Gpi Cyberdefence.

LA DIRETTIVA NIS 2 E LE MISURE TECNICHE DI TIPO PREVENTIVO: I TEST

Rosario Mauro Catanzaro
Manuela Sforza
Chiara D'Errico
Anna Vittoria Sica

Aprile 2025

Gpi Cyberdefence.

Sommario

LA NORMATIVA

La Direttiva NIS 2

Negli ultimi anni, il panorama digitale globale ha assistito a una crescita esponenziale degli attacchi informatici, **evidenziando la vulnerabilità delle nostre infrastrutture tecnologiche**.

Secondo il rapporto Clusit 2025, nel 2024 gli incidenti cyber sono aumentati del 27,4% a livello mondiale e del 15,2% in Italia. Questa escalation non solo minaccia la sicurezza delle informazioni, ma **mette anche a rischio la continuità operativa di servizi essenziali**, con potenziali ripercussioni sulla vita quotidiana dei cittadini.

Per contrastare in modo più efficace queste minacce, l'Unione Europea ha introdotto la Direttiva NIS (Network and Information Security), successivamente evoluta nella NIS 2, recepita in Italia con il Decreto Legislativo n. 138/2024. Questa normativa mira a garantire un elevato livello comune di cybersicurezza, imponendo obblighi stringenti sia alle imprese che alle pubbliche amministrazioni.

Tra gli obblighi principali previsti dalla Direttiva NIS 2 vi sono:

- **Gestione dei rischio e adozione di misure di sicurezza adeguate**: le organizzazioni devono implementare politiche e procedure per gestire i rischi cyber e proteggere i dati.
- **Notifica tempestiva degli incidenti**: è obbligatorio segnalare alle autorità competenti gli incidenti di sicurezza entro 24 ore dalla loro rilevazione.
- **Gestione del rischio e formazione**: le aziende sono tenute a sviluppare piani di gestione del rischio e a garantire una formazione continua del personale in materia di cybersicurezza.

Tuttavia, la NIS 2 non si ferma ad una generica descrizione e propone un elenco dettagliato citando, tra gli adempimenti:

- Governance della cybersicurezza;
- Valutazione e gestione del rischio;
- Obbligo di evidenze documentali per dimostrare diligenza e conformità;
- Piano di continuità operativa e disaster recovery;
- Monitoraggio continuo e piani di mitigazione;
- Gestione degli incidenti e obblighi di notifica;
- Gestione dei rischi legati alla catena di approvvigionamento;
- Formazione continua dell'organo di gestione, dei dipendenti e dei collaboratori;
- Misure tecniche adeguate di tipo preventivo e contenitivo.

Va inoltre sottolineato come la Direttiva NIS 2 assegni all'organo di gestione e, quindi, quando presente, al **Consiglio di Amministrazione, la piena responsabilità dell'attuazione delle politiche di sicurezza**, senza alcuna possibilità di delega. Non solo, ma la gestione del rischio viene estesa a un perimetro ben più ampio di quello aziendale, quello dei **fornitori**, obbligando l'organizzazione ad una verifica stringente degli stessi.

Assume particolare rilevanza il fatto che le scadenze per l'adeguamento a queste disposizioni siano imminenti, anche in considerazione della complessità delle stesse. **Il mancato rispetto di queste scadenze può comportare sanzioni significative e compromettere la reputazione dell'organizzazione**.

La cybersicurezza non è più un'opzione per le aziende, ma una necessità imprescindibile. Le nuove normative rappresentano strumenti essenziali per proteggere individui e organizzazioni dalle crescenti minacce informatiche. È quindi indispensabile che le aziende adottino tempestivamente le misure richieste, non solo per conformarsi alle leggi vigenti, ma anche per salvaguardare la fiducia dei propri clienti e garantire la continuità operativa in un mondo sempre più interconnesso.

Misure tecniche di tipo preventivo: i test

Le misure tecniche preventive sono fondamentali per garantire la sicurezza e l'efficienza all'interno delle organizzazioni. Tuttavia, spesso queste misure sono percepite come complesse e avvolte da un alone di tecnicismo che può renderne difficile la comprensione da parte degli organi di amministrazione. Poiché l'implementazione di tali misure rientra nelle responsabilità dell'organo di amministrazione, è essenziale fornire una descrizione chiara e comprensibile a livello esecutivo. Questo documento si propone di descrivere in modo chiaro e accessibile le principali misure tecniche preventive, al fine di facilitare una loro efficace implementazione e gestione da parte del management aziendale.

Vulnerability Management (VM)

Il **Vulnerabilty Management** o Gestione delle Vulnerabilità è un processo continuo e sistematico volto a identificare, valutare, trattare e mitigare le **vulnerabilità presenti nei sistemi ICT** (Information and Communication Technology). Questo processo è fondamentale per garantire la sicurezza delle informazioni e la resilienza delle infrastrutture tecnologiche di un ente.

La prima fase del processo di VM è l'**identificazione** (Identification) delle minacce attraverso l'utilizzo di strumenti di scansione, al fine di rilevare vulnerabilità note e potenziali nei sistemi e nelle reti.

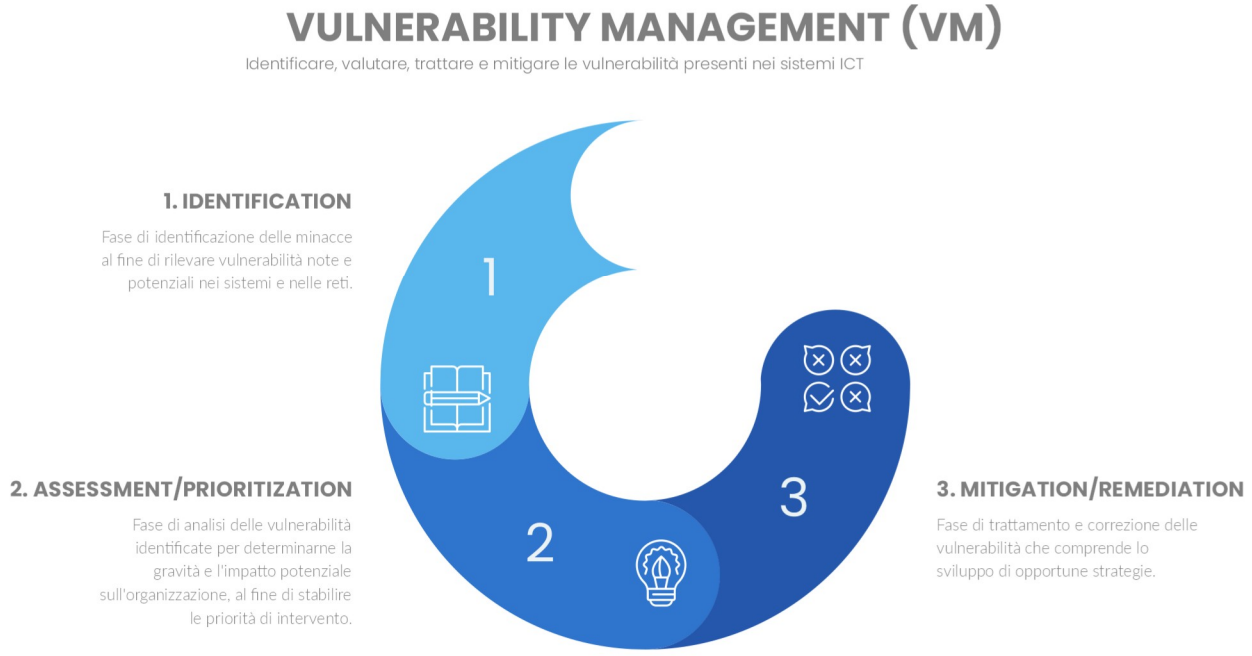
Segue la fase di **classificazione e valutazione** (Assessment/Prioritization), durante la quale vengono analizzate le vulnerabilità identificate per determinarne la gravità e l'impatto potenziale sull'organizzazione, al fine di stabilire le priorità di intervento.

Viene, a questo punto, fornito supporto per indirizzare efficacemente la fase di **trattamento e correzione** (Mitigation/Remediation), che comprende lo sviluppo di strategie per affrontare le vulnerabilità, che possono includere l'applicazione di patch, la modifica delle configurazioni di sistema o l'adozione di misure compensative.

Ovviamente, in maniera circolare e virtuosa, è necessario verificare e **validare i risultati** (Verification), per controllare se le vulnerabilità siano state effettivamente rimosse o mitigate, nonché effettuare un'attività continua di monitoraggio (monitoring) al fine di rilevare nuove vulnerabilità o inefficienze nelle soluzioni adottate.

E' essenziale che l'implementazione delle correzioni (patching) venga effettuata da un'entità differente rispetto a quella che ha il compito di individuare le vulnerabilità, di definire la strategia ed effettuare il controllo delle operazioni. Questa separazione dei ruoli, nota come **segregazione dei compiti** (*segregation of duties*), è una pratica fondamentale per evitare conflitti di interesse e garantire l'integrità del processo di gestione delle vulnerabilità. Ad esempio, chi rileva una vulnerabilità potrebbe non segnalarla correttamente (sia per interesse che per semplice mancanza di conoscenza) se fosse anche responsabile della sua correzione, compromettendo così la sicurezza complessiva del sistema.

Warning: il VM è un'attività ciclica che non va confusa con il **Vulnerability Assessment** (VA), nel quale non è presente la fase di verifica e monitoraggio continuo. Il VM permette di misurare, tramite specifici KPI l'andamento dello stato delle vulnerabilità rilevate, fornendo al management uno strumento per dimostrare la propria diligenza e l'efficacia delle misure adottate nel tempo.



Web Application Security Testing (WAST)

Il **Web Application Security Testing** è un processo sistematico e continuo finalizzato alla protezione e messa in sicurezza delle **applicazioni web e dei siti internet**. Questo processo permette di identificare, valutare, gestire e mitigare le vulnerabilità specifiche delle applicazioni web, garantendo la tutela dei dati degli utenti, prevenendo intrusioni informatiche e assicurando la disponibilità, la riservatezza e l'integrità dei servizi online offerti da un'organizzazione.

Nella sua connotazione più essenziale, il processo di WAST prevede una **prima fase di raccolta di informazioni** preliminari (Information Gathering), con l'obiettivo di raccogliere il maggior numero di informazioni sulla web application e le sue funzionalità, concentrandosi particolarmente sul layer applicativo.

Segue quindi la fase di **identificazione delle vulnerabilità e delle configurazioni deboli** (Testing) nell'applicazione web.

Infine, viene realizzato un **report informativo** (Reporting), con lo scopo di descrivere dettagliatamente le vulnerabilità riscontrate, il loro rischio e impatto potenziale, la probabilità di sfruttamento, i passaggi per la remediation. Ovviamente, la qualità del report dipende dal fornitore, che può limitarsi a fornire un report generale, automatizzato e poco utile ai fini della risoluzione delle problematiche, oppure definire attentamente le strategie più efficaci per risolvere le vulnerabilità individuate, che possono comprendere suggerimenti di interventi correttivi sul codice sorgente, di aggiornamenti di librerie o framework, di revisione delle configurazioni di sicurezza e di contromisure applicative specifiche.

Il WAST si integra con altre metodologie legate alla resilienza operativa digitale come, per esempio, il penetration test che può essere utilizzato come verifica periodica e, comunque, deve essere inserito nel monitoraggio continuo delle vulnerabilità, al fine

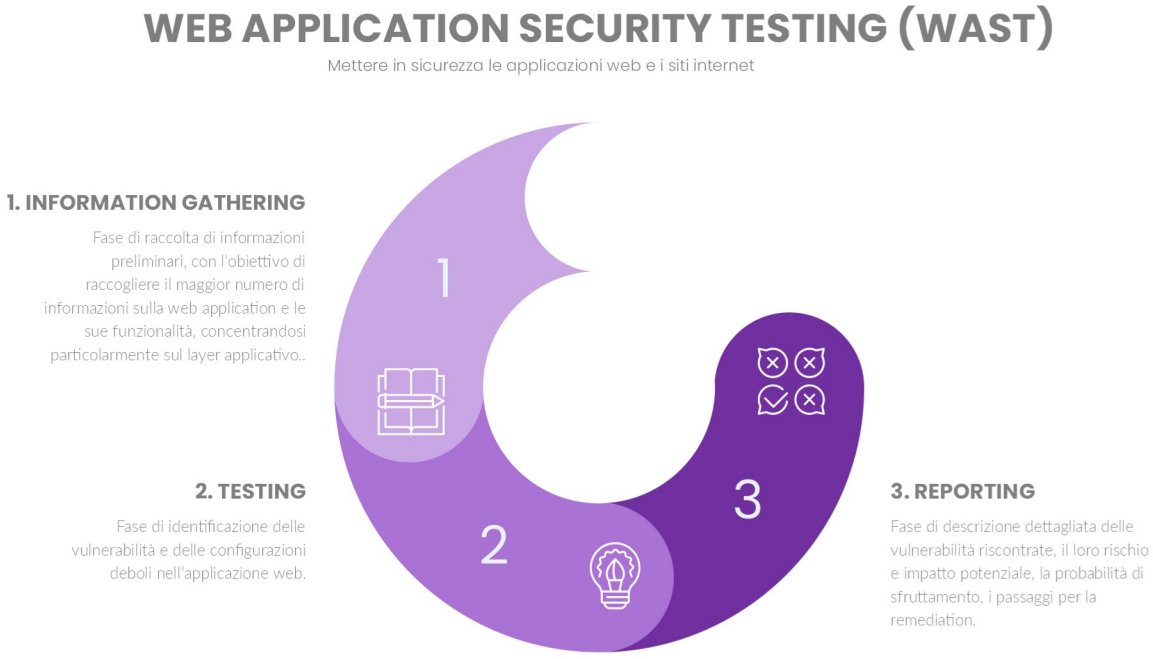
di valutare costantemente l'efficacia delle misure adottate e rilevare tempestivamente l'insorgere di nuove vulnerabilità.

Un ruolo centrale nel processo di WAST è svolto dalle metodologie standardizzate proposte dall'**Open Web Application Security Project (OWASP)**, che offre modelli riconosciuti come la "OWASP Top Ten", che identifica le principali minacce per le applicazioni web, e la "OWASP Testing Guide", che costituisce un quadro di riferimento per effettuare test approfonditi e penetration test efficaci.

È inoltre consigliato affiancare ai test statici degli sviluppatori di software, Static Application Security Test (SAST), anche attività di Dynamic Application Security Testing (DAST), che analizzano l'applicazione nel ciclo dinamico di esecuzione.

È importante sottolineare, infine, che il WAST non deve essere considerato un'attività isolata, bensì va integrato pienamente nel ciclo di vita dello sviluppo software (SDLC), contribuendo così a promuovere una cultura della sicurezza diffusa e assicurando che le applicazioni web siano progettate, realizzate e manutenute con una costante attenzione alla sicurezza.

Anche per il WAST è essenziale segregare i compiti: le attività di identificazione e valutazione delle vulnerabilità devono essere svolte da un'entità differente rispetto a chi si occupa di sviluppare codice e applicare le correzioni.



Penetration Test (PT)

Il **Penetration Test** è un processo strutturato e sistematico volto a identificare, analizzare e valutare le vulnerabilità presenti nei sistemi informatici, nelle applicazioni e nelle reti, **simulando attacchi reali** per verificarne concretamente il livello di sicurezza. Il processo di Penetration Testing inizia con la fase di **raccolta delle informazioni** (Information Gathering), durante la quale vengono identificate le risorse target e raccolti dati preliminari attraverso tecniche di footprinting, raccolta passiva delle informazioni basata su Open Source Intelligence (OSINT) e scanning, raccolta delle informazioni tramite interazioni attive con i sistemi in analisi.

Segue la fase di **identificazione e analisi delle vulnerabilità** (Threat Modeling e Vulnerability Analysis), in cui i tester utilizzano strumenti automatici e manuali per individuare eventuali falle di sicurezza che potrebbero essere sfruttate da un attaccante, come errori di configurazione, vulnerabilità applicative o debolezze architetturali.

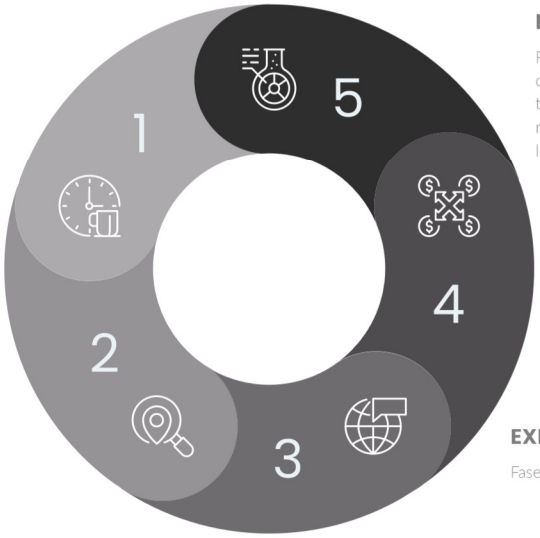
Successivamente, nella fase di **sfruttamento delle vulnerabilità** (Exploitation), le vulnerabilità rilevate vengono utilizzate per simulare attacchi mirati, con l'obiettivo di determinare il reale impatto di un possibile incidente di sicurezza sull'organizzazione. Dopo lo sfruttamento (post-exploitation) si valuta la possibilità di espandere ulteriormente l'accesso ottenuto o di raccogliere informazioni sensibili, misurando il potenziale danno di un attacco riuscito.

Il processo si conclude con la fase di **reportistica** (reporting & remediation), in cui vengono redatti rapporti dettagliati contenenti i risultati dei test, l'analisi del rischio e raccomandazioni mirate per mitigare le vulnerabilità riscontrate. Analogamente al Web Application Security Testing (WAST), il penetration test deve essere svolto periodicamente e integrato in un approccio globale alla sicurezza informatica, al fine di garantire la resilienza continua dell'organizzazione e di promuovere una cultura della prevenzione e protezione dai cyber-attacchi.

Warning: il penetration test verifica se il sistema in esame può essere effettivamente penetrato da un attaccante, non a sanarne le vulnerabilità come, invece, avviene con VM e WAST. Ne consegue che un PT dovrebbe essere effettuato **esclusivamente su sistemi TEST** e **non andrebbe mai effettuato su sistemi in produzione** o non facilmente ripristinabili. Per un PT è sufficiente, infatti, trovare un unico punto di “debolezza” dei sistemi, mentre il VM cerca di individuare tutte le vulnerabilità presenti al fine di sanarle. Diffidate su chi vi propone un PT su sistemi in produzione (nel migliore dei casi sta effettuando un VM invece del PT e, nel peggiore, rischiate di far saltare i vostri sistemi di produzione).

PENETRATION TEST (PT)

identificare, analizzare e valutare le vulnerabilità presenti nei sistemi informatici, nelle applicazioni e nelle reti



INFORMATION GATHERING

Fase di raccolta delle informazioni.

THREATH MODELING E VULNERABILITY ANALYSIS

Fase di identificazione e analisi delle vulnerabilità.

REPORTING & REMEDIATION

Fase di redazione di rapporti dettagliati contenenti i risultati dei test, l'analisi del rischio e raccomandazioni mirate per mitigare le vulnerabilità riscontrate.

POST EXPLOITATION

Fase di valutazione della possibilità di espandere ulteriormente l'accesso ottenuto o di raccogliere informazioni sensibili, misurando il potenziale danno di un attacco riuscito.

EXPLOITATION

Fase di sfruttamento delle vulnerabilità.

Phishing Test

Il **Phishing Test** è un processo strutturato e periodico volto a **simulare attacchi di phishing** nei confronti dei dipendenti e collaboratori di un'azienda, con l'obiettivo di **identificare, valutare e mitigare il rischio derivante da minacce basate sull'ingegneria sociale**.

Tale processo inizia con la fase di **Pianificazione**, in cui vengono definiti obiettivi, scenari realistici e tecniche utilizzate nelle simulazioni, tipicamente basate su e-mail ingannevoli, messaggi SMS o comunicazioni tramite social media.

Segue la fase operativa di **Esecuzione** della simulazione, durante la quale vengono inviati messaggi o comunicazioni che replicano fedelmente le strategie tipiche degli attacchi di phishing, come richieste di informazioni sensibili, inviti a cliccare su link malevoli o download di allegati infetti.

Successivamente, nella fase di **Monitoraggio e Analisi**, vengono raccolti e analizzati i dati relativi alle reazioni degli utenti, valutando il tasso di esposizione al rischio e la capacità di riconoscimento delle minacce da parte delle persone coinvolte.

Il processo si conclude con la fase di **Reporting e Remediation**, nella quale si elaborano rapporti dettagliati contenenti i risultati dei test, evidenziando le aree di criticità e il livello generale di consapevolezza. Questa fase consente inoltre di pianificare e attuare interventi correttivi e formativi mirati, come corsi di sensibilizzazione, aggiornamenti sulla sicurezza informatica o specifiche campagne informative, al fine di migliorare la capacità di riconoscimento e risposta dei dipendenti agli attacchi di phishing, rafforzando così la resilienza complessiva dell'organizzazione verso le minacce informatiche basate sull'ingegneria sociale.

Attack Surface Management (ASM)

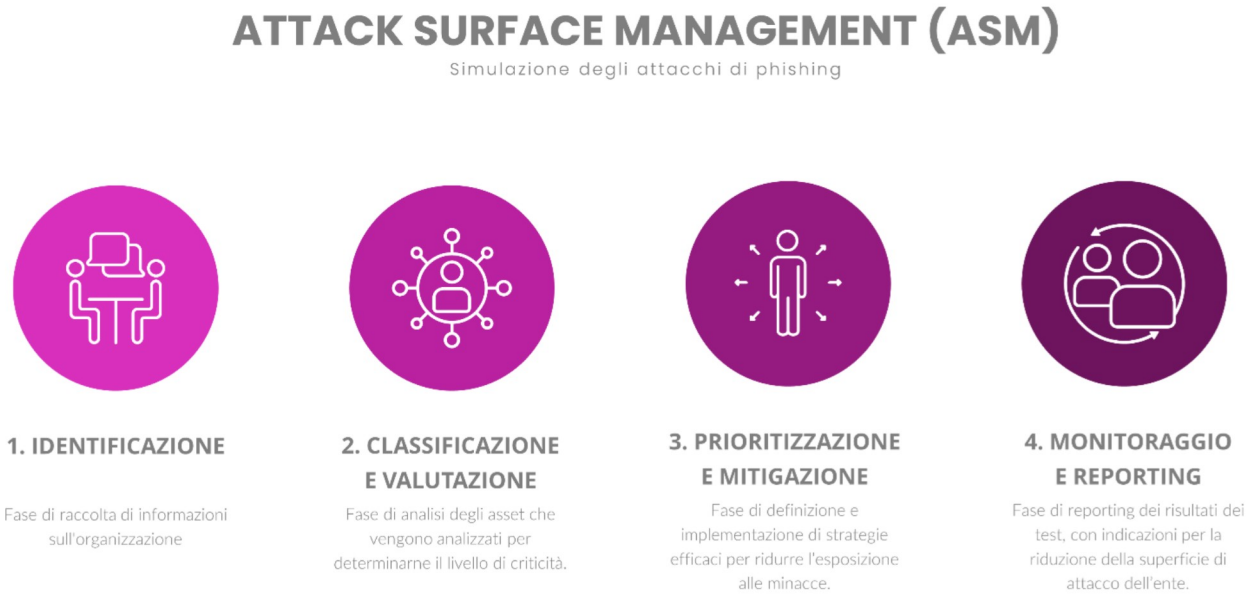
L'**Attack Surface Management** è un processo strutturato e continuativo finalizzato all'identificazione, alla valutazione e alla mitigazione dei rischi legati agli asset digitali dell'organizzazione esposti all'esterno. Questo processo permette di analizzare in maniera approfondita la superficie di attacco aziendale, ovvero tutti i punti di ingresso potenzialmente sfruttabili da attaccanti, tra cui **domini web**, servizi cloud, server, API, dispositivi IoT e ogni altra risorsa accessibile pubblicamente.

La prima fase consiste nell'**Identificazione** degli asset esposti, tramite strumenti automatizzati e tecniche manuali di Open Source Intelligence (OSINT) che consentono di raccogliere informazioni pubblicamente disponibili sull'organizzazione, **individuando potenziali punti di ingresso per eventuali minacce**.

Segue una fase di **Classificazione e Valutazione** delle risorse digitali identificate, durante la quale ciascun asset viene analizzato per determinare il livello di criticità, il grado di esposizione e il rischio potenziale associato.

Successivamente, nella fase di **Prioritizzazione e Mitigazione**, vengono definite e implementate strategie efficaci per ridurre l'esposizione alle minacce, attraverso il suggerimento di interventi che comprendono il rafforzamento delle configurazioni di sicurezza, la rimozione di asset inutilizzati o non autorizzati, l'applicazione di controlli e misure compensative.

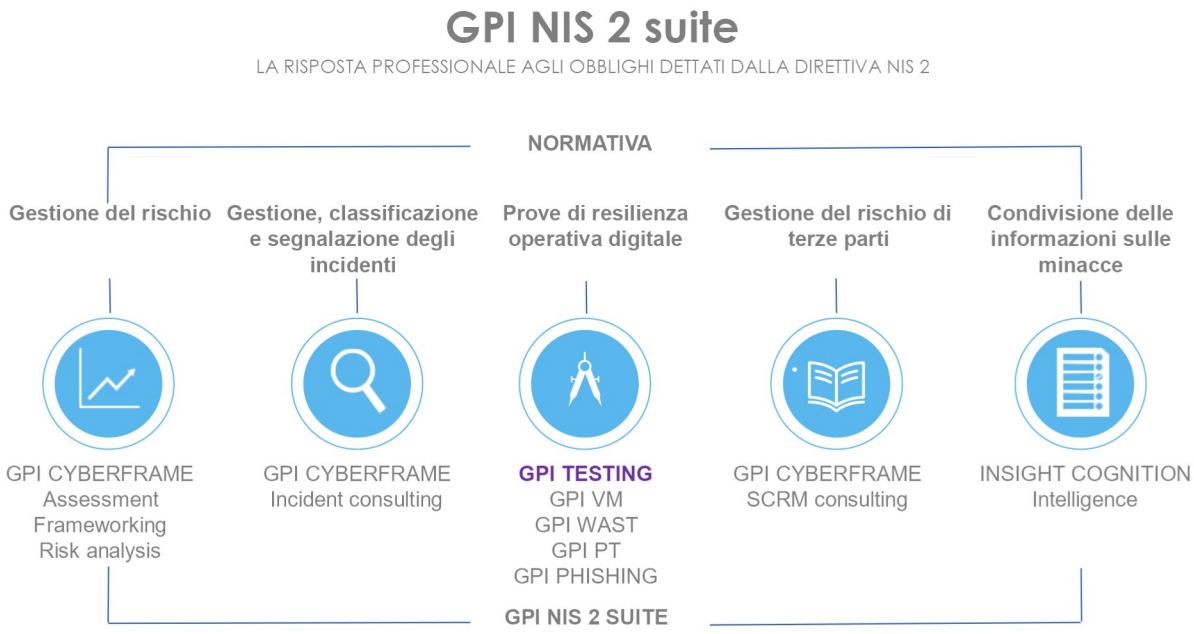
Infine, il processo prevede una fase di **Monitoraggio e Reporting** costante, con strumenti di scansione e attività periodiche di OSINT, che assicurano una vigilanza continua sulle risorse esposte, permettendo di individuare tempestivamente nuovi asset digitali o vulnerabilità emergenti e fornendo input utili per prendere decisioni strategiche volte a ridurre l'esposizione della superficie di attacco e migliorare la sicurezza complessiva dell'organizzazione.



GLI STRUMENTI

GPI NIS 2 SUITE

GPI NIS 2 SUITE è la suite integrata di servizi avanzati per garantire la resilienza operativa digitale delle imprese e delle pubbliche amministrazioni, rispondendo con efficacia alle prescrizioni normative più rigorose.



GPI TESTING

GPI TESTING è la piattaforma metodologica di **GPI NIS 2 SUITE** dedicata allo svolgimento delle prove di resilienza operativa digitale.

- **GPI VM**: un servizio completo e proattivo, basato su tecnologie avanzate e interventi specialistici manuali, per l'identificazione, classificazione e supporto alla correzione delle vulnerabilità nei tuoi sistemi ICT, dotato di aggiornamenti continui e puntuali dei database delle vulnerabilità e documentazione dettagliata per un monitoraggio costante e affidabile.
- **GPI WAST**: valutazioni approfondite della sicurezza delle applicazioni web, che includono test automatici e analisi manuali effettuate da analyst certificati, individuando e ottimizzando la correzione di vulnerabilità critiche proteggendo l'integrità e la riservatezza dei dati aziendali.
- **GPI PT**: simulazioni realistiche e controllate di attacchi informatici verso l'infrastruttura ICT, progettate per evidenziare eventuali punti deboli nelle difese aziendali. Attraverso metodologie rigorose e conformi ai più alti standard di settore, vengono realizzati report completi e dettagliati che consentono di intervenire con precisione ed efficacia.
- **GPI Phishing**: campagne mirate di simulazione di attacchi phishing per misurare la preparazione e la consapevolezza del personale. Questi test**, basati sulla metodologia proprietaria HURMA**, accompagnati da analisi dettagliate sia psicometriche che tecniche, permettono di identificare rapidamente eventuali necessità formative, consentendo interventi mirati di sensibilizzazione e formazione continua del personale.
- **GPI ASM**: attività continua di identificazione e monitoraggio della superficie di attacco digitale, allo scopo di individuare tempestivamente asset esposti o vulnerabili e gestire efficacemente il rischio di cyber-attacchi.

GPI NIS 2 Suite è la soluzione professionale e certificata per una sicurezza informatica conforme, robusta e sempre aggiornata.

Per maggiori informazioni scrivi a: info@gpicyberdefence.com.

LE PERSONE

Get in touch

Rosario Mauro Catanzaro

Rosario Mauro Catanzaro è Amministratore Delegato di GPI Cyberdefence, azienda del gruppo GPI S.p.A., specializzata in Cybersicurezza e difesa digitale. Ricopre, inoltre, l'incarico di Segretario Generale dell'ISAC (Information Security & Analysis Center) di Cassa Depositi e Prestiti.

È Presidente dell'ANPD – Associazione Nazionale per la Protezione dei Dati ed è owner di una delle più numerose community italiane operanti nell'ambito della Cybersicurezza e della Protezione dei Dati, seguito da oltre 50.000 tra professionisti e aziende.

Autore di numerosi articoli e pubblicazioni a tema Cybersicurezza, tra i quali il libro di grande successo *Cybersecurity - benvenuti nell'era della pandemia informatica*, si occupa, nella sua vita professionale, di Cyberdefence Operativa e strategica, con focus su Sanità, Pubblica Amministrazione, Finanza e numerosi altri ambiti produttivi.

Rosario Mauro Catanzaro

Gruppo Linkedin Regolamento DORA, Direttiva NIS 2 e Legge 90/2024

Gruppo Linkedin Cybersecurity & GDPR Italia

Manuela Sforza

Manuela Sforza è Chief Information Security Officer di GPI Cyberdefence. Laureata in Ingegneria Informatica, vanta due ulteriori titoli accademici in Sociologia e Giurisprudenza.

Certificata C|CISO (EC-Council Chief Information Security Officer), CEH (EC-Council Ethical Hacker), CHFI (EC-Council Computer Hacking Forensic Investigator), è coautrice del libro Cybersecurity - benvenuti nell'era della pandemia informatica. Relatrice in numerosi convegni ed autrice di numerosi articoli e pubblicazioni, è esperta di minacce informatiche, con particolare riferimento al Social engineering.

Chiara D'Errico

Chiara D'Errico, laureata in giurisprudenza, ha proseguito gli studi conseguendo un master di II livello in Cybersecurity. E' abilitata all'esercizio della professione forense e svolge la professione di Risk Analyst presso GPI Cyberdefence. Possiede un'approfondita conoscenza delle normative inerenti alla Cybersicurezza e alla Data Protection.

Anna Vittoria Sica

Anna Vittoria Sica, laureata in giurisprudenza, ha proseguito gli studi conseguendo un master in "Protezione strategica del Sistema Paese". Certificata Internal Auditor ISO/IEC 27001 e Internal Auditor ISO/IEC 22301, svolge la professione di Risk Analyst presso GPI Cyberdefence.

Conclusioni

La Normativa NIS rappresenta un passo fondamentale verso una maggiore consapevolezza e maturità nella gestione del rischio informatico. Per le aziende, i test non sono solo un obbligo normativo, ma una necessità per garantire la continuità operativa e la protezione dei dati in un contesto caratterizzato da minacce informatiche sempre più sofisticate. Gli organi di controllo delle organizzazioni devono assumere un ruolo attivo nella definizione e supervisione delle politiche di sicurezza, assicurando che le misure adottate siano efficaci e in linea con le best practice del settore.

In un panorama in cui gli attacchi informatici sono in aumento, la resilienza operativa digitale diventa un elemento cruciale per la salvaguardia dell'intero ecosistema finanziario e la tutela degli interessi di clienti e investitori.

Gpi Cyberdefence.

Gpi Cyberdefence

GPI Cyberdefence è un'azienda del Gruppo GPI, uno dei più importanti player del mercato digitale con oltre 9.000 clienti tra Pubblica Amministrazione, Enti Finanziari e aziende private. Il Gruppo è quotato in **Borsa Italiana** e partecipato da **Cassa Depositi e Prestiti**.

Prima azienda italiana certificata ISO/IEC 27001 e ISO 9001 per il campo applicativo "Progettazione ed erogazione di servizi di Cybersecurity strategica attraverso il **Framework Nazionale per la Cybersecurity e la Data Protection**. Erogazione di servizi di Cybersecurity operativa", GPI Cyberdefence offre una sicurezza informatica conforme, robusta e sempre aggiornata, ed è il partner ideale per adeguarsi alla Direttiva NIS 2, sia per quanto riguarda gli interventi di governance che quelli operativi, con il vantaggio di poter disporre di un interlocutore unico e competente.

https://www.gpigroup.com/en/cyber-security/

info@gpicyberdefence.com