ASSOLOMBARDA

XI° USCITA

Cyber Security News

La Cyber Security News è un'indagine semestrale dedicata agli eventi di cyber security sul territorio di Assolombarda. Le pubblicazioni, realizzate grazie ad una partnership con Exprivia [1], sono l'occasione per avere una panoramica dello stato dei territori dell'associazione in tema di sicurezza informatica. [2]

Di seguito verrà analizzato quanto emerso nel **2024**.

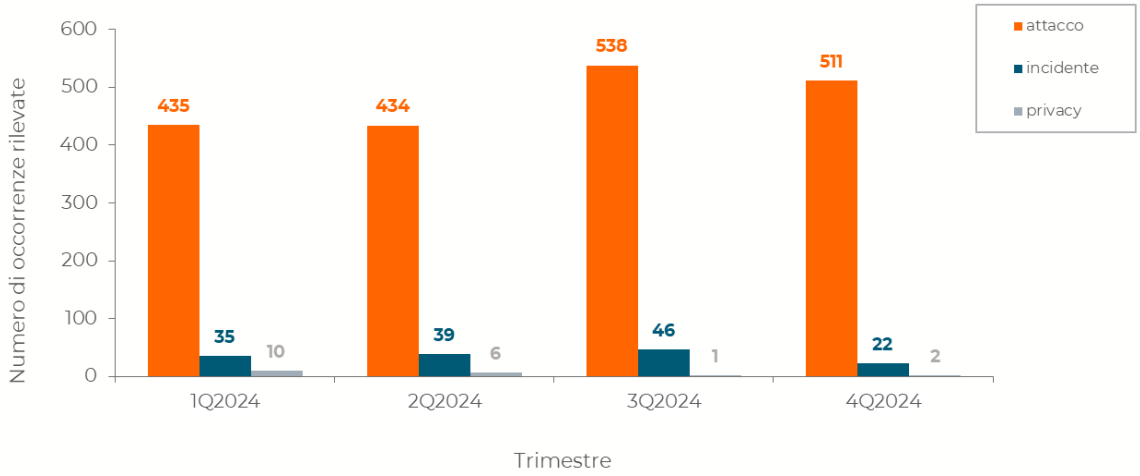
Il territorio di Assolombarda ha registrato **2.079 eventi di sicurezza** nel 2024, segnando un **incremento di 223 casi rispetto al 2023**. Nonostante l'aumento del numero complessivo di eventi, si osserva una **riduzione degli incidenti (-76)** rispetto all'anno precedente. Questo dato suggerisce che le aziende stanno progressivamente implementando strategie e misure di sicurezza più efficaci, riducendo l'impatto degli attacchi riusciti e aumentando la resilienza complessiva del sistema territoriale.

Quando si parla di eventi di sicurezza si considerano:

- **Attacchi**: insieme di azioni intraprese per compromettere un servizio. In presenza di una campagna di phishing indirizzata a molti target, verrà contabilizzata la campagna come un attacco. Il rapporto include campagne criminali intese a sfruttare vulnerabilità di servizi ampiamente utilizzati in Italia.
- **Incidenti**: un attacco che ha avuto successo. Nel caso di un attacco che abbia avuto successo su diverse entità, verranno contabilizzate tutte le istanze di incidenti nei confronti delle varie vittime.
- **Violazioni privacy**: vengono contate non solo le violazioni segnalate dalle istituzioni (ad esempio GDPR), ma anche quelle pubbliche quando queste ultime dovessero essere eclatanti. Ovviamente manterremo il riserbo e non esporremo la vittima, anche se la violazione dovrà essere descritta in una sorgente aperta, ma il dato riteniamo che abbia rilevanza statistica, al pari di incidenti e attacchi.

[1] Azienda internazionale specializzata nel settore dell'Information and Communication Technologies.

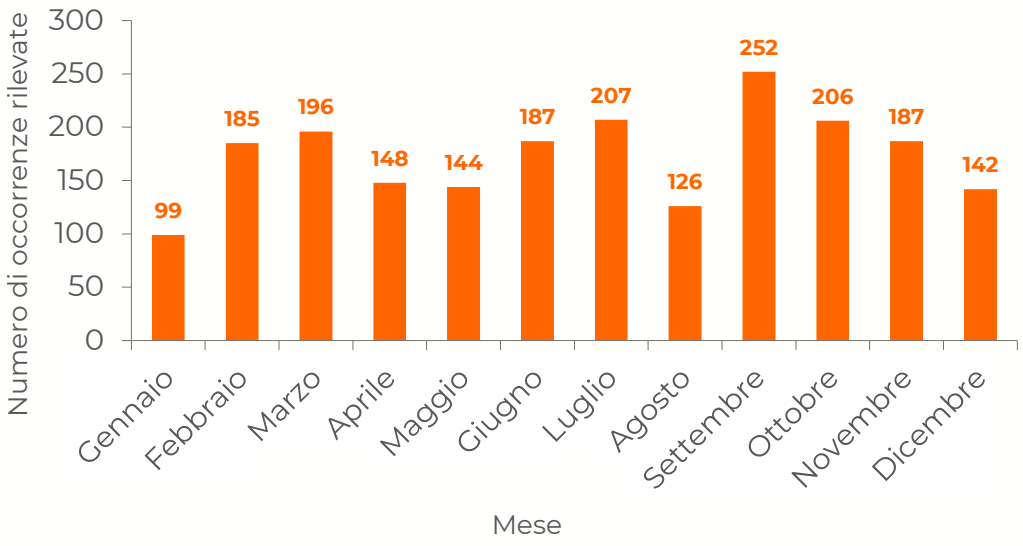
[2] L'Osservatorio Cyber Security di Exprivia colleziona informazioni pubbliche e non, ma crea statistiche utilizzando solo le prime per garantire la confidenzialità delle informazioni e per avere un insieme di dati statisticamente validi e il più possibile solidi. Le statistiche, infatti, vengono aggiornate modificando il numero di sorgenti. Nuove sorgenti vengono inserite solo e soltanto se i dati acquisti sono rilevanti dal punto di vista statistico e integrabili. A ogni record inserito nel rapporto corrisponde una precisa informazione sulla sorgente da cui questo record è stato preso.



Distribuzione temporale

L'analisi della distribuzione mensile degli eventi mostra un andamento altalenante. I **valori minimi si riscontrano a gennaio (99) e ad agosto (126)**, verosimilmente in relazione alla riduzione delle attività durante i periodi di ferie. Al contrario, si osservano **incrementi significativi a luglio (207)**, quando l'approssimarsi della pausa estiva può incidere negativamente sui livelli di attenzione, **e a settembre (252)**, fase di rientro in cui la ripresa della routine operativa può determinare un temporaneo calo di vigilanza.

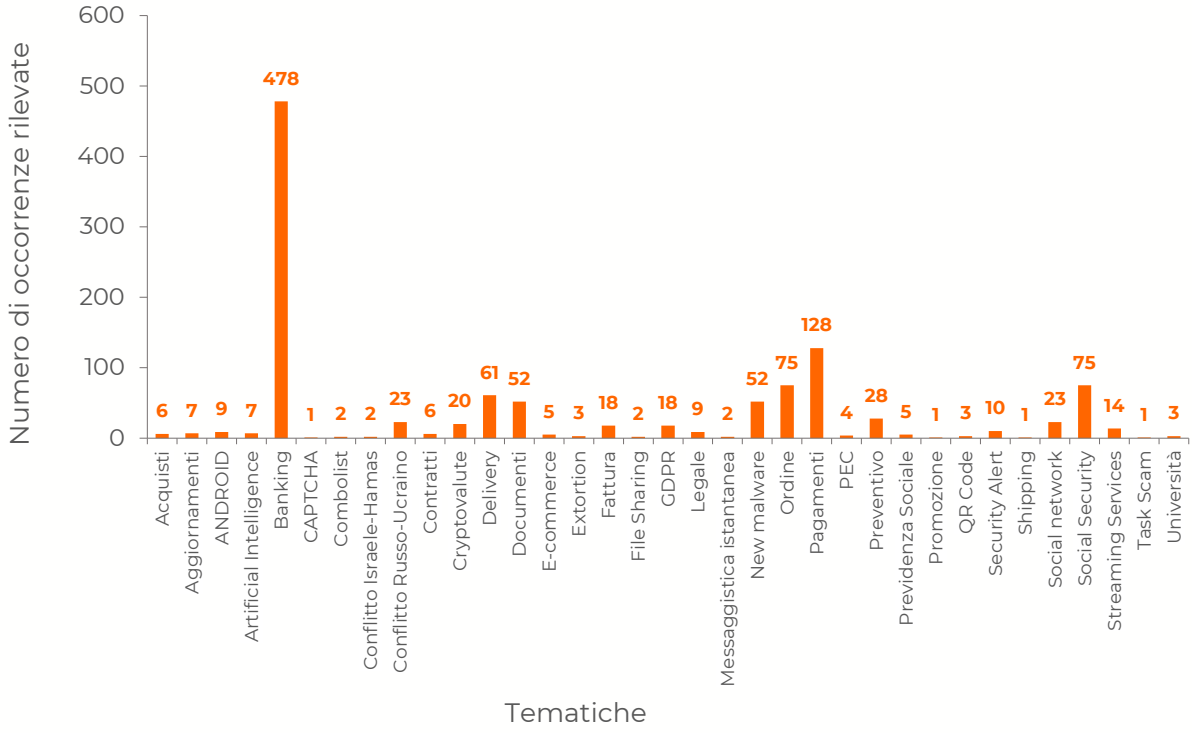
Tali evidenze suggeriscono che **la concentrazione e la consapevolezza degli utenti costituiscono variabili critiche nella mitigazione dei rischi informatici** e che i momenti di transizione stagionale rappresentano fattori di vulnerabilità da considerare nei piani di prevenzione.



Tematiche degli attacchi

Le tematiche degli attacchi hanno riguardato principalmente il **Banking** (478 casi), nonostante un calo significativo rispetto all'anno precedente (–324), e i **Pagamenti** (128). Seguono **Social Security** (75), **Ordini** (75), **Delivery** (61) e **Documenti** (52), a conferma dell'interesse per transazioni e dati sensibili. La voce **New Malware** (52) segnala, invece, minacce più mirate e innovative.

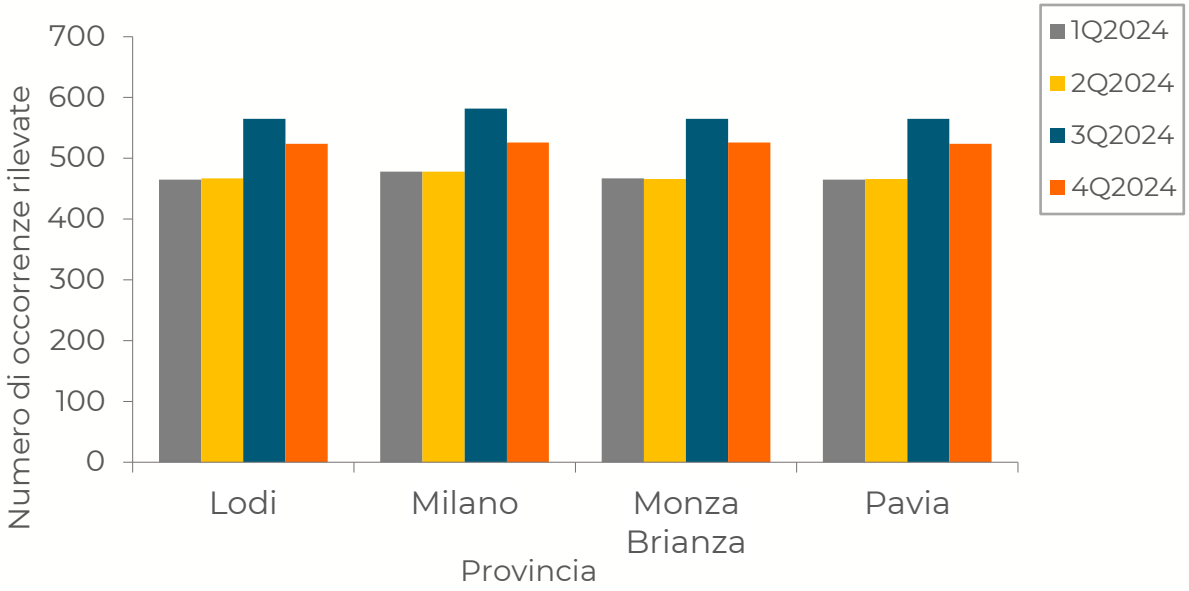
Tutte le altre categorie restano al di sotto dei 30 casi, evidenziando un **panorama frammentato, ma dominato da pochi cluster principali**.



Distribuzione geografica

Come già evidenziato nel report annuale relativo al 2023, l'analisi della distribuzione geografica di attacchi informatici, incidenti e violazioni della privacy mostra una **concentrazione equamente distribuita tra le diverse provincie** (al netto di una leggera prevalenza nella provincia di Milano, probabilmente dovuta alla maggiore presenza di industrie in quest'area), a dimostrazione del fatto che gli attacchi sono ormai pregnanti in tutto il territorio in cui l'associazione opera.

Il numero degli attacchi è riportato considerando che alcuni eventi riguardano tutti i territori ed altri, invece, sono rilevati soltanto in una determinata provincia.



	1Q2024	2Q2024	3Q2024	4Q2024
Lodi	465	467	565	524
Milano	478	478	582	526
Monza Brianza	467	466	565	526
Pavia	465	466	565	524

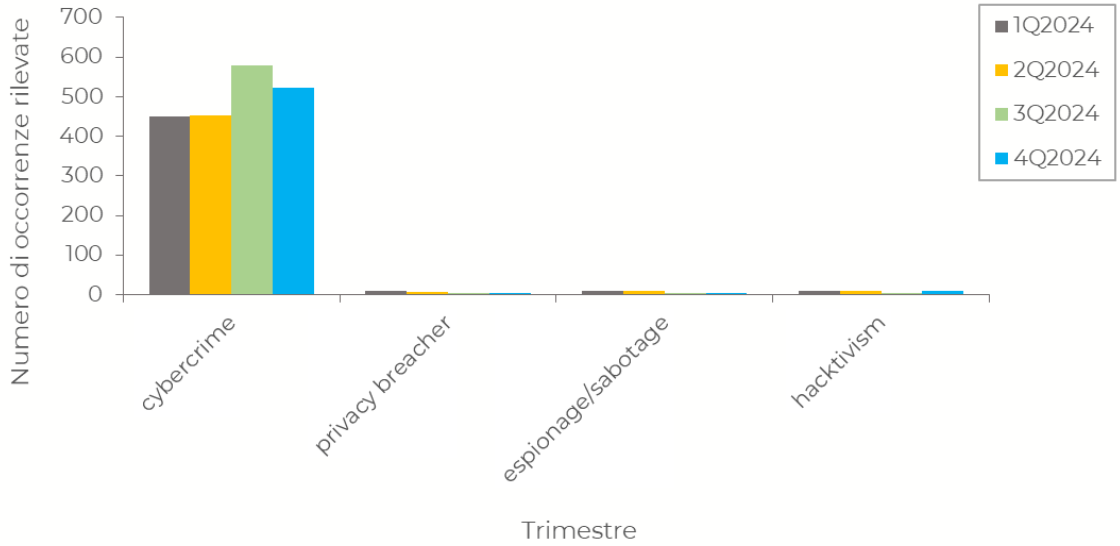
Motivazioni

Nel corso del 2024, il **cybercrime** è stato la spinta dietro alla maggior parte degli incidenti di sicurezza che si sono palesati, con un totale di **2005** episodi registrati, pari a oltre il 96% del totale. In confronto, i casi legati ad **hacktivism**, ovvero quelli che mirano a promuovere un'agenda politica o principi sociali, sono stati significativamente meno frequenti, con **30** episodi. Ancora meno numerosi sono stati i casi legati a **espionage/sabotage** (**24**) e di violazione della sicurezza dei dati (**data breach**), che si sono attestati a **20**.

La predominanza dell'intento economico rispetto a motivazioni ideologiche/politiche o alla violazione dei dati può essere attribuita a una combinazione di fattori:

- innanzitutto, grazie all'**aumento dell'uso di tecnologie digitali per la gestione delle transazioni finanziarie**, i criminali trovano sempre più opportunità di trarre profitto da attività illegali online;

- in secondo luogo, **gli attacchi di cybercrime potrebbero essere più facilmente tracciabili rispetto**, ad esempio, **agli attacchi di data breach**, il che potrebbe falsare i dati dell'analisi. Le vittime degli attacchi di cybercrime, infatti, sono più propense a segnalare gli attacchi alle autorità competenti, rispetto a quelle colpite da data breach, che potrebbero essere meno inclini a segnalare tali violazioni per timore di conseguenze legali o reputazionali.



	1Q2024	2Q2024	3Q2024	4Q2024
cybercrime	451	452	579	523
privacy breacher	10	7	1	2
espionage/sabotage	10	10	2	2
hacktivism	9	10	3	8

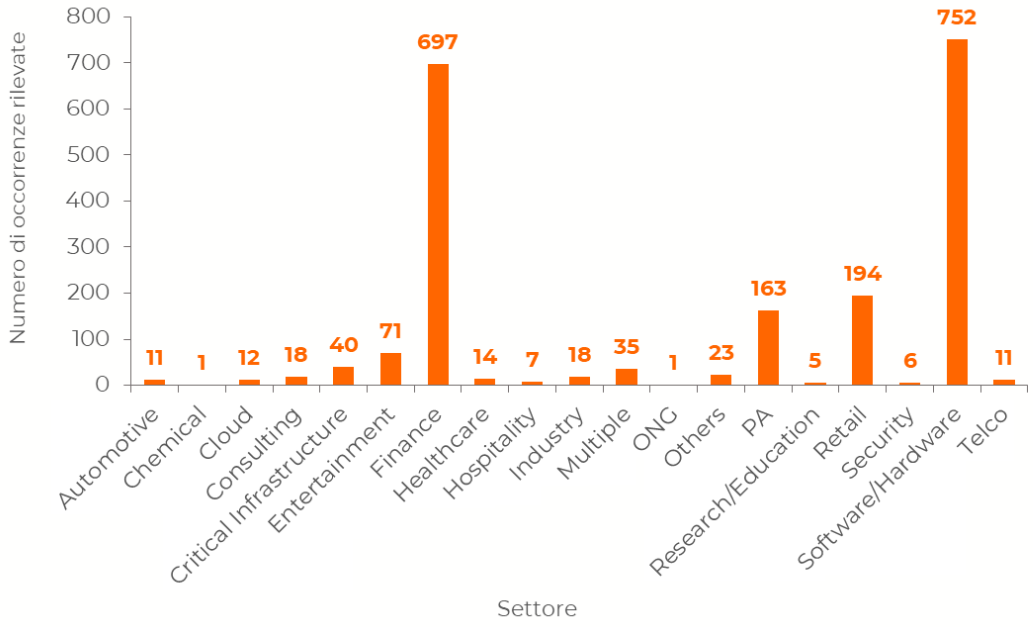
Tipologia di vittime

Gli obiettivi principali per i cybercriminali sono target specifici, quali aziende, istituzioni e organizzazioni di vario genere. Si evidenzia, in generale, come siano stati perpetrati cyber-attacchi in tutti i settori dell'industria presi in esame.

Il settore più colpito è quello del **Software/Hardware**, che registra **752 casi** (+**385** rispetto al 2023), superando il **Finance** (**697 casi**, -**255** rispetto al 2023), storicamente al primo posto. Il comparto tecnologico è diventato un obiettivo sempre più appetibile poiché fornisce le infrastrutture digitali a imprese di ogni settore. Un attacco a un fornitore può generare un effetto domino - il cosiddetto *supply chain attack* - in grado di coinvolgere decine o addirittura centinaia di clienti. Negli ultimi anni si è infatti assistito a un aumento degli attacchi contro provider cloud, piattaforme di software gestionale e altri servizi digitali strategici.

Il Retail e la Pubblica Amministrazione (PA) emergono come settori vulnerabili, sebbene con numeri più contenuti rispetto a Software/Hardware e Finance. Il **Retail**, con **194 casi**, resta un bersaglio interessante per gli attaccanti perché gestisce grandi volumi di dati sensibili dei clienti e transazioni finanziarie quotidiane. La **PA**, con **163 casi**, è particolarmente esposta non solo per il valore dei dati trattati (anagrafiche, documenti fiscali, informazioni sanitarie), ma anche per la rilevanza strategica degli attacchi: colpire enti pubblici può generare forte impatto mediatico e pressione politica, oltre a possibili ripercussioni sulla continuità dei servizi.

Ricordiamo che questa classifica non tiene conto del grado di severità degli attacchi. Infatti, è possibile trovare dei settori in cui gli attacchi sembrano avere numeri residuali, ma hanno avuto un impatto notevole sull'intera supply chain.

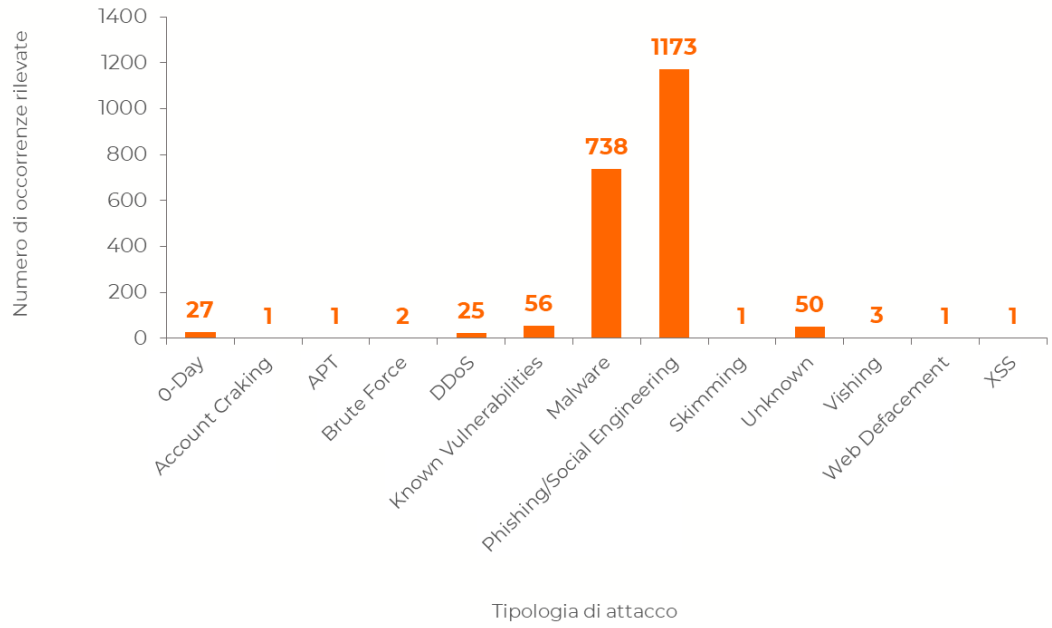


Tecniche di attacco

Anche nel 2024, il **Phishing/Social Engineering** rimane la tecnica più diffusa, con **1173 casi**. Questa strategia si basa sull'inganno per ottenere informazioni riservate dagli utenti, sfruttando l'elemento umano, spesso considerato il punto debole nella sicurezza informatica. L'aumento di questi attacchi sottolinea l'urgente necessità di **formare e sensibilizzare gli utenti** su come riconoscere e prevenire tali minacce.

Al secondo posto troviamo i **Malware** (**738 casi**), software dannosi che possono compromettere o danneggiare i sistemi informatici e che grazie all'impiego dell'AI sono sempre più pericolosi e difficili da individuare.

Infine, si registrano **56** casi di attacchi che sfruttano vulnerabilità già note nei sistemi (**Known Vulnerabilities**) e **50** casi legati a vulnerabilità ancora sconosciute (**Unknown Vulnerabilities**). Sebbene meno numerosi, questi attacchi sottolineano l'importanza di mantenere i sistemi costantemente aggiornati e di adottare misure di sicurezza solide per proteggere le infrastrutture critiche.

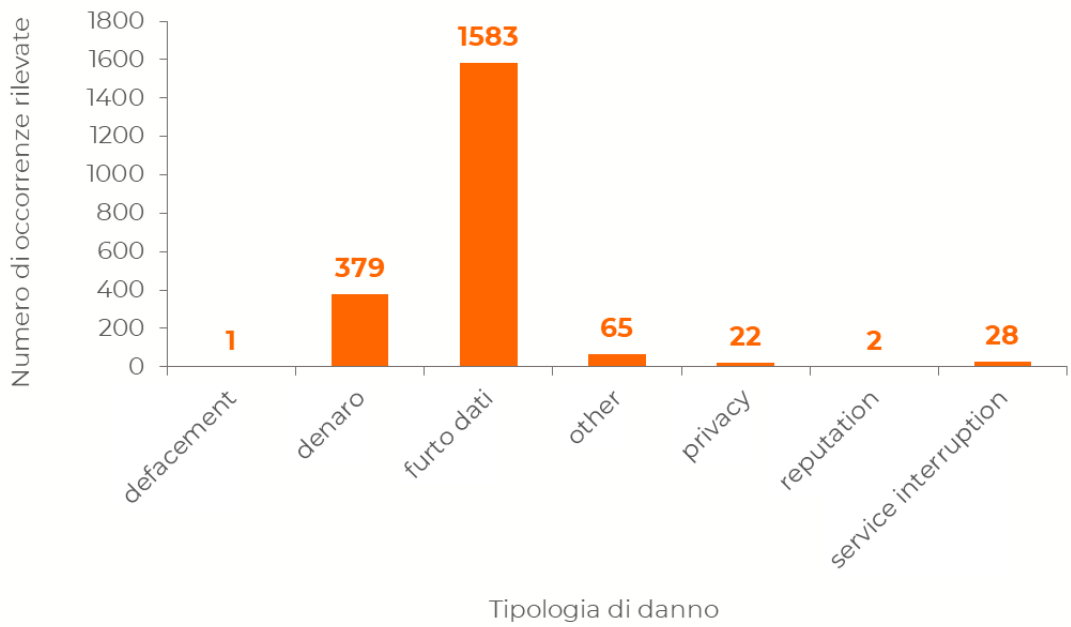


Tipologia di danno

Nel grafico sottostante si riportano le principali tipologie di danno riscontrate nel 2024: il **furto di dati** (personali e aziendali), con **1583 casi** (+**492** rispetto al 2023), rappresenta ancora il danno più diffuso.

In calo, invece, il numero di attacchi finalizzati all'**estorsione di denaro**, con **379 casi** (-**262** rispetto all'anno precedente). Questo danno è strettamente legato all'attività criminale diretta a sottrarre fondi tramite frodi online, ransomware che chiedono riscatti, o tecniche di ingegneria sociale.

Anche se meno frequente rispetto ai danni precedenti, l'**interruzione del servizio** (**28 casi**) ha un impatto notevole sull'operatività aziendale. In un mondo sempre più connesso e legato ai servizi web, questo tipo di danno può portare a perdite economiche indirette significative e alla perdita di fiducia da parte dei clienti.


Numero di occorrenze rilevate
1800
1600
1400
1200
1000
800
600
400
200
0
1
379
1583
65
22
2
28
defacement
denaro
furto dati
other
privacy
reputation
service interruption
Tipologia di danno

Approfondimento Dispositivi Connessi

Visto il contesto digitale in piena evoluzione, è fondamentale capire se tale progresso corre in parallelo alla messa in sicurezza dei servizi.

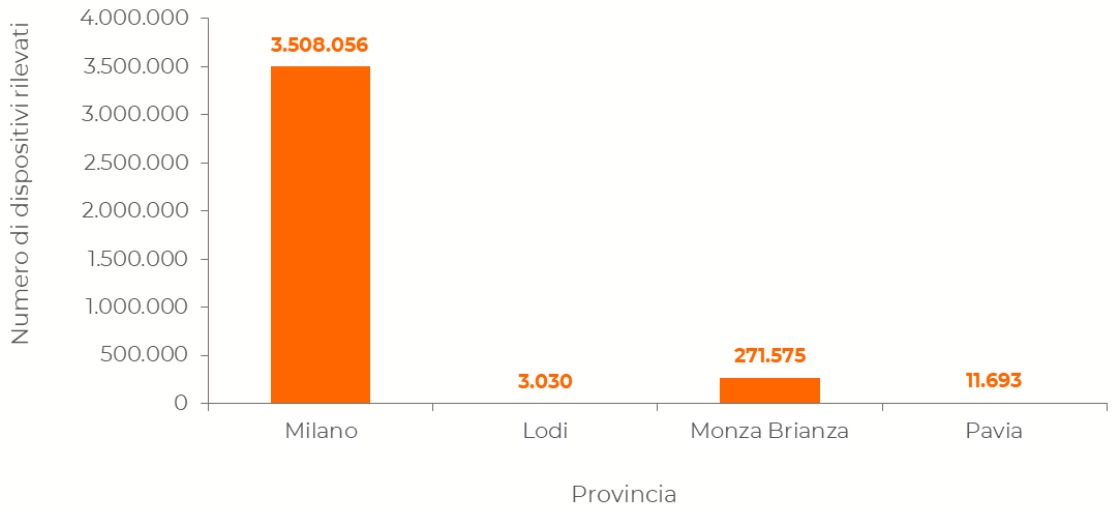
Per rispondere al quesito, Exprivia ha elaborato un'analisi sullo stato di sicurezza dei dispositivi italiani connessi in rete. Per competenza dell'Associazione, si analizzano i dati dei territori di riferimento.

L'obiettivo è duplice: da un lato, osservare l'impatto che l'IoT ha nella sicurezza dell'ecosistema digitale; dall'altro, verificare se i risultati degli investimenti fatti in cybersecurity bilanciano quelli fatti nello sviluppo del digitale.

In Lombardia, nel 2024, si registrano 5.893.257 dispositivi connessi, di cui 3.794.354 nel territorio di Assolombarda.

È opportuno osservare che il numero di **indirizzi IPv4 (dispositivi connessi)** esposti su internet nel territorio di Assolombarda è cresciuto considerevolmente rispetto all'anno precedente (+**1.958.254**). *Il numero complessivo di dispositivi esposti in rete indica il perimetro di un potenziale attacco.*

La suddivisione è la seguente:

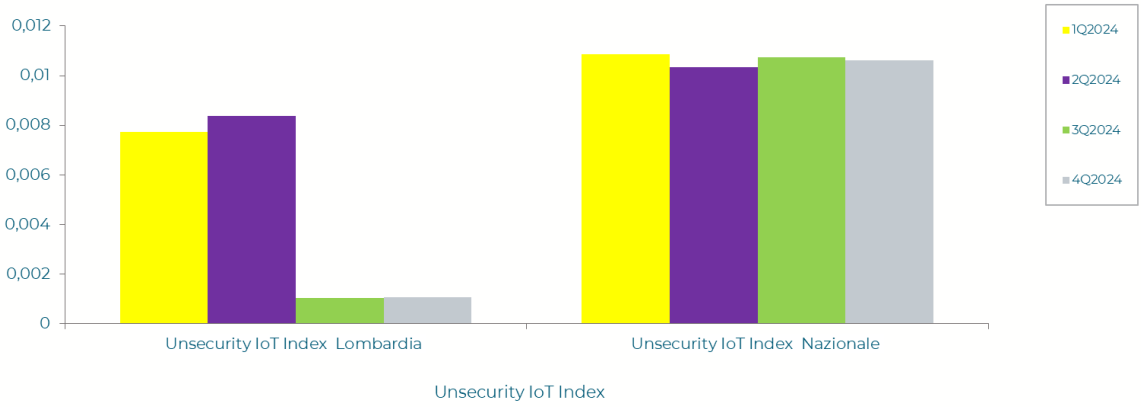


Milano	3.508.056
Lodi	3.030
Monza Brianza	2.71575
Pavia	1.1693
Totale	3.794354

Per valutare lo stato di sicurezza dei dispositivi IoT, Exprivia ha introdotto un nuovo indice di valutazione detto **Unsecurity IoT Index (UII)**. Il valore calcolato mette in relazione il numero di dispositivi IoT vulnerabili con il numero di protocolli privi di autenticazione. Tale indice viene poi comparato con quello nazionale.

Se il valore dell'indice per area geografica è inferiore al valore dell'indice totale italiano il rischio è minimo. Al contrario, se tale valore supera l'indice totale, il rischio di esposizione ad attacchi cyber per i dispositivi IoT in questa area geografica è alto.

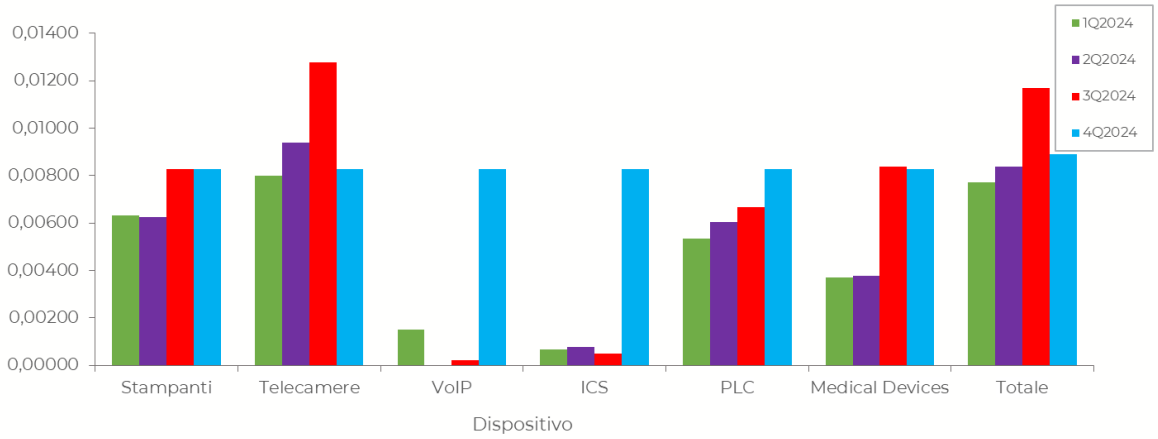
Dalla comparazione con l'UII Nazionale, **la Lombardia risulta avere un livello di rischio associato al proprio ambiente IoT minore rispetto alla media nazionale**.



	1Q2024	2Q2024	3Q2024	4Q2024
Unsecurity IoT Index Lombardia	**0,00772**	**0,00838**	**0,00104**	**0,00107**
Unsecurity IoT Index Nazionale	**0,01086**	**0,01034**	**0,01073**	**0,01061**

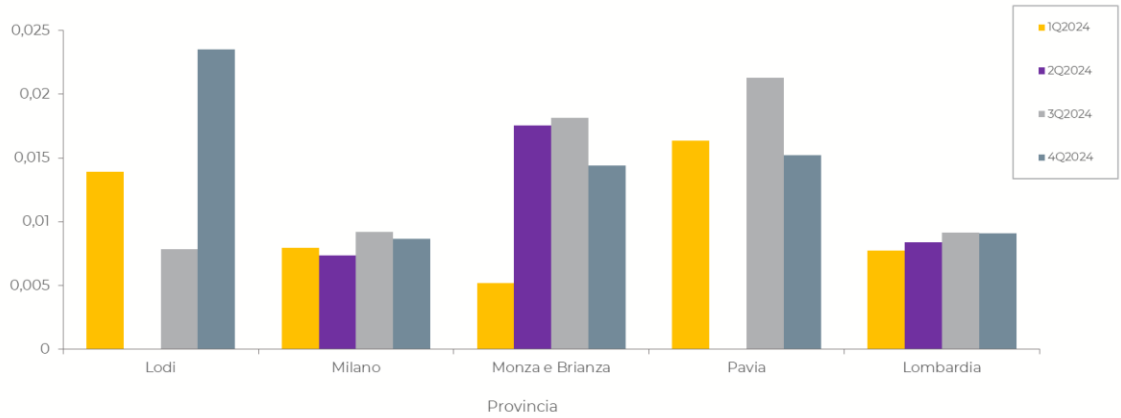
È stato successivamente calcolato l'UII per ogni dispositivo IoT analizzato, al fine di valutare quale dispositivo IoT presenti il maggior livello di rischio in Lombardia.

Come è possibile notare dal grafico sottostante, i dispositivi a maggior rischio nel 2024 risultano essere le **telecamere**, che superano il valore totale. **Stampanti**, **PLC** e **Medical Devices** mostrano un livello di rischio moderato, dato che il loro indice si avvicina al valore totale. D'altra parte, i sistemi **VoIP** e gli **ICS** evidenziano un rischio minore, avendo un indice inferiore rispetto al valore complessivo.



	Stampanti	Telecamere	VoIP	ICS	PLC	Medical Devices	Totale
1Q2024	0,00631	0,00800	0,00152	0,00068	0,00533	0,00370	0,00772
2Q2024	0,00625	0,00940	0,00000	0,00078	0,00605	0,00376	0,00838
3Q2024	0,00829	0,01279	0,00023	0,00051	0,00667	0,00839	0,01168
4Q2024	0,00829	0,00829	0,00829	0,00829	0,00829	0,00829	0,00892

Esaminando le province di riferimento di Assolombarda, si nota che **Milano** presenta un rischio moderato per i dispositivi IoT, con un indice che si allinea sostanzialmente a quello della Lombardia. Al contrario, le province di **Monza e Brianza, Lodi e Pavia** mostrano un rischio elevato, poiché il loro indice supera quello regionale.



Unsecurity Iot Index	1Q2024	2Q2024	3Q2024	4Q2024
Lodi	0,01392	0	0,00784	0,02353
Milano	0,00795	0,00738	0,00920	0,00867
Monza e Brianza	0,00518	0,01756	0,01818	0,01443
Pavia	0,01637	0	0,02128	0,01523
Lombardia	0,00772	0,00838	0,00916	0,00911

ASSOLOMBARDA

Glossario

I termini del glossario provengono da CSIRT Italia, istituito presso l'Agenzia per la cybersicurezza nazionale (ACN).

Attacco DOS e DDOS (Denial of Service e Distributed Denial of Service)

Attacco informatico che mira a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. Nella versione distribuita (DDoS) l'attacco proviene da un gran numero di dispositivi ed è diretto verso un target. Le botnet sono uno strumento per condurre un attacco DDoS.

Brute Force

Metodo di risoluzione di un problema dato mediante l'impiego di un algoritmo che consiste nel verificare tutte le soluzioni teoricamente possibili fino a quando non si trovi quella effettivamente corretta. Nell'ambito informatico, questo metodo si utilizza soprattutto per individuare le password di accesso a un sistema.

Botnet

Rete di computer utilizzata per attacchi da remoto, o per altre finalità, formata da computer infetti (bot o zombie) che, all'insaputa dei legittimi utenti, sono controllati da un utente malevolo (botmaster).

Backup

Salvataggio, totale o parziale, dei contenuti di una memoria.

Cybercrime

Azioni illecite condotte in danno di sistemi informatici o attraverso l'utilizzo abusivo degli stessi, le cui condotte sono punite dal codice penale.

Cyberwarfare

L'insieme delle operazioni militari condotte nel e tramite il cyberspace per infliggere danni all'avversario, statuale o non, consistenti – tra l'altro – nell'impedirgli l'utilizzo efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del cyberspace).

Data breach

Violazione dei dati: nel campo della sicurezza informatica si riferisce alla violazione della sicurezza dei dati, che può avvenire per errore o intenzionalmente, mediante la

distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali di uno o più persone.

Defacing

Con il termine Defacing (in italiano con defacciare) si intende la modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne. Questo tipo di attacco viene eseguito all'insaputa di chi gestisce il sito ed è illegale in tutti i paesi del mondo.

Hactivista

"Hacktivism" è un termine portmanteau coniato all'inizio degli anni '90 che identifica l'uso sovversivo di computer o computer network al fine di promuovere un'agenda politica o principi di connotazione sociale. Chi pone in essere tali pratiche è definito hacktivista o attivista digitale.

Malware

Contrazione di malicious software. Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

Phishing

Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il phisher utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

PLC

Il controllore logico programmabile (in inglese programmable logic controller, spesso in sigla, PLC) è un computer per l'industria specializzato nella gestione o controllo dei processi industriali.

Zero Day

In gergo informatico, si intendono con zero-day (o 0-day) vulnerabilità riferite a sistemi, apparati e applicazioni non ancora note al produttore della tecnologia. La gravità degli zero-day è costituita dall'assenza di aggiornamenti software a fini di mitigazione (cd. patching). Proprio tali caratteristiche rendono gli zero-day oggetto di compravendite illecite da parte di soggetti intenzionati a sfruttarli per finalità intrusive.