Tech*Trend*

8
Ai
Artificial
Intelligence

Cybersecurity
e Studi professionali:
proteggere i dati per garantire la fiducia

TeamSystem

TechTrend

Con questo documento vogliamo fornire a Commercialisti, Consulenti del Lavoro e Avvocati una panoramica sulle soluzioni e strategie di Cybersecurity per proteggere i dati del proprio Studio e quelli dei propri clienti.

Attraverso esempi pratici e case study, inoltre, approfondiremo il ruolo dell'Intelligenza Artificiale nella prevenzione delle minacce cyber, con l'obiettivo di incentivare una cultura della sicurezza informatica tra i Professionisti.

Indice

Cybersecurity e Studi professionali: proteggere i dati per garantire la fiducia

Oggi ogni Professionista si trova a gestire una quantità di dati senza precedenti: **Commercialisti, Consulenti del Lavoro** e **Studi professionali** trattano quotidianamente informazioni sensibili riguardanti clienti, dipendenti, fornitori e transazioni economiche.

Non c'è dubbio che il digitale abbia semplificato e ottimizzato la gestione di queste informazioni, permettendo ai Professionisti di accedere ai dati in qualsiasi momento e rivoluzionando di fatto il modo in cui gli Studi professionali operano. Tuttavia, a fronte di questi vantaggi, cresce anche la responsabilità di proteggere dati e informazioni, inevitabilmente più vulnerabili alla minaccia dei criminali informatici.

Le **minacce informatiche**, infatti, non sono più un problema che riguarda solo le grandi aziende. Se le multinazionali possono contare su interi reparti IT dedicati alla sicurezza, non tutti gli Studi professionali valutano adeguatamente i rischi legati alla Cybersecurity. Le conseguenze di una violazione, però, possono rivelarsi molto importanti: perdita di dati, danni economici, sanzioni legali e, soprattutto, un **colpo irreparabile alla reputazione**. Secondo il Rapporto Clusit 2025, infatti, nel corso degli ultimi cinque anni gli incidenti di sicurezza registrati hanno subito un notevole aumento, evidenziando una tendenza chiara e costante: la media mensile a livello globale è difatti passata da 156 casi nel 2020 a 295 nel 2024. Oltre a registrare un incremento costante nella frequenza degli incidenti, si è osservato un peggioramento anche sul piano delle loro conseguenze. Nel quinquennio analizzato, l'indice medio di gravità (Severity) degli eventi rilevati è cresciuto di anno in anno, amplificando ulteriormente i danni complessivi. Come già accaduto nel 2023, anche nel 2024 circa l'**80% degli incidenti è stato classificato come "grave" o "critico"** (rispetto al 50% del 2020). Tuttavia, nel 2024 si è ridotta la quota degli attacchi "critical", mentre è aumentata quella degli attacchi con severity "high", soprattutto a causa della diminuzione media degli impatti legati ad azioni a scopo cybercriminale.

Cybersecurity e Studi professionali

Non proteggere adeguatamente le informazioni dei clienti può avere risvolti legali molto seri, specialmente se si considera l'esistenza di normative, come il **GDPR, il DORA e la NIS2**, che impongono standard elevati di sicurezza e responsabilizzano direttamente i Professionisti nel caso di una **compromissione dei dati**. Inoltre, gli attacchi informatici sono diventati sempre più sofisticati, con tecniche avanzate che sfruttano anche l'Intelligenza Artificiale per individuare vulnerabilità e penetrare nei sistemi con un'efficacia mai vista prima. Di fronte a questo scenario in continua evoluzione, ignorare il tema della Cybersecurity non è più un'opzione. Il primo passo per evitare rischi potenzialmente disastrosi è acquisire consapevolezza: informarsi, **conoscere le minacce più comuni** e individuare le soluzioni giuste per la propria realtà professionale. D'altro canto, la stessa AI può essere utilizzata per proteggersi: strumenti basati su Intelligenza Artificiale, infatti, possono **monitorare i sistemi in tempo reale, rilevare anomalie, prevenire attacchi** prima ancora che si manifestino e automatizzare le risposte alle minacce.

Questo documento nasce quindi con l'obiettivo di fornire ai Professionisti una guida chiara e concreta per costruire una strategia di sicurezza efficace. Una strategia che si basa su due pilastri fondamentali: le persone e la tecnologia. Da un lato, è fondamentale aumentare la consapevolezza e la formazione, affinché ogni Professionista e i suoi collaboratori sappiano riconoscere i rischi e adottare comportamenti corretti. Dall'altro, è indispensabile dotarsi delle giuste soluzioni tecnologiche per proteggere i dati e garantire la continuità operativa del proprio Studio.

Per saperne di più:

→ Proteggi la tua impresa con la guida completa di TeamSystem

→ Gestione dei dati personali e privacy: le nuove sfide dei Commercialisti nell'era del GDPR

Capitolo 1

Le minacce informatiche per Commercialisti e Consulenti del Lavoro: la situazione in Italia

Secondo il rapporto Clusit 2025, lo scorso anno in Italia si è registrato un aumento del 169% degli attacchi informatici. Un dato allarmante che evidenzia una tendenza chiara: le piccole realtà, incluse le attività professionali, stanno diventando un bersaglio sempre più frequente dei cybercriminali.

Il motivo è semplice: Studi professionali, Avvocati, Commercialisti e Consulenti del Lavoro spesso **non dispongono di adeguate misure di sicurezza**. Rispetto alle grandi aziende, infatti, è meno probabile che abbiano reparti IT strutturati o che investano in strategie di protezione avanzate. Ma non solo, i Professionisti sono particolarmente esposti anche a causa della **gestione di dati riservati,** tra cui informazioni finanziarie, progetti e proprietà intellettuale dei loro clienti. Queste vulnerabilità li rendono facili bersagli degli hacker, che puntano proprio su obiettivi del genere per massimizzare il successo dei loro attacchi.

Il motivo è semplice: Studi professionali, Avvocati, Commercialisti e Consulenti del Lavoro spesso **non dispongono di adeguate misure di sicurezza**. Rispetto alle grandi aziende, infatti, è meno probabile che abbiano reparti IT strutturati o che investano in strategie di protezione avanzate. Ma non solo, i Professionisti sono particolarmente esposti anche a causa della **gestione di dati riservati,** tra cui informazioni finanziarie, progetti e proprietà intellettuale dei loro clienti. Queste vulnerabilità li rendono facili bersagli degli hacker, che puntano proprio su obiettivi del genere per massimizzare il successo dei loro attacchi.

La prima forma di difesa, quindi, è la **consapevolezza:** esistono molteplici tipologie di attacchi, ma spesso le più efficaci sono quelle che sfruttano l'inganno e la scarsa conoscenza delle minacce. Tecniche come il **phishing** – e-mail apparentemente legittime che spingono il destinatario a rivelare dati sensibili – o il **social engineering** – che manipola psicologicamente le vittime per ottenere accesso ai sistemi – sono tra le più diffuse. Basta un clic su un link malevolo o l'inserimento di credenziali in un sito fraudolento per compromettere la sicurezza di un intero Studio professionale. È proprio questo il motivo per cui conoscere queste minacce rappresenta il primo, vero passo per evitarle.

Per iniziare ad avere maggiore consapevolezza è bene conoscere nel dettaglio quali sono le forme di attacco più frequenti – come abbiamo accennato poco sopra. Sempre secondo il Rapporto Clusit 2025 abbiamo:

- **phishing** - che sfrutta l'ingenuità degli utenti per sottrarre dati sensibili - nel 31% dei casi analizzati;
- **social engineering** - tecnica di manipolazione psicologica utilizzata per ingannare le persone e indurle a rivelare informazioni riservate, compiere azioni non autorizzate o facilitare accessi a sistemi informatici;
- **malware** - tra cui virus e trojan capaci di compromettere interi sistemi – nel 24% dei casi;
- **attacchi alle web application** - che evidenziano l'importanza di proteggere le piattaforme digitali utilizzate per il business – nel 13% dei casi;
- **ransomware e comportamenti scorretti** - sottolineano la necessità di rafforzare la formazione interna per prevenire errori fatali – nel 10% dei casi.

Nei prossimi paragrafi analizzeremo nel dettaglio le **principali strategie utilizzate dai cybercriminali**, al fine di aiutare i Professionisti a riconoscerle subito e a proteggere efficacemente i propri dati e quelli dei loro clienti.

1.1 Phishing e social engineering

Se, come è facile immaginare, gli attacchi informatici includono una vasta gamma di tecniche e strategie, talvolta così insidiose da richiedere l'adozione di importanti sistemi di sicurezza, in realtà le prime minacce che i Professionisti dovrebbero essere in grado di riconoscere ed evitare sono quelle che fanno leva sul mero **errore umano**.

Tra queste, le più diffuse che colpiscono gli Studi professionali sono il **phishing e il social engineering.** Il phishing è una truffa informatica che avviene principalmente tramite e-mail ingannevoli, progettate per sembrare provenienti da fonti affidabili, come banche, enti governativi o fornitori di servizi. Queste e-mail contengono spesso **link fraudolenti** che conducono a siti web falsi – la maggior parte delle volte molto simili all'originale - dove la vittima è invitata a inserire credenziali di accesso, dati bancari o altre informazioni riservate. Dati e informazioni che, com'è facile immaginare, finiscono poi nelle mani sbagliate.

Facciamo un esempio: un Commercialista riceve un'e-mail apparentemente inviata dall'Agenzia delle Entrate che lo invita a cliccare su un link, che lo porta su una pagina che sembra, in tutto e per tutto, quella del sito ufficiale dell'ente pubblico. Effettua il login e finisce per fornire dati riservati importanti, che arriveranno dritti nelle mani degli hacker.

La maggior parte delle volte, questi attacchi vanno a buon fine per una semplice **disattenzione** da parte della vittima: spesso, infatti, le e-mail fraudolente presentano una **grammatica scorretta** e i link, per quanto simili all'originale, riportano delle **minime differenze** che potrebbero essere individuate semplicemente prestando maggiore attenzione a ogni singolo carattere. In più, bisognerebbe sempre ricordare che nessun ente legittimo fa richiesta di dati personali via mail, per cui il solo invito a condividerli dovrebbe attivare un campanello d'allarme.

Il **social engineering** si basa su un principio simile: la manipolazione psicologica. Tramite quest'ultima, i cybercriminali convincono le persone a rivelare informazioni riservate o a concedere accesso ai propri sistemi.

Un esempio comune è l'attacco telefonico, in cui un hacker si spaccia per un tecnico IT e convince la vittima a fornire le credenziali di accesso a un sistema aziendale. Altri metodi includono messaggi **SMS fraudolenti (smishing) o chiamate** in cui il malintenzionato finge di essere un cliente o un fornitore.

Parliamo di tecniche non particolarmente complesse, che fanno leva principalmente su **emozioni di allarme, panico e agitazione** che possono facilmente spingere le persone a compiere azioni istintive. Conoscere questo tipo di minaccia, quindi, può aiutare ad analizzare la situazione con maggiore consapevolezza e razionalità laddove si presenti. Proprio per questo motivo è fondamentale informarsi in prima persona e **formare i propri collaboratori** affinché tutti siano in grado di riconoscere i segnali di allarme, come e-mail con richieste insolite o link sospetti, e adottare buone pratiche di sicurezza, per esempio **verificare sempre la fonte di una richiesta** prima di rispondere e condividere informazioni.

1.2 Ransomware e malware

Le tecniche di phishing descritte nel paragrafo precedente non servono solo a rubare credenziali o dati sensibili; spesso, infatti, rappresentano il primo passo per diffondere all'interno dei dispositivi e dei sistemi dello Studio software dannosi, noti come **malware**. I malware possono avere funzioni diverse, dalla semplice raccolta di informazioni fino al completo blocco dei dati. Tra questi, i **ransomware** sono tra i più diffusi, nonché tra i più temibili.

Un ransomware è un tipo di malware che **cripta i file presenti su un dispositivo** o un'intera rete e li rende inaccessibili fino al **pagamento di un riscatto**. I cybercriminali dietro questi attacchi sfruttano tecniche sofisticate per infettare i sistemi e richiedono somme di denaro, spesso in criptovalute, per fornire la chiave di decrittazione. Si tratta, dunque, di un tipo di attacco particolarmente redditizio per i criminali, in quanto le vittime, pur di riavere accesso ai propri dati, sono spesso disposte a pagare cifre elevate nel minor tempo possibile.

Ma **come ci si può esporre a un ransomware?** Questo tipo di malware si diffonde attraverso diversi vettori di infezione, tra cui:

phishing che, come abbiamo avuto modo di vedere, consiste nell'invio di e-mail ingannevoli con allegati o link malevoli che, una volta aperti, scaricano il malware;

download da siti compromessi, dal momento che il ransomware può essere nascosto in software o documenti scaricati da fonti non affidabili;

software pirata, cioè programmi attivati illegalmente (spesso per ridurre i costi) che possono contenere malware nascosti;

chiavette USB infette, ovvero dispositivi USB lasciati incustoditi o consegnati da sconosciuti che possono contenere malware che si attivano automaticamente quando vengono collegati a un computer.

In caso di attacco, seppure la tentazione di pagare il riscatto richiesto dai cybercriminali sia comprensibile, in realtà questa non è mai la soluzione consigliata: non c'è, infatti, alcuna garanzia che i dati vengano effettivamente decriptati e, in molti casi, il pagamento non fa che incentivare ulteriori attacchi.

La soluzione migliore **è affidarsi a specialisti di sicurezza informatica** che possono valutare il danno e tentare un recupero senza cedere alle richieste degli hacker. Sebbene esistano metodi fai-da-te per la decrittazione, questi sono spesso complessi e non sempre efficaci, per cui la strada migliore è rivolgersi a figure specializzate.

L'alternativa? Ancora una volta, la **prevenzione è la strategia più sicura** sia contro questo tipo di minaccia, sia per evitare di dover spendere ingenti somme per il ripristino della situazione.

1.3 Data breach e perdita di dati sensibili

Un **data breach** (in italiano, violazione dei dati) si verifica quando informazioni sensibili – come dati finanziari, anagrafiche di clienti, documenti riservati o credenziali di accesso – vengono **sottratte, esposte o utilizzate senza autorizzazione**. È importante distinguere questo concetto dal **data leak** (perdita di dati): nel data breach i dati vengono intenzionalmente rubati o compromessi da un attore malevolo, mentre nel data leak **le informazioni risultano accessibili o diffuse involontariamente**, spesso a causa di configurazioni errate o scarsa protezione. Un data breach può avvenire in diversi modi: per un errore umano (ad esempio, l'invio accidentale di documenti a destinatari sbagliati), per un attacco hacker o a causa di falle nei sistemi di sicurezza. Il data breach è tra le minacce più pericolose per i Professionisti, perché compromette informazioni riservate e può causare danni economici e reputazionali difficilmente recuperabili. Secondo il Rapporto Clusit 2025, gli Studi professionali figurano nelle prime dieci tipologie di vittime dal 2020 al 2024, anche perché spesso non dispongono di sistemi di difesa avanzati, né di personale che si occupa nello specifico di Cybersecurity.

Le **conseguenze di un data breach** possono essere molto rilevanti. Da un punto di vista finanziario, le realtà colpite devono spesso affrontare **costi legali, sanzioni e perdite economiche dirette.** Bisogna considerare, poi, il tempo necessario per ripristinare l'operatività, con tutte le interruzioni di servizio del caso che impattano la produttività. Tra gli aspetti più critici, però, c'è soprattutto la **perdita di fiducia da parte di clienti e partner,** con conseguenze a lungo termine sull'attività. Anche in questo contesto, dunque, adottare **misure di sicurezza preventive** è essenziale per proteggere i dati e garantire la continuità del proprio lavoro. Prevenire un data breach significa implementare strategie efficaci di protezione, come l'adozione di protocolli di sicurezza avanzati, l'uso di password robuste, il monitoraggio continuo delle reti e la formazione del personale. Tutte azioni, queste, che permettono di tutelare la propria attività e **mantenere la fiducia dei propri clienti.**

Per saperne di più:

→ Data Breach: cos'è e cosa fare in caso di violazione dei dati

→ Social Engineering: cos'è e come difendere la propria azienda

→ I principali tipi di attacchi informatici e come prevenirli

→ PEC sicura: come proteggersi da malware e phishing e tenere al sicuro il tuo business

Capitolo 2

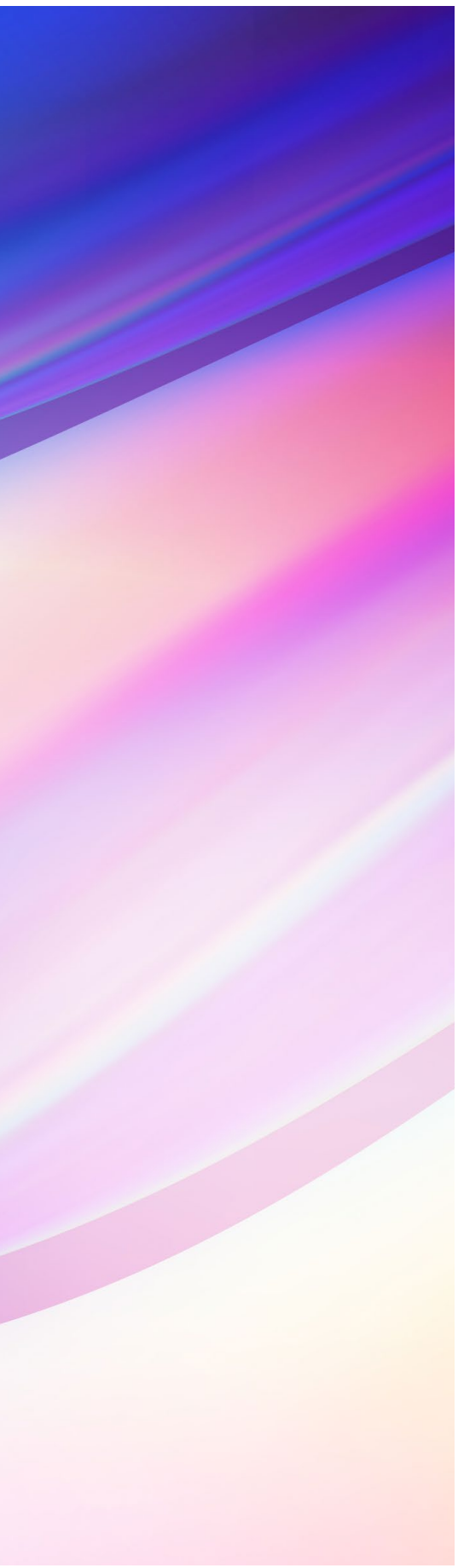
Normative e compliance della Cybersecurity

La protezione dei dati non solo è essenziale per la sicurezza e la reputazione degli Studi professionali, ma è soprattutto una **responsabilità legale:** regolamenti come il **GDPR** (Regolamento Generale sulla Protezione dei Dati), il **DORA** (Digital Operational Resilience Act) e la **NIS2** (Network and Information Security Directive 2) obbligano aziende e Professionisti ad adottare misure di sicurezza adeguate a garantire la riservatezza e l'integrità delle informazioni.

Questi regolamenti hanno imposto **standard elevati per il trattamento dei dati** e hanno stabilito che tutte le imprese e i Professionisti che operano all'interno dell'Unione Europea o che trattano dati di cittadini europei debbano assicurare una protezione rigorosa, con **sanzioni severe in caso di violazione**. Comprendere gli obblighi legali derivanti da queste normative può sembrare complesso, ma è fondamentale per ogni Professionista che gestisce informazioni personali, che si tratti di Consulenti fiscali, Avvocati, Commercialisti o altre figure professionali. Non tenere conto dei regolamenti e delle proprie responsabilità, infatti, espone al rischio di incorrere in sanzioni, ma non solo. Ancora una volta, il pericolo è quello di **perdere la fiducia dei propri clienti** e non essere in grado di mantenere l'integrità dell'attività.

Ma quali sono gli **aspetti normativi più importanti** e come i Professionisti possono assicurare la **conformità alle leggi sulla protezione dei dati**?

Approfondiamo gli obblighi legali legati alla protezione dei dati ed esploriamo le migliori pratiche e i passi concreti che ogni Studio dovrebbe seguire per tutelare la conformità e la sicurezza delle informazioni trattate.



2.1 GDPR e protezione dei dati

Per gli Studi professionali, il GDPR ha comportato significativi cambiamenti nella gestione delle informazioni personali dei clienti e dei collaboratori. Ma di cosa si tratta, esattamente?

Il **Regolamento Generale sulla Protezione dei Dati (GDPR)** è la normativa europea che disciplina in modo organico la protezione dei dati personali. Approvato nel 2016 ed entrato pienamente in vigore il 25 maggio 2018, il GDPR ha lo scopo di garantire ai cittadini dell'Unione Europea un maggiore controllo sulle proprie informazioni personali, rafforzando i diritti degli interessati e stabilendo regole uniformi in tutti gli Stati membri. Il regolamento si applica a qualsiasi soggetto, pubblico o privato, che raccolga, elabori o conservi dati personali, indipendentemente dalla dimensione dell'organizzazione o dalla sua ubicazione geografica. Anche imprese e Professionisti extra-UE sono tenuti a conformarsi qualora trattino dati di residenti nell'Unione.

Il **GDPR** si fonda su alcuni principi cardine:

- **liceità, correttezza e trasparenza** nel trattamento dei dati;
- **limitazione delle finalità** (i dati devono essere raccolti per scopi specifici e legittimi);
- **minimizzazione dei dati** (raccogliere solo ciò che è strettamente necessario);
- **esattezza, integrità e riservatezza** (proteggere i dati da accessi non autorizzati o perdite);
- **accountability** (responsabilizzazione del titolare del trattamento).

L'applicazione di questi principi riguarda ovviamente anche gli Studi professionali, tra cui Studi legali, Commercialisti, Consulenti del Lavoro e altri Professionisti. Questi soggetti devono adottare misure adeguate a **garantire che i dati personali trattati** – anche in quantità contenute – siano **gestiti in modo conforme alla normativa vigente**. Questo comporta, innanzitutto, la necessità di predisporre **procedure e politiche interne** che regolino l'intero ciclo di vita del dato, dalla raccolta alla conservazione, fino alla sua eventuale cancellazione. Ogni attività deve essere documentata, giustificabile e dimostrabile.

Particolarmente rilevante per i Professionisti è il principio di **accountability**, ovvero la **responsabilizzazione del titolare del trattamento**, che corrisponde al soggetto che determina le finalità e i mezzi del trattamento dei dati personali. A differenza della normativa previgente, il GDPR non prevede una lista esaustiva di adempimenti, ma richiede al titolare di valutare autonomamente i rischi associati ai trattamenti effettuati e di adottare misure tecniche e organizzative adeguate al contesto e alla sensibilità dei dati trattati. Tra le misure comunemente richieste rientrano l'adozione di strumenti informatici sicuri, l'utilizzo di password robuste e di sistemi di crittografia, l'aggiornamento costante del software utilizzato, il controllo rigoroso degli accessi ai dati, e la definizione di ruoli chiari per ciascun soggetto coinvolto.

Il regolamento introduce anche due concetti fondamentali: **privacy by design** e **privacy by default**. Questi principi impongono di considerare la protezione dei dati non come un'aggiunta successiva, ma come un elemento strutturale da integrare fin dalla fase di progettazione di qualunque processo, servizio o sistema che comporti il trattamento di informazioni personali. In concreto, significa che lo Studio professionale, nel pianificare le proprie attività, deve adottare strumenti e soluzioni che minimizzino i rischi di violazione e limitino al minimo indispensabile i dati trattati, sia nel formato digitale che in quello cartaceo.

La conformità al GDPR richiede anche una **revisione dell'organizzazione interna dello Studio**. Chiunque abbia accesso ai dati (dipendenti, collaboratori, consulenti esterni) deve essere formalmente autorizzato e formato in modo adeguato. Il titolare del trattamento deve definire con precisione i compiti, le responsabilità e i limiti di intervento per ciascun soggetto, garantendo che il personale agisca secondo procedure tracciabili e conformi alle norme.

Altro principio fondamentale è quello della **trasparenza**: il GDPR impone di informare in modo chiaro e comprensibile gli interessati (ad esempio, i clienti dello Studio) sulle modalità con cui i loro dati vengono trattati. A tal fine, lo Studio deve redigere un'informativa privacy dettagliata e personalizzata, che illustri le finalità del trattamento, la base giuridica, le modalità operative, i tempi di conservazione dei dati e i diritti riconosciuti agli interessati. Tale informativa deve essere facilmente accessibile, aggiornata e scritta in un linguaggio comprensibile anche ai non addetti ai lavori.

Infine, una questione spesso dibattuta riguarda la **figura del DPO (Data Protection Officer)**. Il GDPR prevede l'obbligo di nominarlo solo in determinati casi, ad esempio quando il trattamento dei dati avviene su larga scala, oppure se riguarda categorie particolari di dati sensibili, come quelli sanitari o giudiziari. Per la maggior parte degli Studi professionali – che non trattano dati su vasta scala né svolgono attività di monitoraggio sistematico – la nomina del DPO non è obbligatoria. Tuttavia, il Professionista può decidere di nominarne uno volontariamente, come misura aggiuntiva di garanzia. In alternativa, è possibile affidarsi a un **consulente esterno** che svolga le funzioni del DPO, senza dover creare un ruolo interno. Anche in presenza di tale figura, la responsabilità di garantire la corretta gestione dei dati personali resta in capo al titolare dello Studio, che deve assicurare il pieno rispetto degli obblighi previsti dal regolamento.

2.2 DORA: principi, obblighi e rischi per i Commercialisti

Il **DORA** (Digital Operational Resilience Act) è il regolamento dell'Unione Europea entrato in vigore nel 2023, pensato per **rafforzare la capacità delle organizzazioni del settore finanziario** – e dei soggetti collegati a esso – di resistere, rispondere e riprendersi da incidenti informatici o disservizi digitali. Non riguarda soltanto banche, assicurazioni o grandi intermediari, ma anche tutti i professionisti e le realtà che, direttamente o indirettamente, gestiscono dati sensibili e processi legati al mondo finanziario.

La normativa introduce un quadro comune di regole che si basano su alcuni pilastri fondamentali.

- **Gestione e monitoraggio del rischio ICT:** valutare, prevenire e ridurre i rischi legati ai sistemi informatici.
- **Test di resilienza digitale:** verificare periodicamente la capacità dei sistemi di resistere a incidenti e attacchi.
- **Gestione degli incidenti:** stabilire procedure chiare per rilevare, segnalare e risolvere rapidamente gli eventi critici.
- **Controllo dei fornitori ICT:** monitorare e responsabilizzare i partner tecnologici esterni (Cloud, software, servizi digitali).

Per i Commercialisti, che gestiscono quotidianamente informazioni riservate di clienti, aziende e privati, la DORA non è solo una direttiva tecnica: è uno strumento di tutela professionale e di credibilità. Adeguarsi significa:

- **garantire ai clienti che i loro dati sono protetti** da attacchi e fughe di informazioni;
- **rafforzare la fiducia** e la reputazione dello Studio;
- **evitare conseguenze legali ed economiche** derivanti da mancate misure di sicurezza;
- **allinearsi a standard europei** che diventeranno sempre più vincolanti anche per le piccole realtà.

Ignorare o sottovalutare il DORA comporta rischi rilevanti:

- **violazioni dei dati** con conseguenti sanzioni e perdita di clienti;
- **interruzione dei servizi,** che causa l'impossibilità di accedere a software gestionali, contabilità bloccata, ritardi negli adempimenti fiscali;
- **responsabilità professionale** in caso di danni subiti dai clienti a seguito di incidenti informatici;
- **perdita di reputazione** e fiducia, elemento chiave per la professione di Commercialista.

2.3 NIS2: la nuova frontiera della sicurezza informatica

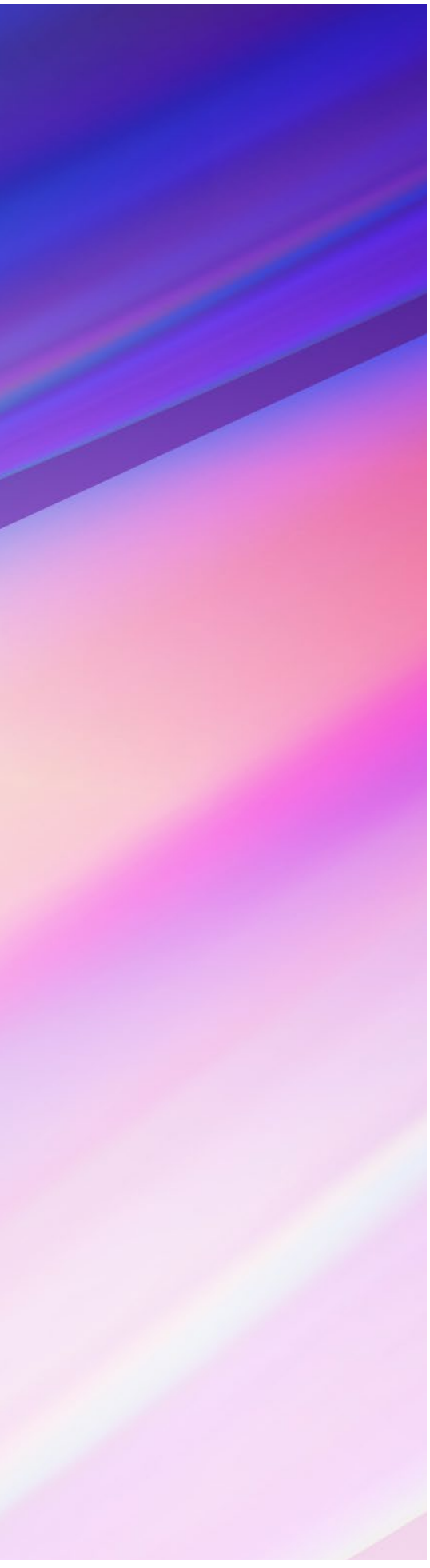
La direttiva europea **NIS2** (Network and Information Security Directive 2), approvata per rafforzare la sicurezza informatica all'interno dell'Unione, rappresenta un'**evoluzione significativa rispetto alla prima NIS del 2016**. Il suo scopo è quello di uniformare gli standard di protezione e gestione dei rischi digitali, **estendendo il campo di applicazione a un numero maggiore di settori e organizzazioni** considerate cruciali per il buon funzionamento dell'economia e dei servizi essenziali.
Pur non essendo destinatari diretti come banche o operatori energetici, anche i Commercialisti sono coinvolti: infatti, custodiscono dati finanziari e personali sensibili e fanno parte di quella catena di soggetti che, se compromessa, può generare gravi conseguenze per clienti e istituzioni.

La direttiva si basa su un approccio integrato alla gestione della sicurezza digitale che comprende:

- una **valutazione continua dei rischi**, con obbligo di adottare misure preventive;
- la **prontezza a reagire agli incidenti,** mediante procedure interne chiare e condivise;
- la **notifica obbligatoria** degli eventi più gravi alle autorità competenti entro tempi molto stretti;
- il **coinvolgimento diretto dei vertici** nella supervisione delle misure di sicurezza;
- una maggiore attenzione alla **catena dei fornitori**, inclusi i servizi informatici utilizzati negli studi professionali.

Trascurare la NIS2 sarebbe un errore: gli Studi professionali oggi sono parte integrante dell'ecosistema digitale. Adeguarsi significa:

- **proteggere la riservatezza dei clienti**, valore centrale nella professione;
- **garantire continuità lavorativa** anche in caso di attacchi informatici o guasti tecnologici;
- **rafforzare il rapporto di fiducia** con aziende e privati che affidano i propri dati;
- **evitare di rimanere indietro rispetto a standard europei** che diventeranno sempre più stringenti.



2.4 ISO 27001 e altre certificazioni di sicurezza

Dimostrare ai clienti e ai partner di poter gestire e proteggere i loro dati in modo sicuro rappresenta oggi un vantaggio competitivo per gli Studi professionali. Ma come si può, in concreto, garantire di adottare le migliori pratiche in materia di sicurezza delle informazioni?

Una delle soluzioni più efficaci è ottenere una **certificazione ISO**, un riconoscimento internazionale che attesta il rispetto di standard di qualità e sicurezza.

Tra le diverse certificazioni, la **ISO 27001** è quella di riferimento per la gestione della sicurezza delle informazioni: si tratta di uno standard internazionale che definisce i requisiti per un **Sistema di Gestione della Sicurezza delle Informazioni** (ISMS - Information Security Management System), ovvero un insieme di processi, politiche e controlli progettati per proteggere dati sensibili da minacce come violazioni, accessi non autorizzati o perdita di informazioni.

La ISO 27001 non si limita a stabilire regole generali, ma offre un **approccio strutturato e basato sul rischio**. Tra le diverse aree tematiche, infatti, alcune sezioni riguardano ambiti come il **controllo degli accessi, la sicurezza operativa** (protezione dei sistemi informatici e delle infrastrutture tecnologiche) o la **sicurezza delle comunicazioni**, che garantisce la protezione delle informazioni scambiate tra diversi soggetti.

Ma perché **ottenere la certificazione ISO 27001 è così importante**? I motivi sono diversi.

Conformità normativa: la ISO 27001 aiuta a rispettare leggi, regolamenti e requisiti contrattuali relativi alla sicurezza delle informazioni, tra cui il GDPR.

Vantaggio competitivo: dimostrare di adottare uno standard internazionale di sicurezza può migliorare la reputazione e aumentare la fiducia di clienti e partner.

Prevenzione degli incidenti: un sistema di gestione certificato riduce il rischio di attacchi informatici, fughe di dati o errori operativi e, di conseguenza, minimizza i possibili danni economici e legali.

Per ottenere la certificazione ISO 27001, prima di tutto è necessario implementare un sistema di gestione della sicurezza delle informazioni, mediante l'identificazione dei rischi e la definizione di misure di protezione adeguate. Successivamente, un **ente di certificazione indipendente effettuerà un audit** per verificare che tutti i requisiti siano rispettati. Una volta superato il test valutativo, si accede alla **certificazione.** Ciò non significa, però, che ottenuta la certificazione si possano allentare le misure di sicurezza: la certificazione, infatti, ha **validità triennale** e vengono effettuati controlli periodici per garantire il mantenimento degli standard.

La ISO 27001 non è il solo standard a rivelarsi utile per Studi e Professionisti: esistono molte altre certificazioni, come la **ISO 9001** che certifica la qualità della gestione aziendale o la **ISO 22301** che riguarda la continuità operativa in caso di emergenze.

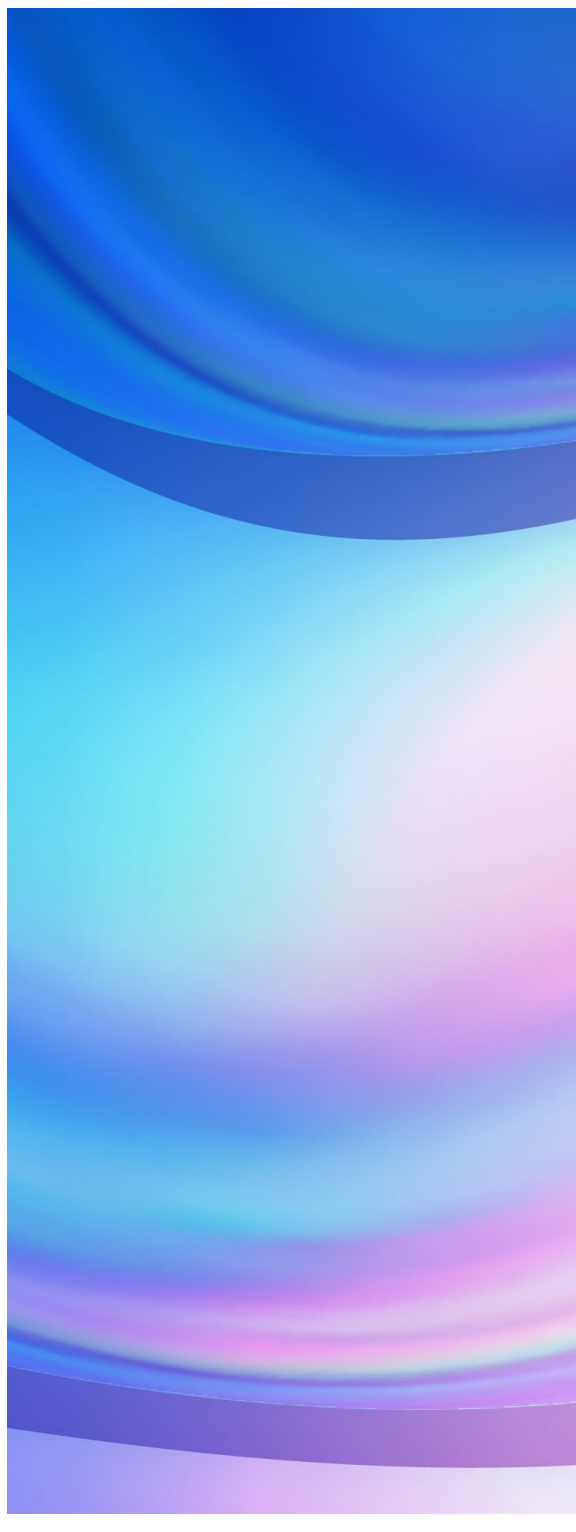
Sebbene queste certificazioni **non siano obbligatorie per legge**, rappresentano un **valore aggiunto** perché offrono un riconoscimento tangibile dell'impegno per la sicurezza, la qualità e la trasparenza; elementi che oggi pesano sempre di più nella scelta di un fornitore di servizi professionali.

Investire in una certificazione ISO significa quindi **distinguersi nel mercato e rafforzare la fiducia dei propri clienti**: in un'epoca in cui i dati sono un asset fondamentale, dotarsi di strumenti adeguati a proteggerli è una scelta strategica che può fare la differenza.

2.5 La responsabilità legale dei Professionisti in caso di data breach

Abbiamo già parlato di **data breach** e di come l'accesso o la divulgazione non autorizzata di dati possa comportare seri danni alla reputazione. È bene chiarire, però, che eventi di questo tipo comportano anche degli **obblighi** precisi da parte del Professionista che, se trascurati, possono portare, oltre che a gravi danni reputazionali e di produttività, a severe **sanzioni.**

Il GDPR stesso fa riferimento al data breach e stabilisce in modo chiaro gli obblighi di notifica in caso di incidente. In particolare, il regolamento prevede che l'autorità di controllo competente venga informata **entro 72 ore dalla scoperta dell'evento**, a meno che non vi siano ragioni fondate per ritenere che l'incidente non comporti conseguenze gravi per gli interessati. Non solo, se la violazione può avere un impatto significativo sui diritti e le libertà delle persone coinvolte (come furto d'identità, frodi, danni finanziari o pregiudizio alla privacy), il titolare del trattamento deve **informare tempestivamente anche gli interessati**, illustrando l'accaduto, le sue conseguenze e le misure adottate per mitigarne gli effetti, come stabilito dall'articolo 34 del GDPR.



Oltre ai danni reputazionali, la mancata gestione di un data breach può avere conseguenze economiche rilevanti: il GDPR prevede **sanzioni fino a 10 milioni di euro o il 2% del fatturato globale** per chi non adempie agli obblighi di notifica e gestione.
Da questo punto di vista, Professionisti e Studi professionali devono predisporre una **strategia preventiva** per affrontare eventuali violazioni. Un buon punto di partenza è la creazione di un **piano di risposta ai data breach**, che definisca chiaramente ruoli, responsabilità e procedure da seguire in caso di incidente, e che includa misure tecniche per individuare e bloccare tempestivamente le minacce, oltre a un piano di **formazione adeguata del personale**, affinché ogni collaboratore sappia come comportarsi davanti a un'anomalia.
Un altro aspetto fondamentale è la **valutazione del rischio**: comprendere quali dati sono più esposti e quali potrebbero essere le conseguenze di una violazione aiuta a definire strategie di protezione più efficaci. Inoltre, è importante **documentare tutte le azioni intraprese per gestire il data breach**, così da poter dimostrare alle autorità di aver agito in modo conforme alla normativa e anche migliorare nel tempo le strategie di protezione e risposta.

Per saperne di più:

→ GDPR – Regolamento generale sulla protezione dei dati

→ Gestione dati personali e privacy: le nuove sfide dei Commercialisti nell'era del GDPR

→ La responsabilità digitale oltre la firma

Approfondimento

Sanzioni per mancata compliance

La mancata osservanza degli obblighi imposti dal GDPR in tema di prevenzione e gestione delle violazioni della sicurezza può esporre al rischio di sanzioni amministrative e penali, oltre che a responsabilità civile. In particolare:

- **sanzioni fino al 2% del fatturato annuo** per violazioni come data breach non segnalato, assenza del registro dei trattamenti dei dati, mancata nomina del DPO (quando necessaria), mancata valutazione d'impatto sulla Protezione dei Dati (DPIA) nei casi richiesti;
- **sanzioni fino al 4% del fatturato annuo** per violazioni come assenza del consenso per il trattamento dei dati, informativa privacy assente o non conforme, mancata esecuzione di un provvedimento del Garante;
- **sanzioni penali** per trattamento non autorizzato di dati personali, diffusione o comunicazione illecita di dati personali su larga scala, false dichiarazioni al Garante o ostacolo all'esercizio delle sue funzioni, acquisizione fraudolenta di dati personali trattati su larga scala;
- **richiesta di risarcimento del danno (responsabilità civile)** nel caso in cui la violazione abbia causato un danno fisico, economico o non materiale, abbia avuto un impatto negativo sulla reputazione della persona coinvolta, abbia riguardato dati coperti dal segreto professionale o abbia implicato la compromissione di dati sensibili o di natura giudiziaria.

Capitolo 3

L'Intelligenza Artificiale come scudo contro le minacce digitali

Negli ultimi anni, il termine Intelligenza Artificiale è diventato parte del linguaggio quotidiano, applicato ai settori più diversi: dalla sanità alla finanza, dalla logistica alla consulenza. Anche l'ambito della Cybersecurity non fa eccezione. La sicurezza, infatti, va considerata come una catena: ogni anello – che sia un processo o una tecnologia – deve essere analizzato con attenzione, perché l'intera catena è sicura solo quando viene rafforzato anche il suo anello più debole. In un contesto in cui le minacce informatiche sono sempre più sofisticate e frequenti, gli strumenti che sfruttano l'AI rappresentano una risorsa strategica per la protezione dei dati e dei sistemi informativi. E se un tempo era considerata prerogativa di grandi aziende, oggi l'Intelligenza Artificiale è accessibile anche a realtà più piccole - come gli Studi professionali - grazie a soluzioni Cloud e strumenti integrati nei sistemi di sicurezza più diffusi.

È così che Cybersecurity e Intelligenza Artificiale avanzano insieme, trasformandosi in un binomio sempre più efficace per anticipare, rilevare e contrastare attacchi informatici. Per uno Studio, questo significa non solo essere pronti a gestire le violazioni, ma anche poter prevenire i rischi in modo intelligente, con strumenti in grado di reagire in tempo reale.

Ma entriamo nel vivo **di come un sistema basato sull'Intelligenza Artificiale supporti la Cybersecurity** e cerchiamo di capire quali sono le caratteristiche che rendono questa tecnologia un vero e proprio ausiliare per la protezione dei dati, il rilevamento e la prevenzione dei rischi.

3.1 L'automazione a supporto della prevenzione degli attacchi

Il tema dell'AI si incrocia spesso col concetto di **automazione**. Questo vale anche quando si parla di software di Cybersecurity, che oggi sfruttano l'Intelligenza Artificiale proprio per sostenere il lavoro umano e migliorare l'efficacia delle strategie di difesa dai criminali informatici. Le minacce informatiche, infatti, sono sempre più sofisticate e rapide nell'evolversi, per cui diventa indispensabile utilizzare un approccio che non si limiti a **rispondere agli attacchi** una volta che si sono verificati, ma che li **prevenga in tempo reale**.

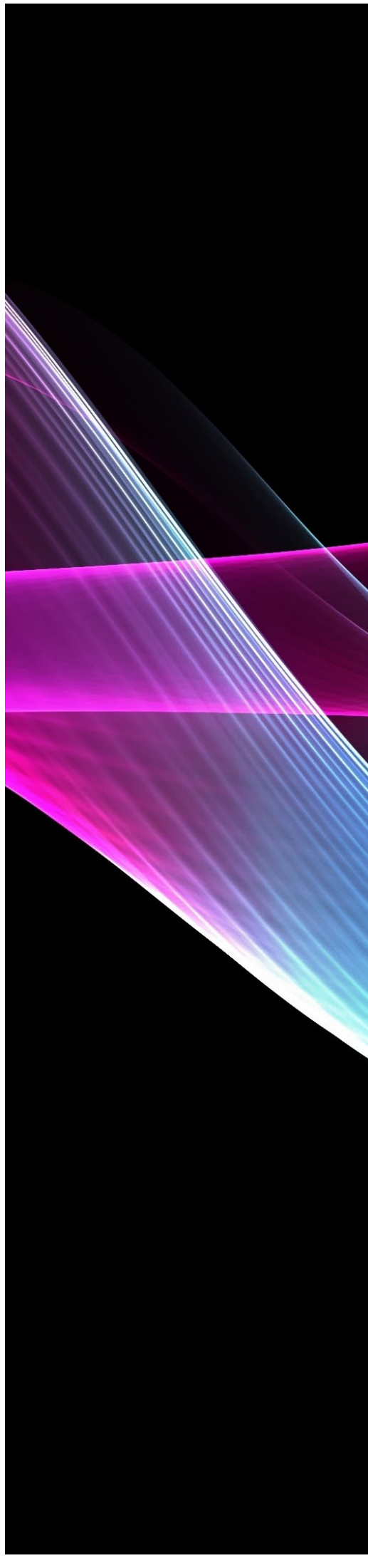
Software di questo tipo utilizzano spesso l'automazione per **apprendere, adattarsi e rispondere a nuovi attacchi** e ridurre, dunque, la necessità di intervento umano. Questo è possibile grazie ai sistemi basati su machine learning, che analizzano continuamente il traffico di rete, il comportamento degli utenti e le interazioni tra dispositivi per identificare qualsiasi deviazione rispetto alla norma. In questo modo, **possono individuare tentativi di intrusione, malware o attività sospette** prima che causino danni significativi. L'AI, infatti, è in grado di riconoscere pattern dannosi, anche in situazioni in cui le minacce non sono ancora state catalogate nei database tradizionali di malware e attacchi informatici. In pratica, mentre un software di sicurezza tradizionale si basa su regole predefinite e su firme di attacco già conosciute, un sistema dotato di AI è in grado di **identificare pericoli emergenti,** senza dover attendere che siano classificati ufficialmente come tali.

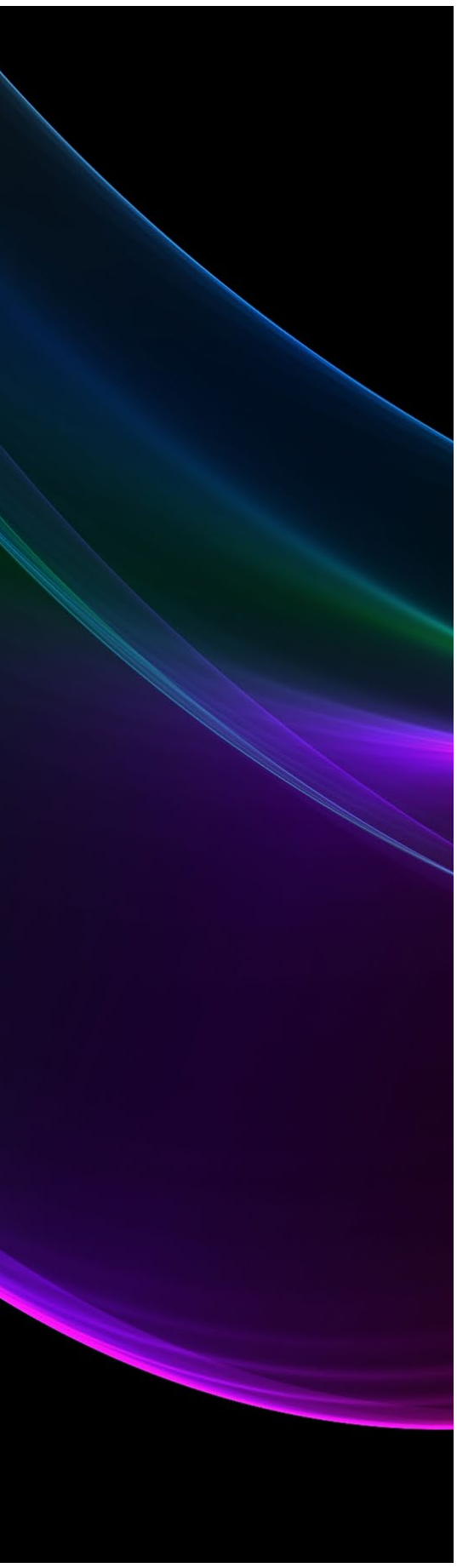
Ma l'AI non agisce esclusivamente in termini di prevenzione e si dimostra fondamentale anche in risposta agli attacchi. In molti casi i software di Cybersecurity possono **bloccare in automatico un accesso sospetto** o isolare un dispositivo compromesso **in pochi millisecondi**, senza dover attendere un intervento umano. I vantaggi sono evidenti: una **notevole riduzione dei tempi di reazione** e un **contenimento immediato del danno**, impedendo che l'attacco si propaghi all'interno del sistema.

Tutto questo si traduce, com'è facile immaginare, in un'**ottimizzazione dei costi**: prevenire un attacco è sempre meno costoso rispetto a dover gestire le conseguenze di una violazione, sia in termini di ripristino dei sistemi sia di eventuali sanzioni per la perdita di dati.

Un ulteriore punto di forza dell'AI è la **capacità di apprendere continuamente**. Ogni attacco tentato, ogni comportamento sospetto e ogni minaccia neutralizzata diventano informazioni preziose per il sistema, che affina costantemente i suoi algoritmi per rispondere in modo sempre più efficace. Questo significa che, con il passare del tempo, l'AI diventa sempre più capace di **prevenire attacchi futuri**.

L'automazione basata sull'AI rappresenta un investimento intelligente per qualsiasi Studio professionale che voglia rafforzare la propria sicurezza digitale con soluzioni di Cybersecurity avanzate.





3.2 Monitoraggio e rilevamento delle minacce

Oggi il volume di dati generato e gestito da Professionisti e Studi professionali è così vasto che l'analisi manuale risulta impossibile. **Identificare minacce informatiche prima che si trasformino in problemi** concreti richiede una rapidità di elaborazione e una capacità di previsione che la mente umana, da sola, non può garantire. In questo scenario, quindi, le soluzioni di Cybersecurity si stanno imponendo come uno strumento indispensabile per rafforzare la sicurezza digitale.

Ma cosa può fare l'AI in ambito Cybersecurity? Partiamo dal presupposto che l'AI è in grado di **analizzare enormi quantità di dati in tempo reale** e, dunque, anche schemi, anomalie e possibili minacce molto prima che un attacco possa concretizzarsi. Come ci riesce? Spesso grazie a sofisticati **algoritmi di Machine Learning**, sistemi di sicurezza informatica che possono apprendere dalle informazioni raccolte e affinare continuamente le proprie capacità di difesa. L'AI è in grado di riconoscere attacchi già noti, ma anche di **identificare comportamenti sospetti** che potrebbero segnalare una minaccia ancora sconosciuta.

È ciò che possiamo definire **prevenzione proattiva**: invece di limitarsi a reagire agli attacchi, le soluzioni basate sull'Intelligenza Artificiale analizzano il comportamento degli utenti e dei sistemi per individuare variazioni anomale. Un accesso insolito a un database, un improvviso picco di traffico in rete o tentativi ripetuti di accesso non autorizzato possono essere segnali d'allarme che l'AI intercetta prima che si verifichi una violazione.

Ma l'Intelligenza Artificiale non si ferma al monitoraggio: è anche uno strumento prezioso per **identificare vulnerabilità nei sistemi informatici**. Verifica continuamente le difese esistenti e può segnalare falle di sicurezza che potrebbero essere sfruttate dagli hacker. Tutto questo, ovviamente, consente di intervenire prima che si verifichi un problema reale.

Per gli Studi professionali, spesso privi di un reparto IT dedicato, questa tecnologia rappresenta dunque un'opportunità fondamentale per **garantire la sicurezza dei dati sensibili senza dover impiegare risorse ingenti.** L'adozione di strumenti di Cybersecurity basati sull'AI permette quindi di rafforzare la protezione dei propri sistemi in modo intelligente e, allo stesso tempo, di migliorare la conformità alle normative sulla protezione dei dati.

3.3 L'AI nei software di Cybersecurity: una difesa accessibile e automatizzata

Dopo aver esplorato le potenzialità dell'AI nel monitoraggio e nella prevenzione degli attacchi, risulta evidente come l'adozione di un software di Cybersecurity che sfrutta l'Intelligenza Artificiale possa apportare immensi benefici.

È importante, però, evidenziare che tali strumenti non sono solo appannaggio di grandi realtà. Al contrario, l'implementazione di strumenti basati sull'AI comporta una **vasta gamma di benefici anche agli Studi professionali che non hanno un reparto IT interno**. Questo, per diverse ragioni:

- l'Intelligenza Artificiale è in grado di **rilevare e bloccare in tempo reale attività sospette**, come tentativi di intrusione o malware, grazie all'analisi di enormi quantità di dati in tempo reale, che consente di identificare rapidamente anomalie e arginare i danni senza la necessità di interventi manuali;

- le minacce informatiche più comuni, come il malware, il phishing e i deepfake, possono essere difficili da rilevare con metodi tradizionali, ma non con l'AI che, attraverso algoritmi avanzati, è in grado di **identificare e bloccare possibili violazioni**;

- le minacce evolvono rapidamente e possono apparire sotto nuove forme, ma i **software basati su AI si aggiornano automaticamente** e si adattano a nuove tecniche di attacco senza richiedere l'intervento di un tecnico.

Stiamo parlando, quindi, di un investimento alla portata di tutti, non solo degli Studi più grandi: oggi è una **necessità strategica per i Professionisti di ogni dimensione**, perché garantisce protezione dei dati, continuità operativa e fiducia da parte di clienti e partner.

Per saperne di più:

→ Differenza tra Intelligenza Artificiale e Machine Learning

→ Come l'Intelligenza Artificiale entrerà negli studi? Le istruzioni della legge delega

Approfondimento

Come funzionano gli algoritmi predittivi

Il modo più semplice per comprendere il funzionamento degli algoritmi predittivi è paragonarlo a quello del nostro sistema immunitario.

Quando il nostro corpo è esposto a un patogeno, il sistema immunitario crea una sorta di "memoria" che lo rende più efficiente nel riconoscerlo e combatterlo in futuro. Gli algoritmi di machine learning funzionano in modo analogo: analizzano i comportamenti passati degli attacchi e sviluppano una "memoria" dei pattern di minacce. Quando se ne presenta una nuova, anche se con caratteristiche leggermente diverse, l'algoritmo riesce a riconoscerla grazie alla somiglianza con quelle precedenti e, ovviamente, a bloccarla tempestivamente, innalzando le difese.

Capitolo 4

Cybersecurity e trasformazione digitale degli Studi professionali

L'avvento delle nuove tecnologie ha indirizzato i Professionisti verso una nuova organizzazione dell'operatività quotidiana e delle strategie aziendali: l'adozione di strumenti digitali ha permesso di ottimizzare i processi e offrire servizi sempre più efficienti ai clienti. La digitalizzazione, infatti, non è più solo un'opzione, ma si rivela necessaria per rimanere competitivi in un mercato in continua evoluzione.

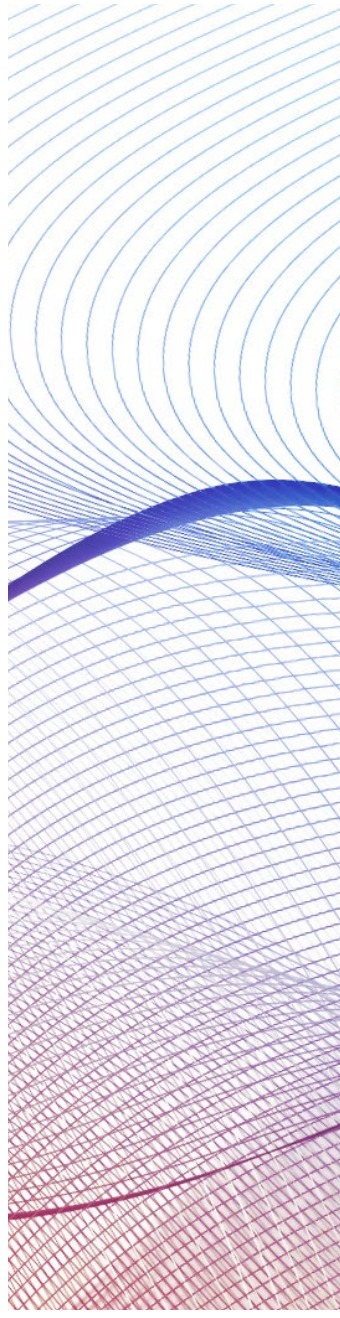
Questo crescente utilizzo della tecnologia, però, porta con sé anche nuove sfide: se da un lato migliora l'efficienza e la rapidità del lavoro, dall'altro espone gli Studi a una superficie di attacco più ampia per i criminali informatici e a un maggior rischio di violazioni dei dati.

Un argomento che tocca ancor di più Commercialisti, Consulenti del Lavoro e altri Studi professionali, che difficilmente dispongono di **reparti IT interni o di figure specializzate nella protezione dei dati.** A differenza delle grandi aziende, che possono permettersi interi team dedicati alla sicurezza informatica, le piccole e medie realtà professionali spesso devono affrontare queste sfide con risorse limitate. Questo rende ancora più importante adottare soluzioni che siano efficaci, ma al tempo stesso semplici da gestire e implementare. Le soluzioni basate su AI, infatti, sono progettate per essere user-friendly, offrono interfacce semplici e comprensibili che permettono anche ai Professionisti senza competenze tecniche avanzate di monitorare e gestire la sicurezza in modo efficace.

Proprio per questo motivo, l'**integrazione dell'AI negli strumenti di Cybersecurity** si rivela un'azione essenziale per proteggere le informazioni e quindi la reputazione dei Professionisti.

Ma come possono, dunque, queste realtà, proteggere i dati e dotarsi di strumenti e tecnologie senza ingenti investimenti e competenze tecniche avanzate?

4.1 Cloud Computing e sicurezza: proteggere i dati in rete



Il **Cloud Computing** ha offerto agli Studi professionali strumenti avanzati per proteggere i propri dati senza dover investire in infrastrutture IT complesse, né possedere competenze tecniche approfondite.

In un contesto in cui la protezione dei dati è sempre più critica, i Professionisti possono contare su un sistema dinamico, **sempre aggiornato e accessibile da qualsiasi dispositivo**, ma che ha anche la capacità di abilitare tecnologie avanzate, come l'Intelligenza Artificiale, che stanno trasformando il modo in cui affrontiamo le minacce informatiche.

Grazie all'integrazione con l'AI, il Cloud non è più solo un archivio virtuale, ma una **piattaforma intelligente che analizza, prevede e risponde agli attacchi** in tempo reale e consente di:

analizzare e processare dati in tempo reale, per individuare schemi sospetti e segnalare possibili minacce prima che possano causare danni;

automatizzare la protezione dei dati mediante algoritmi di machine learning per bloccare attività dannose e adattarsi continuamente a nuove minacce, senza richiedere un monitoraggio costante da parte dei Professionisti;

garantire scalabilità e aggiornamenti continui, dal momento che così come le minacce evolvono, così devono evolversi anche le difese. Con il Cloud, gli Studi professionali possono contare su aggiornamenti automatici e soluzioni che si adattano alle loro esigenze, senza dover investire in hardware o competenze tecniche avanzate.

Da questo punto di vista, dunque, il Cloud si dimostra una valida risorsa per consentire agli Studi professionali di **accedere a una Cybersecurity di alto livello**, con strumenti intelligenti che lavorano in modo autonomo per garantire protezione continua e proattiva.

4.2. Smart working e protezione dei dispositivi remoti

Negli ultimi anni gli Studi professionali hanno abbracciato sempre più l'idea di sfruttare le nuove tecnologie per migliorare l'operatività quotidiana e lo **smart working** è ormai una realtà diffusa anche tra i Professionisti.

Il lavoro da remoto, tuttavia, ha esposto i **dati sensibili a nuovi rischi**. Dispositivi personali o reti domestiche non protette, infatti, possono diventare il punto di ingresso per attacchi informatici, con il rischio di rendere vulnerabili dati e informazioni sensibili.

È qui che i software in Cloud giocano un ruolo chiave: grazie alla loro infrastruttura centralizzata, permettono di gestire la sicurezza in modo uniforme, indipendentemente dal dispositivo o dalla posizione geografica dell'utente. Per ridurre il rischio di attacchi è, però, essenziale adottare alcune strategie:

autenticazione a più fattori che aggiunge un ulteriore livello di protezione oltre alla semplice password e riduce il rischio di accessi non autorizzati;

VPN e connessioni sicure che consentono di criptare il traffico dati e lo proteggono da possibili intercettazioni;

gestione centralizzata degli accessi che aiuta a monitorare e controllare in tempo reale chi accede ai dati, nonché verificare rapidamente i permessi in caso di anomalie;

aggiornamenti e patch automatici per ridurre le vulnerabilità che potrebbero essere sfruttate dagli hacker;

backup regolari che assicurano il recupero dei dati in caso di attacco ransomware o guasti tecnici ed evitano interruzioni prolungate nell'operatività.

Va, poi, detto che la sicurezza informatica nel contesto del lavoro da remoto non è solo una questione tecnica, ma anche organizzativa: i Professionisti dovrebbero sempre promuovere una cultura della sicurezza tra i dipendenti e sensibilizzarli sulle migliori pratiche da adottare per proteggere i dati e garantire la continuità aziendale.

4.3 L'AI nei software gestionali: efficienza e sicurezza per gli Studi professionali

In un panorama tecnologico in costante evoluzione, è però essenziale sfruttare al meglio le tecnologie a disposizione. La **Cybersecurity e la gestione dei dati** richiedono strumenti più avanzati, come l'AI, capaci di adattarsi alle nuove sfide. Integrata nei software gestionali, l'Intelligenza Artificiale migliora le prestazioni dello Studio - garantendo automazione, semplificazione dei processi e maggiore efficienza operativa - e, al contempo, offre una **protezione più avanzata dei dati e delle informazioni sensibili**.

Ma quali sono i benefici dell'integrazione dell'AI nel gestionale di Studio?

- **Automatizzazione di diverse attività time-consuming**, come la classificazione dei documenti, l'inserimento dei dati e la gestione delle scadenze. Tutto ciò permette di ridurre in modo drastico gli errori umani e consente ai Professionisti di concentrarsi su attività a più alto valore aggiunto.

- **Analisi ed elaborazione di enormi volumi di dati in tempo reale** per individuare pattern e tendenze, con l'obiettivo di prendere decisioni più informate e fornire un supporto prezioso nella consulenza ai clienti.

- **Implementazione di sistemi di sicurezza avanzati** che monitorano costantemente gli accessi ai dati e individuano in tempo reale eventuali anomalie o tentativi di attacco.

- Oltre a questi benefici, va evidenziato che l'integrazione dell'AI in un software gestionale offre un **livello di contestualizzazione** ben diverso dai modelli generici come i Large Language Model o i copilot. Un software gestionale con AI, infatti, conosce già la struttura dello Studio, i dati specifici e le dinamiche operative. Questo significa, per gli Studi, **risparmiare tempo** – dal momento che non è necessario fornire di volta in volta dettagli aggiuntivi o spiegare il contesto per ottenere risposte pertinenti – e **migliorare efficienza ed efficacia**, grazie ad analisi più precise che consentono anche di prendere decisioni qualitativamente superiori.

Adottare queste tecnologie significa, quindi, non solo ottimizzare l'efficienza dello Studio, ma anche rafforzare la fiducia dei clienti, sempre più attenti alla tutela delle proprie informazioni. La vera sfida non è più se implementare l'AI, ma **quando e come** farlo. E chi saprà cogliere per tempo questa opportunità avrà un vantaggio competitivo concreto e duraturo.

Per saperne di più:

→ Cos'è il Cloud

→ Iaas, PaaS, Saas: tipi di Cloud e le loro applicazioni

→ Come il cloud può migliorare il lavoro nel tuo Studio di Commercialista

→ Gestire e garantire la sicurezza informatica anche con lo smart working

Capitolo 5

Strategie di sicurezza per gli Studi professionali

Garantire una solida sicurezza informatica non significa necessariamente affrontare spese proibitive o adottare strumenti complessi. Certo, un investimento iniziale è inevitabile, ma ciò che davvero conta è comprendere **quali tecnologie e strategie adottare** per massimizzare la protezione. Un approccio consapevole consente di prevenire incidenti che potrebbero comportare **danni economici ingenti** – si pensi, ad esempio, a un data breach e ai costi legati alla gestione dell'emergenza, alla perdita di fiducia da parte dei clienti e alle sanzioni per violazioni normative.

È fondamentale quindi essere sempre aggiornati sulle nuove tecniche utilizzate dai cybercriminali e sulle contromisure più efficaci per contrastarle.

Ma la sicurezza informatica non si limita solo all'adozione di strumenti e software: proteggere un'attività significa anche **riorganizzare il modo in cui si lavora**, adottare buone pratiche e, soprattutto, formare il personale. Un team preparato e attento, infatti, è una delle migliori difese contro gli attacchi informatici.

In questo capitolo analizzeremo dunque le **strategie di Cybersecurity più efficaci per gli Studi professionali**, nonché quelle anche più facilmente implementabili. L'obiettivo è fornire strumenti pratici e concreti per rafforzare la sicurezza informatica senza stravolgere l'operatività quotidiana. Perché investire in protezione oggi significa evitare problemi domani. E soprattutto, significa lavorare con la serenità di sapere che i dati dei propri clienti e la propria attività sono al sicuro.

5.1 Software di Cybersecurity: protezione avanzata per e-mail, siti web e infrastrutture IT

Abbiamo già parlato dell'importanza di adottare un **software per la Cybersecurity**, ma è fondamentale ribadire che questo strumento rappresenta una difesa indispensabile per proteggere i dati e mantenere il controllo della propria attività. Inoltre, l'**integrazione con l'AI** non fa che potenziarli e renderli ancor più efficaci per arginare possibili attacchi e reagire prontamente. Ma in che modo?

Un **buon software di Cybersecurity che integra l'Intelligenza Artificiale** deve poter garantire:

Analisi e prevenzione delle minacce sulle e-mail

Abbiamo già parlato di quanto le e-mail siano uno dei principali veicoli di attacco informatico. Un software avanzato di Cybersecurity utilizza algoritmi di Intelligenza Artificiale per analizzare in tempo reale il contenuto dei messaggi ricevuti ed è capace di individuare segnali sospetti come tentativi di phishing, link fraudolenti o allegati malevoli. Le minacce vengono, dunque, bloccate prima che possano raggiungere l'utente e in più si riduce il rischio di errori umani, per esempio mediante avvisi chiari quando un'e-mail appare pericolosa.

Protezione proattiva sui siti web

La sicurezza del proprio sito web e dei server è essenziale per evitare intrusioni e furti di dati. In questo contesto, il software si rivela prezioso perché effettua scansioni continue sulle pagine web e sull'infrastruttura digitale, individuando eventuali vulnerabilità sfruttabili da hacker, come falle nei plugin o punti deboli nel codice. Inoltre, offre strumenti di difesa automatizzati che bloccano tentativi di accesso non autorizzati e proteggono i dati dei clienti da eventuali esposizioni.

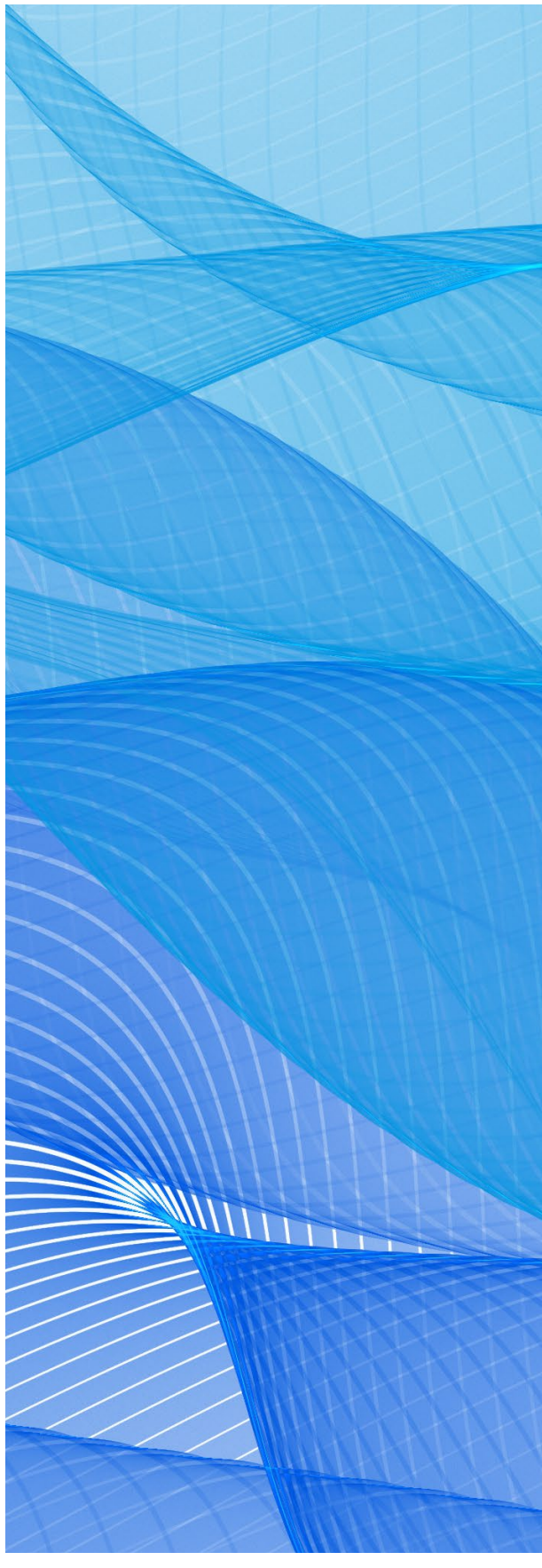
Monitoraggio e difesa dell'infrastruttura IT

Il sistema informatico di uno Studio professionale è spesso costituito da reti, dispositivi e database interconnessi: un'infrastruttura che un software di Cybersecurity dotato di AI può monitorare costantemente, per esempio mediante l'analisi dei comportamenti degli utenti e dei dispositivi connessi. In caso di attività anomale, come tentativi di accesso ripetuti o movimenti di dati insoliti, il sistema può intervenire automaticamente e bloccare l'azione sospetta con l'invio di avvisi agli amministratori.

Si tratta, quindi, di un investimento necessario e strategico, ma anche accessibile e misurato sulle reali esigenze dei Professionisti che ogni giorno lavorano con i dati dei propri clienti.

Infine, è importante evidenziare quanto questi software siano particolarmente adatti anche alle piccole realtà e agli Studi professionali, poiché non solo garantiscono una protezione completa dell'infrastruttura IT, ma sono anche **semplici da utilizzare**. Non richiedono infatti competenze tecniche avanzate, se non una formazione di base del personale, che, come vedremo a breve, rimane comunque un elemento essenziale per qualsiasi strategia di Cybersecurity efficace.

5.2 Backup e disaster recovery



Una solida strategia di Cybersecurity non può prescindere da un **sistema di backup efficace**, che consenta di conservare copie sicure dei dati e di recuperarli rapidamente in caso di perdita o compromissione. È, però, importante specificare che il backup, da solo, non è sufficiente a garantire la continuità operativa in caso di attacco informatico o guasto critico. È in questo contesto che bisogna introdurre il concetto di **disaster recovery**, cioè quell'insieme di piani e processi che consentono di **ripristinare rapidamente l'operatività aziendale** dopo un evento critico.

Un elemento centrale nella progettazione di un piano di disaster recovery è la definizione di due parametri fondamentali:

- il **Recovery Time Objective (RTO)**, ovvero il **tempo massimo accettabile di inattività** che lo Studio professionale può tollerare prima di tornare operativo. Un RTO ben definito consente di misurare l'impatto potenziale di un'interruzione dei servizi e di scegliere le tecnologie e i processi più adatti a contenerlo;

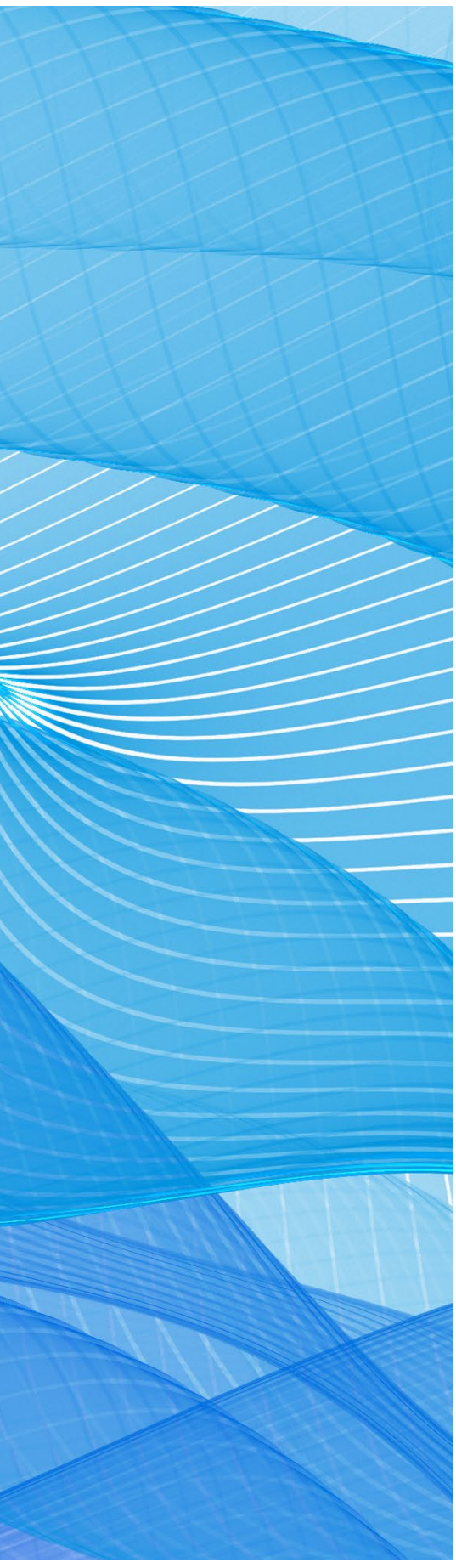
- il **Recovery Point Objective (RPO)**, che rappresenta la **quantità massima di dati che si può perdere**, misurata in tempo. Ad esempio, un RPO di 4 ore implica che l'organizzazione può accettare la perdita di al massimo 4 ore di dati.

Le moderne **soluzioni di backup e disaster recovery basate su Cloud** rappresentano una risposta particolarmente efficiente e sostenibile per i Professionisti. Queste tecnologie, infatti, offrono diversi vantaggi:

- **scalabilità**, che consente di adattare lo spazio e le risorse alle effettive esigenze dello Studio, senza investimenti iniziali onerosi;
- **accessibilità remota**, che permette di gestire i dati e ripristinarli anche da remoto o da altre sedi;
- **aggiornamenti e manutenzione automatica**, che riducono il carico di lavoro per il personale interno o per il consulente IT;
- **elevato livello di sicurezza**, grazie a crittografia dei dati, autenticazione a più fattori e monitoraggio continuo.

Inoltre, molte soluzioni Cloud offrono funzionalità avanzate come il ***versioning* dei file**, ossia il salvataggio di più versioni dello stesso documento, e il **test periodico dei backup**, utile per verificare che i dati siano realmente recuperabili in caso di necessità. Questo ultimo aspetto è spesso trascurato, ma fondamentale: **un backup non testato, infatti, è un backup potenzialmente inutile**.

Infine, va considerato anche l'aspetto **normativo e assicurativo**: un piano di disaster recovery ben documentato e aggiornato può costituire una **prova di diligenza** in caso di ispezioni o contenziosi, oltre a essere spesso richiesto dalle compagnie assicurative per la stipula di polizze cyber risk.



5.3 Protezione delle reti aziendali

Oltre all'utilizzo di software integrati con l'AI, una buona strategia di Cybersecurity si concretizza anche attraverso una serie di azioni fondamentali per proteggere la rete aziendale. Analizziamo, dunque, le principali misure di sicurezza da implementare per tutelare le infrastrutture informatiche dello Studio.

Crittografia dei dati

La crittografia è uno strumento essenziale per proteggere le informazioni sensibili, in quanto le trasforma in un formato illeggibile per chiunque non disponga della chiave di decrittazione. In questo senso, il sistema garantisce che, anche in caso di furto o intercettazione, i dati non possano essere utilizzati da malintenzionati. È fondamentale crittografare non solo i file archiviati sui server, ma anche le comunicazioni, come le e-mail e i trasferimenti di dati tra dispositivi e Cloud.

Utilizzo di una VPN

Una VPN (Virtual Private Network) è uno strumento indispensabile per proteggere la connessione a Internet, soprattutto quando si lavora da remoto o si utilizzano reti Wi-Fi pubbliche. Le VPN creano un tunnel crittografato tra il dispositivo e il server aziendale e contribuiscono a impedire agli hacker di intercettare le informazioni trasmesse. I dati, quindi, rimangono al sicuro anche al di fuori dell'ufficio e l'accesso a documenti riservati e applicazioni sensibili viene protetto efficacemente.

Installazione di anti-malware e antivirus

Per quanto possa apparire banale, un buon antivirus rimane la base della protezione informatica, posto che, per una difesa più efficace, è necessario affiancarlo a un software anti-malware avanzato. Mentre l'antivirus identifica e rimuove virus noti, infatti, l'anti-malware può garantire una protezione da minacce più sofisticate, come ransomware, spyware e trojan. Soluzioni di sicurezza aggiornate in tempo reale e basate sull'AI permettono di riconoscere anche varianti nuove di malware, bloccandole prima che possano causare danni.

Autenticazione a due fattori (2FA)

L'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza agli accessi, dal momento che, oltre alla password, richiede un secondo metodo di verifica, come un codice temporaneo generato da un'app o inviato via SMS. Questo sistema riduce drasticamente il rischio di accessi non autorizzati, anche nel caso in cui le credenziali vengano compromesse. Implementare la 2FA su tutti gli account aziendali, soprattutto quelli relativi ai dati sensibili, è una misura semplice ma estremamente efficace per proteggere l'intera infrastruttura IT.

5.4 Formazione del personale

Come abbiamo visto nei capitoli precedenti, molte minacce informatiche non si basano solo su vulnerabilità tecniche, ma sfruttano l'**errore umano** e la mancanza di consapevolezza. Tecniche come il phishing, gli attacchi di social engineering e il furto di credenziali mirano infatti a **ingannare gli utenti** per ottenere accesso a dati sensibili. Nemmeno il più avanzato software di Cybersecurity può garantire una protezione totale se chi lo utilizza non è in grado di interpretare correttamente gli avvisi di sicurezza o di adottare comportamenti adeguati a evitare rischi.

Per questo motivo, la **formazione del personale** rappresenta un elemento cardine di qualsiasi strategia di sicurezza informatica. Ogni collaboratore, indipendentemente dal ruolo, deve essere consapevole dei pericoli e sapere come comportarsi di fronte a possibili minacce.

In linea generale, è bene che Professionisti e collaboratori dello Studio siano formati su specifiche aree, che gli permettano di:

- **riconoscere tentativi di phishing e social engineering**, imparare a identificare e-mail sospette, link fraudolenti e richieste anomale di dati;
- **gestire in modo sicuro le credenziali**, utilizzare password complesse, comprendere l'importanza dell'autenticazione a due fattori e strumenti di password manager;
- **sfruttare procedure corrette per l'accesso e la condivisione dei dati** e, al contempo, evitare l'uso di dispositivi non autorizzati, limitare la condivisione di documenti sensibili e proteggere le reti Wi-Fi dello Studio;
- **saper rispondere agli incidenti di sicurezza**, segnalare tempestivamente attività sospette e sapere come comportarsi in caso di attacco.

La formazione può essere svolta attraverso **corsi, workshop interattivi, simulazioni di attacchi** (come test di phishing controllati) e aggiornamenti periodici sulle nuove minacce. Ciò che è importante è che diventi un'abitudine consolidata e parte integrante di una strategia che riconosce che un team informato è il miglior alleato nella protezione dei dati e nella costruzione di una sicurezza informatica davvero efficace.
Tali misure, se integrate in modo strategico, costituiscono un'efficace difesa contro molte delle minacce informatiche più comuni. Proteggere i sistemi dello Studio richiede una combinazione di tecnologie avanzate, pratiche operative e una cultura consapevole della sicurezza, elementi che insieme contribuiscono a creare un ambiente digitale sicuro e resiliente.

Per saperne di più:

→ Prevenire attacchi ransomware in azienda. Perché il backup dati non è sufficiente: 4 motivi

→ Certificato di Sicurezza (SSL): cos'è e perché averlo

→ Cos'è la 2FA e come funziona l'autenticazione a due fattori

Approfondimento

Il costo medio di una violazione dei dati

Investire nella sicurezza informatica è essenziale per proteggere gli Studi professionali dalle conseguenze devastanti di una violazione dei dati. Il costo medio globale di una violazione dei dati, infatti, è aumentato del 10% rispetto all'anno precedente, raggiungendo i 4,88 milioni di dollari.
Un incremento che non fa che sottolineare l'importanza di adottare misure preventive efficaci.

L'implementazione di soluzioni basate sull'Intelligenza Artificiale e sull'automazione nella sicurezza ha dimostrato di ridurre significativamente i costi associati alle violazioni.
Le organizzazioni che hanno adottato ampiamente queste tecnologie, infatti, hanno risparmiato in media 2,22 milioni di dollari rispetto a quelle che non lo hanno fatto.
L'investimento in strumenti avanzati si traduce, dunque, in un notevole vantaggio economico.

È significativo notare, inoltre, che il 75% dell'aumento dei costi medi di una violazione è attribuibile alle perdite operative e alle attività di risposta post-incidente. Ciò indica che una preparazione adeguata e piani di risposta efficaci possono mitigare in modo drastico l'impatto finanziario di una violazione.
Investire nella preparazione alla risposta post-violazione significa, quindi, ridurre le perdite economiche e, al contempo, preservare la reputazione aziendale e la fiducia dei clienti.

Conclusioni

Commercialisti, Consulenti del Lavoro e Studi professionali sono alle prese con enormi cambiamenti che richiedono un adeguamento continuo e nuove strategie di difesa. Questo vale, come abbiamo potuto vedere, anche per quanto riguarda la **sicurezza e protezione dei dati e delle reti.**

Ma se da un lato si ha a che fare con tecniche e attacchi informatici sempre più sofisticati, dall'altro le nuove tecnologie consentono di aumentare le proprie barriere protettive, in un'ottica di miglioramento continuo e crescita della fiducia da parte dei clienti.

Gli Studi professionali che comprendono il valore di tecnologie e strumenti come **i software di Cybersecurity,** si trovano un passo avanti nella gestione sicura delle informazioni e avranno la possibilità di proteggersi da attacchi sempre più sofisticati, con una drastica riduzione dei rischi legati a violazioni e perdite di dati.

Mentre i metodi di protezione tradizionali si basavano su azioni reattive – che prevedevano cioè di intervenire dopo che un attacco era già avvenuto – le soluzioni di Cybersecurity avanzate utilizzano un approccio **predittivo e preventivo**. Software avanzati analizzano continuamente il comportamento degli utenti, delle reti e dei dispositivi, sono in grado di riconoscere anomalie e intervenire in automatico per bloccare possibili attacchi prima che possano compromettere dati e sistemi.

Questo significa che gli Studi professionali possono contare su un sistema di difesa attivo, in grado di rispondere immediatamente a qualsiasi tentativo di intrusione. La protezione dei dati non è più un elemento da gestire solo in caso di emergenza, ma un **processo continuo e costante**, integrato nella routine quotidiana dell'attività professionale.

Bisogna, però, essere coscienti che gli investimenti in Cybersecurity hanno anche un'altra fondamentale funzione: rappresentano un **fattore chiave per distinguersi nel mercato e costruire un vantaggio competitivo.** Uno Studio che adotta strategie di sicurezza informatica avanzate tutela i propri dati, così come quelli dei clienti e, in questo modo, trasmette un'**immagine di affidabilità e serietà**.

Oggi più che mai, la fiducia è un elemento essenziale nel mondo professionale. Clienti e aziende cercano partner affidabili, capaci anche di garantire la protezione delle proprie informazioni sensibili. Uno Studio che dimostra di avere un **piano di sicurezza solido**, un sistema di protezione avanzato e un team formato e consapevole delle minacce informatiche si posiziona, dunque, come un **punto di riferimento nel proprio settore**.

Vale la pena aggiungere, inoltre, che investire in Cybersecurity significa anche **evitare costi imprevisti legati a violazioni dei dati** e multe per mancato rispetto delle normative. Tutto ciò consente di lavorare con maggiore serenità ed essere certi di aver compiuto tutti gli sforzi possibili per ridurre i rischi e non perdere efficienza operativa.

In sostanza, possiamo dire che la Cybersecurity non deve essere vista come una spesa, ma come un **investimento che garantisce stabilità, continuità operativa e crescita**. Qualcosa che permette sia di evitare problemi sia di creare nuove opportunità, dal momento che la sicurezza informatica diventa un valore aggiunto che rafforza la **reputazione e la competitività dello Studio.**

Il futuro della professione passa attraverso la capacità di adattarsi e innovarsi. Proteggere i dati, formare il personale e adottare strumenti avanzati di Cybersecurity sono azioni che permettono di guardare avanti con fiducia. Con le giuste strategie, la sicurezza diventa non solo un dovere, ma una leva per il successo.

Per saperne di più:

→ Digital trust: cos'è e perché è importante costruirla

→ Personalizzazione dei servizi digitali (e non) per il Consulente del Lavoro: come distinguersi

Glossario

2FA (Two-Factor Authentication) È un metodo di accesso che richiede due livelli di verifica, ad esempio una password e un codice inviato via SMS. Serve ad aumentare la sicurezza degli account, rendendo più difficile l'accesso non autorizzato anche in caso di furto delle credenziali.

Accountability Indica la responsabilità attiva e documentabile di chi gestisce i dati personali. Chi tratta i dati deve non solo rispettare le normative (come il GDPR), ma anche dimostrare concretamente di aver adottato misure adeguate a proteggerli.

Allegati malevoli Sono file infetti che possono nascondere virus, trojan o altri malware. Spesso vengono inviati via e-mail fingendosi documenti legittimi per indurre l'utente ad aprirli e attivare involontariamente un attacco informatico.

Algoritmi di machine learning Si tratta di modelli matematici usati per "insegnare" a un sistema informatico a riconoscere schemi, imparare da esperienze passate e migliorare nel tempo, ad esempio per individuare minacce informatiche prima che causino danni.

Antivirus È un software progettato per rilevare, bloccare e rimuovere virus informatici e altri programmi dannosi. È una delle soluzioni base per proteggere i dispositivi.

Anti-malware Simile all'antivirus, ma più completo. È progettato per individuare un ampio spettro di software malevoli, inclusi spyware, ransomware e trojan.

Autenticazione a due fattori È una misura di sicurezza che aggiunge un secondo passaggio all'accesso (oltre alla password), come un codice temporaneo. Rende molto più difficile per i cybercriminali entrare in un sistema.

Backup Il backup consiste nel salvare una copia dei dati in un luogo sicuro, così da poterli recuperare in caso di guasto, cancellazione accidentale o attacco informatico.

Cloud computing È l'utilizzo di risorse informatiche (come archiviazione e software) via internet, senza dover installare fisicamente nulla sul proprio dispositivo. È comodo, scalabile e spesso più sicuro.

Compliance Termine che indica il rispetto di leggi, regolamenti e standard (come il GDPR) da parte di aziende e professionisti.

Criptovalute Sono valute digitali come Bitcoin, utilizzate online. A volte vengono richieste come riscatto nei casi di attacchi ransomware, perché difficili da tracciare.

Crittografia Tecnologia che trasforma i dati in un formato illeggibile per chi non possiede la chiave giusta. Serve per proteggere le informazioni da accessi non autorizzati.

Cyber risk È il rischio legato a danni causati da attacchi informatici, come perdita di dati, blocco dei sistemi o furti di informazioni.

Cybercrime Criminalità digitale: comprende tutti i reati informatici, dai furti di dati agli attacchi ai server.

Cybersecurity L'insieme delle pratiche, tecnologie e strumenti che servono a proteggere i sistemi informatici da attacchi e minacce esterne.

Data breach È una violazione dei dati personali, che può avvenire per errore o a causa di un attacco. I dati rubati o esposti possono causare gravi danni economici e reputazionali.

Database Un archivio digitale dove vengono conservati dati organizzati, accessibili e modificabili attraverso software specifici.

Deepfake Contenuti audio o video falsificati tramite AI, spesso molto realistici, usati per ingannare o manipolare.

Disaster recovery Insieme di strategie e strumenti per ripristinare dati e sistemi dopo un evento critico (es. attacco ransomware o guasto tecnico).

DPIA (Data Protection Impact Assessment) È una valutazione formale dell'impatto che un trattamento dati può avere sulla privacy delle persone. È obbligatoria in alcuni casi previsti dal GDPR.

Glossario

DPO (Data Protection Officer) Figura professionale esperta in protezione dei dati che affianca aziende e studi professionali nel garantire il rispetto della normativa privacy.

Firewall intelligenti Strumenti evoluti che analizzano il traffico in entrata e in uscita da una rete per bloccare attività sospette, adattandosi automaticamente alle nuove minacce.

GDPR (General Data Protection Regulation) Regolamento europeo che impone regole chiare sul trattamento dei dati personali e prevede forti sanzioni in caso di violazioni.

Hacker Chi accede (legalmente o illegalmente) a sistemi informatici. Spesso è usato per indicare i cybercriminali che violano la sicurezza dei dati.

Incidenti di sicurezza Eventi che compromettono la riservatezza, l'integrità o la disponibilità di sistemi o dati, come furti, virus o accessi non autorizzati.

Informativa privacy Documento che informa gli utenti su come vengono raccolti, trattati e protetti i loro dati personali.

IT Infrastructure Tutte le componenti tecniche (hardware, software, reti) che costituiscono l'infrastruttura tecnologica di un'organizzazione.

Intelligenza Artificiale Tecnologia che consente ai computer di compiere azioni "intelligenti", come analizzare dati, prevedere comportamenti e riconoscere anomalie.

ISMS (Information Security Management System) Sistema organizzativo per gestire in modo strutturato la sicurezza delle informazioni, spesso certificato tramite la norma ISO 27001.

ISO 22301 Standard che definisce come garantire la continuità operativa anche in situazioni di emergenza (es. attacchi informatici).

ISO 27001 Norma internazionale che stabilisce i requisiti per un efficace sistema di gestione della sicurezza delle informazioni.

ISO 9001 Standard che certifica la qualità nella gestione aziendale e dei processi.

Link fraudolenti Collegamenti ingannevoli che portano a siti pericolosi, usati per truffare o infettare con malware.

Machine learning Sottoinsieme dell'AI che consente ai sistemi di imparare automaticamente dai dati, migliorando nel tempo le proprie performance.

Malware Qualsiasi tipo di software dannoso, incluso virus, ransomware, spyware, progettato per danneggiare o controllare un sistema.

Pattern dannosi Comportamenti o schemi ricorrenti associati ad attività sospette o malevole in ambito informatico.

PEC (Posta Elettronica Certificata) Sistema italiano di posta elettronica che garantisce il valore legale dell'invio e della ricezione dei messaggi.

Phishing Tecnica di truffa in cui si inviano e-mail o messaggi falsi per rubare dati sensibili come password o numeri di carta.

Plugin Componente aggiuntivo che si installa su un programma per estenderne le funzionalità (es. un'estensione per un browser).

Privacy by design Principio secondo cui la protezione dei dati deve essere integrata fin dall'inizio nella progettazione di sistemi e processi.

Privacy by default Principio che prevede impostazioni predefinite orientate alla massima tutela della privacy dell'utente.

Ransomware Tipo di malware che cripta i dati e li rende inaccessibili, chiedendo un riscatto per sbloccarli.

Recovery Point Objective (RPO) Indica quanta perdita di dati è accettabile (es. fino a 4 ore di dati persi) in caso di incidente.

Recovery Time Objective (RTO) Definisce entro quanto tempo i sistemi devono essere ripristinati dopo un'interruzione.

Glossario

Registro dei trattamenti Documento obbligatorio in cui si descrivono tutte le attività di trattamento dei dati personali svolte all'interno di un'organizzazione.

Responsabilità civile Obbligo legale di risarcire danni causati ad altre persone, anche in caso di violazione della privacy.

SaaS, PaaS, IaaS (modelli di Cloud) Diversi modelli di servizio Cloud: SaaS (software online), PaaS (piattaforme per sviluppare app), IaaS (infrastrutture come server virtuali).

Sanctions (sanzioni) Penalità economiche o legali previste per chi viola le normative sulla protezione dei dati.

Smart working Modalità di lavoro da remoto, flessibile, basata su tecnologie digitali.

Smishing Forma di phishing via SMS: messaggi ingannevoli che spingono a cliccare su link o fornire dati.

Social engineering Tecniche di manipolazione psicologica per ingannare le persone e ottenere accesso a informazioni riservate.

Software gestionale Strumento informatico per automatizzare e organizzare le attività di uno Studio, come contabilità, scadenze e fatturazione.

Software pirata Versioni illegali di software, spesso alterate e rischiose perché possono contenere malware.

Spam Messaggi indesiderati, spesso pubblicitari o dannosi, inviati in massa via e-mail.

Spyware Software che raccoglie informazioni sull'utente in modo nascosto, spesso per scopi illeciti.

Trojan Tipo di malware che si nasconde in un software apparentemente legittimo, pronto a danneggiare o spiare il sistema.

URL sospetti Indirizzi web poco affidabili o fraudolenti, spesso usati per attacchi phishing o malware.

User-friendly Indica software o interfacce facili da usare, pensate anche per utenti non esperti.

VPN (Virtual Private Network) Tecnologia che crea una connessione sicura e criptata tra il dispositivo dell'utente e internet, proteggendo la privacy online.

Web application Applicazioni accessibili via browser (es. siti per la gestione contabile), che devono essere protette da attacchi specifici.

Fonti

- **Pedago.it**
  https://www.pedago.it/blog/cyber-security-studio-professionale.htm

- **Intelligenzaartificiale.it**
  https://www.intelligenzaartificiale.it/sicurezza-informatica-e-intelligenza-artificiale/

- **Clusit.it**
  https://clusit.it/rapporto-clusit/

- **Agendadigitale.eu**
  https://www.agendadigitale.eu/sicurezza/commercialisti-la-difesa-dagli-hacker-passa-per-la-compliance-normativa/

  https://www.agendadigitale.eu/sicurezza/privacy/professionisti-e-privacy-breve-guida-agli-adempimenti/

- **Cybersecurity360.it**
  https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/

- **Learn.microsoft.com**
  https://learn.microsoft.com/it-it/security/ransomware/human-operated-ransomware

- **Ordinearchitetti.ge.it**
  https://ordinearchitetti.ge.it/principali-adempimenti-in-materia-di-privacy-per-gli-studi-professionali/

- **Advisera.com**
  https://advisera.com/27001academy/it/che-cose-la-iso-27001/

- **Gsmitalia.it**
  https://www.qmsitalia.it/certificazione-iso-27001-cose-e-perche-e-indispensabile/

- **Corrierecomunicazioni.it**
  https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-e-reti-aziendali-9-azioni-per-proteggere-i-dati/

OFFICINE BONFIGLIOLI

TeamSystem

VERS.01 - DIC.2025

teamsystem.com