La BCE esige un piano. Siete in grado di fornirlo?

La preparazione informatica di fronte all'IA deve essere garantita e dimostrata. Un quadro dei fatti, delle esigenze e delle soluzioni.

Scadenza: 31 ottobre 2026 — Piano d'azione trasmesso al Joint Supervisory Team, con responsabile nominato, budget e calendario.

L'essenziale in breve

La BCE richiede a 109 enti significativi un piano d'azione di cybersicurezza di fronte all'IA, da consegnare entro il 31 ottobre 2026, indirizzato personalmente al presidente del consiglio di amministrazione. Non si tratta di un nuovo corpus normativo, ma di DORA applicato con maggiore rigore: il piano deve essere dimostrabile, non solo plausibile. L'IA riduce infatti la finestra tra la scoperta di una vulnerabilità e l'attacco, da diverse settimane a pochi minuti, rendendo insufficienti i cicli di patch reattivi. La domanda centrale: sapete in tempo reale quali endpoint gestite, quanto sono esposti, e con quale rapidità potete agire?

01

I fatti

Il 7 luglio 2026, la vigilanza bancaria della BCE ha inviato una lettera ai vertici di tutti gli enti significativi (rif. SSM-2026-0301, firmata dalla presidente del consiglio di vigilanza Claudia Buch). Sono interessate 109 banche sotto vigilanza diretta. Entro il 31 ottobre 2026, devono presentare al proprio Joint Supervisory Team (JST) un piano d'azione con misure concrete, responsabili nominalmente designati, budget e personale assegnati, nonché scadenze vincolanti.

Il fondamento giuridico è DORA, il regolamento (UE) 2022/2554. Non si tratta quindi di un nuovo corpus normativo; gli obblighi esistenti vengono semplicemente precisati. La lettera è accompagnata dall'avvertimento del CERS (Comitato europeo per il rischio sistemico) del 25 giugno 2026, il primo avvertimento cyber nella storia di questo organismo. Allo stesso tempo, il questionario annuale sul rischio informatico è stato posticipato da settembre 2026 a febbraio 2027.

In Italia, la Banca d'Italia ha pubblicato il 17 luglio 2026 una propria comunicazione al mercato, che estende un'esigenza analoga alle banche meno significative e alle altre entità sotto la sua vigilanza diretta. Il rapporto e il relativo piano di lavoro devono essere trasmessi alla Vigilanza entro il 31 dicembre 2026, e non il 31 ottobre.

Ciò che chiede la BCE, in sintesi (lettera del 7 luglio 2026) — ecco cosa richiede la vigilanza entro il 31 ottobre 2026:

1. Presentazione di un piano d'azione di cybersicurezza IA al Joint Supervisory Team (JST) competente
2. Misure concrete anziché dichiarazioni d'intenti, con scadenze vincolanti
3. Responsabili nominalmente designati per ogni misura
4. Budget assegnato e personale allocato
5. Avanzamento dimostrabile in ogni momento nei confronti del JST

02

Perché l'urgenza è reale ora

La pressione non viene dal regolatore, ma dal fronte opposto: gli attaccanti hanno compiuto un salto di capacità. Il cambiamento decisivo si riassume in una sola cifra. Costruire un exploit operativo richiedeva un tempo che andava da giorni a settimane; con i modelli di IA di frontiera, oggi bastano minuti o poche ore.

Il CERS parla di un «collasso dei margini difensivi». Lo standard storico dei 90 giorni prima della divulgazione perde così la sua funzione protettiva.

I dati confermano questa valutazione. Nel suo avvertimento CERS/2026/3 del 25 giugno 2026, l'autorità segnala questo crollo del tempo di realizzazione di un exploit, da giorni o settimane a minuti o ore. Nel primo semestre 2026 sono state censite 35.364 nuove vulnerabilità, contro 23.656 nel primo semestre 2025, un aumento del 49,5%. E il CERT-UE conta, nel suo rapporto Threat Landscape 2025, nove incidenti di sicurezza che hanno coinvolto istituzioni europee, due dei quali con vulnerabilità zero-day.

L'avvertimento del CERS in sintesi (avvertimento CERS/2026/3 del 25 giugno 2026):

I modelli di IA di frontiera riducono il tempo di realizzazione di un exploit da giorni o settimane a minuti o ore

Classificazione come rischio cyber sistemico per il settore finanziario europeo (elevato a giugno 2026 dal livello «alto» a «grave»)

Importante: quando la finestra si riduce da diverse settimane a poche ore, ciò che conta non è più tanto la qualità di ciascun controllo preso singolarmente, quanto la velocità con cui potete vedere la vostra situazione, definirne le priorità e dimostrarla.

03

Una questione di vertice: perché riguarda il consiglio

Che la resilienza informatica debba far parte dell'agenda del consiglio di amministrazione non è un'interpretazione di Tanium: è la posizione esplicita delle stesse autorità di vigilanza e sicurezza.

La lettera è stata indirizzata al CEO, non al CISO. La lettera della BCE (SSM-2026-0301) si rivolge direttamente ai presidenti dei consigli di amministrazione ed esige una struttura di governance: responsabili designati, risorse allocate, scadenze vincolanti.

La vigilanza parla di «rischio sistemico». Il CERS utilizza il registro normalmente riservato ai rischi di stabilità finanziaria, come i rischi di concentrazione o di liquidità: il vocabolario della responsabilità del consiglio, non quello del reparto informatico.

I Five Eyes lo affermano esplicitamente: il rischio cyber è «un rischio aziendale centrale e una responsabilità della alta direzione»; i consigli di amministrazione devono verificare che la resilienza regga a un carico reale e non esista solo sulla carta.

La stessa BCE sceglie un linguaggio di governance e di mercato: nella sua lettera del 7 luglio 2026, Claudia Buch, presidente del consiglio di vigilanza, menziona «possibili ripercussioni profonde sulla riservatezza, l'integrità e la resilienza dei sistemi tecnologici». Una comunicazione di mercato e di vertice, non una nota tecnica interna.

Anche la gestione del rischio lo conferma: nell'Allianz Risk Barometer 2026, il rischio cyber (1° posto, 42%) e l'IA (2° posto, 32%) guidano la classifica dei rischi aziendali globali, secondo un'indagine condotta su 3.338 esperti di gestione del rischio.

04

Ciò che le autorità richiedono in modo unanime

La BCE, il CERS, i Five Eyes, l'ENISA e il CERT-UE formulano, indipendentemente l'uno dall'altro, raccomandazioni ampiamente convergenti. Le tre più citate, in ordine di peso nelle fonti:

1. **Visibilità in tempo reale sull'intero parco di asset.** Una visione completa della rete e dei sistemi informativi viene presentata come il fondamento della definizione delle priorità di patch basata sul rischio; la BCE («identificare e proteggere gli asset esposti a Internet») e i Five Eyes la danno anch'essi per scontata. Senza questa base, i due punti seguenti non sono realizzabili.

2. **Accelerare la gestione delle patch e delle vulnerabilità.** L'esigenza più ripetuta in tutte le fonti: la BCE indica una gestione più rapida delle vulnerabilità come priorità assoluta a breve termine; il CERS misura ora il tempo tra scoperta e sfruttamento in «nettamente meno di un giorno». Avvertimento importante dello stesso CERS: correggere più in fretta senza criterio aumenta il rischio di guasti operativi; l'incidente CrowdStrike del 2024 (oltre 5 miliardi di dollari di danni per le sole aziende Fortune 500) viene citato come esempio di allerta. Il messaggio è dunque: correggere più rapidamente, ma con trasparenza e controllo.

3. **Ridurre la superficie di attacco.** Per i Five Eyes, la misura pratica numero uno: limitare gli accessi non necessari e l'accessibilità esterna, chiedendosi se alcuni sistemi debbano davvero essere esposti. La BCE e l'ENISA danno priorità ai sistemi esposti a Internet, al software di terze parti e alle componenti open source: si può ridurre solo ciò che è visibile.

Seguono, con un forte consenso: la gestione dei sistemi legacy e a fine vita (Five Eyes: «impegni strategici»), il monitoraggio e il rilevamento assistiti dall'IA sotto controllo umano, la gestione delle identità e degli accessi comprese le identità non umane, i rischi legati a terzi e ai fornitori di IA compresa la pianificazione di uscita (richiesta da DORA), piani testati di risposta agli incidenti e di gestione delle crisi, e, a fare da cornice a tutto ciò, la governance e la responsabilità a livello di consiglio di amministrazione.

Anche qui: tutte queste raccomandazioni provengono dalle autorità e dalle istituzioni citate, non da Tanium.

05

Cinque domande che il CEO deve porre

Il consiglio di amministrazione risponde personalmente del piano d'azione. Le cinque domande seguenti derivano direttamente dalle aspettative formulate dalla BCE e dal CERS nelle loro comunicazioni; dovrebbero poter trovare risposta in ogni momento.

Prima — Copertura e aggiornamento dei dati: possiamo individuare in ogni momento, senza lacune, quali endpoint, server e carichi di lavoro cloud gestiamo, compresi i sistemi non gestiti e obsoleti? Una risposta solida è possibile solo con un inventario in tempo reale che renda visibili anche i sistemi sconosciuti e obsoleti, non con una CMDB risalente al mese scorso.

Seconda — Velocità di reazione: in quanto tempo correggiamo una vulnerabilità critica, e questa cifra resiste a una verifica? Serve un tempo medio di correzione misurato e con marcatura temporale, non una stima approssimativa.

Terza — Capacità di dimostrazione: potremmo presentare al JST, in tempi brevi, l'avanzamento documentato del nostro piano? Solo se i report possono essere generati con un clic a partire da un'unica fonte di dati, senza doverli raccogliere manualmente durante la notte.

Quarta — Terzi e dipendenze: quali fornitori hanno accesso ai nostri sistemi, e quanto ne dipendiamo? È richiesta una visione documentata degli accessi e delle dipendenze, come previsto da DORA.

Quinta — Responsabilità e governance: chi è il titolare nominale del piano d'azione, con mandato e budget? Serve una persona designata e raggiungibile, non un comitato né una dichiarazione d'intenti.

Dall'esigenza della vigilanza alla risposta operativa: la BCE, il CERS e i Five Eyes indicano cosa fare — visibilità in tempo reale senza lacune su tutti gli asset, tempi di reazione dimostrabilmente brevi e avanzamento documentato, sotto la responsabilità del consiglio. Come raggiungere questo obiettivo sul piano operativo resta aperto. È proprio qui che si trova l'ostacolo reale per la maggior parte degli enti: decine di soluzioni isolate, una CMDB che non riflette la realtà del parco, e prove che devono essere raccolte manualmente. La prospettiva di soluzione che segue mostra come colmare questo divario di attuazione.

06

Prospettiva di soluzione · Tanium

Il fondamento di un piano d'azione solido: invece di decine di soluzioni isolate e una CMDB che non riflette la realtà del parco, Tanium punta su un'unica piattaforma. Un agente leggero su ogni dispositivo e un'architettura a catena lineare (peer-to-peer) interrogano direttamente l'intero parco e forniscono risposte su oltre 100.000 endpoint in meno di 15 secondi, scalabile fino a milioni di dispositivi, senza server di inoltro. Ne risulta una base dati comune e sempre aggiornata, su cui convergono visibilità, patch e prova. Tanium rileva attivamente i dispositivi non gestiti (Forrester: oltre il 98% di copertura), proprio i sistemi che altrimenti indebolirebbero il piano d'azione.

Exposure Management valuta le vulnerabilità e la superficie di attacco in base al rischio reale e rende visibili le dipendenze da terzi, in modo che lo sforzo si concentri dove riduce davvero il rischio. E la prova da un'unica fonte genera report pronti per la vigilanza con un clic, a partire da un'unica base dati; l'avanzamento può essere dimostrato al Joint Supervisory Team in pochi minuti, anziché essere raccolto durante notti intere.

In concreto, questo si traduce in quattro aspetti. Asset Visibility & Discover individua e inventaria tutti gli endpoint, server e carichi di lavoro cloud, compresi quelli non gestiti e obsoleti; questo elimina i punti ciechi e fornisce dati di inventario che resistono a un controllo di vigilanza. Autonomous Patch Management dà priorità alle vulnerabilità critiche e distribuisce le patch sull'intero parco senza attendere una finestra di manutenzione, così che il tempo di correzione si riduce e diventa dimostrabile, un indicatore anziché una stima.

In cifre:

<15 sec	**98%+**	**300.000**
per una risposta su oltre 100.000 endpoint	degli endpoint rilevati (Forrester)	endpoint in oltre 40 paesi

Fonti

Vigilanza bancaria della BCE, lettera ai vertici degli enti significativi (rif. SSM-2026-0301), 7 luglio 2026. bankingsupervision.europa.eu

CERS, avvertimento CERS/2026/3 «sui rischi cyber sistemici legati ai modelli di intelligenza artificiale di frontiera», 25 giugno 2026. esrb.europa.eu

ENISA, Threat Landscape 2025, pubblicato a ottobre 2025 (periodo luglio 2024 - giugno 2025). enisa.europa.eu

FIRST, 2026 Mid-Year Vulnerability Forecast, 15 giugno 2026. first.org

CERT-UE, Threat Landscape Report 2025 — A Year in Review, pubblicato ad aprile 2026. cert.europa.eu

DORA — Regolamento (UE) 2022/2554 sulla resilienza operativa digitale del settore finanziario, 14 dicembre 2022.

BCE, Supervisory Banking Statistics T1 2026 (numero di enti significativi), 19 giugno 2026. bankingsupervision.europa.eu

Five Eyes, linee guida comuni sulle minacce cyber accelerate dall'IA, 2026.

Allianz, Risk Barometer 2026 (indagine su 3.338 esperti di gestione del rischio). allianz.com

Tanium, Platform Architecture e Tanium Discover; studio Forrester Consulting 2021 (> 98% di rilevamento). tanium.com

Tanium, Forrester Wave: Endpoint Management Platforms T2 2026 (Leader); casi cliente JLL e Barclays. tanium.com

Banca d'Italia, Comunicazione al mercato, 17 luglio 2026; Circolare 285, 51° aggiornamento, febbraio 2026. bancaditalia.it

Tanium non intrattiene alcun rapporto con la BCE, il CERS o qualsiasi altra autorità di vigilanza citata, e non rivendica alcun sostegno da parte loro. Tutte le affermazioni di natura regolamentare sono citate con la relativa fonte originale.

TANIUM

Autonomous IT. Unstoppable Business.