VULNERABILITY ASSESSMENT

NIS2	72%	207 gg
CONFORMITÀ	**VULNERABILITÀ**	**TEMPO MEDIO**
obbligo per migliaia di aziende in Italia	rimangono non rilevate senza VA sistematico	per identificare una violazione senza monitoraggio

Il servizio di **Vulnerability Assessment (VA)** consente di valutare in modo sistematico il livello di sicurezza dell'infrastruttura ICT aziendale, identificando vulnerabilità reali e potenziali prima che possano essere sfruttate da attori malevoli. Al termine dell'analisi viene prodotto un **report dettagliato** con la classificazione delle vulnerabilità rilevate (Critical, High, Medium, Low) secondo il framework **CVSSv3**, corredato dalle relative remediation e dal piano di adeguamento alla normativa **NIS2**.

Il servizio è progettato per le organizzazioni soggette alla **Direttiva NIS2** — in vigore in Italia dal 18 ottobre 2024 — che devono dimostrare l'adozione di misure tecniche e organizzative adeguate a proteggere reti e sistemi informativi. Il VA fornisce la baseline di sicurezza necessaria per avviare o mantenere un programma strutturato di gestione del rischio cyber, requisito esplicito della direttiva.

L'assessment è condotto con **metodologia non intrusiva**, seguendo un piano d'azione concordato con il cliente sulla base delle informazioni fornite circa i propri sistemi. Le attività coprono apparati di rete, firewall, server, client, sistemi di virtualizzazione, servizi cloud esposti e applicazioni web, garantendo una visione completa della superficie d'attacco.

Il servizio VA può essere erogato in modalità **"one shot"** per una fotografia puntuale della postura di sicurezza, oppure con cadenza **periodica (trimestrale, semestrale o annuale)** per garantire il monitoraggio continuo delle vulnerabilità emergenti e la verifica dell'efficacia delle remediation applicate.

Analisti certificati · Metodologie CVSSv3, OWASP e NIST · Piena conformità Direttiva NIS2 · UNI EN ISO 9001:2015

COME FUNZIONA IL SERVIZIO

1

Scoping e raccolta informazioni

Definizione del perimetro: asset da includere, tipologia di assessment (internal/external/web), finestre temporali e criteri di esclusione. Viene redatto un documento di scoping condiviso con il cliente per garantire trasparenza e allineamento sugli obiettivi.

2

Discovery e enumerazione

Scansione non intrusiva per individuare host attivi, porte aperte, servizi esposti, versioni software e configurazioni. Viene prodotta una mappa completa della superficie d'attacco che costituisce la base per le fasi successive.

3

Vulnerability scanning e analisi

Utilizzo di scanner professionali (Nessus, Qualys, OpenVAS) con threat intelligence aggiornata per rilevare CVE noti, misconfigurazioni, software obsoleto e credenziali deboli. Le scansioni sono calibrate per minimizzare l'impatto sui sistemi produttivi.

4

Validazione e classificazione

Analisi manuale per eliminare falsi positivi, classificazione CVSSv3 (Critical / High / Medium / Low) e correlazione con il contesto del cliente. Ogni vulnerabilità viene verificata individualmente da analisti certificati per garantire l'accuratezza del risultato.

5

Report e remediation plan

Produzione di un report executive e tecnico con: elenco completo delle vulnerabilità, severity, sistemi impattati, remediation prioritizzate e piano di adeguamento NIS2. Il report è strutturato per essere comprensibile sia al management che al team tecnico.

6

Verifica post-remediation (opzionale)

Re-test mirato per verificare l'effettiva risoluzione delle vulnerabilità critiche e aggiornare il report di conformità. Questa fase opzionale chiude il ciclo di gestione e fornisce evidenza documentale dell'efficacia degli interventi effettuati.

NIS2: SEI IN REGOLA?

La **Direttiva NIS2** (recepita in Italia con **D.Lgs. 138/2024**) amplia significativamente il perimetro dei soggetti obbligati rispetto alla precedente NIS1, includendo nuovi settori e abbassando le soglie dimensionali per le PMI. Le organizzazioni coinvolte devono adottare **misure di sicurezza proporzionate al rischio**, tra cui la gestione sistematica delle vulnerabilità.

1 Soggetti essenziali e importanti

Energia, trasporti, sanità, infrastrutture digitali, PA, spazio e nuovi settori manifatturieri critici.

Sanzioni fino al 2% del fatturato globale.

2 Obblighi tecnici

Gestione del rischio, vulnerability management, sicurezza della supply chain, notifica degli incidenti entro 24/72 ore, test periodici di sicurezza.

Misure proporzionate al rischio.

3 Il VA come punto di partenza

Il Vulnerability Assessment è il primo passo concreto per costruire la conformità NIS2 e dimostrare l'adozione di misure adeguate.

Baseline di sicurezza documentata.

Da NIS1 a NIS2 — cosa cambia

ASPETTO	NIS1	NIS2
Ambito soggetti	Operatori settori critici	+ PMI, manifattura, spazio
Governance	Responsabilità generica	Responsabilità CdA diretta
Sanzioni	Variabili per paese	Fino al 2% fatturato globale
Notifica incidenti	Nessun termine fisso	24h (early warning) / 72h
Supply chain	Non esplicitamente inclusa	Obbligo di valutazione

EMILIA INFORMATICA
let's connect

Richiedi un preventivo
o maggiori informazioni

I consulenti tecnici sono a vostra disposizione.

Tel. 0523.62.70.11 | www.emiliainformatica.it