

Security Testing: analisi critica della Legge 90/2024 e le sue implicazioni sulla cybersecurity in Italia



La cybersicurezza è un tema sempre più rilevante nel panorama italiano e internazionale. Con l'entrata in vigore della **Legge 90/2024** e la **NIS 2**, che richiedono un adeguamento normativo e operativo per una gestione efficiente dei rischi informatici, sono state introdotte nuove disposizioni in materia di sicurezza informatica, con impatti significativi sulle aziende, le pubbliche amministrazioni e gli esperti di cybersecurity.

Uno degli aspetti più dibattuti riguarda il **security testing legittimo**. Se da un lato la legge mira a rafforzare la protezione contro le minacce informatiche, dall'altro solleva dubbi sulle implicazioni per i professionisti della sicurezza IT, in particolare per coloro che si occupano di **penetration testing, vulnerability assessment e red teaming**.

In questo articolo analizzeremo in dettaglio le disposizioni della Legge 90/2024 e di derivazione euro-unitaria in tema di cyber sicurezza, i loro effetti sulla cybersecurity in Italia e le possibili criticità legate all'applicazione della normativa in contesti di security testing.

Cos'è il Security Testing e perché è fondamentale

Il **security testing** è l'insieme delle pratiche e delle metodologie utilizzate per testare la resistenza di sistemi

informatici e reti ad eventuali attacchi. Le attività più comuni includono:

- **Penetration testing (pentesting):** simulazione di attacchi informatici per identificare vulnerabilità sfruttabili da cybercriminali;
- **Vulnerability assessment:** scansione dei sistemi per individuare falle di sicurezza;
- **Red teaming:** esercitazioni avanzate che coinvolgono un team di esperti incaricati di simulare un attacco reale per valutare la capacità di difesa di un'organizzazione.

Queste pratiche sono essenziali per prevenire violazioni dei dati, proteggere le infrastrutture critiche e garantire la compliance alle normative nazionali e internazionali sulla sicurezza informatica.

La Legge 90/2024: Panoramica, introduzioni e obiettivi

La **Legge 90/2024**, entrata in vigore il **17 luglio 2024**, introduce nuovi obblighi per le **pubbliche amministrazioni** e per le **aziende private che operano in settori critici**. L'obiettivo principale della normativa è creare un quadro comune per la gestione della sicurezza informatica, promuovendo la collaborazione tra settore pubblico e privato.

In una visione più ampia e approfondita, il reale scopo della Legge sembra essere quello di concedere alle Pubbliche Amministrazioni centrali ed essenziali più tempo per adeguarsi agli standard imposti dalla **Direttiva (UE) 2022/2555**, su citata, nota appunto come '**Direttiva NIS 2**'. Questo è particolarmente rilevante considerando che le P.A. tendono storicamente a essere meno reattive e tempestive nell'adattarsi ai cambiamenti, anche a causa delle limitate risorse economiche a loro disposizione, come verrà approfondito successivamente.

È comunque fondamentale sottolineare che, già prima dell'entrata in vigore di questa normativa, l'adozione di misure di sicurezza informatica, sia tecniche che organizzative, adeguate a rischi in continua evoluzione, non solo rappresentava un obbligo legale sancito principalmente dal GDPR ma costituiva anche una responsabilità essenziale nei confronti dei cittadini e della tutela dei loro dati personali.

La legge si applica principalmente a due categorie di enti che possiamo definire come:

1. **Primo Cluster:** Pubbliche Amministrazioni centrali ed enti essenziali (es. ministeri, regioni, province autonome, città metropolitane);
2. **Secondo Cluster:** Enti locali di grandi dimensioni (es. comuni con oltre 100.000 abitanti, aziende sanitarie locali, società di trasporto pubblico urbano).

L'inclusione delle ASL risulta particolarmente rilevante, considerando che in precedenza non erano state inserite nel Perimetro di Sicurezza Nazionale Cibernetica previsto dal D.L. 105/2019, nonostante siano spesso tra i principali bersagli degli attacchi informatici, anche a causa della cronica carenza di fondi che le affligge.

Un esempio recente che evidenzia la vulnerabilità del settore sanitario è l'attacco ransomware, presumibilmente di matrice filorussa, che ha colpito il National Health Service (NHS) di Londra, causando gravi ripercussioni sulla salute dei pazienti in condizioni più critiche.

Questi enti devono rispettare obblighi stringenti per la protezione delle infrastrutture informatiche e segnalare tempestivamente eventuali **incidenti di sicurezza**.

Obblighi e Scadenze

- Le PA del primo cluster hanno dovuto conformarsi

immediatamente;

- Gli enti del secondo cluster invece, hanno avuto tempo fino al **17 gennaio 2025** per adeguarsi;
- Obbligo di segnalazione degli incidenti informatici con sanzioni da **25.000 a 125.000 euro** in caso di mancata notifica.

È inoltre fondamentale sottolineare che l'omessa segnalazione di un incidente informatico può comportare responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti coinvolti.

Le sanzioni previste entrano in gioco solo in caso di reiterata inosservanza dell'obbligo di notifica, lasciando all'ACN (Agenzia per la Cybersicurezza Nazionale) il compito di valutarne la gravità. Questo approccio risulta senza dubbio più indulgente rispetto, ad esempio, alle sanzioni applicabili ai soggetti privati secondo il GDPR.

Questa differenza può essere giustificata dal fatto che la normativa in questione è stata introdotta con una **clausola di invarianza finanziaria** e si rivolge principalmente, anche se non esclusivamente, alle pubbliche amministrazioni, le quali operano con vincoli di bilancio stringenti.

Gli enti soggetti alla Legge in esame saranno tenuti a istituire una Struttura dedicata alla cybersecurity, che potrà essere individuata tra quelle già esistenti o, se presente, all'interno dell'ufficio del Responsabile della Transizione Digitale (RTD).

È probabile che molti enti optino per l'accorpamento di questa nuova struttura con uffici già esistenti, soprattutto perché dovrà essere istituita senza costi aggiuntivi, utilizzando esclusivamente le risorse umane, strumentali e finanziarie già disponibili.

Questa limitazione rappresenta una delle principali criticità della normativa, poiché un obiettivo così ambizioso avrebbe

richiesto uno stanziamento di fondi dedicato per garantire un reale rafforzamento della sicurezza informatica. Senza risorse aggiuntive, il rischio è che si tratti di una semplice riorganizzazione interna piuttosto che di un effettivo potenziamento delle capacità di difesa cyber degli enti coinvolti.

Sono tuttavia esentati dall'obbligo di istituire tale Struttura gli organi dello Stato responsabili della prevenzione, accertamento e repressione dei reati, della tutela dell'ordine e della sicurezza pubblica, nonché della difesa e sicurezza militare, comprese le Agenzie di intelligence.

Per completare e rafforzare la Struttura per la cybersecurity, la Legge prevede che gli enti destinatari nominino un **Referente** per la Cybersecurity.

Questa figura può essere assegnata a:

- **Il Responsabile della Transizione Digitale (RTD)**, se già individuato, il che comporterebbe un significativo aumento delle sue responsabilità;
- **Il Referente per la cybersecurity** di un altro ente pubblico, previa approvazione e autorizzazione dell'ente di appartenenza;
- **Un Referente condiviso tra più enti**, attraverso una gestione associata della funzione.

L'introduzione di queste modalità alternative di nomina è particolarmente utile considerando che anche questo incarico deve essere attribuito senza ulteriori costi aggiuntivi. Di conseguenza, la scelta ricadrà probabilmente su dipendenti già in forza presso le Pubbliche Amministrazioni coinvolte.

Tuttavia, come già evidenziato, il vincolo dell'invarianza finanziaria potrebbe ostacolare il raggiungimento degli obiettivi della legge, specialmente per le ASL, che da sempre dispongono di budget limitati per investire in cybersecurity e

ICT.

Inoltre, la normativa stabilisce che il Referente debba possedere competenze ed esperienza nel campo della sicurezza informatica, demandando però all'ente la responsabilità di valutare l'idoneità del candidato. Questo implica che la selezione dovrà basarsi su titoli di studio, master, certificazioni e precedenti esperienze lavorative nel settore, senza però poter procedere con nuove assunzioni o affidamenti esterni, almeno fino all'adozione di un nuovo bilancio consolidato.

Una delle novità più rilevanti introdotte dalla Legge è l'istituzione del **Centro Nazionale di Crittografia** (CNC) presso l'**Agenzia per la Cybersicurezza Nazionale** (ACN).

Il CNC, il cui funzionamento sarà definito da un provvedimento del Direttore Generale dell'ACN, avrà il compito di sviluppare e implementare soluzioni crittografiche avanzate per la protezione dei dati e di promuovere l'adozione di tecnologie di cifratura a supporto della cybersecurity nazionale.

In quest'ottica, il CNC favorirà la collaborazione con università e centri di ricerca per sviluppare nuovi algoritmi proprietari e rafforzare le competenze crittografiche nazionali. L'obiettivo è anche quello di potenziare l'autonomia e l'indipendenza industriale e tecnologica dell'Italia, riducendo la dipendenza da soluzioni sviluppate all'estero.

Uno dei temi più delicati che il CNC potrebbe dover affrontare riguarda il difficile bilanciamento tra la libera accessibilità a tecnologie crittografiche avanzate e le problematiche che queste pongono alle attività di forze dell'ordine, polizia e servizi di intelligence. La crittografia, infatti, se da un lato è fondamentale per la sicurezza informatica, dall'altro può rappresentare un ostacolo spesso insormontabile per le indagini e il contrasto

alle minacce digitali.

Un'altra innovazione significativa introdotta dalla normativa riguarda i contratti pubblici per la fornitura di beni e servizi ICT destinati a contesti strategici per la sicurezza nazionale.

In questi ambiti, i contratti dovranno rispettare specifici requisiti di cybersicurezza, che saranno definiti tramite un Decreto del Presidente del Consiglio dei ministri (DPCM), su proposta dell'ACN e con il parere del Comitato sulla sicurezza della Repubblica. Questo decreto dovrà essere emanato entro quattro mesi dall'entrata in vigore della Legge.

L'obbligo interesserà:

- **Pubbliche amministrazioni;**
- **Gestori di servizi pubblici;**
- **Società a controllo pubblico (escluse le quotate in borsa);**
- **Soggetti privati nel Perimetro di Sicurezza Nazionale Cibernetica.**

Per elementi essenziali di cybersecurity, la legge intende un insieme di criteri e regole tecniche per garantire confidenzialità, integrità e disponibilità dei dati, in proporzione ai rischi per la sicurezza nazionale.

Questa normativa punta a rafforzare la resilienza informatica della supply chain, imponendo ai fornitori e agli appaltatori della PA standard di sicurezza più elevati rispetto a quelli finora richiesti. Sarà interessante confrontare i requisiti previsti dal futuro DPCM con le clausole contrattuali standard europee (SCC) e con gli accordi di protezione dati (DPA) più avanzati nel settore ICT e SaaS.

Cosa accade in caso di incidente informatico?

Innanzitutto, occorre chiarire che con incidente informatico

ci si riferisce ad un evento, intenzionale o accidentale, che compromette la **confidenzialità, integrità o disponibilità** di reti, sistemi informativi o dati.

La Struttura per la cybersecurity e il Referente per la cybersecurity saranno tenuti a segnalare gli incidenti informatici utilizzando la procedura telematica già disponibile sul sito dell'Agenzia per la Cybersicurezza Nazionale, in modo analogo a quanto avviene per le notifiche di violazioni dei dati personali tramite il portale del Garante Privacy.

L'obbligo di segnalazione e notifica degli incidenti si basa sui criteri definiti nella Determina del Direttore Generale dell'ACN del 3 gennaio 2023. In particolare, l'art. 1, lett. f) della Determina definisce gli incidenti informatici come eventi, accidentali o intenzionali, che causano malfunzionamenti, interruzioni (anche parziali), compromissioni o utilizzi impropri di reti, sistemi informativi o servizi digitali.

L'Allegato A della Determina fornisce un elenco dettagliato degli incidenti soggetti a notifica, suddividendoli in diverse categorie, tra cui:

- **Accesso iniziale da parte di soggetti non autorizzati;**
- **Esecuzione di codice dannoso;**
- **Installazione di software malevolo;**
- **Movimenti laterali all'interno della rete;**
- **Azioni sugli obiettivi e attività di spear phishing.**

Si tratta, dunque, di incidenti di sicurezza distinti dalle violazioni di dati personali previste dall'art. 33 del GDPR. Tuttavia, un singolo evento potrebbe contemporaneamente rientrare in entrambe le casistiche, generando così un doppio obbligo di notifica, sia nei confronti del CSIRT dell'ACN (come previsto dalla normativa italiana sulla cybersecurity), sia nei confronti del Garante Privacy (in base al GDPR).

Implicazioni ed effetti della Legge 90/2024 sul Security Testing

L'introduzione della Legge 90/2024 ha suscitato preoccupazioni tra i professionisti della sicurezza informatica, in particolare per il modo in cui le disposizioni potrebbero limitare le attività di security testing.

Vediamo di seguito quali sono allora questi aspetti interessati:

1. Maggiori Restrizioni sulle Attività di Testing:

Uno dei punti critici della legge è la possibile criminalizzazione di alcune attività di **penetration testing** e di **ethical hacking**, se non autorizzate esplicitamente dagli enti interessati. Questo potrebbe rendere più difficile per gli esperti di cybersecurity condurre test proattivi per identificare vulnerabilità.

2. Ambiguità nella Distinzione tra Attività Lecite e Illecite:

Il testo della legge non chiarisce completamente la distinzione tra attività **etiche** e **maliziose**. Ad esempio, un esperto di cybersecurity che individua una vulnerabilità e la segnala senza un'autorizzazione formale potrebbe teoricamente essere perseguito.

3. Impatti sulle Aziende e Sui Professionisti della Sicurezza:

Le aziende che si occupano di security testing potrebbero essere costrette a **rivedere le proprie pratiche** per evitare sanzioni. Alcuni esperti temono che la normativa possa ostacolare il lavoro di chi si occupa di **bug bounty programs** o di **ricerca indipendente sulla sicurezza informatica**.

Possibili soluzioni e miglioramenti alla normativa

Affinché la Legge 90/2024 non diventi un freno per il settore della sicurezza informatica, sarebbe utile e necessario introdurre alcuni **correttivi**:

1. Chiarire il Ruolo del Security Testing:

- Definire esplicitamente cosa costituisce un'attività lecita di **security testing**.
- Garantire che gli **ethical hacker** non vengano perseguiti giudizialmente per attività condotte in buona fede.

2. Creare un Quadro Regolatorio per i Penetration Tester:

- Introdurre un **registro nazionale di penetration tester certificati**, con linee guida precise per le attività autorizzate.
- Stabilire un processo chiaro per ottenere permessi di testing senza eccessiva burocrazia.

3. Incentivare la Collaborazione tra Enti Pubblici e Ricercatori:

- Creare canali ufficiali per la **segnalazione delle vulnerabilità** da parte di esperti indipendenti.
- Promuovere programmi di **bug bounty pubblici** per incentivare la ricerca etica sulla sicurezza.

Conclusioni

La **Legge 90/2024** rappresenta un passo avanti nella protezione delle infrastrutture critiche italiane, ma solleva importanti interrogativi per i professionisti della cybersecurity.

Per garantire che la normativa favorisca realmente la sicurezza informatica senza ostacolare il security testing legittimo, è fondamentale che il legislatore fornisca chiarimenti e implementi misure che permettano ai professionisti del settore di continuare a svolgere il proprio

lavoro in modo etico e conforme alla legge.

Il dibattito su queste tematiche è aperto e nei prossimi mesi saranno cruciali eventuali interventi normativi o regolamenti attuativi che possano risolvere le attuali criticità. La cybersecurity in Italia deve essere rafforzata, ma senza limitare il contributo di chi lavora ogni giorno per renderla più sicura.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/security-testing-legge-90-2024/>