Cybersecurity Report

2022

"Find the right key to unlock your security"

planetica

Consulting for your future.

Prefazione

Quando si tratta di cybersecurity, ogni anno sembra essere peggiore dei precedenti e spesso le misure che attuiamo per contrastare il fenomeno ci sembrano inadeguate.

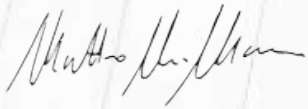
Il Covid-19 ci ha consegnato un'eredità digitale molto più avanzata rispetto al periodo pre-pandemico, contribuendo alla diffusione di asset informatici non solo per le piccole, medie e grandi imprese ma anche nella sfera privata. Tuttavia, "avanzato" non necessariamente è sinonimo di "maturo" e prova ne è l'aumento drammatico del numero di attacchi gravi e dell'entità dei danni da essi causati.
La guerra Russo-Ucraina ha portato la conflittualità anche sul piano cibernetico, ponendoci davanti alla necessità di investire ulteriormente nel rafforzamento delle infrastrutture, al fine di renderle resistenti ad attacchi esterni ma, soprattutto, resilienti.
Il report che Planetica propone quest'anno si inserisce in un lavoro di analisi e approfondimento avviato nel 2018, che ha l'obiettivo di indagare il livello di maturità della cybersecurity in Italia, "sorvegliando" i driver che ogni anno influenzano il contesto in modo diversificato.

Planetica si propone come il partner ideale per supportare aziende e professionisti offrendo un triplice servizio che può essere riassunto nel payoff ***Find the right key to unlock your security*** *che nella pratica si traduce con l'identificazione di eventuali vulnerabilità sul piano della sicurezza informatica (Find); la valutazione della metodologia più adatta in ottica di rafforzamento del comparto IT (the right key); il supporto verso il raggiungimento di una cosiddetta "Cyber Immunity" con l'obiettivo di garantire elevati standard di protezione e sicurezza (to unlock your security).*

Prendere consapevolezza del panorama attuale e del contesto nel quale cresce l'attenzione verso la cybersecurity ci consente di unire le forze e le competenze con quelle del nostro Cliente per contrastare un futuro peggioramento della situazione.

Andrea Rivetti
Presidente & Partner

Matteo Marco Marzan
Amministratore Delegato & Partner



Indice

1. Executive Summary

Proteggere la propria organizzazione da attacchi informatici è da qualche anno una delle maggiori priorità non solo per le aziende italiane ma anche a livello globale: **Data Protection e Sicurezza IT** sono infatti i temi più attenzionati ed occupano di gran lunga il primo posto in materia di investimento per l'innovazione digitale.

Il contesto lavorativo, con il protrarsi della pandemia Covid-19, ha trovato definizione nel cosiddetto "new normal", rinforzando la **consapevolezza delle aziende sulla necessità di consolidare ed integrare le iniziative di sensibilizzazione rivolte al personale**, evidenziando i rischi e le vulnerabilità della sicurezza informatica.

In linea con il trend degli anni passati, anche il 2021 ha visto una **moltiplicazione in termini di numero di attacchi, frequenza e criticità**. I cybercriminali stanno affinando sempre di più le loro strategie concentrandosi su obiettivi ben definiti: la Pubblica Amministrazione si conferma essere il bersaglio preferito, seguito dalle aziende del settore ICT e le PMI.

Per migliorare quindi la gestione dei rischi operativi delle imprese attive nell'UE, la **Commissione ed il Parlamento Europeo hanno raggiunto un accordo provvisorio sulla resilienza operativa digitale (DORA).** Le nuove norme presenti in questo quadro legislativo puntano a stimolare la competitività e l'innovazione europea nel settore finanziario, definendo dei requisiti omogenei per tutti gli Stati membri per gestire la resistenza a perturbazioni e minacce connesse alle Tecnologie dell'Informazione e della Comunicazione (TIC), e per garantire la tutela dei consumatori e la stabilità finanziaria.

In questa direzione, **l'Italia ha stanziato 45 Mld di euro per la transizione digitale**, dimostrando di essere allineata con le direttive europee per rafforzare le difese in ambito cybersecurity sia nella Pubblica Amministrazione sia nel privato per la digitalizzazione dei processi aziendali. Una scelta strategica imprescindibile, derivante dalla necessità di proteggere gli strumenti in cloud che hanno garantito continuità e fluidità al business durante e post pandemia Covid-19.

Molte aziende, infatti, attuano politiche volte a risolvere solo i punti deboli più significativi, tralasciando mediamente un quarto delle vulnerabilità elevate e/o critiche; oppure adeguandosi totalmente alla documentazione messa a disposizione dal fornitore del servizio **senza effettuare un'analisi sulla valutazione dei rischi per mettere in atto adeguate misure tecniche ed organizzative di sicurezza**.

Risulta quindi fondamentale non solo eliminare il rischio di subire minacce informatiche, ma anche sviluppare un piano di Resilienza Operativa: un **connubio di strategie di Business Continuity**, per garantire il ripristino della funzionalità e servizi di un'organizzazione, **e di Disaster Recovery**, per proteggere i sistemi aziendali al fine di ridurre gli impatti in termini economici, operativi e reputazionali che un attacco informatico può causare.

2. Cybersecurity Top trend 2022 - Visione globale

Coerentemente con gli anni precedenti, anche il 2021 riconferma il **trend crescente di attacchi informatici** che oramai da parecchio tempo preoccupa gli esperti a livello globale. Secondo il Rapporto Clusit 2022, sono **2.049 gli attacchi gravi di dominio pubblico** rilevati nel corso del 2021, rispetto ai 1.874 del 2020. Evidentemente, gli attacchi crescono in quantità e "qualità": la classificazione dei ricercatori si basa anche su una valutazione dei livelli di impatto dei singoli incidenti, tenendo in considerazione aspetti economici, sociali, di immagine nonché le ripercussioni dal punto di vista geopolitico.

+9%

attacchi gravi nel 2021

Per quanto riguarda l'analisi dei principali cyber attacchi a livello globale, l'ultima edizione del Rapporto presenta un confronto col triennio '18-'20 effettuato su un campione di 7.144 attacchi classificati tra gennaio 2018 e dicembre 2021. È emerso che **la crescita media mensile anno su anno è stata quasi del 10%**.

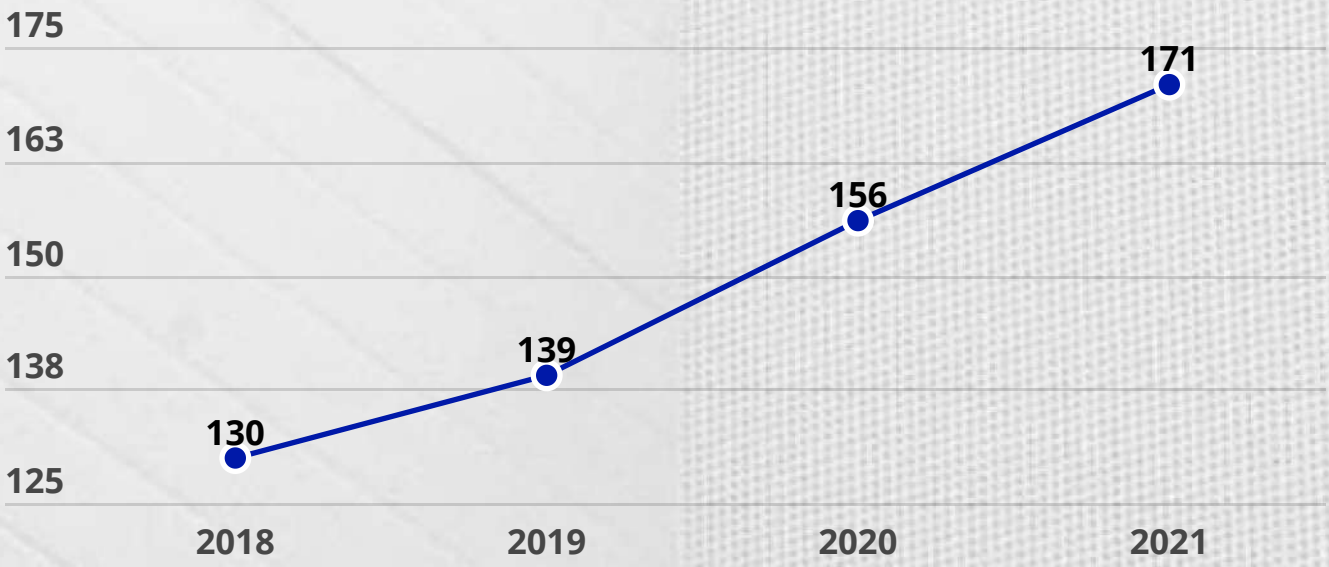


Figura 1 - Media mensile di attacchi (2018 - 2021) - Fonte: Rapporto Clusit 2022

2.1 Attacchi per settore

Sorprendentemente rispetto a quanto ci si aspettava, il Rapporto Clusit ha messo in luce come l'anno appena concluso abbia registrato un **calo nel trend di attacchi rivolti ai "Multiple Targets"**, a favore di cyber attacks mirati ad obiettivi differenziati: sono 307 gli episodi che hanno riguardato la sfera Governativa/Militare (il 15% del totale), registrando un +36,4% rispetto all'anno precedente. Al secondo posto troviamo il settore ICT con 278 attacchi, + 3,3% rispetto al 2020, cioè il 14% del totale, mentre sul gradino più basso del podio ci sono i Multiple Targets con 274 attacchi, in ribasso del 31,7% rispetto all'anno precedente, il cui calo rappresenta un **allarmante cambio di strategia degli attaccanti**. Col termine "Multiple Targets" si intendono tutti gli attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni, appartenenti anche a categorie differenti.

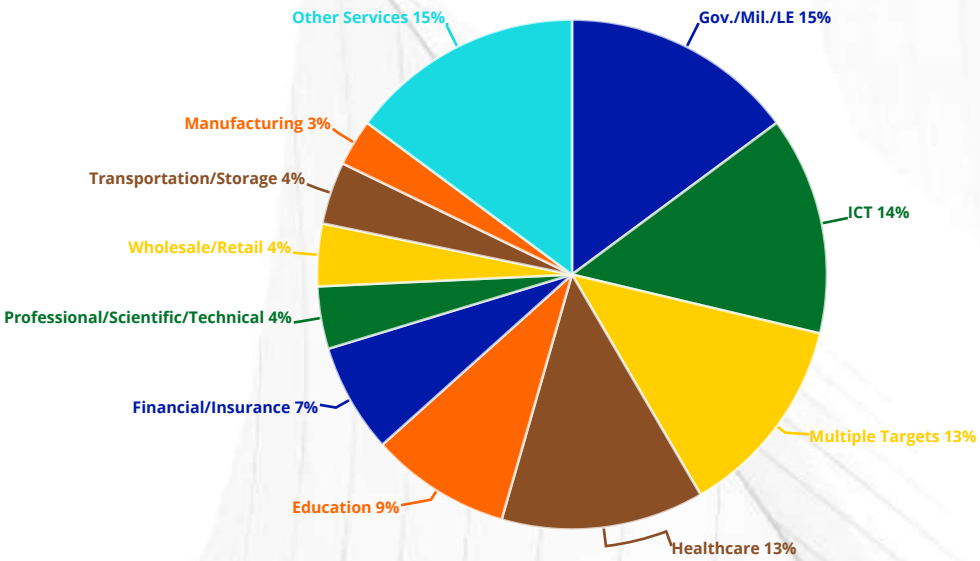


Figura 2 - Distribuzione delle vittime 2021 - Fonte: Rapporto Clusit 2022

Osservando la Figura 3 si può notare la variazione percentuale della categoria "Multiple Targets" rispetto alle altre.

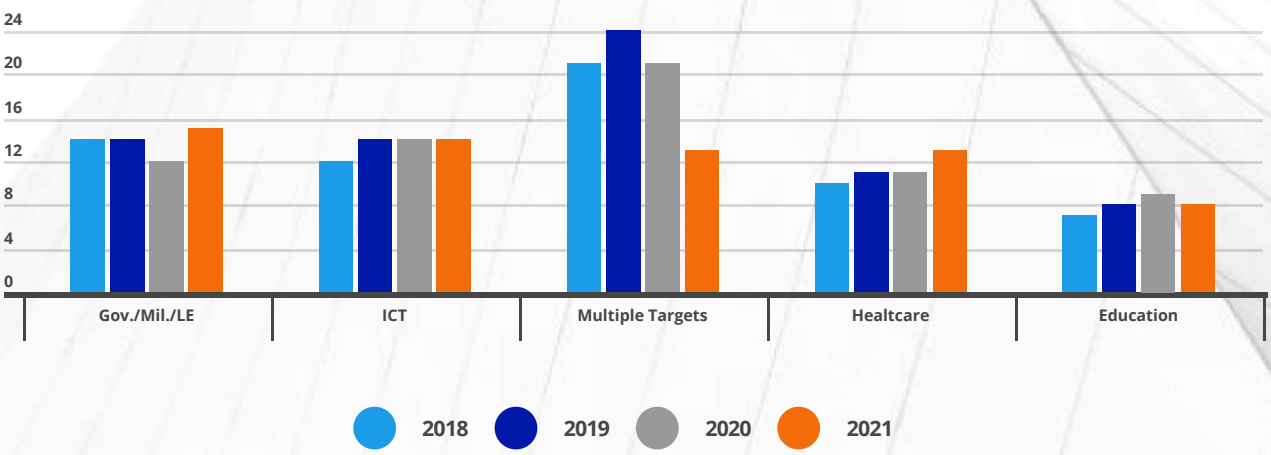


Figura 3 - Evoluzione dei top 5 obiettivi % dal 2018 al 2021 - Fonte: Rapporto Clusit 2022

2.2 Attacchi per tipologia

Nel 2021, rispetto alle quattro principali macro categorie per finalità d'attacco, è il **Cybercrime** a far registrare il numero di episodi più elevato dell'ultimo decennio, aggiudicandosi l'86% del totale con 1.763 offensive.
In ordine, per numero di attacchi, troviamo a seguire: **Spionaggio/Sabotaggio** ed **Information Warfare** rispettivamente con 217 e 49 attacchi, con numeri simili all'anno precedente. Vista la scarsità di informazioni pubbliche in merito e la difficoltà nel distinguere queste due tipologie, è rilevante segnalare che, insieme, rappresentano il 13% del totale degli attacchi.

+16%
di Cybercrime rispetto al 2020

Hacktivism: gli attacchi informatici e le azioni effettuate per finalità politiche o sociali sono in forte diminuzione rispetto al 2020. Si segnala infatti una diminuzione del -58,3% di attacchi anno su anno, per un totale di 20 episodi (1% del totale). Numeri destinati a mutare il prossimo anno a causa del nuovo contesto geopolitico.

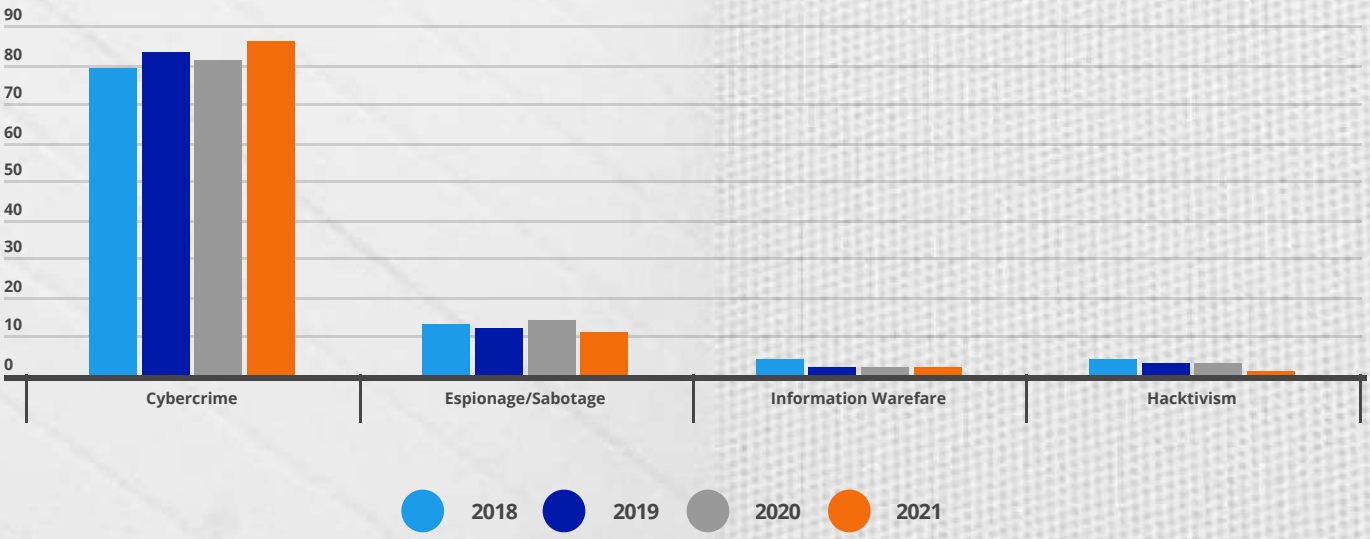


Figura 4– Variazione percentuale delle tipologie di attacco dal 2018 al 2021 - Fonte: Rapporto Clusit 2022

Con riferimento alle **tecniche di attacco**, anche nel 2021 si conferma al primo posto la categoria dei **"Malware"**, ovvero tutte quelle applicazioni finalizzate ad arrecare un danno alla vittima (41% del totale degli attacchi), segnando un trend in rialzo del 7%.
La categoria **"Vulnerabilities"** fa registrare un preoccupante **+60% rispetto al 2020** con 320 attacchi. Le due categorie insieme costituiscono il 57% del totale dei casi analizzati.

Risultano in forte crescita anche le tecniche **“Unknown”** con un **+16,4%** sul 2020 ed un totale di 433 casi su 2049. L'aumento di questa categoria è segnale di una sempre maggior difficoltà ad identificare la tipologia di attacco e la conseguente soluzione di difesa: alla base di questa situazione vi è il fatto che, di norma, gli attacchi subìti non sono resi pubblici fintanto che gli organi di controllo non li identifichino come “Data Breach”, alla luce dei quali, invece, le normative vigenti impongono una notifica agli interessati.

Tra le categorie che invece hanno registrato una **decrescita** nel numero di eventi di sicurezza distinguiamo:

Phishing/ Social Engineering

-32%

attacchi mediante falsa comunicazione di posta elettronica atti a rubare alla vittima informazioni e credenziali di accesso

Distributed Denial Of Services (DDOS)

-8,8%

attacchi che mirano a rendere inaccessibili alcuni tipi di servizi, eseguiti da diversi indirizzi IP

Identity Theft/ Account Hacking

-15,6%

attacchi che utilizzano la frode o l'inganno per ottenere informazioni personali o sensibili di una vittima

3. Cybersecurity Top trend 2022 - Visione Italia

L'analisi contenuta nel Rapporto Clusit relativa allo scorso anno mostra come si sia registrata una crescita del 16% delle violazioni di sicurezza, aumentate dai 36 Mln rilevati nel corso del 2020 ai 42 Mln del 2021. Tra i trend cybersecurity più rilevanti dello scorso anno si osserva la continua crescita di **malware** e **botnet** che si attesta sul **+58% di server compromessi.** I settori più colpiti si confermano il Finance/Insurance e la Pubblica Amministrazione, obiettivi che insieme costituiscono circa il 50% dei casi. A questi si aggiunge quello dell'Industria che presenta l'aumento più significativo, dal 7% del 2020 al 18% del 2021.

46.000

server e device rilevati privi di livelli minimi di protezione

Nell'ultimo anno sono stati rilevati 46.000 tra server e device privi di livelli minimi di protezione e che ancora espongono servizi critici direttamente su Internet. Il numero di questi server in un anno è però diminuito del 16%, un trend che continua da diverso tempo a dimostrazione che le aziende stanno progressivamente aumentando le proprie linee difensive di base.

I server con protezione minima sono diminuiti del

-16%

a dimostrazione dell'aumento delle difese da parte delle aziende

Il Rapporto Clusit presenta inoltre un interessante spaccato sulle minacce pervenute via mail, oggetto di una continua crescita. Il vettore d'attacco principale è l'utilizzo di **URL malevoli** che rappresenta l'87% del totale, in crescita dell'11%. Oltre alla diversificazione degli strumenti utilizzati per provocare danni informatici, varia soprattutto la tecnica scelta per raggiungere l'obiettivo, che può consistere nell'installazione di un software malevolo oppure nel furto dei dati personali degli utenti.

Quest'ultima, in particolare, nota come «**Credential Phishing**», rappresenta la modalità di attacco più utilizzata, con un peso del 60% sul totale, anche se in lieve decrescita. Il 2021 si è inoltre caratterizzato per una crescita di fenomeni fraudolenti che sfruttano il servizio SMS, dovuti in particolare alla diffusione di malware, quali Flubot, veicolati per l'appunto tramite la cosiddetta tecnica dello smishing.

In conclusione, le rilevazioni del 2021 mostrano da un lato un aumento generalizzato degli attacchi informatici, dall'altro una maggiore consapevolezza delle minacce da parte delle aziende e degli utenti che stanno gradualmente rafforzando le misure di difesa e il know-how in ambito Security.

3.1 Strategia Italia

Per sostenere i Paesi Membri, a seguito della pandemia, la Commissione Europea ha emanato dei provvedimenti massivi di politica fiscale rientranti nel fondo noto come **Next Generation EU**, per il quale sono stati stanziati **750 Mld di euro destinati a finanziare i Piani di Ripresa e Resilienza (PNRR)** presentati dagli Stati Membri.

750 mld

di euro destinati a finanziare i PNRR

Il Piano presentato dall'**Italia**, uno dei paesi meno digitalizzati dell'UE, si focalizza su 16 obiettivi riconducibili a **6 missioni**, ovvero: Digitalizzazione e innovazione (1), Transizione ecologica (2), Infrastrutture per una mobilità sostenibile (3), Istruzione e ricerca (4), Inclusione e coesione (5), Salute (6).

La **missione 1 e la missione 4** contengono i **fondi destinati alla cybersecurity ed in particolare alla digitalizzazione della Pubblica Amministrazione** e alle iniziative di partenariati tra il pubblico ed il privato, con l'obiettivo di sviluppare una rete di cooperazione e ricerca.

La principale novità organizzativa prevista dal PNRR è l'introduzione dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**, nata con l'obiettivo di difendere e promuovere la sicurezza e la resilienza della nazione, definire la strategia nazionale di sicurezza informatica, gestire i rapporti di cooperazione internazionale e stimolare un'autonomia e indipendenza tecnologica riguardo a prodotti e processi informatici di rilevanza strategica. Per la creazione e lo sviluppo è previsto un investimento di 527 Mln di euro a partire dal 2022. L'agenzia è attesa come un vero e proprio punto di riferimento per la definizione delle policy aziendali, tanto che i principali impatti previsti dalle organizzazioni sono:

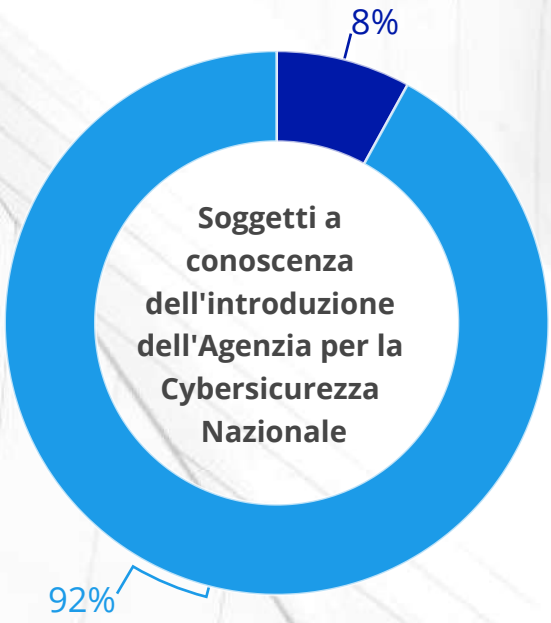


Figura 5 – Soggetti a conoscenza dell'introduzione dell'ACN – Fonte: Osservatorio Cybersecurity e Data Protection

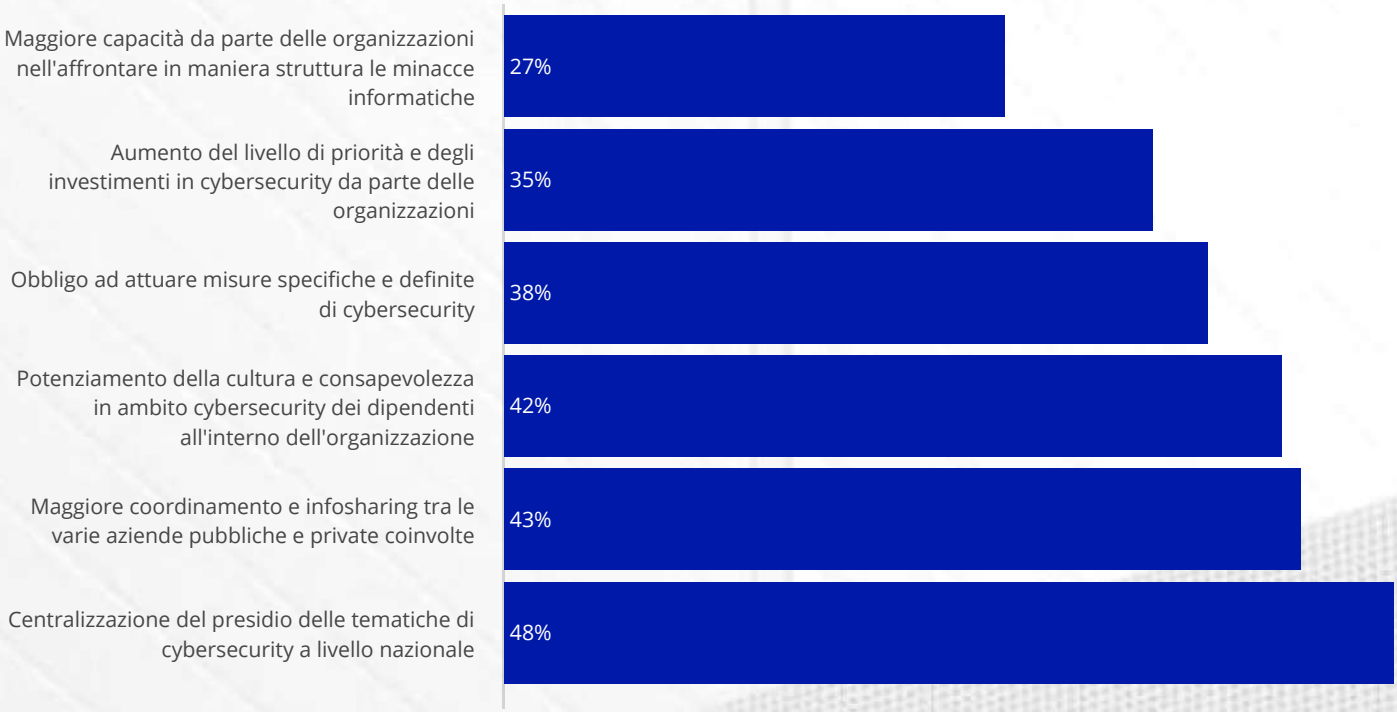


Figura 6 – Principali impatti previsti dalle aziende a seguito dell'introduzione dell'ACN – Fonte: Osservatorio Cybersecurity e Data Protection

3.1.1 Roadmap e ruolo ACN

A livello nazionale si è assistito all'istituzione dell'Agenzia per la Cybersicurezza Nazionale, attraverso l'adozione del D.L. 14 giugno 2021, n. 82. L'ACN nasce con l'obiettivo di assicurare il coordinamento tra i soggetti pubblici coinvolti nella materia e di promuovere la realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica necessarie allo sviluppo digitale del Paese.

Giugno '21

L'obiettivo dell'Agenzia è quello di **perseguire il conseguimento dell'autonomia strategica nazionale ed europea nel settore del digitale**, in sinergia con il sistema produttivo nazionale, nonché attraverso il coinvolgimento del mondo dell'università e della ricerca. L'ACN favorisce inoltre specifici percorsi formativi per lo sviluppo della forza lavoro nel settore e sostiene campagne di sensibilizzazione oltre che una diffusa cultura della cybersicurezza.

Agosto '21

La conversione in legge ad Agosto 2021 ha sancito l'avvio della prima operatività con l'inizio della fase di strutturazione interna e start-up delle attività dell'Agenzia; quindi la pubblicazione del documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud nella Pubblica Amministrazione.

A Gennaio 2022 si è assistito all'**attuazione della Strategia Cloud Italia** con la definizione del modello per la classificazione dei dati e dei servizi della PA, i requisiti per le infrastrutture digitali e per i servizi Cloud destinati a trattare dati e servizi strategici, critici e ordinari. È stata inoltre avviata una collaborazione con il Garante Privacy per la protezione dei dati personali, lo scambio di informazioni e la promozione di buone pratiche di sicurezza cibernetica.

Gennaio '22

Maggio '22

Il 25 Maggio 2022 è stata pubblicata e presentata alla stampa la **nuova Strategia Nazionale di Cybersicurezza**, un percorso all'insegna dell'innovazione che prevede l'attuazione entro il 2026 di 82 misure, riportate nel Piano di Implementazione a corredo delle Strategia. Le principali sfide che la Strategia dell'ACN mira ad affrontare sono:

> Assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo
>
> Anticipare l'evoluzione della minaccia cyber
>
> Contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida
>
> Gestione di crisi cibernetiche
>
> Autonomia strategica nazionale ed europea nel settore del digitale

Diviene operativo il Centro di Valutazione e Certificazione Nazionale (CVCN) per la valutazione di beni, sistemi e servizi ICT, destinati a essere impiegati su infrastrutture che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato.

Luglio '22

4. DORA: Cybersecurity e Resilienza Operativa

Nel più ampio set regolatorio della strategia UE sulla cosiddetta "finanza digitale", si innesta il **Digital Operational Resilience Act** (**DORA**) e cioè il regolamento che mira ad assicurare la resilienza operativa digitale del settore finanziario in Europa in caso di eventi avversi "cyber disruptive". In uno scenario di mercato già in evoluzione, la distanza sociale imposta dalla pandemia da COVID-19 ha sottolineato la necessità di digitalizzare l'economia e imposto un ripensamento su larga scala dell'accesso ai servizi finanziari.

L'oggetto della proposta del nuovo regolamento si attiene alla capacità di un'entità finanziaria di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, per garantire il corretto funzionamento dell'ICT aziendale nella fornitura dei servizi finanziari.

Gli esperti del settore hanno definito il carattere fondante della proposta di regolamento DORA come "un **big bang** della cybersecurity per il sistema finanziario comunitario, con obiettivi comuni sfidanti. Un effetto di istantaneo innalzamento dello standard regionale, che rende il sistema finanziario comunitario più forte e con ricadute anche globali".

La ragione per cui si rende necessario il regolamento DORA, diventa più facilmente intuibile esplicitando le finalità del regolamento, riassumibili in 4 punti:

1. **Centralizzazione del ruolo delle autorità di vigilanza**

   negli ambiti di controllo e valutazione dei presidi adottati dai player finanziari, nella gestione degli incident e valutazione dei rischi dei fornitori ICT integrati

2. **Riduzione delle disparità tra gli Stati membri**

   attraverso la creazione del cosiddetto *level playing field*, ovvero la condivisione di obblighi organizzativi e procedurali nell'identificazione dei rischi ICT

3. **Governance dei rischi ICT e cyber risk**

   con l'obbligo della creazione di una Governance per la valorizzazione dei rischi ICT e cyber quali rischi autonomi in ambito operativo e finanziario

4. **Innalzamento dello standard europeo in materia di cybersecurity**

   con l'obiettivo di anticipare le necessità data l'accelerazione della digitalizzazione ed evoluzione tecnologica in ambito financial services

L'11 maggio 2022 è stato raggiunto un **accordo provvisorio** sulla bozza finale del regolamento DORA che garantirà per l'appunto al settore dei financial services in Europa di essere in grado di preservare la resilienza delle operazioni in caso di gravi break operativi.
All'accordo provvisorio seguirà la procedura di adozione formale e il relativo recepimento di ogni Stato membro, con l'auspicio che in tempi brevi possa vedersi concretizzato un framework operativo condiviso.

Digital Operational Resilience Act

5. La gestione del cyber risk

Un'indagine condotta da Allianz evidenzia come il **cyber risk sia il rischio più temuto per il business per il 2022**. L'elevata preoccupazione destata dal rischio cyber è motivata dall'aumento del valore delle perdite causate dagli attacchi informatici gravi che ammontano a 6.000 miliardi di dollari (3 volte il PIL italiano!).

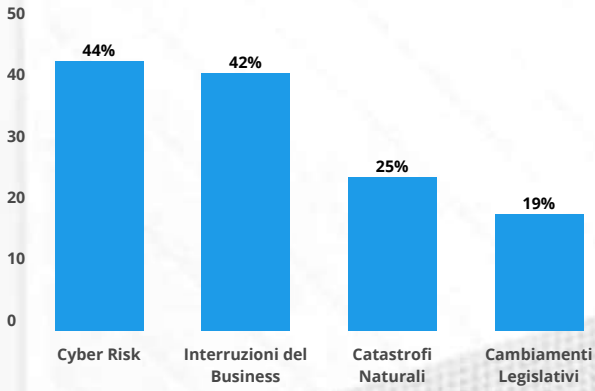


Figura 7 – The top business risks for 2022 – Fonte: Allianz Risk Barometer

+80%

attacchi identificati nella fascia critico-alta del campione di riferimento

Tra il 2021 e il 2022 i cyber attacks sono cresciuti in numero e soprattutto in gravità. Questo fattore ha comportato l'aumento del numero di aziende che fatica a gestire gli attacchi informatici (54% rispetto al campione di riferimento).

Si stima che il **costo di un data breach** per una piccola azienda si aggiri intorno ai **10.000 euro**, con un aumento del 40% per le grandi imprese. Nonostante la maggior parte degli attacchi informatici avvenga tramite Malware, in particolare Ransomware, il numero di incidenti è leggermente diminuito nel quarto trimestre del 2021 (15%), cedendo il titolo di principale vettore d'attacco al Phishing, che registra un aumento del 40% nel terzo trimestre rispetto al secondo trimestre del 2021.

Nel 2022 sarà quindi fondamentale per le aziende **aumentare le attività di patching per rendere più sicuri gli ambienti informatici**, così da poter agire tempestivamente sulle vulnerabilità scoperte e gli exploit dei PoC (Proof of Concept) che diventano pubblici ogni giorno. Con le librerie di siti web e i componenti obsoleti che si classificano in cima alle principali vulnerabilità riscontrate durante il 2021 (37%), è evidente che non tutte le organizzazioni seguono regolarmente le misure di sicurezza di base, come l'aggiornamento del software, per proteggersi dalle minacce informatiche.

Attacchi Ransomware nel quarto trimestre del 2021

-15%

Attacchi Phishing nel terzo trimestre del 2021

+40%

Molte aziende attuano politiche volte a risolvere solo i punti deboli più significativi (senza sviluppare un'ulteriore analisi a causa di restrizioni di tempo o risorse), lasciando mediamente **un quarto delle vulnerabilità elevate e/o critiche non risolte**. Si sottolinea che questi dati sono da considerare limitati in quanto provengono solo da aziende che applicano regolarmente test di penetrazione e re-test. Inoltre, particolare **attenzione va posta sui software gestiti da terze parti**: molte delle librerie, componenti e patch, presentano infatti gravi vulnerabilità dovute agli scarsi controlli che vengono effettuati sugli sviluppi "sicuri" del codice.

Con il mercato delle criptovalute in costante espansione, si prospetta un numero crescente di attacchi informatici di tipo phishing o malware che mirano a cambiare gli indirizzi di memoria degli Smart Contract.

Tutelarsi dai rischi informatici è quindi una priorità sempre più urgente per i leader dell'economia globale che devono agire perseguendo principalmente tre strade. In primo luogo, è necessario **predisporre un piano di sicurezza efficace** nell'individuare eventuali vulnerabilità dei sistemi e che garantisca la protezione del business sia a livello di accessi e di hardware che custodiscono informazioni sensibili, sia attraverso il monitoraggio di software e di sistemi aziendali.

Parallelamente, diventa imprescindibile **investire un adeguato budget nella formazione e nella sensibilizzazione del personale** riguardo la sicurezza informatica, nell'ottica di prevenire parte degli attacchi informatici imputabili al fattore umano. Entrambe le strategie dovrebbero essere affiancate dalla **sottoscrizione di apposite polizze assicurative** che riducano i danni conseguenti da un attacco informatico e garantiscano la resilienza del business. Le polizze cyber agiscono infatti su più fronti: danni diretti, come la perdita dei dati; danni indiretti, tra cui le perdite di profitto, i costi di recupero e più in generale la business interruption; le responsabilità civili verso terzi dei quali l'assicurato detiene informazioni sensibili, critiche, commerciali che costituiscono proprietà intellettuale o personale. Inoltre, le polizze possono prevedere coperture sempre più articolate:

Computer Crime, che garantisce una copertura della perdita finanziaria a seguito di un furto di denaro o titoli

Sociale Engineering Fraud (SEF), nata con l'obbiettivo di assicurare il valore dei fondi trasferiti in modo indebito

Voluntary Shutdown, che copre il danno indiretto anche in caso di arresto volontario dei sistemi per motivazioni ragionevoli

Nonostante il **mercato delle polizze assicurative a copertura del rischio cyber** registri un **aumento del 300%** nell'ultimo anno, si evidenzia la tendenza a classificarsi sempre più come "hard market", ovvero un mercato dove è presente un numero limitato di compagnie assicurative che offrono tutela da attacchi informatici ed una crescente attenzione nel valutare la maturità difensiva delle aziende. Secondo ASSITECA, broker assicurativo operante a livello nazionale, i **costi delle polizze assicurative cyber sono aumentati del 20% circa**, con picchi più elevati nel caso di sistemi poco strutturati.

Parallelamente, variano rispetto al 2021 le figure a cui le aziende decidono di affidare la gestione della sicurezza informatica. Se nel 2020 il 41% delle grandi organizzazioni delega la gestione del rischio Cyber ad una figura specializzata come il **Chief Information Security Officer (CISO)**, nel 2021 la percentuale aumenta del 5%, raggiungendo il 46% delle aziende. Resta invariato al 25% il numero di aziende che affida la gestione della sicurezza informatica al Chief Information Officer (CIO). Diminuisce invece la gestione dei rischi informatici delegata alla figura del Security Manager, passando dal 13% del 2020 al 10% del 2021.
L'11% dei casi ha invece predisposto una figura aziendale per la gestione del rischio cyber diversa da quelle fin qui citate, percentuale diminuita dell'8% rispetto ai dati relativi al 2020.
Cresce invece dal 2% all'8% la quota di soggetti intervistati che dichiara che nella propria organizzazione non è stata nominata una figura preposta a tale ruolo.

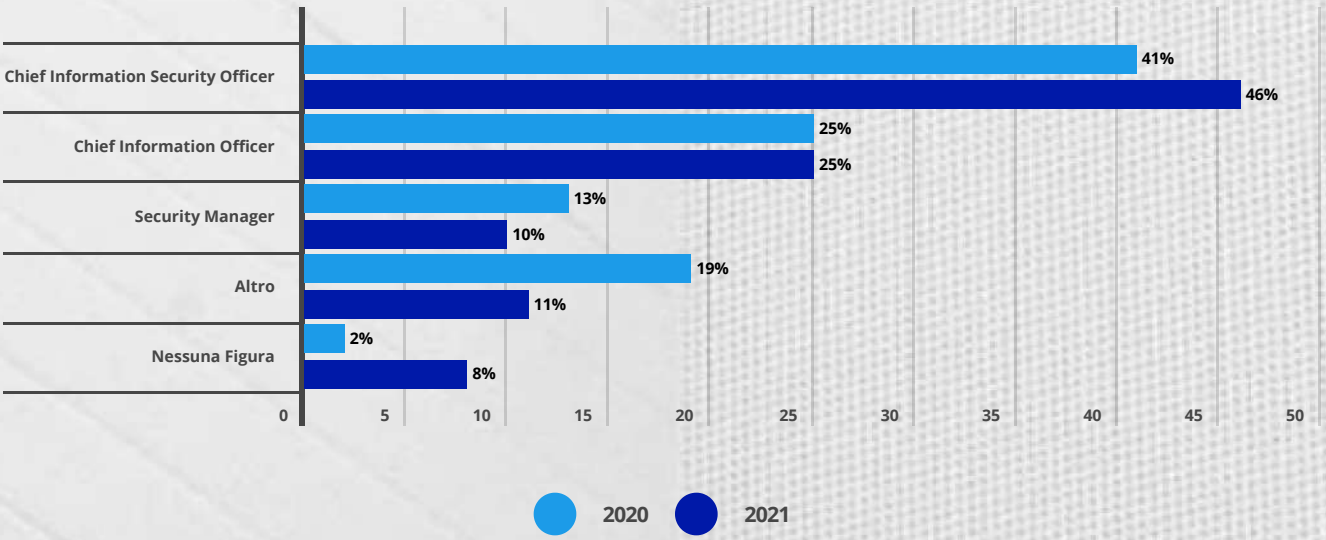


Figura 8 - Figure preposte alla gestione del rischio cyber - Fonte: Osservatorio Cybersecurity e Data Protection

Dal punto di vista del processo di **gestione del rischio cyber**, l'Osservatorio Cybersecurity del Politecnico di Milano offre uno spaccato sulle differenze rispetto al 2019 nel modo di gestire il rischio informatico da parte delle aziende. Il dato fondamentale è rappresentato dall'aumento di organizzazioni che gestiscono il cyber risk **come un rischio a sé stante all'interno di una funzione dedicata**; si è passati infatti dal 40% del 2019 al quasi 50% dello scorso anno, percentuale che dimostra come le aziende acquistino sempre più consapevolezza rispetto al peso e all'importanza che deve essere data alla gestione del rischio informatico. Parallelamente, diminuiscono dell'11% le entità che inseriscono la gestione del cyber risk all'interno di un processo integrato di Risk Management aziendale (dal 49% del 2019 al 38% del 2021).

Allerta invece l'**aumento del 2% di organizzazioni che non monitorano costantemente il rischio cyber** (dall'11% del 2019 al 13% del 2021); probabilmente aziende che tutt'ora scontano, in termini di budget, le conseguenze della pandemia.

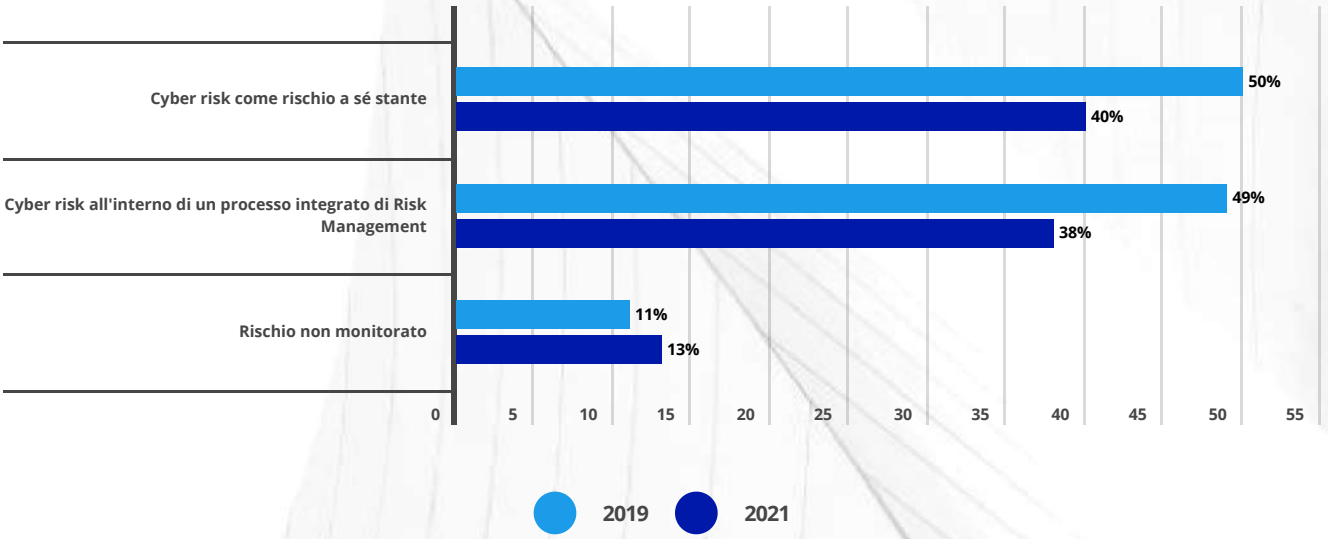


Figura 9- La gestione del rischio cyber - Fonte: Osservatorio Cybersecurity e Data Protection

6. Cybersecurity e Data Protection

GDPR e Cloud Provider: la compliance e la sicurezza dei dati

Il trend di **crescita** delle aziende nell'adozione di **strumenti in Cloud** per garantire continuità e fluidità al proprio business ha contribuito, ad inizio 2022, a focalizzare l'attenzione sul consolidamento degli aspetti di sicurezza e prevenzione degli attacchi informatici. Da un'analisi condotta dall'Osservatorio Cybersecurity & Data Protection, la **totalità delle aziende italiane** che **ha sottoscritto da 1 a 5 contratti di Public Cloud** negli ultimi due anni è pari al 78%. Tra queste, ben il 68% ha all'attivo 5 contratti, percentuale che include non solo grandi realtà ma anche un 23% di imprese di piccole e medie dimensioni.

All'interno di questa fotografia si evidenzia inoltre che solo l'80% delle aziende effettua attività di valutazione della compliance sui propri fornitori in maniera costante e continuativa, con una diminuzione di tendenza del 49% per quanto riguarda l'analisi dei subfornitori, dove viene favorito un controllo più sporadico. **Quasi la metà del campione, tuttavia, basa il proprio esame sulla documentazione messa a disposizione dal fornitore**. Questo approccio di accettazione "passiva" viene adottato specialmente da aziende medio piccole, mentre le **grandi imprese tendono a guidare la valutazione secondo i propri criteri interni**.

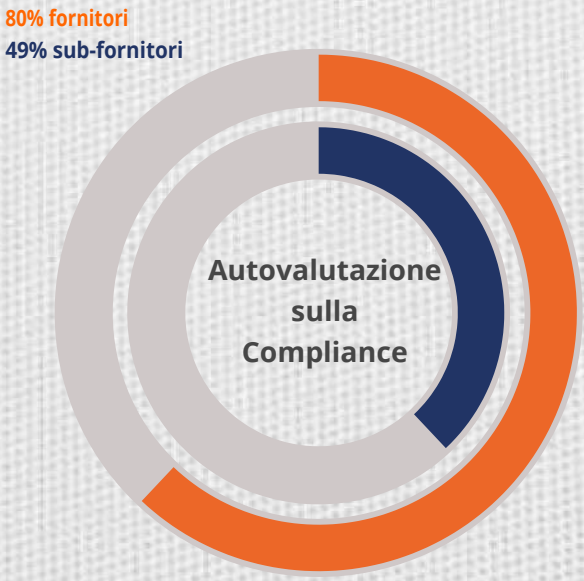


Figura 11 - Differenza percentuale di autovalutazione sulla Compliance tra fornitori e sub-fornitori - Fonte: BULLETPROOF ANNUAL CYBER SECURITY INDUSTRY REPORT

Valutazione del livello di sicurezza

Preoccupa il ridotto livello di attenzione delle aziende all'attività di valutazione della sicurezza, che risulta meno praticata rispetto alla valutazione della compliance alla normativa sui dati personali.

Dall'analisi del campione:

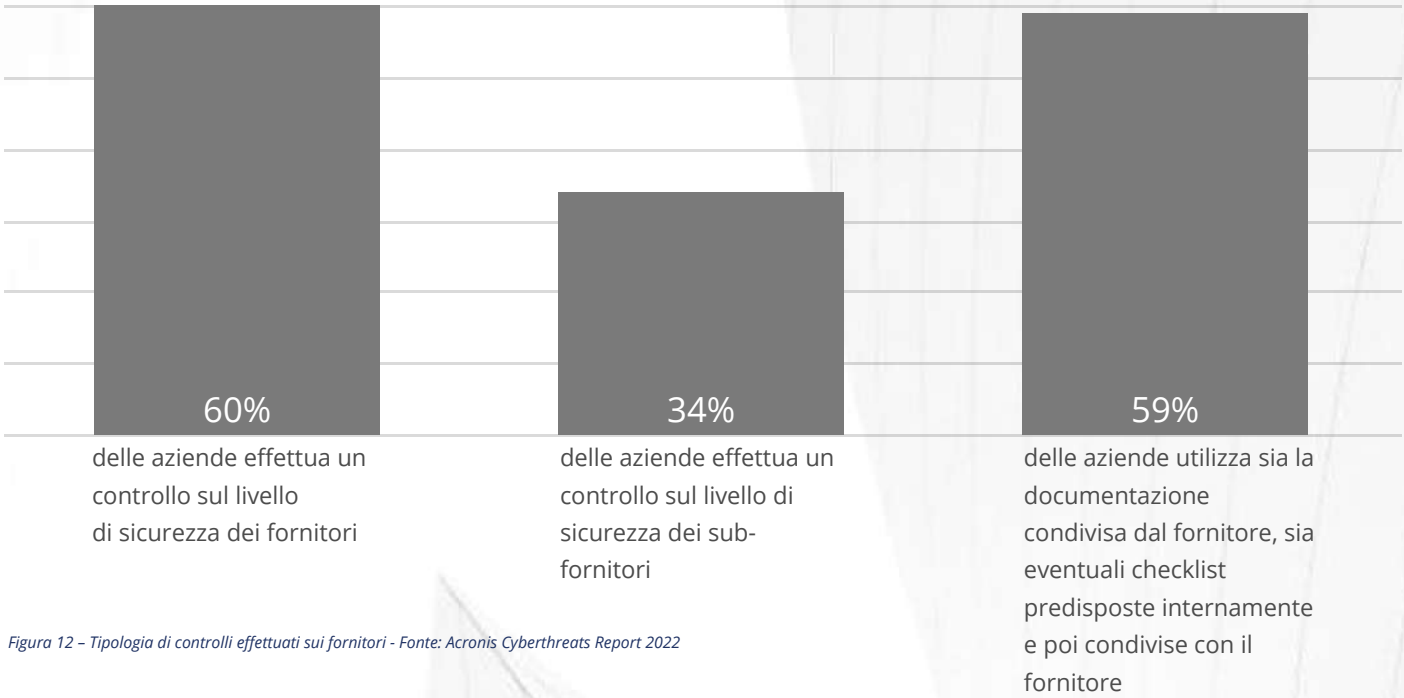


Figura 12 – Tipologia di controlli effettuati sui fornitori - Fonte: Acronis Cyberthreats Report 2022

Questa modalità di analisi della sicurezza segue il trend di influenza della dimensione aziendale osservato precedentemente, confermando la necessità delle grandi aziende di avere una maggiore proattività nella relazione con i fornitori.
Da questa ricerca è possibile evidenziare un **basso grado di maturità dell'impianto normativo attuale**: le analisi delle attività di valutazione della compliance alla normativa ed alla sicurezza dei fornitori a carico dell'azienda avviene in maniera estremamente frammentaria e disorganizzata, risultando inefficiente.

Sicurezza in Cloud

La maggior parte degli incidenti di sicurezza nel Cloud si verificano a causa di configurazioni errate. Questi possono includere la concessione di privilegi eccessivi, l'esposizione involontaria di risorse al pubblico o la mancata modifica di configurazioni predefinite "deboli". **Un quarto delle aziende (27%) ha subito un incidente di sicurezza correlato al Cloud pubblico**, un aumento del 10% rispetto allo scorso anno.

Da inizio anno le configurazioni errate (23%) hanno conquistato la prima posizione come incidente numero uno relativo alla sicurezza, superando i dati esposti per utente (15%) e la compromissione dell'account (15%) rispetto allo scorso anno.

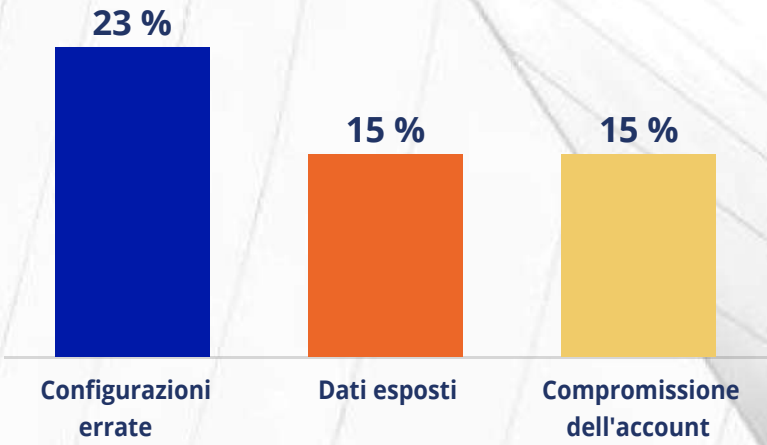


Figura 13 – Principali incidenti di sicurezza legati al Cloud - Fonte: Rapporto Clusit 2022

Questi dati sono preoccupanti soprattutto se rapportati al fatto che il 35% degli intervistati ha più del 50% dei propri carichi di lavoro nel Cloud, con un aumento fino al 75% entro i prossimi 12-18 mesi.

+75% **di utilizzo del Cloud entro i prossimi 12-18 mesi**

Uno degli errori più comuni per la sicurezza legata al Cloud pubblico rappresenta l'uso eccessivo dell'utenza root, ovvero l'utenza che dispone del massimo controllo sul sistema.
Le **best practice** per la sicurezza del Cloud e il benchmark del Center for Internet Security indicano che le organizzazioni dovrebbero evitare di utilizzare l'utente root per attività amministrative e quotidiane, eppure il 27% dei team non presta sufficiente attenzione.
La creazione di ruoli dedicati con autorizzazioni appropriate per l'esecuzione di attività amministrative è molto meno rischiosa dell'utilizzo constante dell'account utente root.
Allo stesso tempo:

Provider

Hanno aumentato i sistemi di protezione dell'11% in un solo anno, implementando funzionalità come il controllo sull'accesso (72%), anti-virus/anti-malware/ATP (60%), autenticazione a più fattori (53%)

Organizzazioni

Il 48% **non abilita l'autenticazione a più fattori** (MFA) su account con privilegi elevati, il che rende più facile per gli aggressori compromettere l'organizzazione se le credenziali dell'account sono trapelate o rubate

Un'ulteriore sfida è rappresentata dalla scelta di uno o più fornitori di servizi Cloud che, secondo l'analisi del campione, sono selezionati attraverso cinque fattori fondamentali:

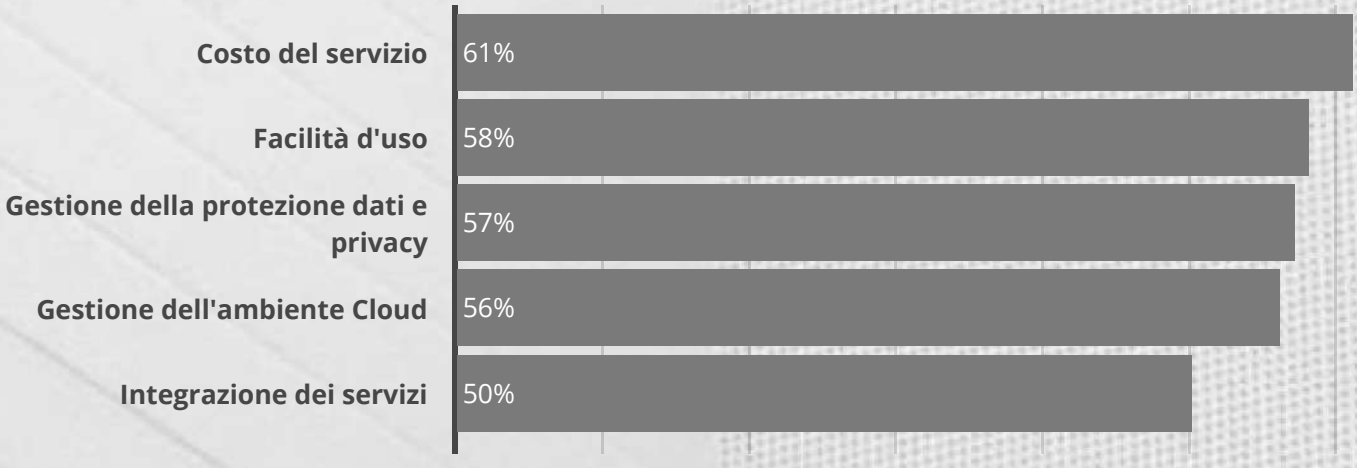


Figura 14 – Drivers per la scelta di un fornitore Cloud - Fonte: Rapporto Clusit 2022

Non sorprende quindi che il 75% degli intervistati abbia citato la necessità di una piattaforma di sicurezza Cloud con un'unica dashboard in cui poter configurare tutte le policy necessarie per proteggere i dati in modo coerente e completo attraverso il proprio footprint Cloud.

80% **degli utenti in azienda deve accedere a 3 o più dashboard di soluzioni di sicurezza separate per configurare le policy Cloud della propria azienda**

6.1 Focus GAIA-X

GAIA-X è un progetto che ambisce a realizzare un'infrastruttura a livello europeo, il cui fine è quello di **raggiungere la sovranità digitale europea nel campo del Cloud**, alimentando la concorrenza con i player stranieri extra-UE, Amazon e Google. L'obiettivo di GAIA-X è fornire "uno standard unico, condiviso tra tutti i Paesi partner", collegando tra di loro i diversi servizi e dando luogo a un **Cloud federato europeo** attraverso un accordo di collaborazione per definire criteri e standard comuni di gestione dei dati e di servizi, prevedendo anche la creazione di una serie di hub regionali.

L'entità giuridica della Fondazione GAIA-X è stata presentata il **4 Giugno 2020** come organizzazione no-profit e ad oggi fatica a decollare a causa degli attriti e delle diverse posizioni dei suoi membri corporate, oltre che di una pesante struttura burocratica.

Figura 15 – Le 29 entità italiane che partecipano al progetto GAIA-X – Fonte: www.wired.it

Il **Consiglio di Amministrazione del consorzio è composto da aziende europee** quali OVHCloud, Airbus, Orange e Deutsche Telekom, ma il coinvolgimento riguarda **anche partner extra europei**: tra le crescenti organizzazioni che hanno aderito al progetto – ad oggi circa 320 – ci sono alcune che rappresentano gli interessi di aziende esterne, come Bitkom, CISPE e Digital Europe che sono la voce dei vari Amazon, Google e Microsoft all'interno di GAIA-X. E sono proprio i servizi Cloud di Amazon, Microsoft e Google che in questo ultimo periodo hanno consolidato il loro dominio sull'Europa, conquistando il 69% del mercato (il più grande Cloud player europeo, Deutsche Telekom, rappresenta solo il 2%).

Di conseguenza, iniziative parallele sono già state lanciate dall'UE per ovviare ad una minore dipendenza dalle società tecnologiche non europee: un gruppo di aziende europee di software e hardware (tra cui NextCloud, Scaleway ed altre aziende insoddisfatte dei progressi di GAIA-X) ha lanciato un'associazione chiamata Euclidia, un **servizio di Cloud all'avanguardia che consenta all'Europa di divenire leader globale senza seguire i modelli americani o asiatici**.

7. Trend & Outlook

Lo scorso anno ha mostrato segnali positivi relativamente al **valore del mercato della cybersecurity in Italia** che ha raggiunto quota **1,55 Mld di euro**, con un aumento della spesa pari al +13% rispetto al 2020. Due anni fa, la pandemia da Covid-19 ha costretto la maggior parte delle aziende ad una rivisitazione delle priorità, spesso tradotta in un arresto degli investimenti in sicurezza informatica. Se nel 2020 infatti la crescita del mercato si era cristallizzata al 4% con un aumento degli investimenti pari al 40%, il 2021 si caratterizza con un trend positivo che vede una crescita dei fondi stanziati per le attività di cybersecurity pari al 61%.

1,55 mld
+13%

Senza dubbio, la trasformazione digitale, accelerata anche dal contesto pandemico, ha contribuito alla **definizione di nuovi trend e tecnologie** che determinano un mutamento delle priorità legate alla sicurezza informatica. Le aziende devono necessariamente rivisitare i propri processi di business in funzione delle implicazioni sulla sicurezza che emergono da nuove soluzioni e approcci tecnologici.

Le principali tendenze emerse nel corso del 2020 possono essere definite come il frutto dei radicali cambiamenti che la pandemia ha causato: lo scorso anno, infatti, **migrazione su Cloud** e **Smart/Remote Working** occupavano i primi posti tra le necessità più urgenti per la maggior parte delle aziende italiane. Entrambi i trend si riconfermano per il secondo anno consecutivo come aventi impatto rilevante e sono tra di loro interconnessi. Il lavoro da remoto e l'alternanza casa-ufficio continuano, e continueranno, a rappresentare una modalità imprescindibile per molti lavoratori, rendendo di fatto necessario implementare soluzioni a tutela del perimetro aziendale e applicazioni e infrastrutture in ambienti Cloud che da un lato garantiscano l'accesso di dati da remoto e dall'altro assicurino un backup.

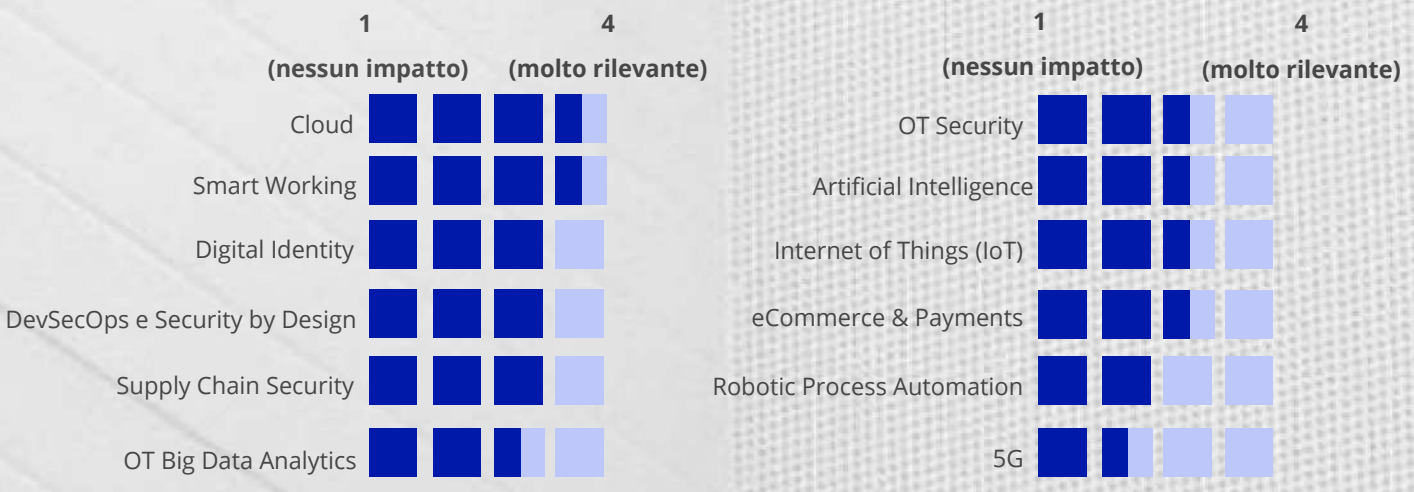


Figura 16 - L'impatto dei trend del digitale sulla cybersecurity - Fonte: Osservatori Digital innovation - Politecnico di Milano

New entry nel podio delle priorità d'investimento per le aziende italiane è la **Digital Identity** che sperimenta un picco di attenzione a scapito di Artificial Intelligence, Internet of Things e Robotic Process Automation che scendono dal terzo posto al fondo della classifica. La necessità di rivisitare i modelli di gestione della sicurezza aziendale in funzione di un accesso sicuro a risorse e dati critici anche da remoto, rappresenta un impatto rilevante per quasi l'80% degli intervistati dall'Osservatorio del Politecnico di Milano. Il monitoraggio delle identità e degli accessi così come la gestione dei privilegi, rappresentano un'area di crescente criticità e, per questo motivo, le organizzazioni ricorrono sempre più spesso a sistemi di autenticazione multi-fattore o passwordless, avviandosi più che mai verso la strada della Digital Identity.

Si delineano inoltre come nuovi trend rispetto allo scorso anno, seppure con impatti diversi, anche l'**eCommerce & Payment** e il fenomeno del **5G**. Il primo aspetto viene identificato come una necessità da oltre un'azienda su tre, poiché sempre più comuni e gravi sono le implicazioni legate a eCommerce e sistemi di pagamento innovativi, anch'essi accelerati dagli effetti della pandemia. I rischi in questo ambito sono riconducibili alla possibilità sempre più elevata di subire truffe o data breach a seguito dei quali vengono rubate informazioni sensibili sui clienti, anche afferenti all'ambito finanziario.

Un segnale positivo è sicuramente rappresentato dalla rilevanza che viene attribuita alle pratiche di **DevSecOps e Security by Design** sulle quali le aziende mirano ad investire con l'obiettivo di includere i requisiti di sicurezza già nelle prime fase di progettazione. Lo sviluppo di nuove applicazioni e la maintenance di quelle esistenti dovrebbero includere l'integrazione automatizzata degli standard di sicurezza in ciascuna fase di software development, coadiuvato da un approccio di Security by Design che si basa su misure come il monitoraggio continuo, l'utilizzo di credenziali e l'aderenza a pratiche di programmazione migliori.

In linea con i trend del 2020, la **Supply Chain Security** si posiziona al quinto posto fra le tendenze riscontrate dalle organizzazioni nel 2021. La sempre più diffusa tendenza ad esternalizzare le attività relative alla gestione operativa dell'IT ha ampliato il bacino di terze parti autorizzate a connettersi alla rete dell'azienda e, di conseguenza, anche le possibilità di subire un attacco informatico. La necessità, trascurata per molto tempo, di mettere in sicurezza l'intero ciclo di acquisizione di servizi ed applicazioni IT è diventata ora una top priorità.

8. Prossimi passi

Nell'attività di definizione del budget ICT per i prossimi anni, le aziende dovranno considerare diversi aspetti tenendo a mente come obiettivo non solo quello di eliminare il rischio di subire un attacco informatico ma quello di **ridurre gli impatti in termini economici, operativi e reputazionali** che questo può causare. Il protrarsi delle modalità di lavoro ibride, lo sviluppo di infrastrutture e applicativi Cloud, l'implementazione di soluzioni che integrino la Digital Identity, il ricorso a tecniche di AI, IoT e RPA per approcciare le minacce in modo più tecnologico ed infine, la messa in sicurezza di tutta la catena di fornitura. Sono questi i top trend attorno ai quali devono ruotare gli investimenti in materia di sicurezza informatica.

Smart Working

Più nel dettaglio, anche quest'anno la suddivisione degli investimenti dedicati alla sicurezza informatica deve tener conto della tendenza allo Smart/Remote Working: le aziende continueranno a prediligere un'organizzazione del lavoro che contempli sia la presenza in ufficio che i turni da remoto. A tal proposito, è fondamentale **investire** in una strategia efficace che metta in **sicurezza tutti i processi aziendali** e il **lavoro dei singoli dipendenti**.

Migrazione su Cloud

Parallelamente, urge finanziare iniziative di **migrazione su Cloud** che prevedano l'**implementazione di sistemi di backup** per consentire alle aziende di salvare in rete i dati evitando così episodi, tra l'altro molto frequenti, di estorsione e ricatto a seguito di esfiltrazioni di dati da parte di malintenzionati. La dimostrazione dell'importanza di ciò arriva dalla Pubblica Amministrazione. L'aumento dei casi di data breach, soprattutto durante il periodo pandemico, ha infatti portato il Governo italiano ad avviare un'iniziativa per la creazione del Polo Strategico Nazionale (PSN), ovvero un Cloud per la Pubblica Amministrazione caratterizzato da livelli di sicurezza rinforzati. Il Polo sarà realizzato entro la fine del 2022 e, a partire dalla sua creazione, le Pubbliche Amministrazioni dovranno adottare soluzioni Cloud con l'obiettivo di completare la migrazione del 75% degli enti entro il 2025.

Digital Identity

Per garantire livelli di sicurezza elevati, le aziende dovranno inoltre **investire nel rafforzamento di autenticazione ed accessi**, implementando soluzioni volte a recepire l'utilizzo dell'Identità Digitale.

Artificial Intelligence, Internet of Things & Robotic Process Automation

Nei prossimi anni sarà inoltre necessario sviluppare un approccio "tecnologico" alla cosiddetta threat detection, ovvero la rilevazione automatica di minacce informatiche. Ciò sarà reso possibile soprattutto grazie ad **investimenti nell'Artificial Intelligence, l'Internet of Things e la Robotic Process Automation**. Tali iniziative torneranno poi utili anche nelle attività di monitoraggio e verifica degli standard di sicurezza di fornitori terzi, in un'ottica di **rafforzamento della Supply Chain Security**.

9. Focus settore Automotive

Il settore Automotive sta vivendo una profonda trasformazione, trainata soprattutto da esigenze di sostenibilità e nuove regolamentazioni nei termini di sicurezza ed emissioni. Negli ultimi 10 anni la maggior parte dei controlli elettromeccanici è stata sostituita da **controlli elettronici comandati da software** e centraline specializzate. Questa trasformazione ha avuto un impatto enorme sulla progettazione dei nuovi veicoli, rendendo sempre più sofisticate le architetture elettriche/elettroniche e aumentando gli scenari che possono inficiare il corretto comportamento delle funzionalità di una vettura.

Infatti, attraverso le reti di bordo connesse a Internet su cui viaggiano i segnali che sovrintendono alle funzioni di guida, **una vettura di ultima generazione può generare e condividere una quantità di dati enorme**, che possono essere utilizzati per gli scopi più diversi, sia commerciali che tecnici.

Questo ha portato i **veicoli** a diventare **bersagli di attacchi** sia tramite connessione remota (73%) sia tramite accesso fisico alla vettura (27%), generando la necessità di mantenere un continuo scambio di informazioni tra le varie industry. Infatti, l'**Automotive**, rispetto ad altri settori in cui sono presenti sistemi ICT, coinvolge un **numero considerevole di fornitori** impiegati per la realizzazione di componenti, centraline, sensori ed attuatori. Dunque, la nuova sfida del settore è rappresentata dall'**identificazione delle possibili minacce** che possono emergere e i relativi rischi analizzati e gestiti su tutta la filiera dello sviluppo prodotto, definendo una strategia di cybersecurity che copra l'intera filiera e permetta di attivare reazioni tempestive ed adeguate a qualsiasi tipo di attacco.

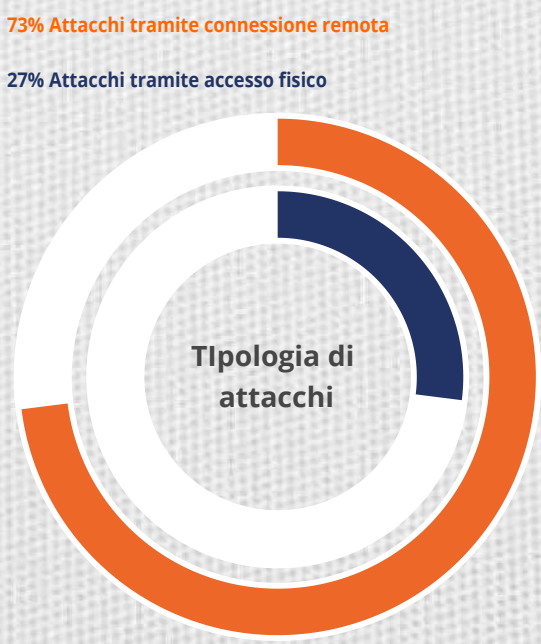


Figura 10- Attacchi nel settore automotive - Fonte: Rapporto Clusit 2022

10. Focus Cyberwar: Anonymous e gruppi hacker

Il 27 aprile 2007 in Estonia un attacco informatico causa il collasso del sistema bancario, dei media e di numerosi servizi governativi. Dietro quest'offensiva nascosta della Russia venne coniata per la prima volta la parola cyberwar.

La parola **cyberwar** può essere appunto definita come un **attacco o una serie di attacchi che prendono di mira diverse strutture di un paese o una nazione intera**. Possiede aspetti tecnico-operativi che a seconda del caso sono definiti sia offensivi (come intercettazione di dati, inabilitazione delle reti e degli equipaggiamenti informatici nemici, attacco ad infrastrutture critiche, ecc.), sia difensivi (come l'irrobustimento degli hardware, software e reti per aumentarne la resilienza) che ibridi.

cyberwar

Con il termine "guerra" si sottolinea quindi la finalità distruttiva. È importante non confondere tra guerra cibernetica e attacco informatico "fine a sé stesso": la guerra ha finalità più ampie e lo spazio cibernetico è utilizzato come strumento, medium, con l'obiettivo reale di causare più danni possibili alle infrastrutture nemiche.

Le principali tipologie di attacco utilizzate in una cyberwar sono suddivise in sette categorie:

Spionaggio - Monitoraggio e uso di botnet per estrapolare informazioni sensibili

Sabotaggio - Compromissione di organizzazioni o enti governativi

Attacchi DDoS - Interruzione di sistemi critici con blocco degli accessi a siti web

A Sorpresa - Attacco massiccio improvviso per indebolire le difese nel contesto di una guerra ibrida

Rete elettrica - Manomissione dei sistemi di approvvigionamento elettrico

Propaganda - Attacchi attraverso fake news o ai media nazionali

Economia - Compromissione dei computer di istituti economici e banche

Nei primi mesi del 2022 la Cybersecurity and Infrastructure Security Agency (CISA) ha monitorato un **aumento di attacchi informatici legati all'invasione dell'Ucraina** da parte della Russia: gli hacker russi e, per la controparte, i volontari chiamati alla «cyberesistenza» dal governo ucraino, insieme a gruppi internazionali di hacktivismo hanno frequentemente messo in atto forme di vandalismo digitale modificando indebitamente alcune pagine web (con attacchi detti, in gergo, di deface) o rendendo temporaneamente inaccessibili alcuni siti (denial-of-service o DoS).

Questi **attacchi** continuano ad essere la **parte invisibile della guerra**, dove pian piano sono andati a posizionarsi diversi schieramenti formati da attori di varia natura ed affiliazione: hacker bielorussi di regime e gruppi cybercriminali di matrice russa da un lato, hacker ucraini e patriottici, cyberpartigiani bielorussi anti-Lukashenko, pezzi di attivismo come **Anonymous** e GhostSec, dall'altro.

La resistenza ucraina ha più volte attaccato Sberbank, una delle maggiori banche russe che si stava ritirando dall'Europa a causa delle sanzioni, ma anche Glonass, il sistema satellitare globale di navigazione russo, le ferrovie bielorusse, le telco e i vari servizi di bancomat in Russia per danneggiare soprattutto le operazioni di ritiro dei risparmi in massa dagli istituti di credito e debito. Anonymous è riuscita ad esempio a "defacciare", ovvero violare il sito e modificarne la home, vari media russi come ad esempio TASS, Kommersant, E1, Fontanka inserendo un messaggio con il presunto numero di soldati russi morti in guerra.
Tuttavia, molti attacchi sono avvenuti anche in direzione contraria: Microsoft ha più volte segnalato una serie di malware indirizzati verso istituzioni e agenzie governative ucraine e alcuni media come il Kyv Post avrebbero subito pesanti attacchi.

L'escalation di questa guerra virtuale e senza confini fisici ha portato anche l'Italia ad essere vittima di alcuni pesanti attacchi informatici. Il sito del Senato, dell'Istituto Superiore della Sanità e dell'Automobile Club italiano hanno subito attacchi da un gruppo attivista russo noto come Killnet, un gruppo di volontari specializzati nei DDoS.

È sempre più importante valutare la prontezza di una nazione nella risposta alla cyberwar. L'**utilizzo di un cyberwar game** risulta uno degli strumenti più apprezzati per esporre le lacune, aumentando le difese e migliorando la cooperazione tra le varie entità. L'esercizio di simulazione può avvenire attraverso le seguenti modalità:

Test di diverse circostanze

Simulando il rilevamento degli attacchi o la mitigazione dei rischi dopo che l'infrastruttura critica è già stata compromessa

Meccanismi di cooperazione

Intensificando la collaborazione tra team e persone migliorando la risposta in caso di crisi

Test in scenari inusuali

Diversificando le squadre in una di attacco e una di difesa per allenare e testare la risposta ad attacchi originali e difficilmente frequenti

Sviluppo di politiche informatiche

Testando l'efficacia delle politiche di guerra cibernetica attraverso un wargame informatico

Sul territorio nazionale opera in prima linea lo CSIRT (Computer Security Incident Response Team), che risponde all'Agenzia per la Cybersicurezza Nazionale (ACN), tramite la pubblicazione di bollettini contenenti **raccomandazioni in merito alla prevenzione e al monitoraggio della sicurezza dei sistemi informatici.**

Nel contesto di un mondo sempre più connesso alla rete, una guerra di natura informatica assume un peso via via crescente, condizionando molto spesso le dinamiche di un conflitto anche senza dover necessariamente abbracciare le armi o sparare alcun missile.

11. Focus Finance

6.000 Mld

E' l'impressionante valore dell'ammontare delle perdite dovute agli attacchi informatici gravi inerenti al cyber risk, in **aumento del 24%** rispetto al 2020.

Tra i settori più colpiti dal rischio cyber va inserito quello finanziario: particolarmente rilevante, a questo proposito, è il fenomeno del **financial fraud** che, tramite il furto delle credenziali d'accesso ai sistemi bancari o di pagamento, porta a transazioni fraudolente all'insaputa del titolare. I vettori utilizzati per questo tipo di attacco sono:

FINANCIAL MALWARE
Furto di credenziali o manipolazione di una transazione

SIM SWAP
Hacking del dispositivo mobile tramite emulazione del software dello smartphone

CREDENTIAL THEFT
Phishing per il furto di credenziali di accesso e autenticazione forte. In questo panorama le parole chiave diventano pianificare, prevenire e proteggere

Gli impatti di questo fenomeno travolgono anche il **mercato assicurativo** che attualmente conta un numero abbastanza limitato di compagnie che coprono i rischi informatici a causa della carenza di informazioni dettagliate e complete in merito agli incidenti informatici.

Ciò comporta un aumento dei costi assicurativi delle polizze cyber che, secondo quanto riportato da ASSITECA, hanno subito un aumento del 20% per i rinnovi nel secondo semestre e fine anno 2021, limitando il bacino di aziende assicurate contro le frodi finanziarie.

+20%

Costi assicurativi delle polizze cyber nel 2021

Deepfake

Il fenomeno del financial fraud si propaga anche attraverso l'utilizzo dei cosiddetti **deepfake,** contenuti multimediali che sfruttano la capacità tecnologica dell'intelligenza artificiale di sintetizzare immagini e voci umane per creare contenuti falsi ma estremamente realistici.
La diffusione di alcune fake news, spesso senza alcuna fonte credibile a sostegno, fa capire come un deepfake ben fatto abbia la capacità di sembrare reale ed essere dunque molto pericoloso.

Gli obiettivi sono molteplici:

Mirati
Quando il contenuto è utilizzato per attaccare un **obiettivo specifico**: ad esempio, si pensi ad un cittadino che riceve un falso video personalizzato, accompagnato da una classica e-mail truffa in cui un conoscente dichiara di essere nei guai e di aver bisogno di soldi

Massivi
Consideriamo un'azienda il cui dirigente invii apparentemente un video o un audio in cui chiede ai suoi collaboratori di provvedere al pagamento urgente di una fattura, anche se l'importo è abbastanza ingente e del tutto inaspettato

La diffusione di massa di video fasulli (o audio, che possono riprodurre intercettazioni ambientali), sulle dichiarazioni di politici o importanti Top Manager, hanno un impatto potenzialmente enorme sull'**opinione pubblica**, alimentando la sfiducia nelle istituzioni e influenzando il mercato, col rischio di far crollare improvvisamente il valore di un titolo per eccesso di vendite a seguito di una notizia falsa. Basti pensare al caso di una nota catena di distribuzione di videogiochi, in cui gli utenti di un social network hanno condizionato sostanzialmente il valore del titolo, dimostrando l'efficacia e gli impatti di un'azione collettiva sul mercato azionario.

La realizzazione di un contenuto fake non è di per sé reato, a meno che l'obiettivo sia quello di commettere un'azione criminale. Chiaro è che le piattaforme dovranno necessariamente essere coinvolte: se da una parte la loro azione verterà sulla moderazione dei contenuti pubblicati, dall'altra sarà necessario educare gli utenti all'uso, comprensione e valutazione di ciò che si trovano di fronte. L'arma che abbiamo a disposizione è quindi la **conoscenza** e, non da meno, affidarsi a professionisti della gestione e valutazione del rischio.

12. Conclusioni

Dall'attuale analisi dello scenario, ci si aspetta che le tendenze delineate seguano il trend di crescita registrato durante quest'anno: l'esplosione delle **vulnerabilità che sfruttano i fornitori di terze parti**, la crescita delle **criticità zero-day** come vettore d'attacco e la capacità degli hackers di riadattarsi e proliferare con nuove minacce **ransomware**, rendono la sicurezza informatica un must have per tutte le aziende a prescindere dal mercato in cui operano.

Per le organizzazioni è sempre più importante **considerare investimenti in ottica di cybersicurezza**, come risulta evidente dall'aumento deciso della spesa in sicurezza informatica registrata nel 2021 in quasi tutti gli ambiti di mercato. Una spesa necessaria, considerando le crescenti tensioni geopolitiche che hanno caratterizzato i primi mesi del 2022. I recenti contrasti tra Russia e Ucraina hanno dimostrato come la **guerra moderna si combatta anche su un nuovo campo di battaglia, internet**, mietendo vittime non solo tra enti governativi e militari ma anche nel settore privato.

Data quindi la frequenza, la gravità, i rischi e l'imprevedibilità dei contesti che stimolano la diffusione di nuove tipologie di cyber attacks, è fondamentale investire non solo nell'adeguamento tecnologico, ma anche e soprattutto nella **Resilienza Operativa**, che deve essere vista come una combinazione di strategie diverse. Da un lato, un piano di Business Continuity deve garantire il ripristino della funzionalità dei sistemi di un'organizzazione; dall'altro, le misure di cybersecurity devono riuscire a proteggere i sistemi aziendali che, attraverso apposite strategie di Disaster Recovery, saranno in grado di rispondere efficacemente agli attacchi.

All'interno di questo contesto Planetica, grazie alla profonda esperienza settoriale maturata, si posiziona come il partner ideale per indirizzare le scelte strategiche e operative delle aziende nell'ambito della cybersecurity.

13. Indice delle figure

14. Bibliografia e sitografia

Clusit, *Rapporto Clusit 2022 sulla sicurezza ICT in Italia*, 2022

Bulletproof, *Bulletproof Annual Cyber Security Industry Report*, 2022

ENISA, *Interoperable EU Risk Management Framework*, 2022

Osservatorio Cybersecurity e Data Protection, *Il panorama di riferimento per la Cybersecurity e lo scenario di mercato*, 2022

Allianz, *Allianz Risk Barometer 2022*, 2022

Azienda Banca, *L'Open Banking non è (ancora) come immaginavamo*, n°270 2022

SOPHOS, *Interrelated threats target an interdependent world*, 2022

World Economic Forum, *The Global Risks Report 2022*, 2022

TWT, *Gli atteggiamenti delle medie e grandi aziende italiane di fronte alle sfide del cambiamento tecnologico Cyber Security*, 2022

https://www.cybersecurity360.it/

https://www.pwc.com/it/it/services/consulting/digital-operational-resilience.html

https://www.cybersecurity360.it/cybersecurity-nazionale/lagenzia-cyber-prende-forma-approvati-i-primi-tre-regolamenti-attuativi-ma-e-solo-linizio/

https://www.wired.it

Contatti

Andrea Rivetti

Presidente & Partner

+39 335 651 6375

andrea.rivetti@planetica.it

Matteo M. Marzan

Amministratore Delegato & Partner

+39 348 930 3095

matteo.marzan@planetica.it

Team di lavoro

Samantha Franceschin

Consultant

Antonio Alfarano

Junior Consultant

Fabrizio Brioschi

Junior Consultant

Per maggiori informazioni:

Tel: +39 02 82785 740 E-mail: segreteria@planetica.it Indirizzo: Via Crocefisso 5, Milano