CASA & ASSOCIATI

La più recente frontiera della compliance: la cybersecurity e gli adempimenti per le PMI

Avv. Silvia Rosina e Avv. Davide Mazzucato

Introduzione

Normativa di riferimento

- Direttiva (UE) n. 2555/2022 (c.d. NIS2);
- D. lgs n. 138/2024 (recepimento della NIS2);
- Regolamento (UE) n. 679/2016 (General Data Protection Regulation – c.d. GDPR);
- D.lgs. 101/2018 (adeguamento, della normativa italiana, a quanto previsto dal GDPR).

1) Direttiva (UE) n. 2555/2022 (c.d. NIS2)

La Direttiva NIS2 disciplina la sicurezza delle reti e dei sistemi informatici in tutta l'Unione Europea, rafforzando la resilienza cibernetica di settori pubblici e privati considerati critici. In particolare:

- estende l'ambito di applicazione a più settori e aziende, imponendo l'adozione di misure di sicurezza adeguate per prevenire, rilevare e rispondere agli incidenti informatici;
- prevede obblighi di notifica degli incidenti significativi entro tempistiche precise (24-72 ore);
- impone responsabilità diretta al top management e stabilisce sanzioni severe in caso di inadempienza;
- rafforza il ruolo delle autorità nazionali e promuove la cooperazione tra Stati membri.

L'obiettivo è garantire un livello comune elevato di cybersicurezza a livello europeo.

2) D. lgs n. 138/2024 (recepimento della NIS2)

Il D. Lgs. 138/2024 disciplina l'attuazione in Italia della Direttiva (UE) 2022/2555 (NIS2) e stabilisce le misure per garantire un livello elevato di cybersicurezza su tutto il territorio nazionale.

In particolare:

- estende gli obblighi di sicurezza a un ampio numero di soggetti pubblici e privati operanti in settori critici e importanti, tra cui: energia; sanità; trasporti; finanza; acqua potabile; acque reflue; infrastrutture digitali; gestione dei servizi TIC; spazio; pubblica amministrazione; servizi postali e di corriere; gestione dei rifiuti; fabbricazione, produzione e distribuzione di sostanze chimiche; produzione, trasformazione e distribuzione di alimenti; fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro; fabbricazione di computer e di prodotti di elettronica; fabbricazione di apparecchiature elettriche; fabbricazione di macchinari e attrezzature n.c.a.; fabbricazione di autoveicoli, rimorchi e semirimorchi; fornitori di servizi digitali; ricerca;
- impone alle aziende l'adozione di misure tecniche e organizzative adeguate per la gestione dei rischi informatici;
- introduce obblighi di notifica degli incidenti significativi entro 24 ore, con aggiornamenti successivi;
- rafforza il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) come autorità competente per il coordinamento e la vigilanza;
- definisce sanzioni pecuniarie e responsabilità dirette per i vertici aziendali in caso di violazioni;
- mira a creare un sistema armonizzato e integrato con gli altri Stati membri dell'UE per la protezione delle infrastrutture digitali e dei servizi essenziali.

In sostanza, il decreto disciplina chi è obbligato, cosa deve fare per proteggere i propri sistemi informatici, e cosa rischia se non lo fa, nell'ambito della strategia nazionale di cybersicurezza.

3) Regolamento (UE) n. 679/2016 (General Data Protection Regulation – c.d. GDPR)

Il Regolamento (UE) n. 679/2016, noto come GDPR (General Data Protection Regulation), disciplina la protezione dei dati personali delle persone fisiche nell'Unione Europea e la libera circolazione di tali dati. È entrato in vigore il 25 maggio 2018 e ha uniformato la normativa sulla privacy in tutti i Paesi UE.

In sintesi, il GDPR:

- stabilisce i principi fondamentali per il trattamento dei dati personali (liceità, correttezza, trasparenza, minimizzazione, integrità, ecc.);
- definisce i diritti degli interessati, come accesso, rettifica, cancellazione (diritto all'oblio), portabilità e opposizione;
- impone obblighi precisi ai titolari e responsabili del trattamento, inclusa la tenuta di un registro e la valutazione d'impatto (DPIA);
- richiede, in alcuni casi, la nomina del Responsabile della Protezione dei Dati (DPO);
- introduce l'obbligo di notifica delle violazioni dei dati (*data breach*) entro 72 ore;
- prevede sanzioni molto elevate (fino a 20 milioni di euro o il 4% del fatturato annuo globale).

L'obiettivo del GDPR è garantire che i dati personali siano trattati in modo sicuro, lecito e trasparente, rafforzando la fiducia dei cittadini europei nel digitale.

4) D. lgs. 101/2018 (adeguamento, della normativa italiana, a quanto previsto dal GDPR)

Il D. Lgs. 101/2018 disciplina l'adeguamento dell'ordinamento italiano al Regolamento (UE) 2016/679 (GDPR). In altre parole, serve a integrare e armonizzare la normativa nazionale in materia di protezione dei dati personali con quanto previsto dal GDPR. In particolare:

- modifica il Codice della Privacy (D .Lgs. 196/2003), mantenendone alcune parti compatibili con il GDPR e abrogandone altre;
- definisce i compiti del Garante per la protezione dei dati personali come autorità nazionale indipendente;
- stabilisce regole specifiche per il trattamento di dati in ambiti particolari, come: rapporti di lavoro, sanità, ricerca scientifica, giornalismo e libertà di espressione;
- prevede agevolazioni per PMI e microimprese, e introduce meccanismi di semplificazione;
- definisce il regime sanzionatorio nazionale in coerenza con quello europeo;

In sostanza, il D. Lgs. 101/2018 è il ponte tra il GDPR europeo e la normativa italiana, rendendo pienamente operativa la protezione dei dati personali in Italia secondo le nuove regole europee.

Il *data breach* e l'incidente informatico

Il c.d. *data breach (*art. 4 comma 12 del GDPR)

L'art. 4, comma 12, del "GDPR" definisce la violazione dei dati personali (o data breach) come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

Il *data breach può rappresentare* un incidente di sicurezza.

Di seguito alcuni esempi di *data breach* maggiormente ricorrenti:

- la perdita o furto di documenti contenenti dati personali o di dispositivi (es. dispositivi mobili, computer, tablet, ecc.) della società o personali contenenti dati personali;
- accesso non autorizzato dall'interno o dall'esterno della rete della società (es. hacking) od ogni altra violazione dei sistemi IT che potrebbe determinare la perdita, la compromissione, l'accesso o la divulgazione delle informazioni della società;
- installazione di software malevolo o virus scaricato sui dispositivi forniti dalla società;
- informazioni cartacee o elettroniche della società inviate al di fuori dell'azienda che non giungano al destinatario voluto o che siano recapitate a un destinatario non voluto;
- violazione dei controlli obbligatori di sicurezza delle informazioni che potrebbe comportare la perdita o la compromissione delle informazioni della società;
- diffusione non sicura delle informazioni della Società che sono state classificate come interne, confidenziali o segrete.

Il c.d. *data breach (*art. 4 comma 12 del GDPR) - continua

OBIETTIVO → eliminare o comunque ridurre al massimo tutte le conseguenze dell'incidente, non solo in tema privacy --> Know How, analisi statistiche, campagne di marketing, pianificazioni, progetti, brevetti ecccc..

- I danni economici e di immagine **potrebbero essere incalcolabili** mettendo a serio rischio la stessa tenuta e continuità aziendale;
- In tutte le ipotesi di *data breach*, dunque, determinate sarà gestire tutte le potenziali conseguenze, a 360°:
  - tutela dell'immagine e della reputazione (fisica e online);
  - gestione dei canali social, motori di ricerca, media e delle comunicazioni all'esterno;
  - gestione dei rapporti con i fornitori e stakeholder;
  - responsabilità nei confronti dei soggetti cui le informazioni si riferiscono;
  - comunicazione delle notizie di reato alle pubbliche autorità e gestione del relativo procedimento;
  - gestione di tutte le potenziali richieste di risarcimento del danno.
- L'attività e l'assistenza di legali e professionisti specializzati è, dunque, determinante.

«Gestione» del *data breach*

- Costituzione di una *task force* di esperti (legali, tecnici, informatici etc);
- gestione protocollo *data breach*;
- notifica/comunicazione al garante privacy/interessati **entro 72 h;**
- **verifica e analisi del *data breach:***
    1) è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche → **non occorre la notifica al Garante e la comunicazione agli interessati;**
    2) è probabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche MA LA VIOLAZIONE NON comporta un rischio elevato per i diritti delle persone → **è necessaria la notifica al Garante ma non agli interessati;**
    3) la violazione comporta un rischio elevato per i diritti delle persone → **è necessaria la notifica al Garante e la comunicazione agli interessati.**
- interlocuzione e collaborazione con il Garante per la Protezione dei Dati Personali;
- annotazione dell'incidente nel registro dei *data breach*.

Sanzioni in caso di *data breach (*ma non solo…)

L'art. 83 GDPR distingue due gruppi di sanzioni amministrative particolarmente importanti:

- nel primo gruppo rientrano le **violazioni ritenute di minore gravità**, per le quali sono comunque previste sanzioni pecuniarie di importo **fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore;
- per le **violazioni di maggiore gravità** sono previste sanzioni pecuniarie **fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

Tuttavia, il secondo comma dell'art. 83 individua tutta una serie di parametri a cui il Garante dovrà fare riferimento nel momento di determinare la sanzione e adeguarla al caso specifico.

Tra le altre, spicca quanto previsto alla lettera c) che richiede di valutare

- "***le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati***";

nonché la lettera f) che richiede di valutare

- "***il grado di cooperazione con l'Autorità di Controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi***".

Gli incidenti in materia di sicurezza informatica ai sensi del d.lgs. 138/2024

Ai sensi del d.lgs. 138/2024 (art. 2 comma 1 lett. t), **l'incidente** è un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi.

***

La normativa in materia di *cybersicurezza* disciplina anche i **«quasi – incidenti»** (c.d. *near miss*), ossia gli eventi che avrebbero potuto configurare un incidente senza che questi ultimi si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato.

Gestione degli incidenti in materia di sicurezza informatica ex d.lgs. 138/2024

Al netto dell'adozione di misure tecniche, operative e organizzative, adeguate per gestire i rischi legati alla sicurezza dei loro sistemi informativi e di rete, in caso di incidente significativo (1), è obbligatoria una notifica tempestiva all'Agenzia per la Cybersicurezza Nazionale (ACN). La procedura prevede una prima comunicazione entro 24 ore dall'accertamento dell'incidente, seguita, entro le 72 ore successive, da una notifica dell'incidente che, ove possibile, aggiorni le informazioni della prima comunicazione e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione.

***

(1) Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Sanzioni previste dal d. lgs 138/2024

Gli organi di amministrazione e direttivi sono responsabili dell'approvazione e del monitoraggio delle misure adottate, nonché della formazione in materia di sicurezza informatica. La mancata osservanza di questi obblighi può comportare sanzioni amministrative pecuniarie significative, **fino a 10 milioni di euro o il 2% del fatturato annuo mondiale per i soggetti essenziali, e fino a 7 milioni di euro o l'1,4% del fatturato per i soggetti importanti**.

Perché è importante adeguarsi a quanto previsto dalle normative in materia di privacy ed in materia di cybersicurezza?

- Oggigiorno **tutte le imprese si avvalgono di strumenti elettronici e informatici, e ciò ai fini di utilizzare e conservare i dati di cui sono in possesso per esercitare la propria attività;**
- per **qualsiasi impresa** dotata di strutture informatiche e un accesso ad internet **la cyber security è, oggi, una priorità imprescindibile;**
- di conseguenza, **implementare precise politiche di cyber security**, che proteggano i dati e le informazioni da intrusioni esterne, **rappresenta una fondamentale misura di sicurezza** di cui tutte le imprese devono dotarsi.

- La progressiva ed inesorabile digitalizzazione del quotidiano, ha portato le imprese a disporre e gestire una mole rilevante di dati che possono concernere svariate attività (marketing, pubblicità, gestione del magazzino, *know how*, brand, reputazione online, produzione etc.). **Questa mole di dati ha un valore economico in molti casi assai rilevante;**
- l'impresa, dunque, ha una precisa responsabilità in primo luogo **nei confronti di sé stessa**, ma anche **nei confronti degli interessati**, a cui i dati e le informazioni si riferiscono, oltre che **nei confronti del mercato;**
- senza contare che, al di là delle questioni squisitamente concernenti il GDPR, in molti casi l'impresa conserva dei dati (disegni, modelli etc.) che appartengono a terzi ed a cui bisogna porre ancora più particolare attenzione (si pensi al terzista che conserva disegni e progetti del committente ai fini di produzione).

Che conseguenze potrebbe subire l'impresa in caso di mancato adeguamento?

- Danno reputazionale sul mercato;
- interruzione del business (addirittura fino a «pagamento del riscatto»;
- sottrazione di informazioni critiche e riservate (i.e. segreti commerciali), con pericolo di diffusione delle stesse;
- rischio di contenzioso con clienti/fornitori;
- rischio di vedersi sottoposti ad attività di accertamento istituzionale (da parte di ACN/Garante per la protezione dei dati personali), con possibile applicazione di sanzioni.

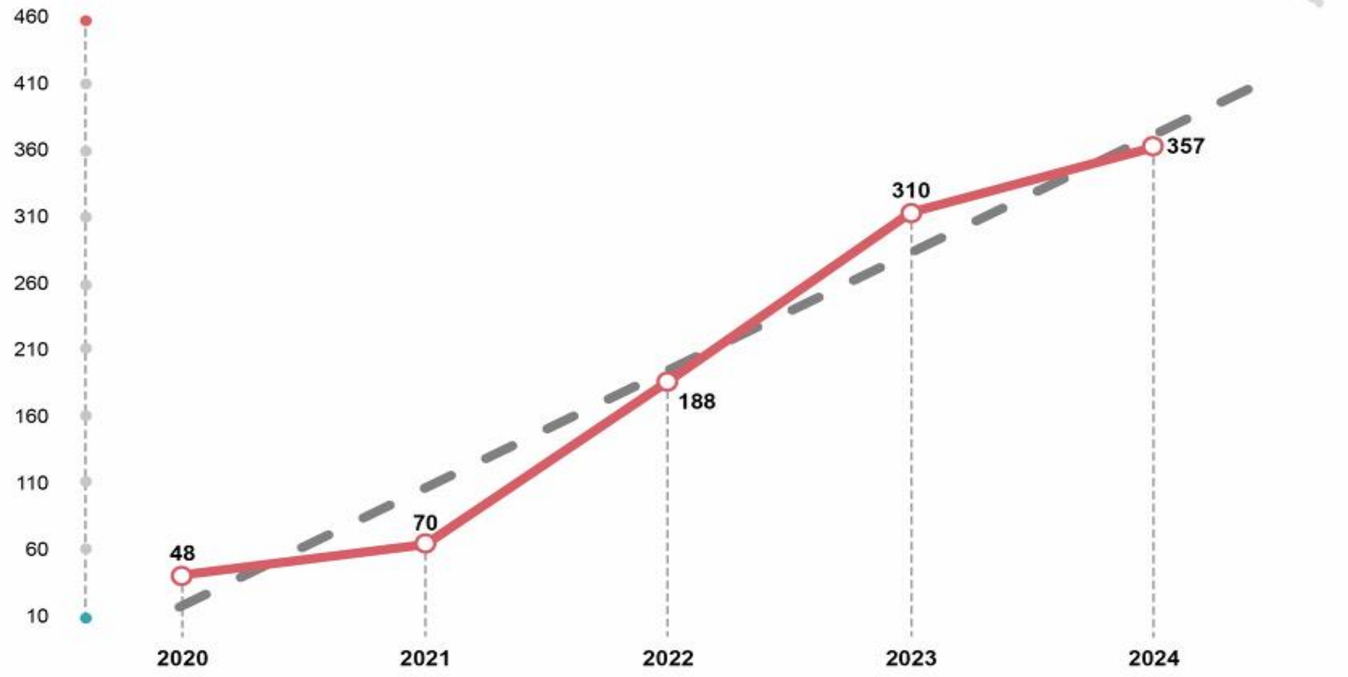
Tutto ciò comporta, in sintesi, il rischio di subire notevoli pregiudizi sia dal punto di vista patrimoniale sia dal punto di vista reputazionale.

Un po’ di dati…..

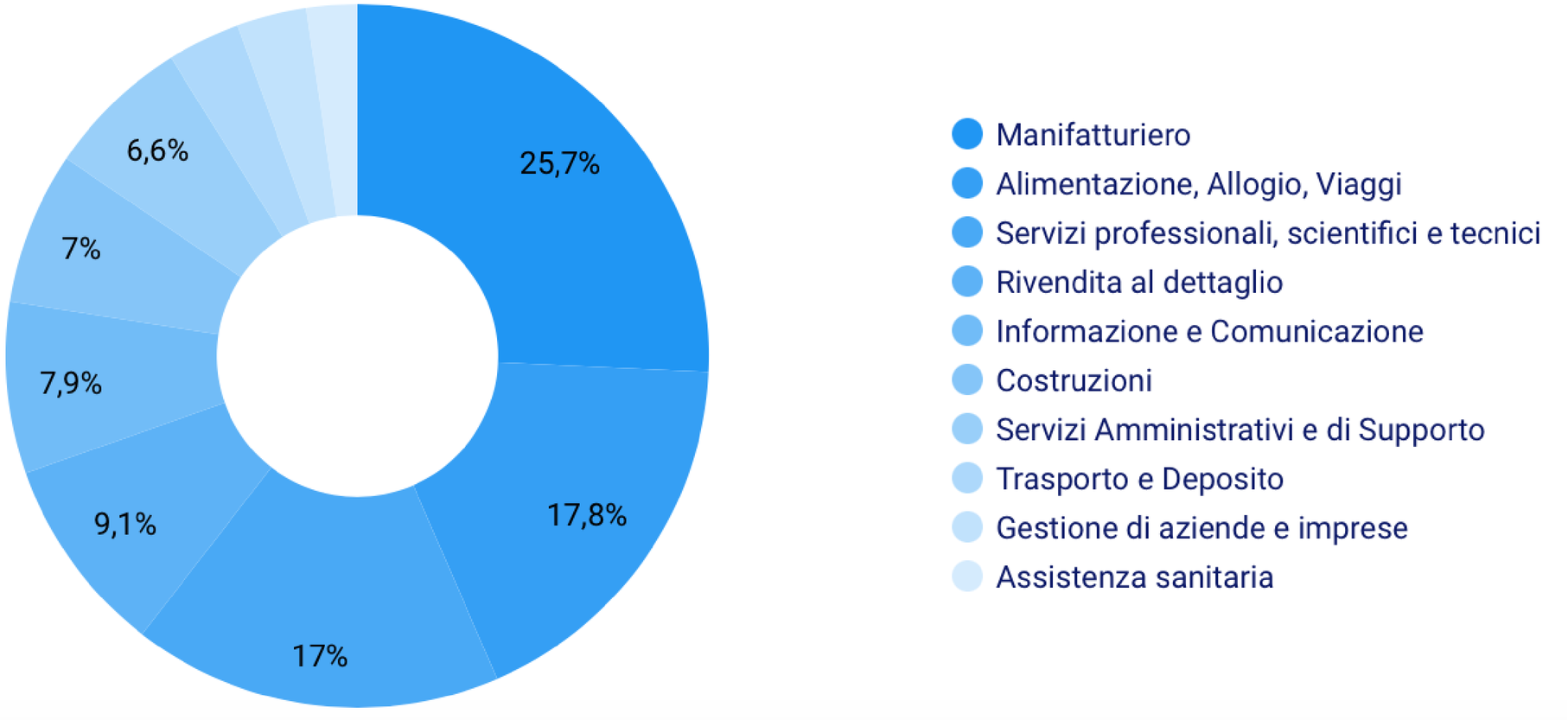
Incidenti Cyber in Italia 2020 -2024

+15%
è la crescita degli incidenti subiti in Italia nel 2024 rispetto al 2023

39%
è la percentuale degli incidenti subiti in Italia nel 2024 rispetto al totale dal 2020



© Clusit - Rapporto 2025 sulla Cybersecurity

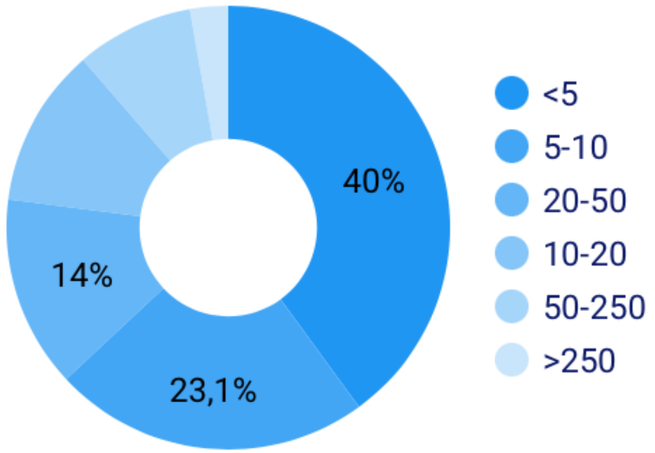


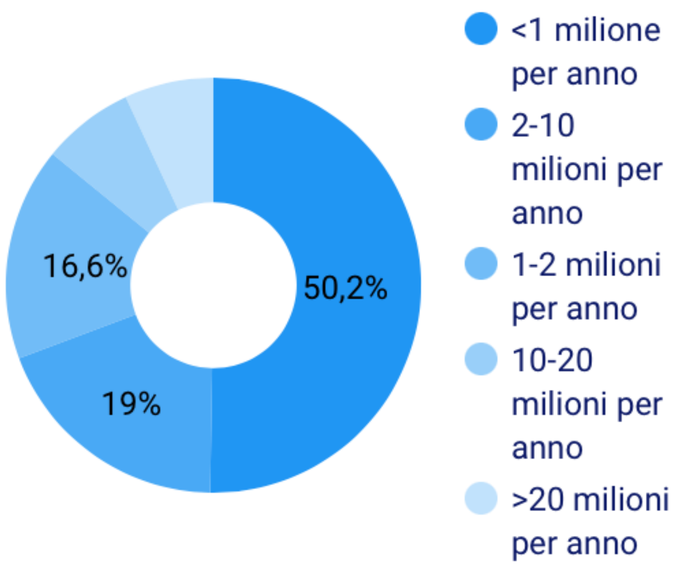
Fonte: Rapporto Clusit sulla cybersicurezza in Italia e nel mondo 2025

Tipologie di attacchi

Fonte: Rapporto Clusit sulla cybersicurezza in Italia e nel mondo 2025

Distribuzione attacchi informatici per numero di dipendenti e fatturato





Fonte: Rapporto Clusit sulla cybersicurezza in Italia e nel mondo 2025

Che cosa possono/devono fare le imprese per proteggersi e tutelarsi?

Premessa: il principio di responsabilizzazione (accountability) e l'approccio basato sul rischio

- Tutto quanto sopra considerato quindi, possiamo concludere che la **cybersecurity costituisce uno dei principali rischi d'impresa** che dev'essere governato per evitare di essere esposti a responsabilità e danni collaterali;
- il **principio di accountability (responsabilizzazione)** è entrato ufficialmente a far parte del vocabolario giuridico italiano con l'entrata in vigore del GDPR, che per la prima volta ne ha disciplinato a livello normativo definizione, portata e applicabilità;
- **il legislatore**, percorrendo un solco già segnato in tema di *compliance,* **non indica più**, nel dettaglio, **ciò che l'imprenditore è tenuto ad adottare** per adeguare la propria attività d'impresa alle normative di settore, ma si limita ad indicare **solo l'obiettivo da raggiungere**, **ovvero ridurre al minimo il rischio nello specifico settore di riferimento ai fini di conformarsi alla legge**. La scelta, su quali accorgimenti e misure adottare, spetta quindi all'imprenditore;
- l'**approccio basato sulla *risk analysis***: al fine di individuare, documentare ed implementare quelle che si ritengono essere le migliori misure di sicurezza per evitare i rischi cyber, in ottica accountability, sarà preliminarmente necessario effettuare una precisa mappatura dell'esistente e una specifica analisi dei rischi. Solo dopo, sulla base dei risultati, individuare le misure di sicurezza.

Analisi del rischio e prevenzione dell'incidente informatico
*
l'importanza dell'adozione di adeguati modelli organizzativi nonché di adeguate coperture assicurative

- In ottica di *accountability* nonché di prevenzione del rischio **diventa fondamentale l'adozione di modelli organizzativi basati sull'analisi dei rischi e sull'implementazione di protocolli volti a ridurne al minimo la portata**;
- tutte le normative di settore sono volte alla prevenzione del rischio, **e solo in via residuale** mera gestione della violazione;
- al netto dei regolamenti/policy/procedure che la società ha adottato al fine di adeguarsi a quanto previsto dalla normativa in materia di privacy, si segnala la «necessità» per le imprese di valutare l'implementazione di un modello di organizzazione, gestione e controllo ai sensi e per gli effetti del d.lgs. 231/2001;
- l'adozione di una polizza assicurativa «cyber risk» non è importante solo per evitare di doversi far carico di eventuali sanzioni in caso di violazione dei sistemi informatici o furto dei dati. Una copertura assicurativa che tenga conto del profilo di rischio della propria attività aiuta anche a contenere i danni reputazionali e di immagine, a coprire i danni materiali che potrebbero perfino compromettere la stabilità finanziaria dell'impresa nonché ad evitare blocchi alla produzione in caso di attacco esteso ai sistemi informatici.

Analisi del rischio e prevenzione dell'incidente informatico
*
Misure tecniche ed organizzative

In ossequio al principio dell'accountability, della privacy by design, della privacy by default nonché di quelli principi relativi alla normativa in materia di sicurezza, l'impresa deve mettere in atto adeguate misure tecniche ed organizzative.

Tali misure devono essere adottate tenuto conto dei seguenti aspetti:

- il rischio: dev'essere valutata la probabilità e la gravità delle violazioni;
- i costi di attuazione delle misure;
- lo stato attuale della tecnica e dell'arte;
- i principi della cybersecurity e della privacy, tra cui confidenzialità, integrità e disponibilità dei dati;
- la natura, l'oggetto, il contesto e le finalità del trattamento dei dati.

Misure tecniche

Esempi di misure tecniche di sicurezza informatica includono

- l'installazione di sistemi di autorizzazione e segregazione accessi logici;
- l'adozione di credenziali di autenticazione volte a consentirne l'accesso unicamente a soggetti per i quali è possibile una univoca identificazione;
- l'installazione di firewall, antivirus, antimalware o sistemi similari volti alla protezione di rischi di intrusione indebita ai sistemi informatici;
- la predisposizione di protocolli di comunicazioni sicuri;
- l'adozione di sistemi di logging;
- la predisposizione di misure di backup & restore, volte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici;
- la realizzazione di *vulnerability assessment* e di penetration test;
- crittografia dei dati sensibili.

Misure organizzative

Esempi di misure organizzative di sicurezza includono:

- l'adozione di **policy per gli utenti** volte a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati **nell'utilizzo delle risorse informatiche**;
- **policy per la gestione di richieste** relative all'esercizio dei diritti dagli interessati;
- di **una struttura organizzativa interna** in materia di privacy con definizione di ruoli e responsabilità dei soggetti che trattano dati personali all'interno dell'organizzazione;
- di un **sistema di controllo**, tanto dei trattamenti effettuati da terzi quanto di quelli effettuati all'interno della struttura aziendale;
- **procedura per la gestione dei *data breach* nonché di altri incidenti in materia di sicurezza**;
- sottoscrivere una **polizza assicurativa contro il cyber risk** (vedi *infra*);
- controlli fisici e digitali **dell'accesso ai dati**;
- politiche per la predisposizione delle **password**;
- autenticazione a **due fattori**;
- obblighi di riservatezza (da inserire anche in appositi non disclosure agreement) per il personale e per i terzi;
- scelta dell'ubicazione del server.

E la formazione….?

L’importanza della formazione

La formazione in materia di sicurezza informatica e privacy è una misura di carattere organizzativo ed è diventata un **pilastro fondamentale per la conformità normativa e per la protezione concreta di dati e sistemi**, soprattutto in ambito aziendale e istituzionale. Con l’entrata in vigore del D. Lgs. 138/2024 (attuativo della Direttiva NIS 2) e la sempre attuale applicazione del GDPR (Reg. UE 2016/679), l’importanza di formare il personale non è solo una buona prassi, ma un obbligo normativo e strategico.

Obbligo legale

Il D. Lgs. 138/2024 richiede che i soggetti essenziali e importanti formino regolarmente il personale in materia di *cybersicurezza*. Questo è previsto come misura organizzativa per prevenire e gestire gli incidenti informatici. Il GDPR, all'art. 39, prevede, tra i compiti del DPO, anche quello di formare e sensibilizzare il personale sul trattamento dei dati personali e le relative misure di sicurezza.

Prima barriera difensiva

Le minacce informatiche (phishing, ransomware, social engineering...) puntano spesso sull'errore umano. Un utente formato è meno vulnerabile e può riconoscere segnali di pericolo.

Allo stesso modo, conoscere i principi della privacy (come minimizzazione, riservatezza, diritti dell'interessato) aiuta a evitare trattamenti illeciti o comunicazioni improprie di dati.

Responsabilità aziendale, continuità operativa e fiducia

In caso di violazione o *data breach*, l'adozione di percorsi formativi può essere una prova di diligenza, utile a ridurre sanzioni o responsabilità. Inoltre, l'attività di formazione rafforza la cultura della sicurezza in azienda, responsabilizzando tutte le maestranze.

Una struttura con personale preparato riesce a rispondere più efficacemente agli incidenti, riducendo tempi di inattività, danni economici e reputazionali e, di conseguenza, aumentando la fiducia di clienti, partner e utenti.

Come, nel concreto, alcuni enti hanno gestito incidenti in materia di cybersicurezza?

Casi di insuccesso…..

1. **Violazione dei dati presso l'USL 6 Euganea di Padova (2021-2022)** - l'USL 6 Euganea ha subito due attacchi informatici che hanno portato al potenziale furto di circa 17.000 documenti contenenti dati sensibili. Il Garante ha imposto una sanzione di 22.000 euro, sottolineando l'importanza di rafforzare le misure di sicurezza per proteggere i dati personali;
2. **Attacco informatico alla Regione Lazio (2021)**: Un grave attacco ransomware ha colpito la Regione Lazio, bloccando i sistemi informatici e compromettendo dati sensibili. Il Garante ha sanzionato LAZIOcrea con una multa di 271.000 euro e la Regione Lazio con 120.000 euro, evidenziando carenze nelle misure di sicurezza adottate.
3. **Attacco *ramsonware* alla società Alf Uno S.p.A. (società trevigiana che opera nel settore del mobile con il marchio Alf DaFrè)** (febbraio 2025): l'attacco ransomware avvenuto nella notte tra lunedì 10 e martedì 11 febbraio, ha compromesso i sistemi informatici, bloccando logistica, comunicazioni e produzione. La conseguenza immediata è stata la sospensione del lavoro per i 350 dipendenti, costretti alla cassa integrazione temporanea.

.....e casi di successo

1. **Fashion Box S.p.A. (febbraio 2025):** il caso si riferisce alla sottrazione di dati sensibili che riguardavano non solo i propri sistemi interni, ma anche le informazioni di dipendenti, clienti e partner commerciali. Attraverso una tecnica di "brute force", un metodo che consiste nel tentativo sistematico di indovinare password o credenziali attraverso l'inserimento di un grande numero di combinazioni automatiche; in seguito la violazione veniva comunicata al Garante Privacy. Diverse misure adottate: rafforzamento dei sistemi di protezione informatica, l'aggiornamento delle infrastrutture IT e un maggiore investimento nella formazione del personale, protocolli di sicurezza più rigorosi per la protezione dei dati,

2. **Luxottica Group S.p.A. (settembre 2024)**: in tal caso, vi è stata la sospensione del secondo turno produttivo negli stabilimenti di Agordo e Sedico, nel bellunese, e il blocco delle attività produttive in Cina. La chiusura preventiva degli apparati informatici e la corretta configurazione dei sistemi di difesa dell'azienda pare abbiano consentito di respingere l'attacco degli hacker impedendo l'accesso e la conseguente sottrazione di dati e informazioni riservati su utenti, consumatori e proprietà intellettuali dell'azienda. Come accedono: sfruttano vulnerabilità (sevizi di accesso remoto configurati male e accessibili dall'esterno, problemi sui server) o tramite social engineering.

3. **Bonfiglioli S.p.A. (motori, riduttori e motoriduttori) (giugno 2019)**: in quest'ultimo caso, vi è stata, da parte degli hacker, la disattivazione di alcuni sistemi di controllo aziendale e a cifrare una gran quantità di dati archiviati sui server. In cambio, gli hacker hanno chiesto un riscatto di 340 Bitcoin (equivalenti a circa 2,4 milioni). La società ha scelto di non assecondare le richieste dei criminali in quanto era preparata all'evenienza, invero è stata in grado di bloccare l'attacco "grazie ad immediate azioni di bonifica" e all'immediata disconnessione da Internet dei server principali.

«I dati sono una cosa preziosa e dureranno più a lungo dei sistemi stessi – Tim Berners Lee»

Grazie per l’attenzione