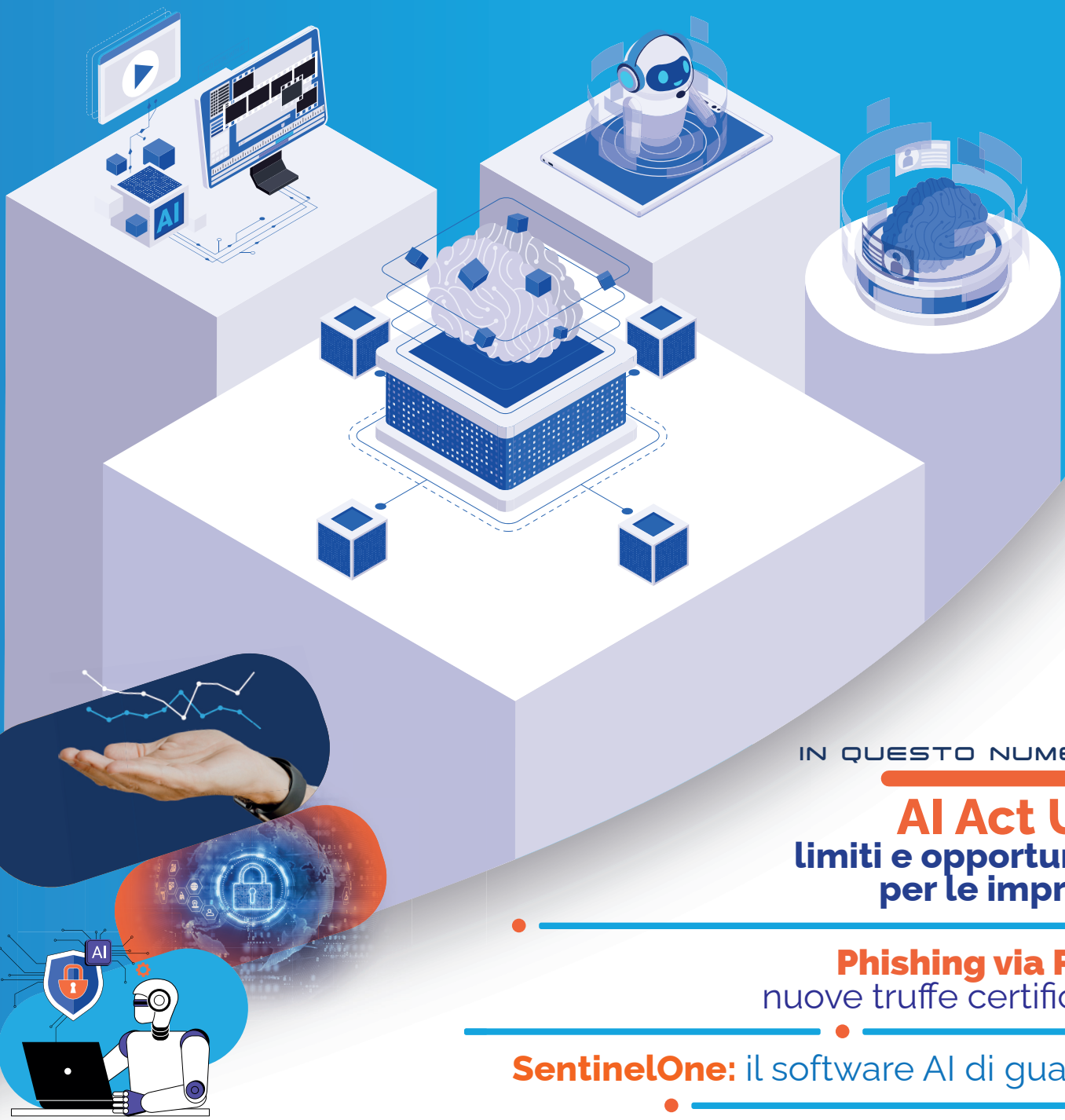
IT•NEWS

N. 25 MAG./GIU. 2025

L'indispensabile road-book
per rendere sempre più digitale e competitiva la tua impresa



IN QUESTO NUMERO

L'EDITORIALE

A cura di **Alessio Angioli**

AI Act UE

Limiti e opportunità per le imprese

Con l'entrata in vigore, il 2 febbraio 2025, delle prime disposizioni vincolanti del Regolamento Europeo sull'Intelligenza Artificiale (AI Act), prende forma un framework normativo strutturato sulla Base del Rischio (Risk-Based), con l'obiettivo di **armonizzare l'approccio europeo allo sviluppo e all'impiego dell'AI**, tutelando sicurezza, diritti fondamentali e trasparenza algoritmica.

AI - Classificazione del rischio

Il regolamento segmenta i sistemi di intelligenza artificiale in quattro classi di rischio, con obblighi progressivamente più stringenti:

CATEGORIA	DESCRIZIONE	OBBLIGHI
RISCHIO INACCETTABILE	Sistemi con impatti critici su diritti umani e sicurezza (es. social scoring, sorveglianza biometrica abusiva)	**Divieto assoluto di utilizzo, sviluppo e commercializzazione**
RISCHIO ELEVATO	AI in settori regolamentati e critici: sanità, giustizia, trasporti, finanza, istruzione	Requisiti di conformità, valutazioni d'impatto, gestione del rischio
RISCHIO LIMITATO	Interfacce utente (es. chatbot) e AI generativa	Obbligo di trasparenza e disclosure verso l'utente finale
RISCHIO MINIMO O NULLO	Applicazioni a basso impatto (filtri spam, AI nei videogiochi)	Nessun obbligo specifico

I·TEAM

Pratiche vietate dal 2 febbraio 2025

I seguenti impieghi dell'AI sono considerati **non conformi** all'ordinamento europeo:

- Manipolazione psicologica occulta o subliminale
- Sfruttamento di vulnerabilità (età, disabilità, status sociale)
- Profilazione predittiva del comportamento criminale
- Riconoscimento emozionale in ambienti scolastici e lavorativi
- Creazione di database biometrici da fonti non autorizzate
- Classificazioni biometriche discriminatorie (es. etnia, religione, orientamento sessuale)
- Riconoscimento facciale in tempo reale in spazi pubblici, salvo eccezioni giudiziarie circoscritte

Obblighi per i fornitori di sistemi a Rischio Elevato

Le imprese che sviluppano o integrano sistemi IA a Rischio Elevato sono tenute a:

- Implementare **sistemi di gestione del rischio** e **controlli di qualità**
- Eseguire **valutazioni di impatto sui diritti fondamentali**
- Garantire la **tracciabilità dei dati e delle decisioni automatizzate**
- Predisporre **documentazione tecnica dettagliata**
- Notificare i sistemi alle autorità nazionali competenti (ancora non definite in Italia)

Timeline attuativa

Febbraio 2025
Avvio divieti per AI a rischio inaccettabile

Agosto 2025
Inizio applicazione degli obblighi per i **modelli di AI generali** (GPAI – General Purpose Artificial Intelligence)

Agosto 2027
Entrata in vigore delle norme per i sistemi AI integrati in prodotti regolati

Sanzioni previste

VIOLAZIONE	IMPORTO MASSIMO
Pratiche vietate o violazioni su dati	Fino a **35 milioni €** o **7% del fatturato globale**
Altri obblighi dell'AI Act	Fino a **15 milioni €** o **3% del fatturato globale**
Informazioni incomplete o false	Fino a **7,5 milioni €** o **1,5% del fatturato globale**
PMI: applicazione della soglia **più bassa** tra quelle indicate	
Grandi imprese: applicazione della **soglia più alta**	

Cosa deve fare un'impresa che adotta l'AI?

- **Mappatura interna** dei sistemi AI esistenti e futuri
- **Identificazione del livello di rischio secondo la classificazione AI Act**
- **Verifica dell'allineamento normativo con AI Act, GDPR, NIS2**
- **Adeguamento dei processi di audit, documentazione formazione**
- **Valutazioni d'impatto proattive su privacy e diritti digitali**

L'APPROFONDIMENTO DEL MESE

PHISHING VIA PEC
nuove truffe certificate

A cura di
Marco Cecchi

La PEC (Posta Elettronica Certificata) sono ormai parte integrante della vita delle aziende italiane e, data la percezione di grande sicurezza, è usata comunemente e tranquillamente per inviare comunicazioni ufficiali, documenti sensibili e, soprattutto, le fatture elettroniche. Proprio per questo, la PEC è diventata un bersaglio privilegiato per i cybercriminali, che cercano di spingere le aziende a inviare dati riservati o a effettuare bonifici verso conti bancari fraudolenti, attraverso falsi messaggi che imitano perfettamente la corrispondenza ufficiale.

Come funziona la truffa via PEC

Sono utilizzate caselle PEC "hackerate" per inviare email dall'apparenza legittima. Ecco lo schema tipico, studiato per creare urgenza, fare leva sulla fiducia nei confronti della PEC e impedire una verifica accurata:

- **Spoofing del mittente:** il messaggio arriva da un indirizzo PEC reale, spesso appartenente a un professionista o a un'azienda, ma controllato dai truffatori
- **Finta comunicazione ufficiale:** il testo annuncia un cambio dell'indirizzo per l'invio delle fatture elettroniche al Sistema di Interscambio (SdI), gestito dagli hacker
- **Allegati mancanti o falsificati:** viene menzionato un allegato firmato digitalmente, spesso con estensione .p7m, che però non è presente o è dannoso
- **Tracciamento occulto:** il messaggio contiene script invisibili che tracciano l'apertura dell'email e l'attività dell'utente, puntando a domini controllati dagli hacker

Una minaccia in crescita

Il **CERT-AGID** (Computer Emergency Response Team della Pubblica Amministrazione) segnala un costante aumento di casi in cui le PEC sono usate per diffondere malware come AsyncRat, sfruttando tecniche avanzate come il Domain Generation Algorithm (DGA) per aggirare i controlli di sicurezza.

Come riconoscere i messaggi sospetti

- **Oggetto simile a:** "Invio File <XXXXXXXXXX>", con una stringa di 10 cifre casuali
- **Allegati apparentemente firmati digitalmente**, con estensione .p7m, che in realtà non esistono
- **Richieste urgenti di modifica dell'indirizzo SdI,** spesso senza una giustificazione plausibile

Cosa fare per proteggersi dai Phishing?

1. **Verifica sempre i mittenti e i link:** passa il mouse sopra gli URL prima di cliccare e confronta l'indirizzo mostrato con quello reale
2. **Evita di cliccare sui link direttamente:** meglio copiarli e analizzarli in un ambiente sicuro, senza aprirli
3. **Non aprire allegati sospetti:** soprattutto se non attesi o non coerenti con le attività in corso
4. **Usa VPN evolute:** alcune VPN offrono protezioni aggiuntive contro siti malevoli e phishing
5. **Forma il personale:** la security awareness è fondamentale; organizza corsi formativi per insegnare a riconoscere le minacce e reagire in modo corretto
6. **Monitora le caselle PEC:** controlla regolarmente le configurazioni, l'accesso e le anomalie nei flussi di comunicazione

Protezione proattiva, non solo reattiva

L'unico modo per proteggere davvero l'azienda è quello di adottare un approccio proattivo, costruendo una cultura aziendale della sicurezza informatica. I-TEAM è a disposizione per aiutare le aziende a valutare i rischi, adottare misure concrete e formare il personale.

Perché la sicurezza non è un optional.

A cura di
Paolo Vannini

SentinelOne® il software AI di guardia

Attacchi ransomware, vulnerabilità zero-day, exploit avanzati e mille altre minacce informatiche in costante evoluzione: i rischi per le aziende sono reali, consistenti e pericolosi, ed è necessario dotarsi di soluzioni di sicurezza avanzate per la protezione degli endpoint.

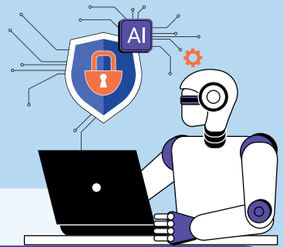
SentinelOne è una delle piattaforme più innovative in questo ambito, grazie alla sua architettura autonoma basata su Intelligenza Artificiale e Machine Learning, con profili Singularity Control e Singularity Complete particolarmente adatti per le aziende.

Cos’è SentinelOne

SentinelOne è una piattaforma di sicurezza per endpoint e cloud, progettata per rilevare, prevenire e rispondere automaticamente e in tempo reale alle minacce informatiche. A differenza delle soluzioni tradizionali di cybersicurezza, SentinelOne utilizza un modello di AI comportamentale per identificare attività anomale e bloccare gli attacchi prima che causino danni.

I vantaggi di SentinelOne

- **Autonomia operativa:** rileva e risponde senza necessità di intervento manuale
- **Storyline™:** costruisce una narrativa continua delle attività su un dispositivo per fornire informazioni complete sugli attacchi
- **Rollback con un click:** in caso di compromissione, è possibile riportare il sistema allo stato precedente



I PROFILI

Singularity Control

Include tutto quello che le aziende desiderano per una protezione avanzata degli endpoint:

- Prevenzione e rilevamento basati su AI
- Firewall integrato e controllo delle porte USB
- Controllo delle applicazioni e dei dispositivi
- Visibilità in tempo reale sugli eventi di sicurezza

a partire da €3,00 per endpoint

Singularity Complete

Il profilo ideale per le aziende con un reparto IT strutturato, che desiderano non solo bloccare le minacce, ma anche investigare e rispondere in modo avanzato agli incidenti di sicurezza:

- EDR (Edpoint Detection and Response) completo
- Visibilità estesa con Storyline Active Response (STAR)
- Capacità di threat hunting proattivo
- Analisi forense degli incidenti
- Rollback con un clic anche per ransomware

a partire da €9,00 per endpoint

Perché scegliere SentinelOne

I-TEAM, in qualità di partner tecnologico specializzato in soluzioni di cybersecurity, è in grado di supportare le aziende nell’implementazione e nella gestione di SentinelOne, fornendo:

- Consulenza tecnica
- Integrazione con le infrastrutture presenti
- Monitoraggio e gestione proattiva degli alert
- Formazione e supporto operativo

In un contesto dove i tempi di risposta e la capacità di prevenzione sono critici, SentinelOne si pone come una soluzione all’avanguardia per le aziende che vogliono proteggere i propri asset digitali.

A cura di
Marco Melucci

vtenext CRM intelligente, impresa vincente

Digitalizzare le imprese è un passo fondamentale ma la tecnologia, ormai, è già in grado di **predire, personalizzare, automatizzare**, in modo da stare dietro alle crescenti esigenze del mercato e stare al passo con le ambizioni imprenditoriali.

Le soluzioni esistono già: **VTENEXT**, il CRM - Customer Relationship Management di nuova generazione, non è solo uno strumento gestionale ma è il cervello operativo che collega tutti i tuoi processi aziendali, guidato da logiche intelligenti, dati concreti e automazione reale.

VTENEXT: dall’organizzazione alla predizione

Cosa può fare la release 2025 di VTENEXT basato su Intelligenza Artificiale?

- **Anticipare i bisogni dei tuoi clienti** prima ancora che si esprimano
- **Guidare i tuoi commerciali** con suggerimenti bassati sui dati effettivi
- **Automatizzare le risposte e i flussi decisionali** in tempo reale
- **Creare Buyer Personas,** profili cliente personalizzati
- **Monitorare KPI dinamici** che si aggiornano con l’evolversi dei business

VTENEXT: perché fa la differenza

- **Conversazioni intelligenti.** La nuova AI gestisce chat, email e interazioni web, fornendo risposte precise e pertinenti, anche fuori orario
- **Gestione dei contatti potenziata.** Le informazioni sono ricche di dettagli utili: non solo nomi e numeri, ma comportamenti, interessi e potenziale valore commerciale
- **Processi in costante ottimizzazione.** La piattaforma analizza i flussi, segnala colli di bottiglia, propone ottimizzazioni e, in pratica, impara di continuo

VTENEXT: caratteristiche e vantaggi

- **Open Source**
- **100% personalizzabile**
- **Disponibile in Cloud e on-Premises**
- **Full Integration** con ERP, e-commerce, centralini VoIP e strumenti di marketing automation
- Integrazione automatica con **i sistemi BPM** (Business Process Management)

VTENEXT: per un’azienda più agile, veloce ed efficiente

I-TEAM, partner certificato VTENEXT, è pronto ad accompagnarti in un percorso di trasformazione intelligente, calibrato sui tuoi obiettivi, compreso il percorso formativo, casi concreti, demo pratiche e una roadmap personalizzata.

I·TEAM

Cinque società che si sono unite per dare forma a un grande progetto:
aiutare le imprese a crescere nella digitalizzazione
e nella rivoluzione digitale, per avere performance
sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti
dell'economia e della società contemporanea.

Allyou.srl

ego communication

GLOBALNET ITALIA

OMEGA SISTEMI
Soluzioni Informatiche Professionali

NETWORK PRIVACY

PANTAREI INFORMATICA
La tecnologia resa semplice

WWW.I-TEAM.TECH

Via Benedetto Dei 64 • 50127 FIRENZE • Numero Verde 800-199760 • info@i-team.tech