CENTRO STUDI TIM

Verso la NIS2

Gli effetti sulle imprese e sull'economia italiana della nuova Direttiva sulla cybersecurity

Introduzione

La crescente digitalizzazione delle imprese espone il sistema produttivo globale ad attacchi cibernetici sempre più frequenti e sofisticati che rendono inefficaci le politiche vigenti in termini di sicurezza informatica e di protezione dei dati. La normativa NIS (Network Information Security) è stata rivista dalla Commissione Europea alla luce di questo nuovo scenario, che si aggiunge ad una crescente instabilità geo politica e la comparsa di un nuovo tipo di criminalità legato al sabotaggio di sistemi informatici ed al furto di dati personali ed aziendali.

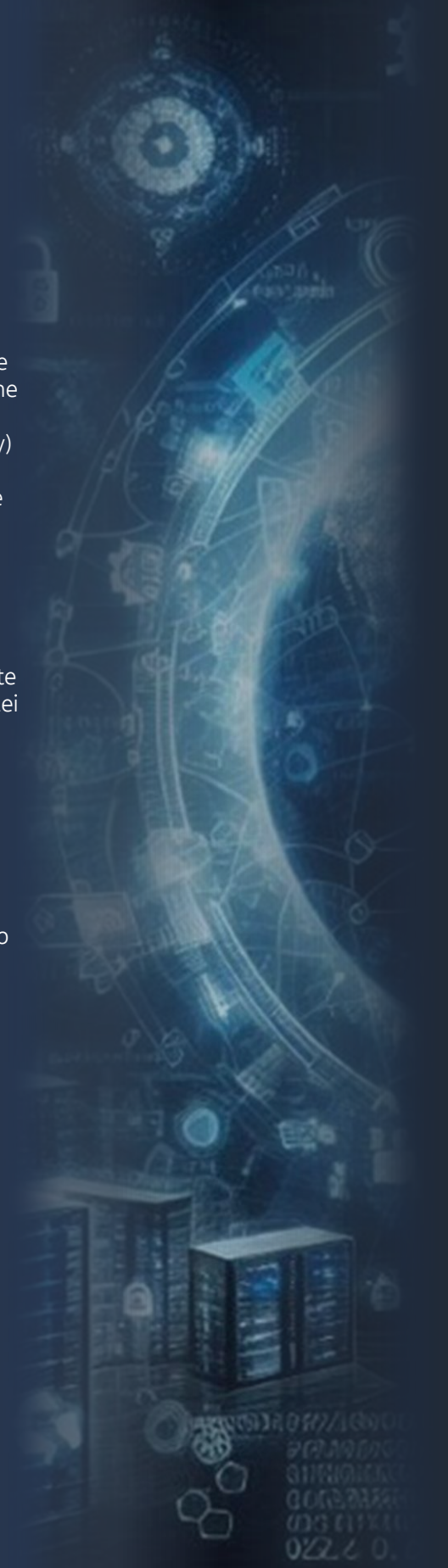
La NIS2 si propone di adeguare gli standard di sicurezza informatica e di lotta al cybercrime nel nuovo contesto, che vede le imprese sempre più connesse e quindi esposte a rischi di natura digitale, mettendo a repentaglio i dati dei clienti e con essi la loro reputazione sul mercato. Gli attacchi verso la singola azienda si possono propagare e compromettere la sicurezza di intere filiere sino a configurarsi come rischio a livello di sistema Paese.

Questo studio vuole analizzare gli impatti economici e le esternalità positive dall'adozione della NIS2 in Italia partendo dall'analisi dello scenario di cybersicurezza nazionale. Le risultanze sono una elaborazione del Centro Studi TIM di dati provenienti delle principali fonti in materia, come l'Agenzia di Cybersicurezza Nazionale (ACN) o la stessa Commissione Europea che ha prodotto la normativa usando anche dati del SOC di TIM.

Lo studio si prefigge inoltre di studiare i benefici per le aziende dall'adozione della NIS2 ed il beneficio a livello paese

Buona lettura

CENTRO STUDI
TIM

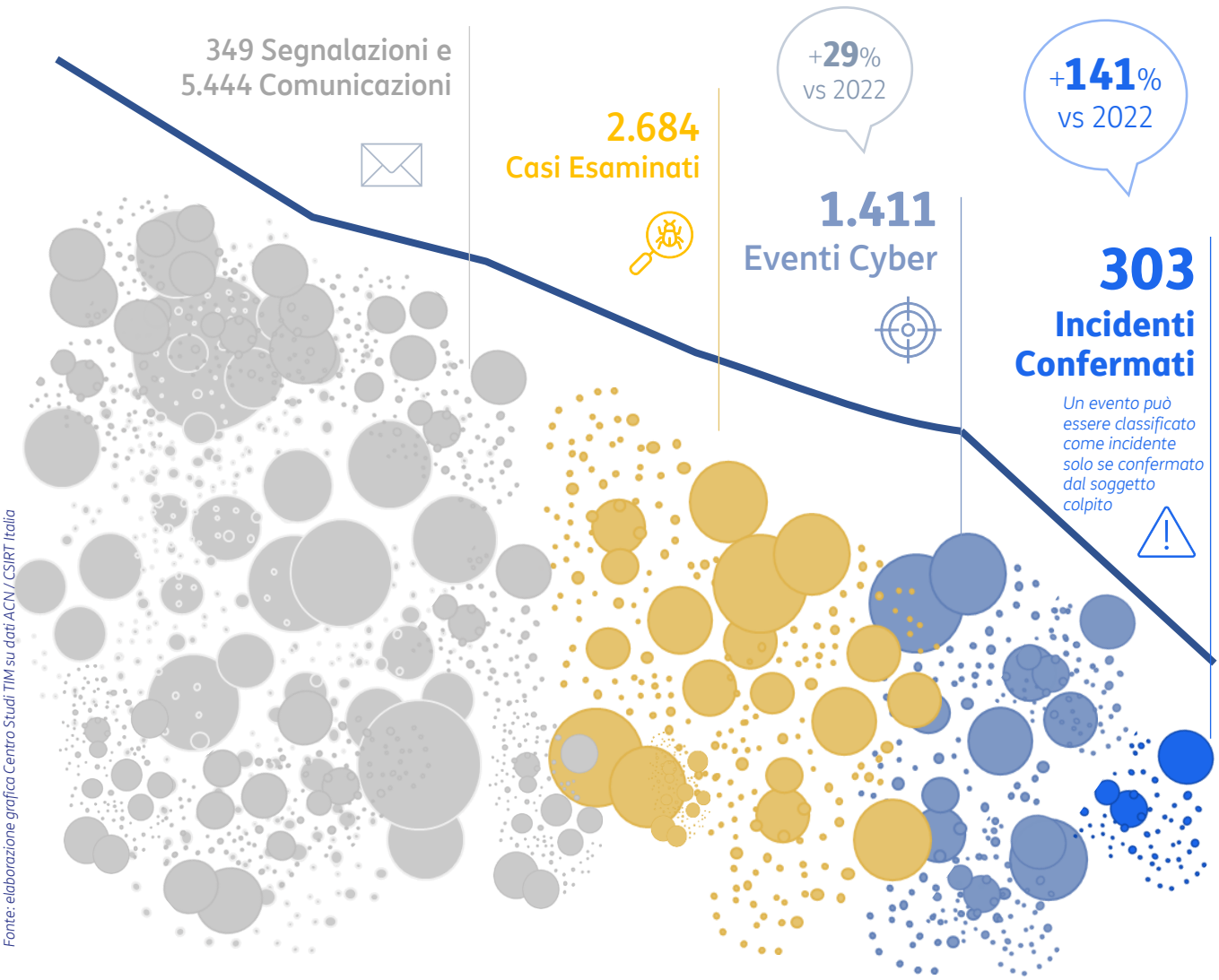


Lo scenario Cyber in Italia

Numeri rilevanti in Italia
Gli eventi cyber rilevati dall'ACN

In Italia il numero di attacchi cyber è in forte crescita con un'accelerazione molto significativa negli ultimi anni. Il numero di eventi cyber gestiti nel 2023 dallo CSIRT Italia – la struttura tecnico operativa dell'Agenza di Cybersecurity Nazionale (ACN) – è stato di 1411 unità (+29%) a fronte di oltre 5.400 comunicazioni ricevute, di cui 2684 esaminate per verificare eventuali conseguenze.

Questa mole di eventi ha generato 303 incidenti, ossia casi accertati in cui l'evento ha generato conseguenze in termini di integrità, disponibilità o confidenzialità delle informazioni del soggetto colpito. Il numero degli incidenti cresce del 141% rispetto all'anno precedente (erano stati 126 nel 2022).



Fonte: elaborazione grafica Centro Studi TIM su dati ACN / CSIRT Italia

UN FENOMENO CHE STA ESPLODENDO: CRESCITE A TRE CIFRE

Secondo i dati di CSIRT Italia, riportati nella Relazione Annuale dell'ACN, sono stati 3302 i soggetti target di attacchi informatici (+187%) in forte crescita gli asset a rischio: sono 3624 quasi 4 volte quelli del 2022 (764), una forte accelerazione dettata dalla maggior dipendenza di imprese e cittadini dal digitale ma anche dal deterioramento del quadro geopolitico globale che ha portato ad un forte impulso del cybercrime.

Segnalazioni
+331%

Incidenti
+141%

Soggetti Target
+187%

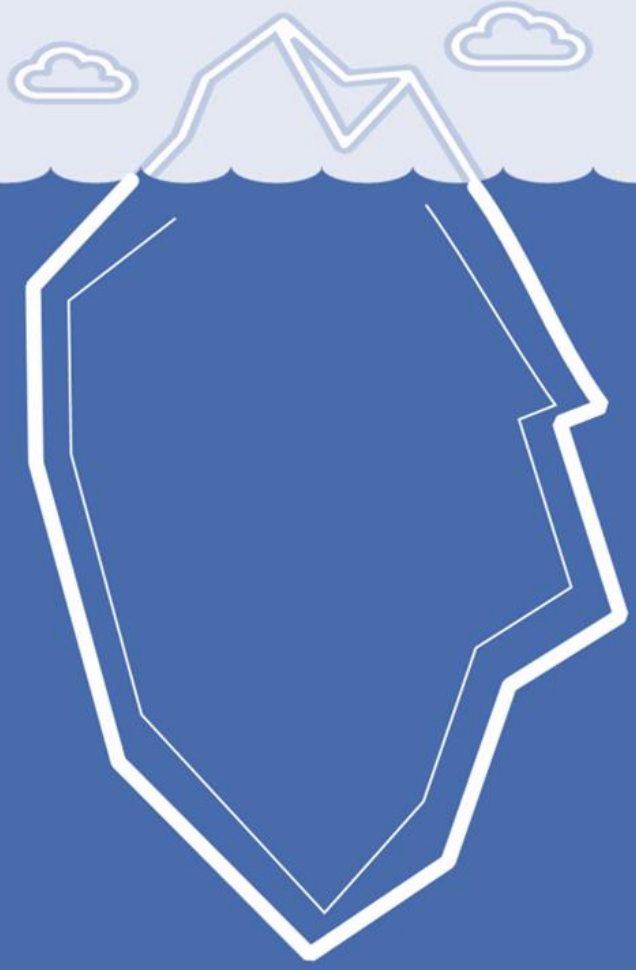
Asset a Rischio
+374%

***Fonte**: Relazione Annuale ACN 2023*

CON DIMENSIONI ANCORA PIÙ ESTESE RISPETTO ALLE RILEVAZIONI UFFICIALI

La crescita degli eventi cyber registrata dall'ACN mostra quanto il fenomeno sia in forte crescita, ma la portata va oltre le rilevazioni ufficiali

Spesso gli incidenti resi noti sono solo una frazione di quelli che avvengono, essendo quelli riportati da enti pubblici od aziende medio-grandi per normativa vigente.



Imprese con più di 10 addetti in Italia

0,25 milioni

Rimangono fuori dal conteggio gli incidenti non rilevati o non riportati da entità che non hanno l'obbligo di comunicazione (es. PMI) anche per evitare danni reputazionali. Il mancato rilevamento e reporting di incidenti impedisce azioni di mitigazione moltiplicando i rischi di incidenti lungo la filiera con conseguenti danni economici a tutto il sistema Paese.

Imprese con meno di 10 addetti in Italia

4,4 milioni

All'incirca il 95% del totale

Fonte: Elaborazione Centro Studi TIM su dati ISTAT

CENTRO STUDI TIM

Diverse tecniche di attacco
DDoS e Malware i più diffusi

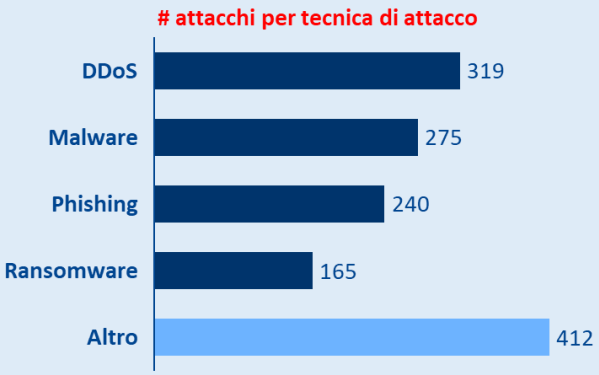
Tra le tecniche di attacco informatico in Italia prevalgono gli attacchi di tipo DDoS (Distributed Denial of Service). Questo tipo di attacco è in forte ascesa con l'inasprirsi della situazione geopolitica, dal momento che sono spesso utilizzati per creare tensioni da gruppi affiliati a Stati (State-sponsored Groups).

Il Distributed Denial of Service (DDoS) rappresenta la tecnica d'attacco più utilizzata nel 2023 (319 attacchi) che crea maggiori incidenti in Italia (111) con la maggior incidenza (38% degli incidenti) e crescita (+35 p.p, rispetto al 2022). Una delle principali ragioni per sferrare un attacco DDOS è quella di interrompere dei servizi di utilità pubblica (es. prenotazioni in strutture sanitarie) provocando danni economici e interruzioni ad infrastrutture e servizi essenziali di un paese.

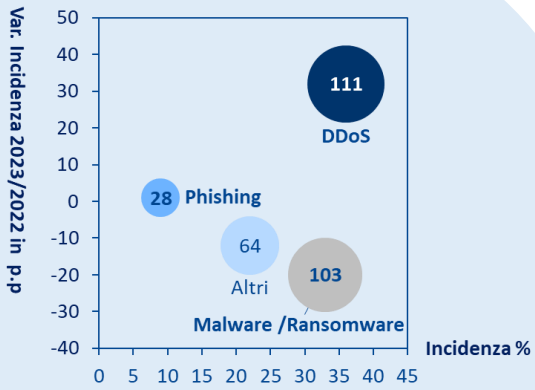
In questo quadro, il DDoS diventa uno strumento offensivo utilizzato per la cosiddetta guerra ibrida, al pari di altre tecnologie digitali. Questo tipo di attacco ha effetti anche sulle imprese, mettendo a rischio la loro continuità operativa, con potenziali ripercussioni a lungo termine sulla fiducia dei clienti e sulla reputazione aziendale anche presso gli investitori.

Gli attacchi DDoS si stanno non solo intensificando ma anche sofisticando grazie a nuove strategie di attacco creando incidenti con sempre maggiore intensità

Attacchi



Incidenti



Fonte: Elabprazione Centro Studi TIM da Report Annuale ACN

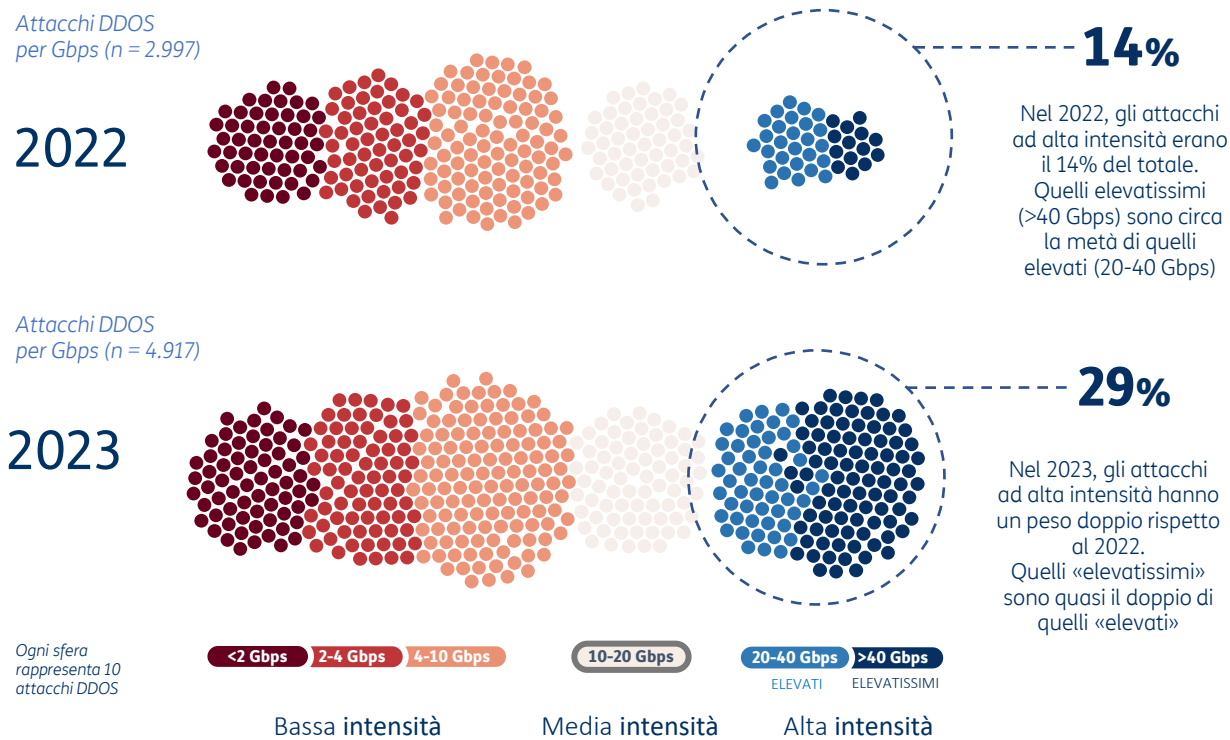
Attacchi DDoS
nel 2023 raddoppia il «peso» degli attacchi ad alta intensità

Il fenomeno degli attacchi ad alta intensità può essere meglio osservato confrontando gli attacchi DDOS 2023 con quelli dell'anno precedente.

Nel 2022, gli attacchi ad alta intensità, ossia superiori a 20 Gbps erano stati il 14% del totale, all'incirca la metà in termini di incidenza rispetto al 2023. Il grafico riportato in basso mostra in modo evidente quanto siano cambiate le proporzioni tra le diverse classi di intensità tra un anno e l'altro.

In particolare, si può notare come non solo cresca il peso degli attacchi ad alta intensità sul totale, ma anche come, all'interno di questa classe, gli eventi ad intensità elevatissima, superiore ai 40 Gbps, diventino più rilevanti di quelli che hanno una intensità tra i 20 ed i 40 Gbps. Anche questo è una spia di come si stia modificando il panorama degli attacchi DDOS.

Attacchi DDoS in Italia per livello di intensità: 2022 vs 2023



Fonte: Gruppo TIM

ANCHE A LIVELLO EUROPEO, DDOS e RANSOMWARE SONO GLI ATTACCHI PIÙ DIFFUSI

L'ENISA, l'agenzia della cybersecurity europea, nell'ambito dello European Threat Landscape, individua 8 tipi di attacchi cyber, eventi diretti consapevolmente ad arrecare danno ad organizzazioni, aziende e privati per finalità differenti.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

THE HATEFUL EIGHT

Attacco DDOS (Distributed Denial of Service). Mira a rendere inutilizzabile una risorsa e/o un servizio sovraccaricando i componenti delle infrastrutture di rete

RANSOMWARE. Mira a prendere il controllo delle risorse (dati, asset, ecc.) per chiedere un riscatto. In crescita: attacchi a doppia estorsione con esfiltrazione preventiva di dati

Minacce di INGEGNERIA SOCIALE. Comprende un'ampia gamma di attività che sfruttano l'errore con l'obiettivo di ottenere l'accesso a informazioni o servizi.

Attacchi alle CATENE DI FORNITURA. Prendono di mira il rapporto tra organizzazioni e fornitori (es. penetra la rete di un'azienda per esfiltrare dati all'azienda cliente)

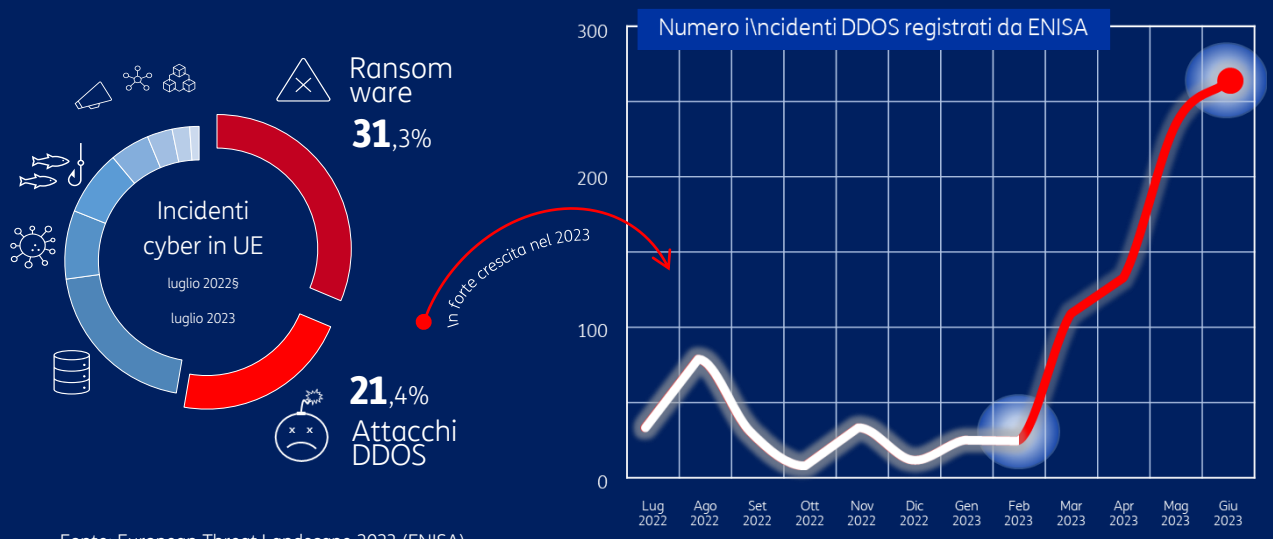
MALWARE. Programma che esegue un processo non autorizzato con impatto negativo sull'integrità o sulla disponibilità o sul funzionamento di un sistema.

Minacce ai DATI. Accesso non autorizzato ai dati per sottrazione, divulgazione e manipolazione. Spesso combinato con ransomware e attacchi DDOS

Minacce alla RETI e ad Internet. Incidenti in cui si verifica un'interruzione intenzionale o non intenzionale dell'accesso ad internet o delle comunicazioni elettroniche

DISINFORMAZIONE. Imprese e privati presi di mira da campagne di disinformazione prevalentemente finalizzate a screditarne la reputazione o creare incertezza

Nell'ultimo rapporto annuale European Threat Landscape di ottobre 2023, l'ENISA evidenziava che le due minacce più diffuse a livello europeo erano rappresentate dal Ransomware e dal DDOS che insieme rappresentavano circa la metà del totale degli attacchi rilevati



Fonte: European Threat Landscape 2023 (ENISA)

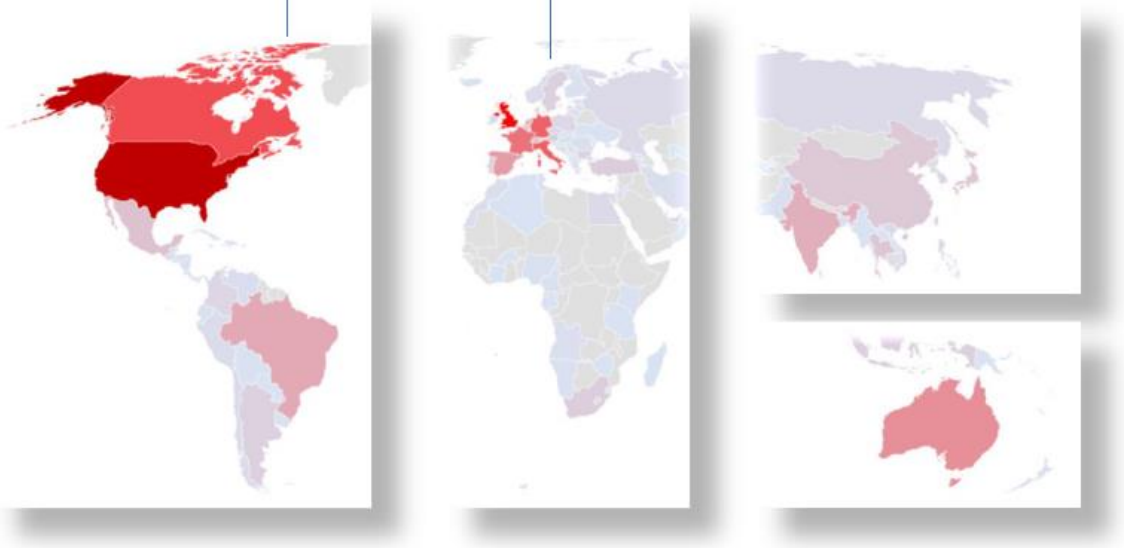
L'ITALIA NELLE CLASSIFICHE EUROPEE E MONDIALI

1° paese
In UE **per attacchi**
Ransomware

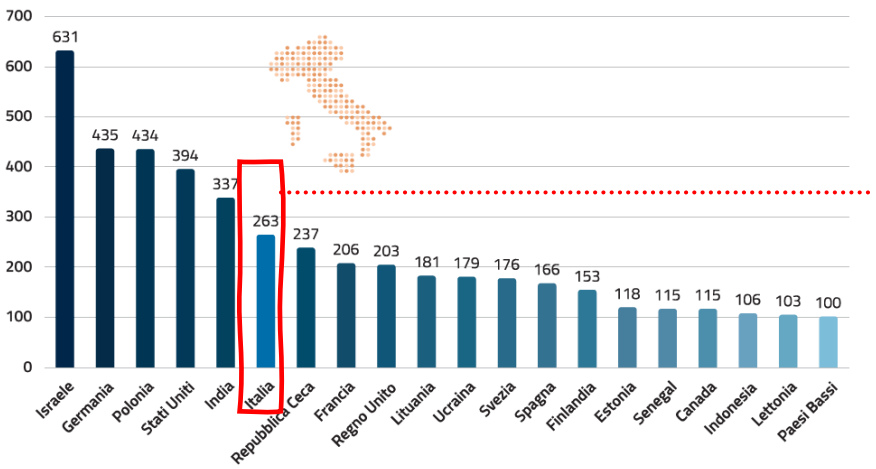
Gli **STATI UNITI** sono il Paese più colpito da attacchi ransomware rivendicati
2.217 attacchi
48% del totale

L'**UNIONE EUROPEA** rappresenta il secondo bersaglio a livello mondiale
884 attacchi
19% del totale

L'**ITALIA** è il primo paese UE per attacchi ransomware complessivi
176 attacchi
~**4**% del totale



Fonte: Gruppo TIM



Fonte: Relazione Annuale 2023 (ACN)

L'Italia è il
6° paese
più colpito
al mondo per attacchi DDoS
(3° in EU)

Confronto internazionale
un Paese più vulnerabile ed in ritardo sugli investimenti in cybersecurity

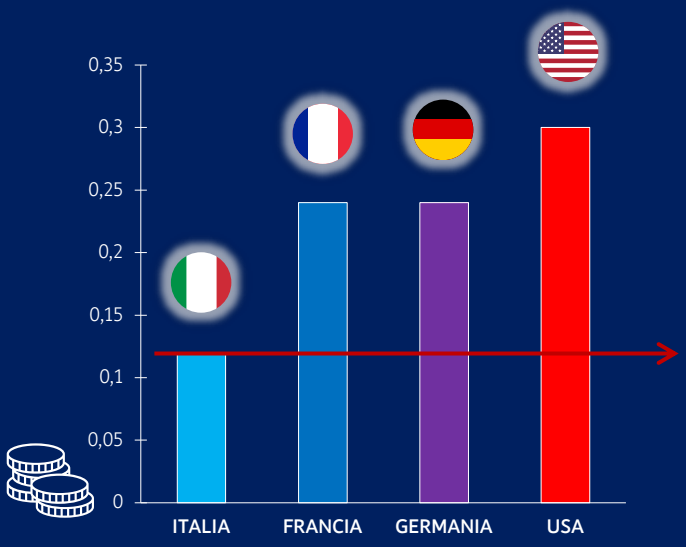
La vulnerabilità del Sistema Italia è fortemente influenzata dal livello di investimenti di aziende e Pubblica Amministrazione in cybersecurity.

Nel 2023, la spesa in cybersecurity in Italia si aggirava attorno ai 2 miliardi di euro, un valore particolarmente basso in rapporto a altri paesi di riferimento. In effetti, questo valore rappresenta all'incirca lo 0,12% del PIL nazionale, mentre in Francia e Germania la spesa in cybersecurity si attesta attorno allo 0,24% - esattamente il doppio rispetto all'Italia – e negli USA questo valore cresce fino allo 0,3% del PIL.

Si può evidenziare anche una più bassa priorità di investimento in cybersecurity rispetto alle altre spese ICT: se guardiamo ai budget stanziati dalle aziende, in Italia si destina alle spese di sicurezza informatica circa il 4,4% del totale ICT, contro una media europea del 9%.

Spesa cybersecurity in rapporto al PIL in Italia

0,12% del PIL



Fonte: Elaborazione Centro Studi TIM

In rapporto al PIL, l'Italia spende la metà di Paesi europei comparabili, come Francia e Germania, e ancora meno rispetto agli USA

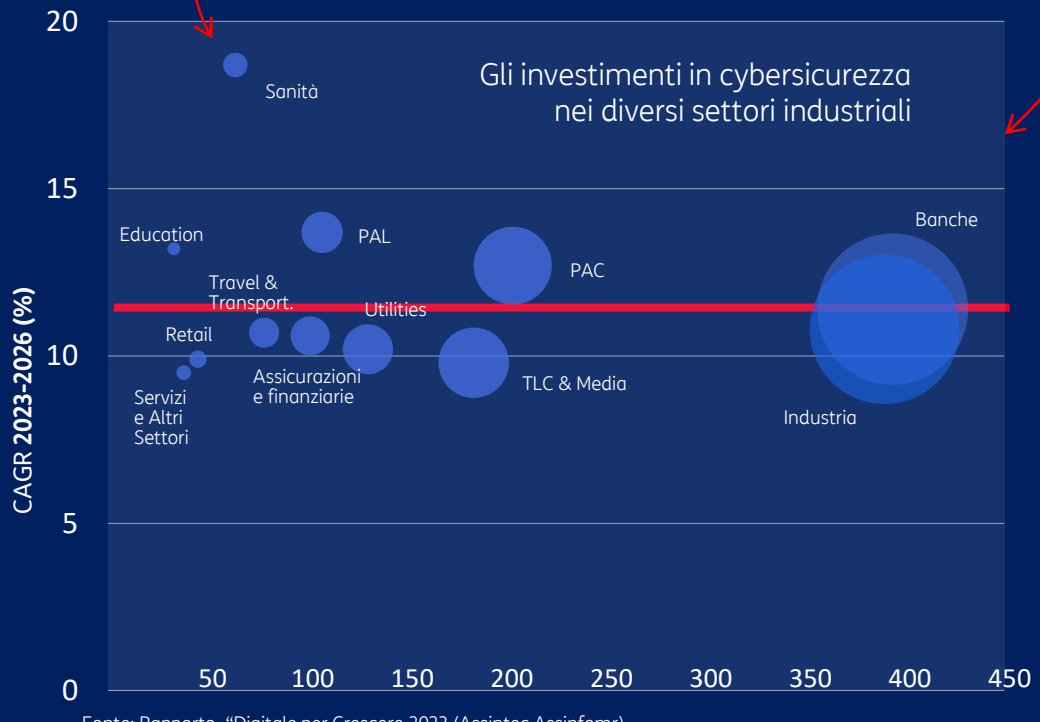
IN ITALIA IL PANORAMA DEGLI INVESTIMENTI IN CYBERSECURITY È MOLTO VARIEGATO

Sanità

il settore con la maggior crescita attesa (+19% in media l'anno tra il 2023 ed il 2026)

Banche e Industria

sono i settori che investono di più in cybersicurezza nel nostro Paese (circa €400 milioni nel 2023)



Fonte: Rapporto "Digitale per Crescere 2023 (Assintec Assinfomr)

Perché è importante che tutti i settori investano in cybersecurity?

Un rischio in crescita: ATTACCHI ALLE CATENE DI FORNITURA

Sempre più spesso gli attaccanti cercano di colpire un obiettivo sfruttando le debolezze dei sistemi di difesa di imprese fornitrici. Questo sistema di attacco attraverso terze parti è in forte crescita. Secondo il Threat Report di ENISA, oltre il 60% delle imprese dichiara di essere stato colpito attraverso le catene di fornitura.

Le imprese e la cybersecurity in Italia

Attacchi Cyber
I servizi pubblici sono un target prioritario

Tutti gli Osservatori concordano sulla crescita molto intensa degli attacchi cyber negl iultimi anni. Molto differente è invece la lettura che ne viene data quando si entra nei dettagli: a seconda dei punti di osservazione e delle tassonomie adottate, la panoramica può assumere una connotazione differente.

Secondo i dati dell'ACN, dei circa 1.400 eventi cyber registrati, poco più di 1.100 sono attribuibili a settori specifici. I restanti eventi sono multitarget, ossia indirizzati a più settori contemporaneamente.

Un'attività di mitigazione preventiva, ad esempio, come quella realizzata dagli operatori di telecomunicazione per gli attacchi di tipo DDoS può ridurre di molto il volume degli eventi che vengono registrati dalle Agenzie Nazionali di Cybersecurity. Un altro aspetto determinante ai fini statistici riguarda il tipo di soggetti colpiti. Alcune imprese ed alcuni settori hanno un obbligo di comunicazione, altri no. La NIS2, ampliando il numero di soggetti e di settori che rientrano in questa casistica, potrà aumentare il volume dei dati raccolti, senza tuttavia arrivare a definire con esaustività il fenomeno.

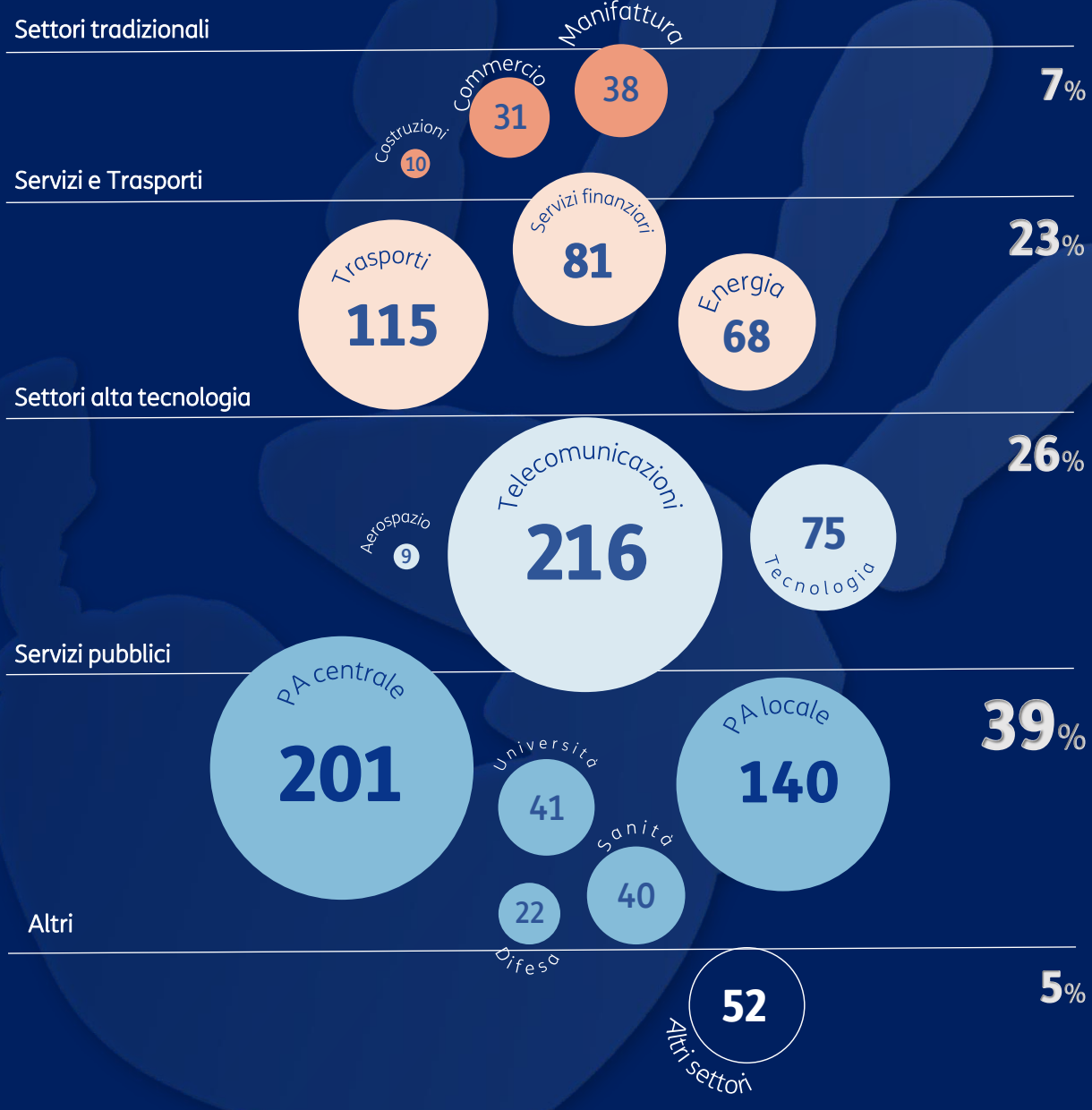
Secondo i dati ACN, il settore più interessato da eventi è quello delle telecomunicazioni anche in considerazione dell'enorme mole di dati gestiti. Gli operatori che si trovano in questo ambito sono chiamati a evidenziare all'ACN tutti gli eventi che osservano sulle proprie reti e infrastrutture. Una «posizione di frontiera» che porta in alto il settore nelle statistiche degli eventi registrati da ACN.

Nel complesso, le imprese che offrono servizi pubblici, la PA centrale e locale, la Sanità, l'Università e la Scuola, la Difesa, attraggono il 40% degli attacchi totali. Dato il loro ruolo istituzionale, questi attori rappresentano un target prioritario per azioni guidate da motivazioni di tipo politico o sociale, da attacchi motivati dall'evoluzione del quadro geopolitico. Un attacco di tipo DDoS può provocare la paralisi di alcune attività, creando disservizi che si propagano in tutto il sistema, interessando cittadini e imprese. Allo stesso tempo, si tratta anche di soggetti che hanno spesso grandi bacini di dati e possono attrarre anche attacchi di tipo ransomware per estorcere somme di denaro rilevanti in cambio dei dati trafugati. Tuttavia i finanziamenti previsti dal PNRR sono destinati a migliorare la protezione degli enti pubblici in Italia.

Come abbiamo visto, non tutti gi eventi si traducono automaticamente in incidenti. Le capacità di difesa, attiva e proattiva dei diversi soggetti possono fare la differenza. All'incirca 1 evento su 4 registrato da ACN si è tradotto in un incidente, con impatto confermato dal soggetto colpito.

ATTACCHI CYBER

PER L'ACN 4 EVENTI SU 10 SI INDIRIZZANO VERSO SERVIZI PUBBLICI



Fonte: Elaborazione Centro Studi TIM su dati ACN

Il settore privato
7 aziende su 10 hanno percepito attacchi in aumento

Le finalità degli attacchi verso il settore privato, che resta uno dei target più esposto ad incidenti informatici, sono molteplici. In alcuni casi, le azioni si pongono l'obiettivo di esfiltrare dati dell'azienda o segreti industriali di enorme valore commerciale.

Quando l'attacco ha una finalità estorsiva, viene richiesto un riscatto (ransomware). Nel corso del tempo questa modalità si è ulteriormente trasformata: i Gruppi Ransomware più strutturati attivano modelli definiti «a doppia estorsione»: per mettere pressione alle vittime si ricorre al blocco/distruzione delle risorse, ma anche ad un'esfiltrazione preventiva di dati ed informazioni che, se diffuse online, creano danni di vario tipo (penali, legali, di concorrenza, reputazionali...).

I fattori di rischio cyber sono molto variegati nelle aziende di qualsiasi dimensione. Singolarmente il fattor di rischio principale è quello umano, dovuto spesso ad una non adeguata formazione e cultura della sicurezza dei dipendenti.

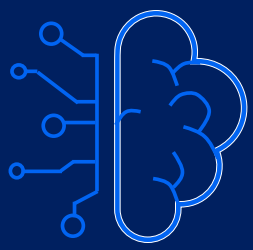
Ma complessivamente sono i fattori tecnici quelli alla base dell'alta vulnerabilità delle aziende al pericolo cyber. Sistemi IT non aggiornati con le ultima patch di sicurezza e sistemi operativi obsoleti sono i fattori più impattanti, seguiti da una scarsa attenzione alla sicurezza della filiera. Anche nel mondo della cybersicurezza l'Intelligenza Artificiale sta diventando un tema chiave sia per combattere il cybercrime, sia per rendere gli attacchi più dirompenti ed efficaci.

Più di 7 grandi imprese su 10 hanno percepito un aumento degli attacchi

imputati sia all'aumento complessivo degli attacchi (nel 76% dei casi), sia alla maggior capacità di rilevazione (48%), anche grazie all'Intelligenza artificiale

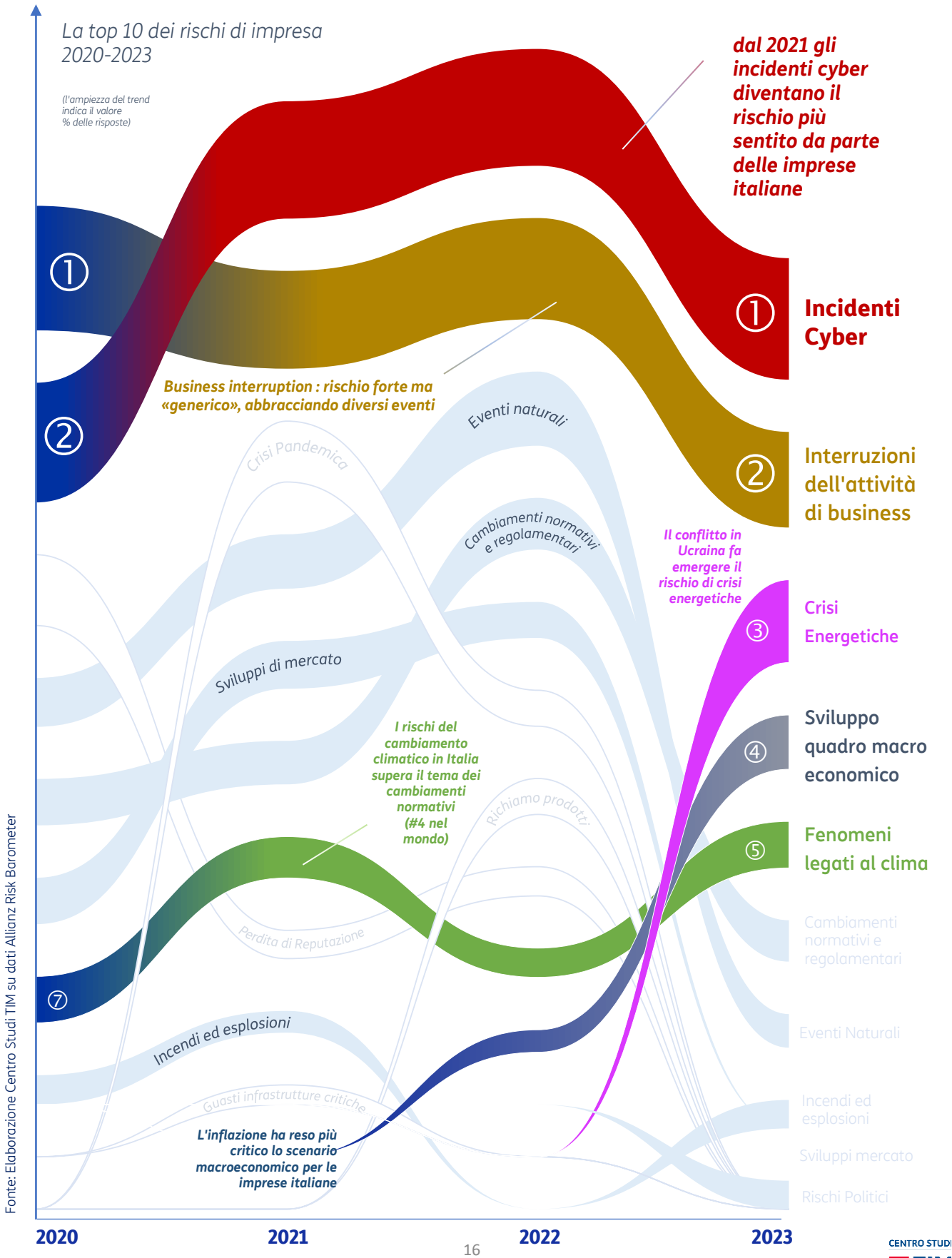
Quasi 6 grandi imprese su 10 utilizzano l'AI per la cybersecurity

Ma solo il 22% la utilizza in maniera estesa per identificare anomalie, nuove minacce o correlazione di eventi. tuttavia l'AI può anche essere utilizzata per rendere più dirompenti gli attacchi



Fonte: Indagine CISO Osservatorio Cybesecurity del Politecnico di Milano

CYBERSECURITY: RISCHIO #1 PER LE IMPRESE ITALIANE



Fonte: Elaborazione Centro Studi TIM su dati Allianz Risk Barometer

CENTRO STUDI TIM

La cybersecurity delle PMI
Anche tra le PMI la dimensione fa la differenza

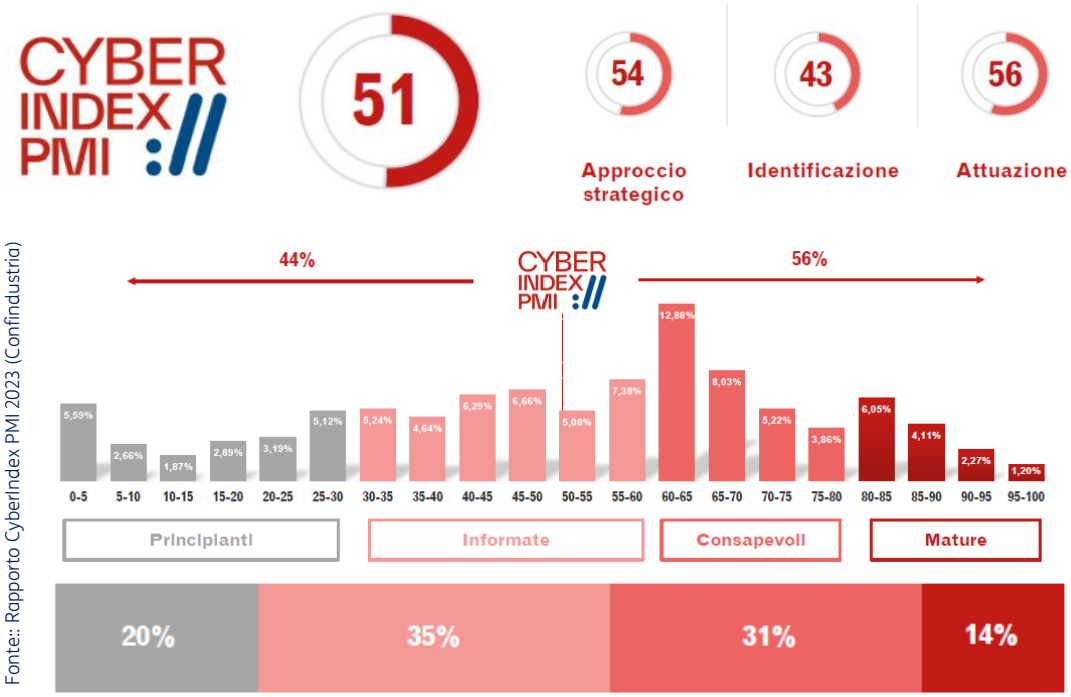
Nella maggior parte dei casi gli attacchi sono rivolti ad aziende di piccola e media dimensione, che rappresentano secondo ISTAT il 99,6% del tessuto economico italiano, la maggior parte delle quali sotto i 10 dipendenti. Tale tipologia di azienda ha una minor consapevolezza dei rischi legati alla cybersecurity e quindi risulta maggiormente esposto, Quando operano in una filiera possono risultare la catena debole della sicurezza con potenziali conseguenze verso altre aziende collegate. Secondo uno studio realizzato da Confindustria per calcolare il Cyber Index PMI in Italia l'esposizione al rischio delle PMI è cresciuta di pari passi alla loro digitalizzazione che ha portato all'adozione di strumenti informatici sempre più avanzati L'esposizione delle PMI aumenta anche per la appartenenza a filiere critiche dal punto di vista della sicurezza o filiere internazionali dove operano con paesi in cui non vige una normativa nazionale (come NIS in Europa).

Il 13% delle PMI dichiara di avere subito un incidente cyber negli ultimi anni ma non sempre gli incidenti vengono rilevati o resi noti.

Secondo la studio, contestualmente, anche le percezione del rischio è migliorata: l'86% delle PMI conosce e teme almeno una minaccio tra ransomware, malware DDoS e phishing ed il 91% teme conseguenze da un attacco. Il 61% si ritiene un bersaglio ma solo il 32% si ritiene preparato per un attacco.

Complessivamente nel 2023 il CyberIndex PMI in Italia è risultato pari a 51/100. La parte più deficitaria è risultata l''identificazione del rischio cyber per non disponere di adeguamenti strumenti e skills specifici in azienda.

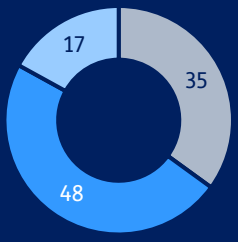
Il CyberIndex PMI aumenta all'aumentare della dimensione aziendale.



Fonte:: Rapporto CyberIndex PMI 2023 (Confindustria)

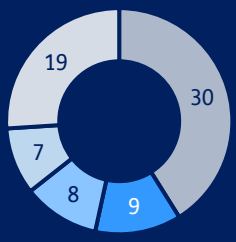
LE PMI E LA CYBERSECURITY

L'83% usa strumenti digitali



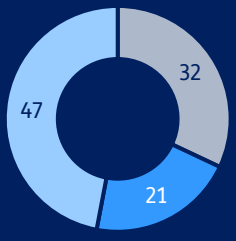
- Strumenti digitali avanzati
- Strumenti digitali di base
- Nessuno

Il 52% opera in filiere critiche



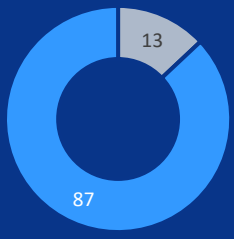
- Fornitori ITZ o imprese 1k+ addetti
- Coinvolgimento di infrast. critiche in filiera
- Attività in Paesi instabili
- Sedi e/o impianti all'estero
- Relazione con PA

Il 53% è esposto su mercati internazionali



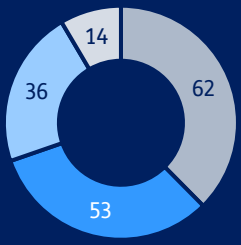
- > 10% di vendite ITZ
- < 10% di vendite ITZ
- No Export

Il 13% dichiara una violazione negli ultimi 4 anni



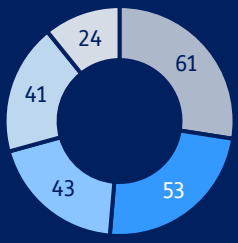
- Subito violazione cyber
- Nessuna violazione

L'86% conosce e teme 1+ minacce



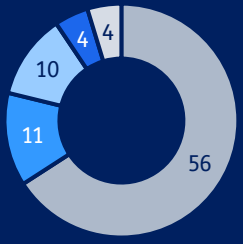
- Ransomware
- Social Engineering
- Malware
- DDoS

Il 91% teme conseguenze da attacchi cyber



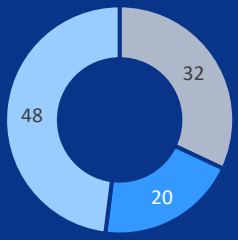
- Business Continuity
- Alterazione Dati
- Estorsione
- Costi di ripristino
- Reputazione

Il 61% si ritiene un bersaglio



- Dati clienti e fornitori
- Brevetti
- Partecipazione a filiera strategica

Solo il 32% si ritiene preparato per attacchi cyber



- Preparati
- Poco preparati
- Impreparati

Fonte:: Rapporto CyberIndex PMI 2023 (Confindustria)

La NIS2

Dalla NIS alla NIS2: Un cambiamento necessario

Obiettivi e tempistica della NIS2

La Direttiva sulla sicurezza delle reti e dei sistemi informativi («NIS2») delinea i requisiti di cybersicurezza per le organizzazioni operanti nell'Unione Europea (UE) al fine di garantire un livello elevato e comune di protezione tra gli Stati membri.

La NIS2 affronta le limitazioni della precedente direttiva, inizialmente istituita nel 2016, introducendo requisiti più rigorosi, un'estensione dell'ambito di applicazione delle entità e dei settori che devono conformarsi e maggiori sanzioni per l'inosservanza. La nuova direttiva si applica alle grandi e medie organizzazioni operanti in settori critici come l'energia, i trasporti, la manifattura, l'acqua e la sanità, nonché le banche, la finanza, i servizi digitali. Inoltre, la NIS2 potrà essere applicata anche alle piccole imprese nel caso in cui queste ultime siano fornitrici di aziende che rientrano nella normativa oppure se coinvolte in specifici settori definiti critici dalla NIS2.

A seconda delle loro dimensioni e del settore in cui operano, le organizzazioni rientrano nelle categorie **"Essenziali"** o **"Importanti".** Entrambe devono rispettare le stesse misure di sicurezza, ma le entità essenziali sono monitorate proattivamente e sono soggette a sanzioni più gravi in caso di inosservanza. Poiché NIS2 è una direttiva europea, spetta a ciascuno Stato membro dell'UE recepirla nella propria legislazione nazionale e farla rispettare. I requisiti chiave sono comuni, ma le leggi locali definiscono procedure e linee guida di attuazione specifiche, puntando agli stessi obiettivi in tutta l'UE: garantire la resilienza dei **settori critici,** salvaguardare le infrastrutture europee ed evitare un effetto domino in caso di gravi attacchi informatici.

A questo scopo, le disposizioni della normativa mirano a garantire che le organizzazioni che fanno parte della catena di fornitura delle infrastrutture critiche comprendano la loro esposizione ai rischi informatici, applichino le best practice di cybersicurezza e siano in grado di rilevare, gestire, rendicontare e segnalare gli incidenti in tempi definiti e più brevi. La **mancata conformità** alla NIS2 comporta **sanzioni finanziarie** significative, stabilendo la **responsabilità degli organi amministrativi e direttivi aziendali** e rafforzando il ruolo delle **agenzie locali per la cybersicurezza** nel monitorare e controllare le organizzazioni.

La nuova Direttiva dovrà essere recepita negli ordinamenti giuridici nazionali entro il **17 OTTOBRE 2024**. NIS2 sarà applicata a partire dal 18 ottobre 2024, anche se gli Stati membri avranno tempo fino al 17 aprile 2025 per finalizzare l'elenco delle organizzazioni che devono conformarsi.

DA DOVE SIAMO PARTITI
LA DIRETTIVA NIS DEL 2016

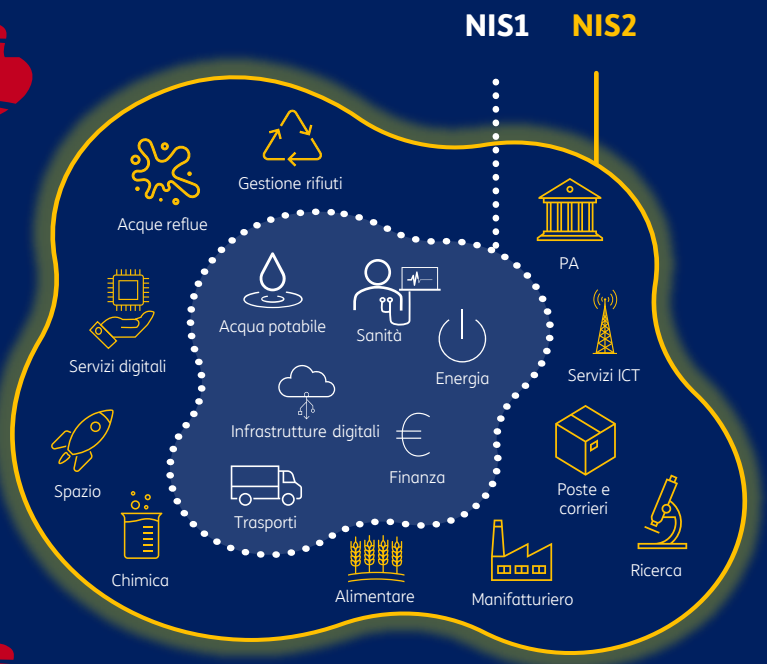
La Direttiva NIS originale, adottata nel 2016, è stata la prima normativa a livello europeo ad aver stabilito requisiti minimi di sicurezza informatica per gli "operatori di servizi essenziali" (OSE) e "fornitori di servizi digitali" (DSP) in settori strategici. Questa Direttiva ha rappresentato un importante passo avanti nella promozione della cybersicurezza nell'Unione Europea, introducendo obblighi di segnalazione degli incidenti, di adozione di misure di sicurezza e di designazione di autorità nazionali competenti.

LA NIS 2: PERIMETRO, SETTORI E SCALA

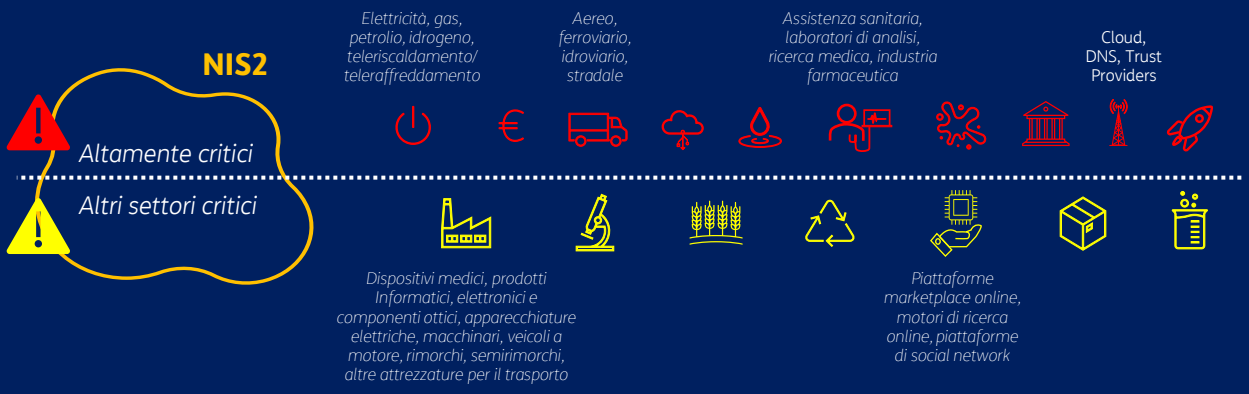
I criteri per la definizione degli enti sottoposti a normativa dalla NIS1 hanno portato a differenze ed incongruenze nelle scelte operate dai diversi Paesi Membri. Per superare l'incertezza e fare maggiore chiarezza, è stato definito un differente criterio, classificando in soggetti in entità essenziali ed entità importanti in base all'appartenenza a settori altamente critici (rispetto a settori critici) ed alla dimensione dell'azienda

PERIMETRO ESTESO

NIS2 amplia il perimetro della NIS1 introducendo nuove misure con il fine di rendere tutto il sistema economico europeo più resiliente agli attacchi esterni.



CLASSIFICAZIONE DI SOGGETTI E SETTORI



SOGLIA DIMENSIONALE

	dipendenti	fatturato	Settori **altamente critici**	Altri settori **critici**
Grandi imprese	**250**+	M€ **50**+	Entità **Essenziali**	Entità **Importanti**
Medie imprese	**50**-**249**	M€ **10**-**50**	Entità **Importanti**	Entità **Importanti**
Piccole imprese	< **50**	M€ <**10**	*Coinvolte solo se rientrano nei settori definiti critici dalla NIS2*	
Micro imprese	< **10**	M€ ≤**2**		

CENTRO STUDI TIM

La nuova Direttiva: Chi si deve adeguare e cosa deve fare

Chi deve conformarsi alle nuove disposizioni

Nella versione 2016 della Direttiva NIS, spettava agli Stati membri designare le organizzazioni soggette alla regolamentazione. NIS2 non solo si applica a più settori industriali, ma ora tutte le organizzazioni con più di **50 dipendenti** e ricavi annui superiori a **10 milioni** di euro devono conformarsi, siano esse **pubbliche** o **private**, nonché le piccole aziende che rientrano nella catena di fornitura.

Gli Stati membri possono decidere di aggiungere entità più piccole all'elenco se ritenute avere un ruolo chiave nell'economia o nella società locale. L'ambito di applicazione di NIS2 è descritto in due allegati che elencano i settori industriali a cui la direttiva si applica automaticamente. **L'allegato I** della normativa elenca i settori **altamente critici**, mentre **l'allegato II** elenca gli **altri settori critici**.

Secondo la NIS2, il termine "entità" descrive qualsiasi organizzazione che deve conformarsi alla Direttiva. Come già anticipato, le entità operanti nei settori elencati nell'Allegato I possono essere classificate come "Essenziali" o "Importanti", a seconda delle loro dimensioni e dei loro ricavi. Le entità nell'Allegato II possono rientrare solo nella categoria "Importanti". Entrambe le categorie devono soddisfare gli stessi requisiti e conformarsi alle stesse misure di sicurezza ma, mentre le entità Essenziali saranno monitorate in modo proattivo, le entità Importanti saranno sottoposte ad audit solo a seguito di un incidente di cybersicurezza. Le entità Essenziali andranno incontro a sanzioni più elevate. In altre parole, il controllo sulle entità Essenziali è più rigoroso a causa delle maggiori conseguenze sul sistema economico nazionale derivanti dall'inosservanza della normativa.

Le misure previste dalla NIS2

Le misure di sicurezza informatica che le entità Essenziali e Importanti devono rispettare sono definite da ciascuno Stato membro nella fase di trasposizione nazionale della direttiva. NIS2 impone un approccio di gestione del rischio con un elenco di misure di sicurezza di base da implementare:

- ***Analisi del rischio*** *e politiche di sicurezza del sistema informativo.*
- ***Gestione degli incidenti****, compresa la prevenzione, la rilevazione, la risposta e il recupero.*
- *Misure di* ***continuità aziendale****, come backup e ripristino dei disastri, e gestione delle crisi.*
- *Sicurezza della* ***catena di approvvigionamento****, compresi gli aspetti relativi alla sicurezza delle relazioni tra ciascuna entità e i suoi fornitori diretti o i fornitori di servizi.*
- *Sicurezza nell'acquisizione, nello sviluppo e nella manutenzione di* ***reti e sistemi informativi****, compresa la gestione e la divulgazione delle vulnerabilità.*
- *Politiche e procedure per* ***valutare l'efficacia delle misure*** *di gestione del rischio informatico.*
- *Pratiche di sanificazione informatica di base e* ***formazione*** *sulla sicurezza informatica.*
- *Politiche e procedure riguardanti l'uso della* ***crittografia*** *e* ***dell'encryption.***
- *Sicurezza delle* ***risorse umane****, politiche di controllo degli accessi e gestione dei beni.*
- *Utilizzo della* ***multifactor authentication****, comunicazioni voce, video e messaggistica sicure e sistemi di comunicazione d'emergenza sicuri tra le entità.*

PASSO DOPO PASSO
IL DECALOGO NIS2 PER LE IMPRESE

L'art 21. prevede nuove misure attuative per garantire la sicurezza

RISK MANAGEMENT
Strutturare politiche di analisi dei rischi e di sicurezza dei sistemi informatici organizzativi

GESTIONE INCIDENTI
Creare piani operativi e procedure standardizzate di gestione degli incidenti informatici

BUSINESS CONTINUITY
Assicurare la continuità operativa con backup, procedure di crisis response e disaster recovery

SUPPLY CHAIN
Garantire la sicurezza della catena di fornitura, compresi i rapporti con le terze parti esterne

SICUREZZA DEI SISTEMI
Mettere in sicurezza gli asset informatici e di rete in ogni fase, dallo sviluppo e alla manutenzione

STRATEGIE CYBER
Creare strategie e procedure per valutare l'efficacia delle misure di contrasto ai rischi di cyber sicurezza

FORMAZIONE
Creare e rispettare pratiche di igiene informatica di base e garantire formazione in materia di cybersecurity

CRITTOGRAFIA
Stabilire politiche e procedure relative all'uso della crittografia e della cifratura per le attività organizzative

SICUREZZA DEL PERSONALE
Garantire la sicurezza informatica per il personale, impostando strategie di controllo dell'accesso e gestione degli attivi

AUTENTICAZIONE A PIÙ FATTORI
Usare soluzioni di autenticazione a più fattori o di autenticazione continua e sistemi di comunicazione protetti

La nuova Direttiva
Obblighi di notifica e sanzioni

Sebbene la Direttiva NIS abbia sempre richiesto alle organizzazioni di segnalare gli incidenti di sicurezza informatica, NIS2 rende **obbligatoria la segnalazione degli incidenti "significativi"** e descrive un processo chiaro e rigoroso per farlo. Per mantenere la conformità, le entità devono notificare gli incidenti al **Computer Security Incident Response Team** (CSIRT) o qualsiasi altra autorità competente del proprio Paese secondo la tempistica illustrata in basso, una volta verificatosi un incidente.
Le entità devono implementare meccanismi di rilevamento e risposta agli incidenti, identificandoli rapidamente e valutandone l'impatto.

La Direttiva NIS2 richiede a ciascuno Stato membro di designare almeno **un'autorità competente** che ne guidi l'attuazione nel Paese e verifichi la conformità delle entità all'interno del suo campo di applicazione. Devono inoltre essere istituiti **CSIRT** per monitorare e analizzare le minacce e gli incidenti, raccogliere evidenze forensi, avvisare le entità e altri stakeholder rilevanti e fornire assistenza quando necessario.

La versione del 2016 della direttiva NIS attribuiva agli Stati membri il compito di definire **sanzioni** per la non conformità.

Ciò portava a disparità evidenti in tutta l'UE.

Le sanzioni sono comminate in seguito a audit, ispezioni e controlli e possono andare da semplici avvertimenti a ordini di interruzione di condotta non conforme alla direttiva, di attuazione di misure, di informazione al pubblico sino a sanzioni amministrative pecuniarie nella seguente misura:

- ***soggetti «essenziali»**: le sanzioni amministrative possono arrivare fino a **10 milioni** di euro o ad almeno il **2%** del fatturato mondiale totale annuo dell'organizzazione;*
- ***soggetti «importanti»**: le sanzioni amministrative possono arrivare fino a **7 milioni** di euro o almeno **all'1,4%** del fatturato mondiale totale annuo*

Inoltre, agli enti essenziali può essere sospesa la certificazione o l'autorizzazione a operare. L'autorità può anche designare un funzionario per il monitoraggio e supervisionare la conformità con cui l'ente monitorato è tenuto a collaborare senza riserve.

Come anticipato, gli **organi amministrativi e direttivi** delle organizzazioni possono essere ritenuti responsabili delle violazioni e sono tenuti ad approvare le misure di cybersicurezza adottate, supervisionarne l'attuazione, partecipare a corsi di formazione e fornire formazione adeguata ai dipendenti.

Su richiesta delle autorità potranno essere richiesti aggiornamenti specifici

entro

24ORE

Obbligo di segnalare qualsiasi incidente significativo entro 24 ore dal momento in cui se ne è venuti a conoscenza, indipendentemente dal fatto che abbia avuto un impatto diretto sulle operazioni.

entro

72ORE

Rapporto aggiornato dal momento in cui si viene a conoscenza dell'incidente, descrivendo la natura dell'incidente, la sua gravità, gli impatti e gli indicatori di compromissione.

entro

1MESE

Una descrizione dettagliata dell'incidente deve essere presentata entro 1 mese, spiegando le possibili cause, le misure di mitigazione in corso e l'impatto transfrontaliero.

Un punto d'attenzione
La Supply Chain

Una delle novità più importanti è sicuramente l'attenzione che la proposta di Direttiva NIS 2 riserva alla necessità di assicurare la **sicurezza delle supply chain**, riconoscendo che le minacce di attacchi cibernetici possono derivare anche da vulnerabilità di fornitori terzi. Per i soggetti impattati dalla NIS 2 diventa quindi fondamentale contemplare una pianificazione della gestione dei rischi cyber che riguardi anche la catena di fornitura affinché non sia essa il veicolo di attacchi ed eventi malevoli alle pratiche di cybersecurity dei fornitori e dei fornitori di servizi.

L'obbligo di proteggere la supply chain comporta che saranno impattati dalla NIS 2 anche soggetti appartenenti a categorie non citate espressamente dalla normativa. I soggetti interessati dovranno notificare alla filiera gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura dei loro servizi.

Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino, senza indebito ritardo al proprio CSIRT o alla propria autorità competente, eventuali «incidenti significativi» che hanno un impatto significativo sulla fornitura dei loro servizi. Senza indebito ritardo il CSIRT o l'autorità competente fornisce una risposta al soggetto notificante con un riscontro iniziale sull'incidente significativo e, se richiesto, orientamenti e consulenza operativa sull'attuazione di possibili misure di attenuazione.

Gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati prodotti, servizi e processi ICT, anche acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei per la cybersicurezza adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. In effetti, parallelamente alla NIS2, la Commissione Europea sta intervenendo attraverso la definizione di schemi di certificazione di sicurezza per prodotti e servizi fondamentali per il mondo dei servizi digitali. Il primo schema di certificazione redatto a livello UE è stato quello che ha definito dei criteri comuni (EUCC - Common Criteria). Sono oggi in discussione gli schemi di certificazione per la cybersecurity di Servizi Cloud (EUCS) e Reti 5G (EU5G).

Alla Commissione è conferito il potere di adottare, qualora siano stati individuati livelli insufficienti di cybersecurity, atti delegati al fine di integrare la presente direttiva specificando quali categorie di soggetti essenziali e importanti sono tenute a utilizzare determinati prodotti, servizi e processi ICT certificati o a ottenere un certificato nell'ambito di un sistema europeo di certificazione della cybersecurity adottato a norma dell'articolo 49 del regolamento (UE) 2019/881.

L'ENISA (Agenzia dell'UE per la Cybersicurezza) gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cybersicurezza, sui certificati europei di cybersicurezza e sulle dichiarazioni UE di conformità

Tali misure risulteranno onerose per le aziende in perimetro NIS2 ma il beneficio sarà maggiore delle spese di adeguamento

Costi & benefici NIS2: per imprese e Sistema Paese

Costi di adeguamento: Alcune stime

Da uno studio di impatto realizzato dalla **Commissione Europea** in occasione della revisione della NIS1 e basato su dati Gartner risulta che la **spesa in cybersecurity** è pari a poco più del **9%** della **spesa ICT** delle aziende a livello globale, ossia allo **0,52%** dei ricavi. Sulla base di questi dati, lo studio fornisce una valutazione dei costi che le imprese dovranno sostenere per adeguarsi alla NIS2. Tale stima viene realizzata anche utilizzando i costi storici sostenuti dalle imprese in occasione dell'introduzione della NIS1. Lo studio d'impatto sostiene che i costi per le imprese possano aumentare fino al 22% della spesa. Questo significa portare il costo complessivo della spesa in cybersecurity **dal 9 al 11% della spesa ICT** ossia dallo 0,52% allo 0,68% dei ricavi complessivi dei settori che dovranno adeguarsi alle nuove disposizioni.

Più basso è il costo che dovranno sostenere invece i settori che già avevano ottemperato alle disposizioni della NIS1. Per questi ambiti, le spese di adeguamento a NIS2 aumenteranno del **12%** portando la spesa in cybersecurity dal 9 a **10%** del budget **ICT** pari allo **0,58%** dei ricavi.

Spese di adeguamento alla NIS2 dei NUOVI SETTORI

+ 22%
le spese cyber passano dal 9 al 11% del budget ICT

Spese di adeguamento alla NIS2 dei SETTORI GIÀ INCLUSI NELLA NIS1

+ 12%
dal 9 al 10% dei budget ICT

Lo studio Frontier Economics

A livello europeo, verranno spesi oltre 31 miliardi di euro per l'adeguamento alla NIS2

Secondo uno studio di **Frontier Economics** viene stimato a **31,2 miliardi di euro** il costo di adeguamento a N\IS2 per le aziende europee (0,31% del fatturato delle aziende in perimetro NIS2) – **1,3 miliardi di euro** per le aziende già in perimetro NIS1 (+0,2% delle ricavi), **29,9 miliardi di euro** per i nuovi settori (+0,32% dei ricavi)

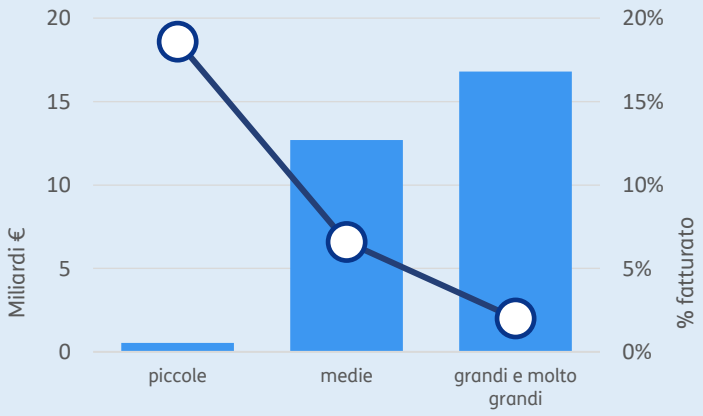
Simulazione impatto NIS2
Costi di adeguamento

Quali sono i benefici a livello aziendale della NIS2? E quali sono quelli a livello Paese? In base ai dati dello studio d'impatto della Commissione Europea nonché alle valutazioni che ha effettuato ENISA sulle spese sostenute dalle imprese per ottemperare agli obblighi previsti dalla NIS1 ed ai valori che possono essere recuperati sui costi che comporta l'esposizione ad un attacco cyber, è possibile effettuare alcune simulazioni.

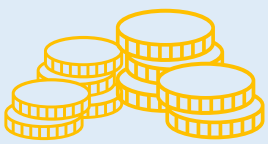
I costi di adeguamento

Lo studio d'impatto della Commissione Europea ha effettuato le proprie valutazioni considerando una platea di circa 110 mila imprese, da cui si desume che il costo medio di adeguamento alla NIS2 è valutato a circa **280 mila euro** ad azienda. Si tratta di un costo complessivo che include la formazione del personale, l'acquisizione di competenze non presenti nel perimetro aziendale, l'acquisto di soluzioni software e di nuovi apparati, gli eventuali servizi di consulenza per l'adeguamento ed altre spese.

Si tratta tuttavia di una spesa media, che può variare in funzione della dimensione aziendale e della complessità del business. Bisogna considerare che – se le spese in valore assoluto sono più elevate per le aziende di maggiori dimensioni, tale situazione si ribalta quando valutiamo le spese di adeguamento in rapporto al fatturato aziendale. Per avere un termine di paragone, per l' adeguamento alla NIS1, ENISA stima che le grandi aziende (circa 4% del totale impattato dalla normativa) abbiano speso tra 1 e 2,5 milioni di euro, mentre il 60% circa abbia sostenuto un costo che varia tra 100 mila ed un milione di euro. Ci sono comunque il 30% di aziende che ha speso meno di 100 mila euro. Una situazione, dunque, molto variabile ma che può darci un punto di riferimento per fare una valutazione di quale spese le aziende dovranno sostenere per adeguarsi alla NIS2, sempre considerando che alcune aziende, quelle finora non incluse nel perimetro della NIS1, partono da zero.



Costo incrementale in EU per dimensione aziendale



costi di implementazione

% del fatturato

Small business > 50 dipendenti, Medium Business tra 50 e 250 dipendenti; Large e Very Large Business >250 dipendenti

Fonte: Elaborazione Centro Studi TIM su dati ENISA

Simulazione impatto NIS2
Conseguenze di un attacco cyber

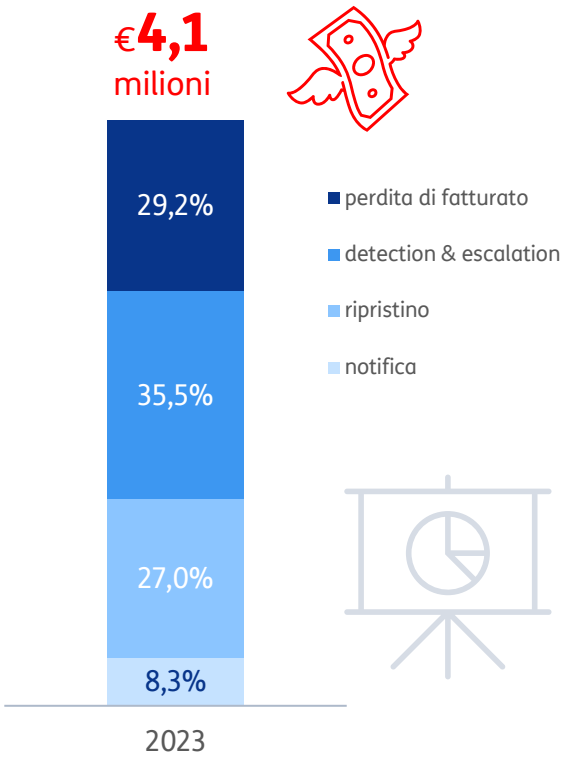
Per fare una stima dei costi e dei benefici che derivano dal passaggio alla NIS2 dobbiamo anche tenere in considerazione il danno che devono sopportare le aziende che sono oggetto di un attacco cyber.

Stima dei danni di un incidente cyber

I costi di un incidente cyber hanno un'ampia variabilità. Una survey condotta da Microsoft su aziende con più di 500 addetti ha rilevato che, negli ultimi 12 mesi, il 74% delle aziende aveva subito un attacco indirizzato ai dati. In media gli attacchi cyber avevano prodotto 59 incidenti (di cui il 20% severi) con un costo per incidente di circa 240 mila euro. Se ipotizziamo che tutti gli incidenti siano severi, possiamo derivare che complessivamente il danno economico annuo possa arrivare fino a quasi **15 milioni di euro**.

In base ad altre fonti, i costi complessivi di un **data breach** possono essere anche molto più alti. Secondo uno studio di IBM Security realizzato su un vasto campione di aziende di varie dimensioni a livello globale, le conseguenze complessive di un data breach costa mediamente **4,1 milioni di euro**. In **Italia** si è stimato un impatto di circa **3,6 milioni di euro**.

I costi relativi ad un data breach sono l'insieme di più fattori. Il **30%** dei costi è imputabile alla perdita di fatturato e ben Il **35,5%** – la componente con il peso maggiore - è attribuibile alla **rilevazione** ed **escalation** dell'incidente. Il **27%** è rappresentato dai costi per il **ripristino dei dati** e, infine, il restante **8,3%** dai costi di **notifica**



Fonte: Cost of a Data Breach (IBM, 2023)

I COSTI DI UN DATA BREACH

- *aumentano del **27%** quando è coinvolta una **infrastruttura critica;***
- *esplodono quando i data violati sono dell'ordine dei **50 milioni;***
- *sono influenzati dalla **compliance regolatoria** per un **±5%** sul costo*

Simulazione impatto NIS2
I benefici per le aziende e il Paese

Analisi costi benefici di adeguamento alla NIS2

I costi di adeguamento alla NIS2 per una azienda - in base ai dati storici di NIS - possono variare da meno di 100 mila euro sino a oltre 5 milioni di euro in base alla dimensione dell'azienda, al settore di appartenenza e a seconda che l'azienda fosse già in perimetro NIS1 o meno.

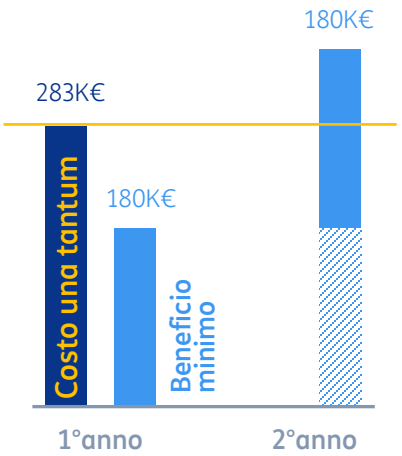
Il costo medio di adeguamento a livello europeo è di 283 mila euro per una medio grande azienda .

Secondo l'indagine di ENISA in Italia il 60% delle aziende medio grandi ha una spesa di adeguamento compresa tra 100 mila ed 1 milione di euro, che aumenta al crescere della dimensione d'azienda.

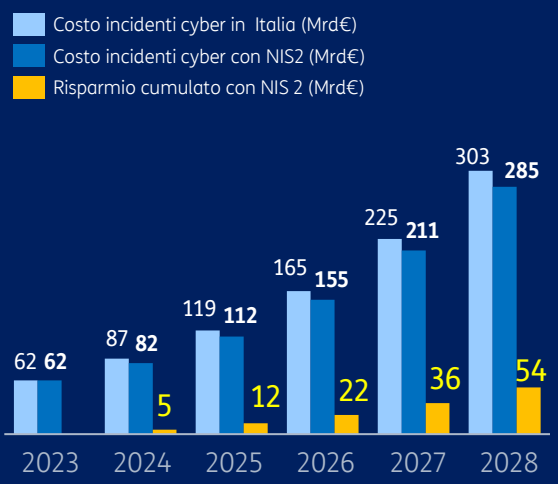
Secondo lo studio di impatto della Commissione Europea l'introduzione della **NIS2** genererà una diminuzione degli incidenti del **6% annuo**

Per una grande azienda che subisce 60 incidenti annui, con un costo che può variare dai 3 milioni ai 15 milioni di euro a seconda della percentuale degli incidenti severi, il beneficio annuo con NIS 2 può valutarsi dai **180 mila ai 900 mila euro annui**

Ciò prefigura un **ROSI (Return on Security Investments) positivo già da 2° anno.**



Fonte: Elaborazione Centro Studi TIM su dati ENISA



Fonte: Elaborazione Centro Studi TIM su dati STATISTA

I benefici per il sistema Paese

La cybersecurity avrà costi previsti rilevanti per l'Italia nei prossimi anni. Secondo uno studio di Statista, i costi in assenza di contromisure aumenteranno da **62 miliardi di euro** nel 2023 a **303 miliardi di euro** nel 2028, con un CAGR del **37,4%**

Considerando una riduzione degli incidenti del 6% annui a prezzi costanti, il **beneficio cumulato** per il sistema paese sarà di **54 miliardi di euro** sino al **2028.**

CENTRO STUDI TIM

CENTRO STUDI

TIM

Verso la NIS2

Gli effetti sulle imprese e sull'economia italiana della nuova Direttiva sulla cybersecurity

Agosto 2024