tenuti a segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi che impattano sulla sicurezza dei prodotti con elementi digitali commercializzati nel mercato interno dell'Unione Europea. Il resto delle obbligazioni previste dal CRA si applicherà a partire dall'11 dicembre 2027.

I primi utenti della piattaforma di autovalutazione OCCTET hanno evidenziato una sfida comune: molte PMI dispongono già di misure di sicurezza, ma mancano della visibilità, della documentazione e dei processi necessari per dimostrare come vengono gestiti rischi e vulnerabilità dei software.

«OCCTET offre alle PMI indicazioni pratiche e strumenti open source, disponibili gratuitamente e pensati per essere facili da usare, per aiutarle a prepararsi al CRA e gestire le vulnerabilità software», ha dichiarato Sebastien Heurtematte, coordinatore del progetto. «Con l'avvicinarsi delle scadenze del CRA e il rapido emergere di vulnerabilità critiche, è fondamentale sviluppare la capacità di identificare e rispondere ai rischi in maniera veloce ed efficiente. Supportare lo sviluppo, il miglioramento e l'accesso a questi strumenti attraverso comunità attive e collaborazione continua tra PMI, sviluppatori e comunità open source sarà essenziale per rendere il mantenimento della sicurezza software più accessibile.»



Un percorso pratico dalla valutazione all'azione

Il toolkit OCCTET combina più servizi che supportano le organizzazioni, dalla valutazione iniziale fino alla gestione delle vulnerabilità e alla documentazione.

PMI e progetti open source possono ora accedere e testare i seguenti servizi:

- **Valutare la preparazione**: il CRA Self-Assessment Portal aiuta le PMI a capire come il CRA si applica al loro caso, valutare il livello di preparazione e identificare le aree che richiedono maggiore attenzione. La valutazione guidata e gratuita traduce le disposizioni del CRA in domande strutturate, punteggi e raccomandazioni pratiche.
- **Identificare i componenti software**: Eclipse Apoapsis (istanza OCCTET) identifica componenti open source, dipendenze e licenze, basandosi sull'OSS Review Toolkit e sulle vulnerabilità note. Può inoltre generare report e documentazione a supporto della conformità normativa pronti per il CRA, incluse le distinte base del software (Software Bill of Materials, SBOM), che forniscono un inventario standardizzato dei componenti software contenuti in un prodotto.
- **Esaminare i risultati e intervenire**: Bitsea Curator (istanza OCCTET) combina analisi automatizzata e revisione umana per aiutare gli utenti a verificare le informazioni sul software, valutare se le vulnerabilità interessano i loro prodotti, dare priorità ai problemi e documentare le decisioni prese. Questo strumento supporta inoltre la creazione di rapporti relativi alla sfruttabilità delle vulnerabilità (VEX, Vulnerability Exploitability eXchange), che registrano se un prodotto è interessato o meno da una vulnerabilità nota.
- **Riutilizzare informazioni software condivise**: il Federated OSS Assessment Database, vulnerablecode.io, fornisce informazioni sui pacchetti open source, incluse le loro origini, licenze, avvisi di sicurezza, vulnerabilità e SBOM di riferimento. Il suo dimostratore pubblico PurlDB supporta la generazione di SBOM di riferimento per oltre 20 milioni di pacchetti, mentre l'integrazione con VulnerableCode collega le informazioni sulle vulnerabilità ai pacchetti software interessati.

Il toolkit è stato validato rispetto a scenari complessi e reali di dipendenze software in dieci diversi ecosistemi tecnologici. I test hanno incluso progetti open source ampiamente utilizzati, analisi su larga scala dell'intero portafoglio di progetti della Eclipse Foundation, nonché un numero crescente di casi d'uso reali di PMI. Questa estesa validazione dimostra la capacità del toolkit di operare su tecnologie, dimensioni di progetto e catene di fornitura software diverse.

I test hanno dimostrato la capacità degli strumenti del kit di analizzare strutture di dipendenze complesse, identificare vulnerabilità, supportare la revisione umana e monitorare le problematiche di sicurezza nel tempo.

Conoscere e collaborare con OCCTET

Il progetto Open-Source Compliance: Comprehensive Techniques and Essential Tools (OCCTET) riunisce leader industriali, esperti di cybersecurity, rappresentanti delle PMI e organizzazioni open source per rendere la sicurezza del software e la preparazione al CRA più accessibili, trasparenti ed economicamente sostenibili.



PMI e progetti open source possono esplorare il toolkit e le risorse disponibili su occtet.eu.

Le organizzazioni interessate a testare i servizi utilizzando prodotti reali e flussi di lavoro di sviluppo, e a fornire riscontri per il loro miglioramento, possono visitare la pagina OCCTET Get Engaged.

OCCTET, con la collaborazione e il lavoro dei partner del progetto, aiuta organizzazioni e comunità open source a prepararsi al CRA.

Attraverso l'Open Regulatory Compliance (ORC) Working Group, i partecipanti stanno sviluppando specifiche tecniche, linee guida, materiali formativi e altre risorse basati sul contributo della comunità, al fine di sostenere l'attuazione del CRA nell'intero ecosistema open source.

Queste risorse includono l'ORC Learning Hub, una piattaforma gratuita che fornisce formazione pratica e specifica per ciascun ruolo, al fine di aiutare gli sviluppatori e i manutentori di software open source, i responsabili dei progetti, i team di prodotto e i professionisti della sicurezza informatica e della conformità normativa a comprendere come il CRA si applichi alle rispettive attività e ad attuarne concretamente i requisiti.

Informazioni sul progetto OCCTET

Open Source Compliance: Comprehensive Techniques and Essential Tools (OCCTET) è un'iniziativa finanziata dall'UE, focalizzata a supportare PMI e progetti open source a orientarsi tra i requisiti di cybersecurity e conformità previsti dal Cyber Resilience Act.

Coordinato dalla Eclipse Foundation, il progetto sta sviluppando una suite integrata di strumenti gratuiti e open source per la valutazione della preparazione, l'analisi delle dipendenze software, la gestione delle vulnerabilità, la generazione di SBOM e la documentazione di conformità.

Il progetto OCCTET ha ricevuto finanziamenti dal programma Digital Europe nell'ambito del contratto di sovvenzione n. 101190474.

Il contenuto non riflette necessariamente le opinioni della Commissione Europea. La Commissione Europea non è responsabile per qualsiasi utilizzo che possa essere fatto delle informazioni qui contenute.



CYBER
Think Tank
ASSINTEL

Unisciti alla nostra community!

Scrivi a segreteria@assintel.it per avere maggiori info

I danni della “mancata” cybersicurezza

A cura di Ranieri Razzante



A conferma del quadro che emerge dalle recenti cronache dei cyberattacchi, i dati contenuti nel Global Cyber Loss Report di Hackmanac, secondo il quale, nel primo semestre del 2026, gli incidenti informatici registrati in Italia hanno generato perdite economiche stimate in circa 468,18 milioni di dollari, con un incremento del 33,3% rispetto ai sei mesi precedenti, devono allarmarci non poco.

Il dato, riferito a 407 episodi osservati tra gennaio e giugno, colloca il nostro Paese al nono posto nella graduatoria mondiale delle perdite economiche riconducibili al cybercrime.

La stima elaborata non rappresenta, pertanto, una rilevazione ufficiale dei danni effettivamente contabilizzati dalle imprese, ma costituisce un indicatore significativo dell’esposizione economica al rischio informatico. Sinceramente, ci si aspettava cifre più contenute!

Un aspetto particolarmente importante riguarda la natura dei costi generati da un attacco. Il danno comprende una pluralità di conseguenze: interruzione dei processi produttivi, indisponibilità dei servizi, recupero delle infrastrutture tecnologiche, gestione delle informazioni compromesse e possibili ripercussioni sui rapporti commerciali.

A tali effetti si aggiungono le conseguenze reputazionali e i costi derivanti dalla necessità di ripristinare la fiducia di clienti e partner. I cosiddetti “danni diretti” e “danni indiretti”, mai troppo preventivabili.

Il quadro delineato dal rapporto evidenzia, inoltre, un'evoluzione delle modalità attraverso cui vengono realizzati gli attacchi.

Accanto al ransomware, assume crescente rilevanza la sottrazione illecita di informazioni aziendali, spesso accompagnata dalla minaccia di diffusione pubblica dei dati acquisiti.

A livello globale, secondo Hackmanac, nel primo semestre del 2026 il furto di dati ha rappresentato il 48,2% delle perdite economiche riconducibili alle violazioni, superando la quota attribuita agli attacchi ransomware. Questa tendenza dimostra come la compromissione delle informazioni costituisca una fonte di rischio autonoma, che non può essere affrontata esclusivamente attraverso strumenti tradizionali di prevenzione e risposta agli attacchi.

In tale contesto, la cybersecurity deve essere integrata nei processi decisionali e nei sistemi di gestione aziendale.



Diventa essenziale predisporre adeguate misure di prevenzione, procedure di gestione degli incidenti e piani di ripristino. Altrettanto importante è il monitoraggio degli accessi ai sistemi, la protezione delle credenziali, l'individuazione tempestiva di eventuali trasferimenti anomali di informazioni e la predisposizione di misure idonee a contrastare attacchi diretti a compromettere la disponibilità dei servizi digitali. Se ne parla in ogni sede, ma pare che lo stato di avanzato lavori sia ancora rallentato.

I dati diffusi da Hackmanac restituiscono un'indicazione chiara: il rischio informatico produce conseguenze che travalicano la dimensione tecnologica e incidono direttamente sulla stabilità economica delle imprese.

Investire nella sicurezza digitale significa, pertanto, non soltanto ridurre la probabilità di subire un attacco, ma soprattutto tutelare il patrimonio informativo, preservare la continuità delle attività e rafforzare la capacità dell'organizzazione di affrontare situazioni di crisi.

La cybersecurity si configura così come un elemento imprescindibile della strategia aziendale e della governance dei rischi, nonché come un investimento necessario per garantire resilienza e competitività in un contesto economico sempre più dipendente dalle infrastrutture digitali.

Ai Consigli di amministrazione delle imprese tutte il compito di farsi carico anche del gap culturale!

È infatti un problema di governance, credo, più che di cultura. Anzi, un mix delle due.

Per dirla con quelli che amano le lingue, commitment ed awareness; in uno, la consapevolezza che la cybersecurity è ormai parte del nostro quotidiano, più dell'intelligenza artificiale.

Le storie di questi ultimi giorni, con gli attacchi alle supply chain dei supermercati, lo dimostrano ancora di più: una preoccupante trascuratezza per quelli che sono i servizi di "sopravvivenza" dei cittadini.

Chi vuole destabilizzare lo fa sulle infrastrutture critiche ed ora, di più, su quelle che stanno a latere di esse. I supermercati sono privati, si dirà, ma hanno acquisito una figurazione "pubblicistica" di non poco significato strategico.

L'insistenza che, nei nostri scritti e nei nostri convegni, oltre che, ovviamente, nelle statistiche delle Autorità, dedichiamo alla supply chain, con Nis2 che ci ha riempiti di raccomandazioni sulla catena dei fornitori, è più che motivata e mai troppa.

I danni diretti sono grandi, e lo dimostra il rapporto sopra citato; ma quelli indiretti, specie reputazionali, mi pare stiano diventando insostenibili.

Oltre all'effetto "panico" che, in questi casi così speciali, non devono sottovalutare le Autorità dedicate.



MA È SOLO UN FRIGORIFERO!

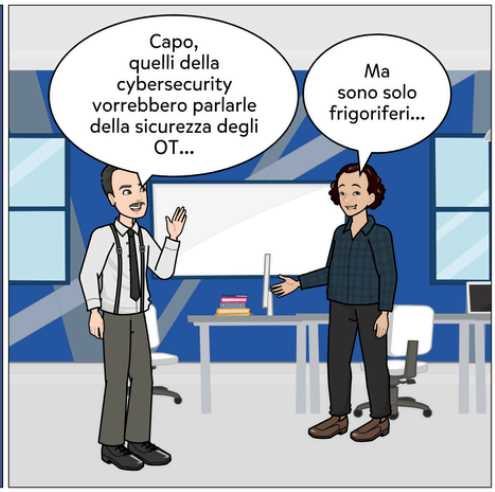
OGGETTI COMUNI, PERICOLI COMPLESSI
(e REALI)

by NWN SOLUTIONS

CYBER Think Tank ASSINTEL

www.assintel.it
info@assintel.it

Confcom Assintel























Dalla compliance alla resilienza: perché la convergenza normativa richiede un sistema di gestione integrato



A cura di Marco Scognamiglio

Dal 2025 le imprese italiane, comprese molte PMI, devono gestire un quadro normativo sempre più articolato. DORA è applicabile al settore finanziario dal 17 gennaio 2025, il Data Act dal 12 settembre dello stesso anno e la NIS2, recepita con il D.Lgs. 138/2024, è entrata nella fase attuativa. Nel 2026 si sono aggiunti ulteriori obblighi dell'AI Act e del Cyber Resilience Act, che sarà pienamente applicabile dall'11 dicembre 2027. Il punto non è più seguire una norma alla volta, ma governare requisiti diversi senza moltiplicare processi, strutture e costi.

Un quadro regolatorio sempre più interconnesso

La NIS2 porta la cybersicurezza sempre più dentro la governance dell'organizzazione, intervenendo su gestione del rischio, incidenti, continuità operativa, supply chain e responsabilità degli organi di amministrazione e direttivi. DORA segue una logica analoga nel settore finanziario, concentrandosi sulla resilienza operativa digitale, sulla gestione del rischio ICT e sulle dipendenze da terze parti ICT. L'AI Act introduce invece un approccio basato sul rischio, con obblighi differenziati in funzione dei sistemi e dei modelli AI e del ruolo ricoperto dai diversi operatori. Il Cyber Resilience Act interviene sui prodotti con elementi digitali, introducendo requisiti di cybersecurity che riguardano anche progettazione, sviluppo, produzione e gestione delle vulnerabilità: gli obblighi di reporting si applicano dall'11 settembre 2026 e le principali disposizioni dall'11 dicembre 2027.

Il Data Act, applicabile in via generale dal 12 settembre 2025, introduce infine regole armonizzate sull'accesso equo ai dati e sul loro utilizzo, con particolare attenzione anche ai dati generati dai prodotti connessi.

Non tutte le PMI sono soggette alle stesse norme e il perimetro va verificato caso per caso. I requisiti, tuttavia, convergono spesso su governance, gestione del rischio, conoscenza degli asset, incident management, continuità, terze parti e verifica dell'efficacia. Questa convergenza può trasformare la pressione normativa in un'opportunità organizzativa.

Standard e certificazioni: una struttura metodologica, non una scorciatoia normativa

Gli standard dei sistemi di gestione offrono una base utile per integrare requisiti diversi. ISO 9001 introduce approccio per processi, risk-based thinking e miglioramento continuo; ISO/IEC 27001 applica questi principi alla sicurezza delle informazioni, ISO 22301 alla continuità operativa, ISO/IEC 20000-1 ai servizi IT e ISO/IEC 42001 alla gestione dell'intelligenza artificiale.

La certificazione non sostituisce la conformità legislativa, ma fornisce un metodo per organizzare processi, responsabilità, controlli, evidenze, audit e riesami.

È emblematico il caso dell'AI Act dove il rapporto tra



tra compliance normativa e sistemi di gestione è già concreto: l'applicazione degli standard armonizzati rimane volontaria, ma quelli pubblicati nella Gazzetta ufficiale dell'UE possono conferire una presunzione di conformità rispetto ai requisiti coperti: EN 18286:2026, primo standard armonizzato pubblicato a supporto dell'AI Act, è stato progettato per integrarsi con sistemi di gestione già esistenti, come ISO/IEC 42001 o ISO 9001.

In questo scenario, la direzione più efficace è un sistema integrato, non una somma di schemi separati che genera sovrapposizioni, contraddizioni e difficoltà di audit.

Un solo processo, più esigenze di compliance

Creare un sistema per ogni norma significa descrivere più volte gli stessi processi, attribuire responsabilità potenzialmente diverse, ripetere le verifiche sui fornitori e raccogliere più volte le stesse evidenze.

L'alternativa è ragionare per capacità organizzative, costruendo processi, responsabilità e controlli comuni sui quali innestare le specificità dei diversi schemi applicabili, senza replicare strutture e attività già esistenti. È da questa logica che nasce il Sistema di Gestione Integrato.

Board e top management assicurano indirizzo e supervisione. Le funzioni specialistiche, come cybersecurity, risk management, compliance, privacy, qualità e business continuity, portano metodo e controllo. I process owner di IT, Operations, Procurement, HR e delle altre aree traducono gli indirizzi in attività operative. L'Internal Audit, o una funzione indipendente, ne verifica l'applicazione.

Una control library comune consente di definire ogni controllo una volta e mapparlo verso i diversi schemi. La stessa logica può essere applicata a risk assessment, formazione, fornitori, audit ed evidenze, riducendo duplicazioni, incoerenze e costi della compliance.

Dalla norma al processo: un esempio concreto di integrazione

Gestione degli incidenti e continuità operativa dimostrano efficacemente come più schemi possano convergere in un Sistema di Gestione Integrato.

Nel quadro NIS2 italiano, l'art. 24 del D.Lgs. 138/2024 include la gestione degli incidenti tra le misure di gestione dei rischi per la sicurezza informatica, mentre l'art. 25 disciplina la notifica degli incidenti significativi al CSIRT Italia. Le specifiche di base definite da ACN con la Determinazione 379907/2025 traducono questi obblighi in misure operative e le successive Linee Guida ACN descrivono un processo che attraversa preparazione, rilevamento, risposta, ripristino e miglioramento.

La ISO 22301:2019 richiede un Business Continuity Management System che comprenda Business Impact Analysis e risk assessment, strategie e soluzioni di continuità, piani e procedure, esercitazioni e miglioramento. L'obiettivo si allarga quindi dall'incidente cyber alla capacità dell'organizzazione di continuare a erogare prodotti e servizi anche in presenza di eventi disruptive.

DORA, per le organizzazioni che rientrano nel suo perimetro, rende ancora più evidente questa integrazione. L'art. 11 del Regolamento (UE) 2022/2554 richiede una ICT Business Continuity Policy e piani di risposta e ripristino, prevede una



Business Impact Analysis e richiede il test periodico dei piani. L'art. 12 aggiunge requisiti specifici su backup, restoration e recovery.

DORA introduce quindi un livello di dettaglio particolarmente significativo sulla resilienza ICT, sul testing e sulla capacità di ripristino.

Il punto è che questi requisiti non dovrebbero generare tre processi separati.

Un'organizzazione può costruire un unico processo di Incident, Crisis e Business Continuity Management, definendo ruoli ed escalation comuni, criteri per valutare criticità e impatti, modalità di attivazione della crisi, comunicazioni interne ed esterne, strategie di risposta e ripristino, gestione dei backup, esercitazioni e lesson learned.

Su questa base comune possono poi essere esplicitati gli adempimenti specifici richiesti dai diversi schemi, come la notifica al CSIRT Italia prevista dalla NIS2 o i requisiti più dettagliati di ICT recovery e testing previsti da DORA.

È questo, in concreto, il valore dell'integrazione: non cercare di uniformare norme che hanno finalità e perimetri differenti, ma riconoscere i processi che hanno in comune e costruirli una sola volta, aggiungendo dove necessario i controlli specifici di ciascun framework.

La stessa logica può essere applicata al risk management, all'Asset Governance, alla gestione dei fornitori, alla formazione e all'audit.

Dalla documentazione alla prova di resilienza

Un sistema integrato non può fermarsi alle policy. Tabletop exercise, simulazioni di crisi, test di disaster recovery, verifiche dei backup e prove dei flussi di escalation mostrano se ruoli, comunicazioni e decisioni funzionano davvero.

È qui che la compliance documentale diventa resilienza operativa.

Le norme cambiano, i processi rimangono.

Un Sistema di Gestione Integrato consente di recepire nuovi requisiti senza creare strutture parallele, riducendo duplicazioni e concentrando le risorse sull'obiettivo comune: governare il rischio e garantire resilienza al business.





La minaccia silenziosa: comprendere il cyber espionage in Italia



A cura di Sofia Scozzari

In Italia, il cyber spionaggio rappresenta una minaccia attuale e persistente, sebbene spesso sottovalutata. A differenza di problematiche più eclatanti, come il ransomware, raramente si manifesta in modo evidente: non ci sono richieste di riscatto, interruzioni di servizio o pubblicazione di dati rubati. I casi emergono spesso solo mesi dopo, tramite informazioni di terze parti, e molti, verosimilmente, non vengono mai scoperti.

Ciononostante, l'attività di cyber espionage in Italia è più diffusa e variegata di quanto si pensi. Con Hackmanac, abbiamo condotto un'analisi dei casi di cyber spionaggio di pubblico dominio che hanno riguardato l'Italia nel periodo compreso tra il 2024 e il 2026, che ha messo in luce diverse tipologie di attività di intelligence parallele. Di seguito, prendiamo in considerazione le evidenze principali, esaminandone tre aspetti: il motivo per cui l'Italia attira tanta attenzione, le modalità con cui i principali attori agiscono contro gli obiettivi italiani e gli strumenti che utilizzano, spesso condivisi.

Perché l'Italia?

L'Italia è presa di mira principalmente per ciò che rappresenta e per il ruolo geopolitico che riveste.

L'analisi condotta mostra almeno otto logiche di interesse distinte alla base dei casi italiani:

- **Sostegno all'Ucraina e logistica NATO:** il gruppo russo APT28 ha incluso l'Italia in una campagna, avviata già nel 2022, contro le entità logistiche e tecnologiche che forniscono aiuti all'Ucraina. Sia l'autore che il movente sono stati documentati da agenzie governative occidentali.

- **Competenze nei settori aerospaziale, della difesa e dei droni:** nel settembre 2025, un'azienda aerospaziale italiana è stata colpita dal gruppo nordcoreano Lazarus nell'ambito di una più ampia campagna contro le aziende europee del settore della difesa.

- **Diplomazia e affari esteri:** un campione associato al gruppo russo Turla, rilevato in Italia nel febbraio 2024, utilizzava un'esca relativa agli affari esteri italiani. L'ipotesi di un attacco mirato all'Italia è considerata plausibile, nonostante le evidenze non siano del tutto conclusive.

- **Dissidenti cinesi e relativi investigatori:** una violazione dei sistemi del Ministero dell'Interno, avvenuta tra il 2024 e il 2025, ha portato alla sottrazione di dati relativi a circa 5.000 agenti della Digos. Secondo la Polizia, l'obiettivo era localizzare i dissidenti cinesi presenti in Italia e identificare gli investigatori impegnati nelle indagini sui gruppi cinesi.



- **Intelligence governativa ed economica:** un gruppo state-aligned operante dall'Asia ha probabilmente compromesso alcuni enti governativi italiani nel 2025, concentrandosi in particolare sui ministeri che si occupano di questioni economiche e diplomatiche.

- **Posizione strategica dei fornitori IT:** l'intrusione presso la società **Sistemi Informativi**, facente parte del gruppo IBM che opera nel settore pubblico, ha un evidente valore potenziale in termini di intelligence, sebbene né l'autore né il movente siano stati resi noti.

- **Sorveglianza di dispositivi mobili:** diverse operazioni di spyware commerciale hanno preso di mira utenti italiani, ma il committente e i criteri con cui gli obiettivi sono stati selezionati spesso non sono noti.

- **Informazioni riservate sulla Difesa:** a luglio 2026 due ex funzionari dei servizi segreti italiani sono stati arrestati con l'accusa di aver trasmesso informazioni sulla difesa a un presunto ufficiale russo.

Modelli operativi a confronto

Nel loro insieme, i casi italiani presentano un numero limitato di modelli operativi, che si contraddistinguono per quattro fattori:

- **Entry point:** l'ingegneria sociale rappresenta il denominatore comune di attori molto diversi tra loro. È nota la campagna in cui Lazarus ha adescato degli ingegneri con false offerte di lavoro. APT28 e il cluster asiatico TGR-STA-1030 di norma utilizzano invece lo *spearphishing*, una tipologia di phishing particolarmente mirato, personalizzando i messaggi in base alla lingua o al contesto istituzionale della vittima. Alcuni operatori di spyware commerciale, come SIO, convincono le vittime a installare applicazioni contraffatte di WhatsApp o di operatori di telefonia mobile, infettandole in questo modo con spyware. Alcuni cluster legati alla Cina, come Ink Dragon, sfruttano i server web esposti su Internet, mentre Salt Typhoon prende tipicamente di mira i router delle telco e APT28 combina phishing e sfruttamento di VPN, webmail e router. Un'ulteriore tecnica, più rara, può arrivare addirittura ad escludere la vittima dall'equazione: è il caso di Graphite, un sofisticato spyware del vendor israeliano Paragon Solutions, che ha perseguito i propri obiettivi in Italia tramite un *exploit zero-click* su WhatsApp, ovvero sfruttando una vulnerabilità che ha consentito di installare malware nei dispositivi delle vittime senza alcuna interazione da parte dell'utente (da cui "zero-click"). Fortunatamente queste problematiche costituiscono l'eccezione più che la regola, dal momento che la maggior parte delle intrusioni perimetrali sfrutta vulnerabilità note non individuate o non *patchate*.

- **Persistenza:** una volta all'interno dei sistemi infettati, i gruppi di cyber espionage, di norma più sofisticati dei convenzionali cybercriminali, utilizzano svariate tecniche per consolidare la loro permanenza, concentrando i loro sforzi maggiormente nel far apparire come legittime le loro attività, piuttosto che nel nascondersi. Il traffico malevolo dei comandi con le conseguenti esfiltrazioni viene fatto transitare attraverso servizi comuni (Microsoft Graph, Outlook, siti WordPress compromessi, hosting di file su cloud, ecc.). File eseguibili legittimi vengono utilizzati per caricare codice dannoso sui sistemi e le vittime compromesse possono diventare dei tramiti per i bersagli successivi. Due noti gruppi russi utilizzano stili distinti: APT28 sfrutta le identità compromesse e la posta elettronica, abusando dei permessi delle caselle di posta, registrando MFA e utilizzando token OAuth rubati, mentre Turla si avvantaggia con backdoor multiple, payload che si attivano solo sul dispositivo della vittima e accessi compromessi ottenuti da altri gruppi. Altri gruppi si focalizzano su configurazioni di rete, in particolare di router e impostazioni DNS, dettagli a cui poche aziende prestano attenzione, a meno che non ne monitorino appositamente le modifiche.

- **Raccolta:** le operazioni orientate alle infrastrutture raccolgono inizialmente dati in modo esteso per poi selezionarne i più utili successivamente. Le compromissioni, a partire da router e apparati di rete esposti a Internet, iniziano in modo opportunistico, in base alle vulnerabilità riscontrate. Le intrusioni nelle reti di telecomunicazioni raccolgono traffico e registri delle chiamate su larga scala, analizzati in seguito, mentre le campagne mirate alle reti governative puntano ad ottenere informazioni economiche e diplomatiche. Una singola intrusione in una rete istituzionale può essere in grado di fornire una mappa dettagliata delle persone coinvolte, sfruttabile successivamente, oltre che informazioni molto sensibili. All'estremo opposto, la sorveglianza mobile è precisa per definizione: nell'indagine italiana che vedeva coinvolto lo spyware Graphite sono stati compromessi tre smartphone, mentre nella campagna che simulava l'app WhatsApp sono stati presi di mira circa 200 utenti, ciascuno selezionato individualmente. Altre tipologie di intrusione prendono di mira un ambito specifico per carpirne il know-how proprietario. È il caso del gruppo Lazarus che si concentra su settori altamente specializzati (aerospaziale, difesa, ecc)

- **Livello umano:** la violazione tecnologica è spesso solo uno dei numerosi passaggi che compongono operazioni più ampie. Fonti interne, supporti fisici e pagamenti possono fornire informazioni molto dettagliate e sensibili, a dimostrazione del fatto che il rischio insider dovrebbe essere valutato alla stessa stregua del rischio cyber.

La difficoltà di attribuzione

Sebbene difficili da individuare, le operazioni di cyber spionaggio risultano ancora più complesse da attribuire.

Il repertorio di tecniche spesso si sovrappone: phishing, side-loading di DLL, sfruttamento di server esposti e abuso di servizi cloud legittimi ricorrono sia tra attori russi, cinesi e nordcoreani, sia tra quelli commerciali. Ed è proprio questa sovrapposizione a complicare l'attribuzione delle campagne, ostacolando di conseguenza la corretta comprensione delle motivazioni.

Due gruppi possono sfruttare la stessa vulnerabilità o riutilizzare lo stesso schema di phishing senza alcun legame operativo. Il quadro è reso ancora più opaco dal fatto che accessi e strumenti circolano tra attori diversi (credenziali compromesse ed exploit venduti nei forum, malware offerto in modalità as-a-service, ecc.). Un'intrusione può quindi portare le tracce di un attore diverso da quello che la sta sfruttando.

L'intrusione in Sistemi Informativi è stata inizialmente associata al gruppo Salt Typhoon dalla stampa, ipotesi poi esclusa da IBM. Allo stesso modo, il caso Digos viene spesso messo in relazione con cluster cinesi specifici, senza trovare riscontro in alcun indicatore pubblico.

È importante ricordare che un'attribuzione affidabile richiede elementi solidi: l'identificazione dell'attore da parte di un governo, infrastrutture condivise, analisi di malware o dati telemetrici.

Come prepararsi?

L'Italia è strutturalmente esposta al fenomeno del cyber spionaggio, che in gran parte avviene in modo silenzioso.

Ciononostante, esistono buone pratiche per prepararsi e proteggersi:

- **Mappare l'esposizione degli asset**, valutando quale logica di interesse potrebbe applicarsi per gli attaccanti. Il risultato di questa valutazione è fondamentale per determinare quali modelli operativi siano maggiormente rilevanti in base al modus operandi tipico dei gruppi di attaccanti principali.

- **Gestire e risolvere le vulnerabilità note sul perimetro**, inclusi router, gateway VPN e dispositivi di rete che spesso non rientrano nei normali cicli di patch, e monitorarne le modifiche di configurazione.

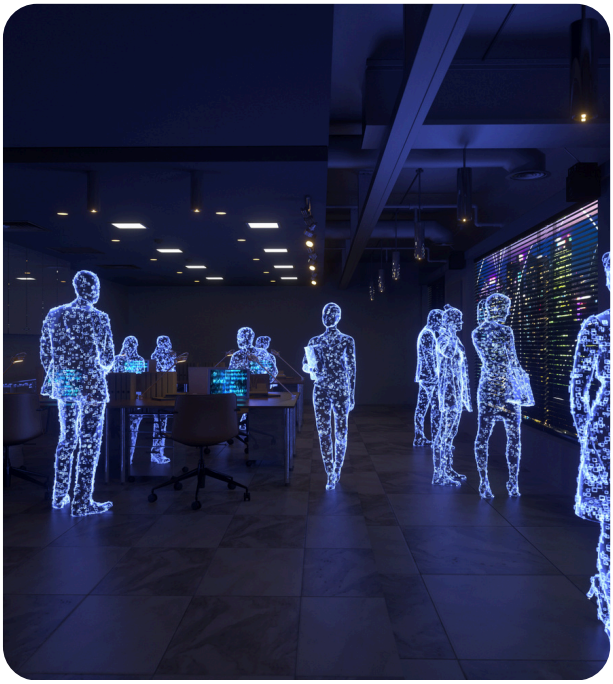
- **Proteggere identità e posta elettronica**, spesso il principale veicolo iniziale per operazioni di spionaggio, adottando l'autenticazione a più fattori resistente al phishing (ad esempio chiavi FIDO2), impostando avvisi sulle modifiche alle autorizzazioni delle caselle di posta e rivedendo periodicamente le autorizzazioni OAuth.

- **Monitorare l'utilizzo dei servizi cloud legittimi**, perché è proprio lì che gli attaccanti più esperti nascondono le proprie attività.

- **Estendere la protezione ai dispositivi mobili del personale più esposto** (dirigenti, ingegneri, funzionari e giornalisti), effettuando controlli sul sideloading delle app, ovvero l'installazione di applicazioni da file esterni (come gli .apk su Android). Sensibilizzare, inoltre, su phishing, vishing (voice phishing) e smishing (SMS phishing), inclusi i messaggi che simulano operatori telefonici o servizi bancari.

- **Includere il rischio insider nella valutazione delle minacce**, considerando il fattore umano come potenziale punto di ingresso di un'operazione di cyber spionaggio più ampia.

La vera domanda per le aziende italiane, quindi, non è quale gruppo potrebbe prenderle di mira, ma quali risorse le rendano un obiettivo appetibile e quanto tempo impiegherebbero per accorgersene.



Oltre i questionari: la resilienza sistemica comincia dalla mappa del software



A cura di Michele Slocovich

L'AI accelera lo sviluppo, ma anche la propagazione dei rischi non lineari. NIS2, DORA e AI Act pongono una sfida comune: conoscere i sistemi per renderli resilienti.

La resilienza digitale non dipende soltanto dalla capacità di difendersi dagli attacchi, ma anche dalla conoscenza dei sistemi da proteggere. In un ecosistema applicativo complesso, un componente apparentemente marginale può sostenere servizi essenziali e una modifica circoscritta produrre conseguenze difficili da prevedere.

L'ho visto accadere: un servizio scritto vent'anni fa, ritenuto marginale, alimentava tre applicazioni centrali mai mappate insieme. Quando è andato in crisi, l'impatto ha superato il componente coinvolto: mancava una visione completa delle dipendenze. Nel software, il rischio non coincide con la somma delle vulnerabilità dei singoli componenti. Dipende anche da come sono collegati e dalle funzioni che sostengono: è la topologia a determinare come un problema locale possa diventare sistemico.

Con l'intelligenza artificiale generativa, che consente di scrivere e modificare codice più rapidamente, questa dinamica diventa ancora più rilevante.

Pur intervenendo su ambiti diversi, le normative condividono un presupposto: proteggere i servizi richiede di conoscere gli asset digitali, le loro relazioni e gli effetti dei cambiamenti.

L'AI accelera il codice, non la conoscenza del sistema

Secondo il report OSSRA 2026 di Black Duck, circa l'85% delle organizzazioni usa assistenti AI per scrivere codice; il 76% di quelle che ne vietano l'utilizzo ammette che gli sviluppatori li impiegano comunque. La produzione accelera, spesso su sistemi legacy stratificati in decenni, con tecnologie diverse, database condivisi e documentazione non sempre aggiornata.

Il problema non è soltanto che l'AI possa generare codice sbagliato: può produrre codice plausibile senza conoscere l'architettura complessiva e le relative dipendenze. Così una scelta apparentemente locale può avere effetti non lineari su altri componenti, anche a distanza, sia temporale sia logica.

Più aumenta la velocità degli interventi, dunque, più diventa importante valutarne l'impatto. Il costo vero non è generare codice: è generare codice «quasi giusto» su larga scala senza poter verificare cosa cambia nel sistema.

Dalle dichiarazioni alla verifica del software

La stessa esigenza riguarda la supply chain. Questionari, certificazioni e clausole contrattuali descrivono ciò che il fornitore dichiara, ma non sempre ciò che ha effettivamente consegnato.



Il report OSSRA 2026 rileva che l'87% delle codebase analizzate contiene almeno una vulnerabilità open source e che il 65% delle organizzazioni ha subito un attacco alla supply chain software nell'ultimo anno. Librerie vulnerabili, componenti obsoleti e debolezze strutturali possono restare invisibili finché non si analizza il codice integrato.

Per verificare la gestione del rischio dei fornitori ICT richiesta da DORA, alle valutazioni contrattuali vanno affiancati criteri tecnici misurabili. La ISO/IEC 5055 offre un riferimento per valutare le debolezze strutturali del software: sicurezza, affidabilità, efficienza e manutenibilità. La documentazione acquista valore nel confronto con evidenze ricavate dal codice.

Andare oltre i questionari significa passare da ciò che il fornitore dichiara a ciò che il codice dimostra. È così che anche gli addendum contrattuali previsti da DORA possono diventare verificabili.

Dalla conoscenza degli asset alla resilienza operativa

Anche la NIS2 presuppone di sapere quali asset proteggere, quali processi critici dipendono da essi e quali fornitori possono influenzarli. Un inventario compilato manualmente, tuttavia, rischia di diventare obsoleto ogni volta che il software cambia.

L'analisi del codice permette di ricostruire i percorsi transazionali end-to-end e individuare applicazioni, componenti e dati che sostengono realmente un processo.

È la stessa conoscenza necessaria a DORA per valutare l'impatto di un'interruzione prima che si verifichi: senza una visione delle dipendenze, si può rafforzare il perimetro di sicurezza senza rendere più resiliente il sistema nel suo insieme.

La conoscenza del software diventa altrettanto importante quando entra in gioco l'AI Act. Per i sistemi di intelligenza artificiale ad alto rischio, il regolamento prevede obblighi di gestione del rischio, documentazione tecnica, registrazione degli eventi, supervisione umana e requisiti di robustezza e cybersecurity.

Ma un sistema di AI non vive isolato: opera dentro applicazioni esistenti, legge dati condivisi e chiama servizi legacy. Documentarlo e supervisionarlo richiede di sapere dove è innestato e cosa tocca.

Il rinvio di alcuni obblighi previsto dal Digital Omnibus non dovrebbe essere interpretato come un invito ad aspettare, ma come un'opportunità per prepararsi.

Software Intelligence: una mappa, più normative

La Software Intelligence ricava dal codice una rappresentazione oggettiva delle applicazioni: funzionamento, architettura, dipendenze, flussi di dati e debolezze strutturali. La mappa mostra come componenti e processi siano collegati e offre una base comune: inventario degli asset per la NIS2, rischio ICT e di terze parti per DORA, documentazione e tracciabilità per l'AI Act. Le norme non chiedono mappe diverse, ma richiedono di leggere la stessa mappa con lenti diverse.

Ripetendo l'analisi nel tempo, debolezze strutturali, componenti obsoleti e vulnerabilità diventano indicatori utili a verificare se gli interventi riducono davvero il rischio.

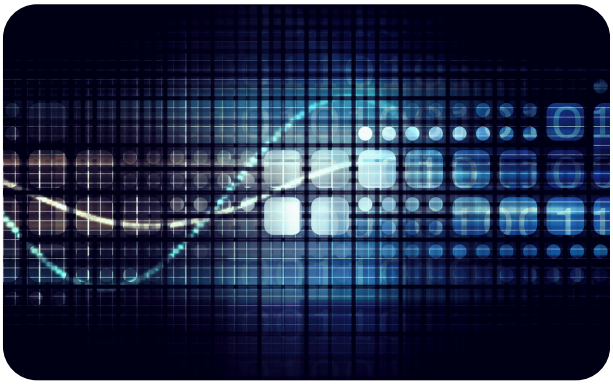
La resilienza si gioca anche nel codice che si modifica

L'European Chips Act richiama l'attenzione sulla resilienza dell'intera filiera digitale. La filiera non termina con i semiconduttori: prosegue nel software che sostiene servizi e processi. Conoscere i propri sistemi significa comprendere anche la propria parte di questa catena di dipendenze.

Un assistente che genera codice non è automaticamente un sistema ad alto rischio ai sensi dell'AI Act, ma il codice prodotto può essere integrato in un sistema di pagamento, in un servizio sanitario o in un'infrastruttura critica. La criticità dipende dal componente modificato, dalle sue dipendenze e dalle conseguenze di un errore. Se la regolazione guarda allo strumento, la governance deve guardare all'impatto.

La compliance, in questa prospettiva, non frena l'innovazione: la stessa mappa che serve per essere conformi è quella che permette di far lavorare l'AI in sicurezza sui sistemi esistenti.

La sfida non è soltanto accelerare lo sviluppo, ma governare il cambiamento: capire prima, trasformare con l'AI, verificare con le evidenze.



Quando un estraneo ruba i tuoi cookie: il punto in cui privacy e cybersecurity si incontrano



A cura di Laura Valentini

Per molti utenti i cookie sono ancora quella fastidiosa finestra che compare quando si apre un sito web e che bisogna chiudere, accettare o configurare prima di poter continuare a navigare.

Per chi si occupa di protezione dei dati personali il discorso è, ovviamente, molto diverso: consenso, profilazione, pubblicità comportamentale, tracciamento, cookie wall, corretta configurazione dei banner. Temi sui quali discutiamo ormai da anni.

Ma c'è un altro aspetto del quale, secondo me, parliamo ancora troppo poco: i cookie sono anche una questione di sicurezza.

Una ricerca condotta da NordVPN sui dati raccolti dagli infostealer tra giugno 2025 e giugno 2026 ha individuato oltre 52 miliardi di cookie sottratti. Per dare una dimensione al fenomeno: nel dataset analizzato erano oltre quattro volte più numerosi rispetto a tutte le altre categorie di dati rubati considerate complessivamente.

A questo punto la domanda sorge abbastanza spontanea: perché un criminale informatico dovrebbe essere così interessato ai nostri "biscottini"?

Non tutti i cookie servono soltanto a ricordare le nostre preferenze.

I cookie possono svolgere funzioni molto diverse.

Alcuni permettono ad un sito di ricordare determinate preferenze, altri vengono utilizzati per finalità statistiche o pubblicitarie, altri ancora sono collegati alla gestione dell'autenticazione e delle sessioni.

Ed è su questi ultimi che vale la pena soffermarsi.

Un cookie di sessione può consentire al sito di riconoscere un utente che ha già effettuato l'accesso. Se viene sottratto da un dispositivo compromesso mentre la sessione è ancora valida, un attaccante può tentare di riutilizzarlo per presentarsi al servizio come se fosse l'utente già autenticato.

Tradotto: in determinate circostanze potrebbe non avere nemmeno bisogno di conoscere la password.
È il cosiddetto "session hijacking", il dirottamento della sessione.

Questo non significa, naturalmente, che ogni cookie rubato permetta automaticamente di entrare in un account. Significa però certamente che proteggere le credenziali e trascurare ciò che accade sul dispositivo e sul browser - dal quale quelle credenziali vengono utilizzate - non è una grande strategia di sicurezza.

Anche un cookie che non apre una porta può raccontare molto.



Non ci sono, però, soltanto i cookie di sessione.

Cookie pubblicitari, identificatori e strumenti di tracciamento possono fornire informazioni sulle nostre abitudini di navigazione, sui servizi che utilizziamo, sui nostri interessi e sui comportamenti online.

E qui emerge un aspetto che, anche dal punto di vista della protezione dei dati personali, non dovrebbe essere sottovalutato: un dato apparentemente poco significativo può diventare molto più interessante quando viene messo in relazione con altri dati.

Se ai cookie aggiungiamo indirizzi e-mail, credenziali, dati di compilazione automatica, file e informazioni sul dispositivo, il quadro cambia.

Il rischio non dipende più dal singolo elemento, ma dalla capacità di collegare informazioni diverse e ricostruire un profilo sufficientemente dettagliato della persona. Un patrimonio informativo che può essere utilizzato anche per rendere molto più credibili phishing, social engineering e altre forme di attacco mirato.

Privacy e cybersecurity: continuare a separarle non ha molto senso.

Questo, a mio avviso, è il punto sul quale vale davvero la pena soffermarsi.

Nella pratica professionale continuo a vedere organizzazioni nelle quali privacy e sicurezza informatica vengono gestite come due compartimenti separati.

Da una parte il GDPR, con informative, registri, nomine e procedure, affidato al consulente privacy, al DPO o all'ufficio legale.

Dall'altra firewall, antivirus, autenticazione, aggiornamenti e gestione degli endpoint, materia dell'IT.

Una divisione molto ordinata sulla carta. Molto meno nella realtà.

Il GDPR, del resto, non ha mai concepito la protezione dei dati personali come un esercizio esclusivamente documentale. L'art. 32 richiede al titolare e al responsabile del trattamento l'adozione di misure tecniche e organizzative adeguate al rischio ed il considerando 39 richiama espressamente la necessità di garantire un'adeguata sicurezza dei dati personali.

Quindi no: la sicurezza informatica non è un argomento "altro" rispetto alla compliance privacy.

Ne fa parte.

E vicende come quella dei miliardi di cookie sottratti dagli infostealer servono anche a ricordarcelo.

Gli infostealer sono malware progettati per sottrarre informazioni dai dispositivi compromessi: credenziali memorizzate, cookie, dati di compilazione automatica, file e altre informazioni presenti nel browser o nel sistema.

E non servono necessariamente attacchi degni di un film.

Phishing, allegati malevoli, falsi aggiornamenti, software proveniente da fonti non affidabili e download compromessi possono essere sufficienti.

Per questo continuo a ritenere che la formazione delle persone sia una delle misure di sicurezza più concrete che un'organizzazione possa adottare.



Non l'unica, certamente, e non può diventare l'alibi per scaricare sull'utente responsabilità che spettano all'organizzazione. Ma resta indispensabile.

Password robuste, autenticazione a più fattori, aggiornamenti, protezione degli endpoint, corretta gestione delle sessioni e configurazioni adeguate devono convivere con procedure comprensibili e persone che sappiano riconoscere almeno i comportamenti maggiormente rischiosi.

Perché quando un incidente di sicurezza coinvolge dati personali, il problema smette molto velocemente di essere soltanto dell'IT.

Diventa valutazione del rischio per gli interessati, gestione del data breach, accountability e, quando ne ricorrono i presupposti, notifica al Garante e comunicazione agli interessati.

Ed ecco che i due mondi che avevamo diligentemente tenuto separati tornano inevitabilmente ad incontrarsi.

La compliance, da sola, non protegge nessuno se rimane sulla carta!

Possiamo avere informative perfettamente aggiornate, registri dei trattamenti completi, nomine correttamente predisposte e procedure formalmente impeccabili, ma non possiamo pensare che questo significhi, da solo, avere protetto i dati personali.

Allo stesso modo, possiamo avere un'infrastruttura tecnologica eccellente, ma se non sappiamo chi deve fare cosa quando qualcosa va storto, se le responsabilità non sono definite e se chi utilizza quotidianamente i sistemi non è formato, manca comunque un pezzo importante.

È per questo che preferisco parlare di sistema di protezione dei dati, piuttosto che di una serie di adempimenti.

La parte giuridica, quella organizzativa e quella tecnica devono necessariamente dialogare, e devono farlo in maniera semplice. E più aumenta la complessità dei sistemi che utilizziamo, meno possiamo permetterci che procedano ciascuna per conto proprio.

I 52 miliardi di cookie sottratti fanno certamente notizia.

Ma forse la parte più interessante di questa ricerca non è il numero.

È ricordarci che dietro quello che chiamiamo genericamente "dato" può esserci una sessione autenticata, un'identità digitale, un insieme di abitudini, interessi e comportamenti e, alla fine di tutto, una persona.

Ed è proprio quella persona che dovremmo ricordarci di proteggere quando parliamo tanto di privacy quanto di cybersecurity.



NIS2: la sicurezza si costruisce nel budget 2027



A cura di Enzo Veiluva

L'attuazione delle misure di base NIS 2 rappresenta la costruzione delle fondamenta del sistema europeo di sicurezza, non il punto di arrivo. Per le aziende è il momento di finanziare un percorso che unisca tecnologie, procedure e competenze, con un orizzonte di lavoro almeno biennale.

È oramai chiaro a tutti che la scadenza di ottobre 2026 non ha concluso il percorso della NIS2. Per i soggetti inseriti nell'elenco NIS nel 2025, il termine richiamato dall'Agenzia per la cybersicurezza nazionale riguarda l'attuazione delle misure di sicurezza di base. Considerarlo il momento in cui archiviare l'adeguamento, in attesa delle misure rafforzate sarebbe però un errore: la sfida è trasformare quanto avviato in una capacità stabile di proteggere dati, sistemi e continuità operativa e definirne il mantenimento nel tempo.

Per questo le aziende devono definire da subito un budget per il 2027. La sicurezza non può dipendere soltanto da scadenze ed emergenze: richiede investimenti iniziali, risorse per la gestione e margini per migliorare. E L'attuazione delle misure di base NIS 2 rappresenta la costruzione delle fondamenta del sistema europeo di sicurezza, non il punto di arrivo. Per le aziende è il momento di finanziare un percorso che unisca tecnologie, procedure e competenze, con un orizzonte di lavoro almeno biennale.

È fondamentale comprendere che il mantenimento del sistema NIS 2 richiederà:

- attività periodiche di aggiornamento e revisione;
- evoluzione delle misure tecniche e organizzative;
- rafforzamento progressivo delle capacità operative richieste dai nuovi standard normativi;
- sostenibilità operativa delle strutture interne;
- incrementi di costi che perverranno dai propri fornitori.

Non si tratta di spendere di più a prescindere, ma di assegnare priorità, responsabilità e coperture economiche agli interventi necessari, partendo dai rischi e dai servizi da garantire.

L'acquisizione di tecnologie sarà una componente rilevante di questo percorso, ma il costo non si esaurisce nell'acquisto. Gli strumenti devono essere integrati, aggiornati e utilizzati da persone competenti.

Una piattaforma di monitoraggio serve se qualcuno analizza le segnalazioni e interviene; individuare una vulnerabilità è utile se esiste un processo per correggerla; le copie di sicurezza devono accompagnarsi a prove di ripristino. Licenze, manutenzione, supporto e competenze vanno quindi pianificati insieme.



Il budget 2027 va ragionato sulle attività che dovranno essere messe in campo:

- formazione continua del personale tecnico, amministrativo e dirigenziale;
- aggiornamento periodico delle competenze specialistiche;
- attività di audit interno ed esterno;
- verifiche di conformità e assessment periodici;
- monitoraggio continuo delle misure implementate;
- gestione documentale e aggiornamento delle procedure;
- potenziamento dei presidi di cybersecurity interne e verso i fornitori;
- servizi di reperibilità e supporto operativo esteso;
- gestione degli incidenti e attività di remediation;
- adeguamento costante alle evoluzioni normative e tecnologiche;
- revisione delle architetture digitali e dei modelli organizzativi.

Sono solo alcune voci che andrebbero prese in considerazione, per un'attuazione efficace e mantenimento nel tempo del “sistema sicurezza”.

Altrettanto importante è consolidare le procedure.

Un documento approvato non basta: occorrono responsabilità chiare e processi conosciuti e verificati per consentirne la piena applicazione.

Il budget deve finanziare anche questo lavoro, evitando che la dimensione organizzativa resti separata dell'investimento tecnologico.

Lo stesso vale per i fornitori: affidare un servizio all’esterno non elimina la necessità di chiarire le responsabilità, verificare le garanzie e governarne il funzionamento.

La programmazione dovrebbe prevedere sia il costo del servizio sia le risorse interne necessarie a seguirlo. È nell’integrazione tra tecnologie, persone e processi che prende forma un percorso di sicurezza rafforzato.

Per sostenerlo è opportuno guardare almeno al biennio 2027–2028: non come a una nuova scadenza normativa, ma come a un orizzonte gestionale.

Consolidare i controlli ed applicarli, completare le integrazioni ed investire nelle tecnologie per provare le capacità di risposta sono priorità da affiancare al miglioramento continuo, senza rinviare gli interventi urgenti.

La scadenza di ottobre è stata dunque una tappa, non il traguardo. Il budget 2027 sarà la scelta con cui trasformare la conformità iniziale in un investimento duraturo nella resilienza dell’azienda.



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 italiana delle imprese digitali e rappresenta le aziende dell'ecosistema tecnologico e digitale italiano. Aderisce a Confcommercio, 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.



Confcom

Assintel

CYBER Think Tank ASSINTEL