Governance e servizi digitali della cyber sicurezza

dinova

interacta

GRUPPO Maggioli

Claudia Ciampi

Responsabile Cyber Risk & Governance

dinova

GRUPPO Maggioli

Scenario normativo di riferimento per la Cybersecurity

Misure minime di sicurezza ICT AgID

Le Linee Guida attuano la direttiva del DPCM 1/8/15 e forniscono alle PA dei criteri per stabilire il **livello di protezione di un'infrastruttura ICT rispetto alle minacce cyber più frequenti**.

Legge n. 90 del 28 giugno 2024

in vigore dal 02 luglio 2024 riguardante "Disposizioni in materia di **rafforzamento della cyber sicurezza nazionale e di reati informatici**"

Direttiva Europea NIS 2 "Sicurezza delle reti e delle informazioni" recepita in Italia con DLgs. nr. 138/2024

Direttiva UE 2022/2555 in vigore dal gennaio 2023, sulla **Sicurezza delle reti e delle informazioni**, che abroga e sostituisce la precedente Direttiva NIS 1 del 2016 nell'ottica di modernizzazione dell'attuale quadro europeo in tema di cybersecurity.

Misure minime di sicurezza ICT

Attuano la direttiva del DPCM 1/8/15 e forniscono alle PA dei criteri per stabilire il livello di protezione di un'infrastruttura ICT per le esigenze operative.

AGID | Agenzia per l'Italia Digitale

Queste misure rappresentano un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle Amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

Misure minime di sicurezza ICT

3 LIVELLI DI APPLICAZIONE

Livello Minimo (M)

E' quello al quale ogni PA, indipendentemente dalla sua natura e dimensione, deve **necessariamente essere o rendersi conforme**.

Livello Standard (S)

E' il livello, superiore al minimo, che ogni PA deve considerare come **base di riferimento** in termini di sicurezza.

Livello Avanzato (A)

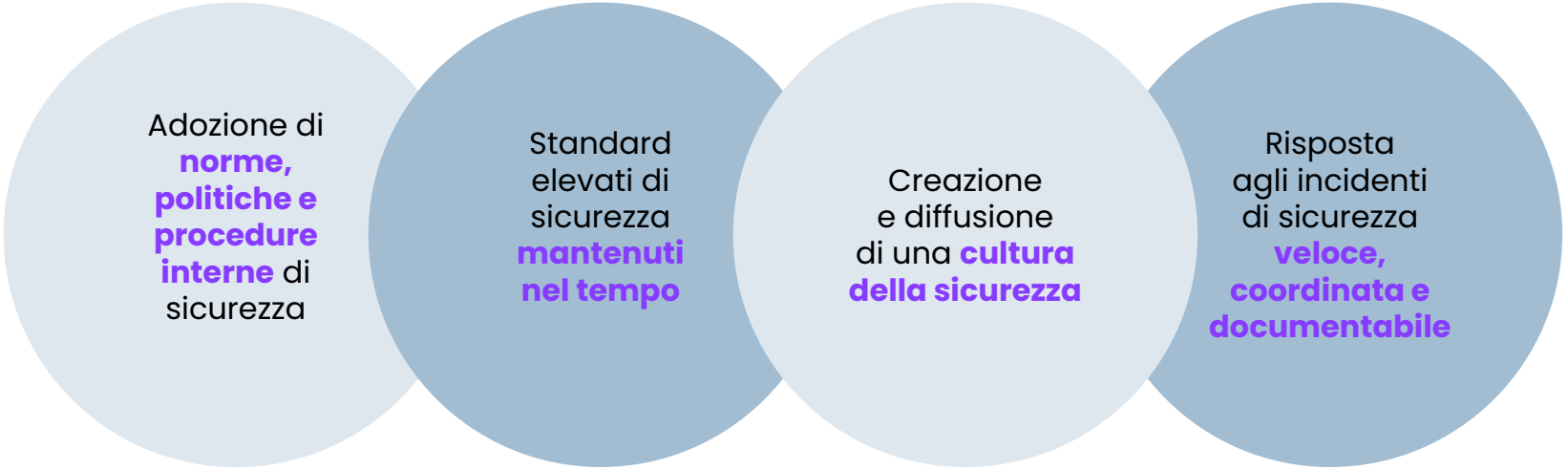
Deve essere adottato dalle **PA maggiormente esposte a rischi** (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come **obiettivo di miglioramento** da parte di tutte le altre organizzazioni.

MISURE MINIME DI SICUREZZA

- **ABSC1** - Inventario dei dispositivi autorizzati e non autorizzati
- **ABSC2** - Inventario dei software autorizzati
- **ABSC3** - Proteggere le configurazioni di HW e SW
- **ABSC4** - Valutazione e correzione continua della vulnerabilità
- **ABSC5** - Uso appropriato dei privilegi di amministratore
- **ABSC8** - Difese contro i malware
- **ABSC10** - Copie di sicurezza
- **ABSC13** - Protezione dei dati

Compliance Misure minime di sicurezza ICT

Obiettivi



Compliance Misure minime di sicurezza ICT

Il nostro approccio

Referente Cyber a disposizione dei clienti con **forti competenze normative, tecniche e legali**

Framework digitale dinamico già pronto all'uso, creato secondo normative, standard e best practice, in cui avere traccia di tutti i documenti di sicurezza (norme, politiche, procedure) e dei processi con **Interacta**

Servizio continuativo di **consulenza, formazione e supporto** in grado di gestire tutti gli aspetti in modo efficace e misurabile.

Legge n. 90 del 28 giugno 2024 in vigore dal 02 luglio 2024:

"Disposizioni in materia di rafforzamento della cyber sicurezza nazionale e di reati informatici"

Nuove responsabilità per le PA e per le Aziende partecipate

La legge impone alle Amministrazioni Pubbliche tra le altre cose, l'obbligo di segnalare in modo tempestivo gli incidenti informatici subiti, e di nominare un Responsabile della Cybersicurezza, migliorando tanto la capacità di prevenzione quanto quella di risposta agli attacchi cyber.

dinova

GRUPPO Maggioli

A chi si applica

- ✔ **PA centrali** incluse nell'elenco annuale ISTAT
- ✔ **Regioni** e le **province autonome** di **Trento e di Bolzano**
- ✔ **Città metropolitane**
- ✔ **Comuni** con popolazione **superiore a 100.000 abitanti**
- ✔ **Comuni capoluoghi di regione**
- ✔ **Società** di **trasporto pubblico urbano** con bacino di utenza non inferiore a 100.000 abitanti
- ✔ **Società** di **trasporto pubblico extraurbano** operanti nell'ambito delle città metropolitane
- ✔ Aziende **sanitarie locali**;
- ✔ **Società *in house*** degli enti fin qui richiamati, qualora siano fornitrici di **servizi informatici**, dei **servizi di trasporto** sopra indicati, dei servizi di **raccolta, smaltimento o trattamento di acque reflue** urbane, domestiche o industriali, ovvero servizi di **gestione dei rifiuti**

Obblighi normativi

1. Sviluppo **politiche** e **procedure di sicurezza** delle informazioni.
2. Produzione e aggiornamento di un **piano di gestione del rischio informatico**.
3. Produzione e aggiornamento di sistemi di **analisi preventiva** di **rilevamento del rischio informatico**.
4. Produzione e aggiornamento di un documento che definisca i **ruoli** e l'**organizzazione del sistema per la sicurezza delle informazioni**.
5. Pianificazione e attuazione dell'adozione delle **misure previste** dalle **linee guida per la cybersicurezza** emanate da **ACN.**
6. Monitoraggio e valutazione continua delle **minacce alla sicurezza** e delle **vulnerabilità dei sistemi** per il loro pronto aggiornamento.
7. In caso di uso di programmi e applicazioni informatiche e di comunicazione elettronica che impiegano soluzioni crittografiche, rispetto delle **linee guida su crittografia** e **conservazione delle password** adottate da ACN e dal Garante Privacy.

Obblighi normativi

8. verifica delle **vulnerabilità note** su programmi e applicazioni informatiche e di comunicazione elettronica in uso
9. Individuazione formale della **Struttura** e del **Referente per la cybersicurezza** in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza. Il Referente per la cybersicurezza può essere individuato anche nella figura del *Responsabile per la transizione al digitale*.
10. Qualora i soggetti non dispongano di personale dipendente fornito di tali requisiti, possono **conferire l'incarico** di Referente per la cybersicurezza a un **dipendente di una pubblica amministrazione**, previa autorizzazione di quest'ultima.
11. Il Referente per la cybersicurezza svolge anche la funzione di **punto di contatto unico** dell'amministrazione con **l'Agenzia per la cybersicurezza nazionale** (ACN).

Sanzioni

Con riguardo all'obbligo di **comunicazione degli incidenti di sicurezza e correzione delle vulnerabilità** viene previsto:

- Applicazione della **sanzione amministrativa** pecuniaria **da un minimo di 25.000 euro a un massimo di 125.000 euro**, se l'inadempimento è reiterato nell'arco di 5 anni
- **Responsabilità disciplinare e amministrativo-contabile** nei confronti dei **funzionari** e dei **dirigenti** responsabili.

Riguardo gli adempimenti inerenti l'adozione di **politiche** e **procedure** di sicurezza, **analisi preventiva**, **rilevamento** e **gestione del rischio** informatico, questi rientrano nel quadro delle misure di sicurezza introdotte con la Direttiva NIS 2, quindi si applicano le **sanzioni definite dal D.Lgs 138/2024** di recepimento.

Direttiva Europea NIS 2

“Sicurezza delle reti e delle informazioni”

Direttiva UE 2022/2555 in vigore dal gennaio 2023, sulla sicurezza delle reti e delle informazioni, **recepita in Italia con D.Lgs. 138/2024 del 4 settembre**, la quale abroga e sostituisce la precedente Direttiva NIS 1 del 2016 nell’ottica di modernizzazione dell’attuale quadro europeo in tema di cybersecurity.

La NIS 2 ha il chiaro intento di rafforzare il livello globale di cybersicurezza, onde garantire “**l’adozione di misure tecniche e organizzative adeguate contro i rischi cyber**» attraverso un aumento delle capacità di resilienza in base ad un approccio proattivo di prevenzione e minimizzazione degli impatti che gli incidenti di sicurezza possono determinare.

NIS 2

D.Lgs. 138/2024 di recepimento nell’ordinamento Italiano

dinova

GRUPPO Maggioli

A chi si applica

Soggetti Essenziali (>250 dipendenti o un fatturato annuo >50 ML o il totale di bilancio annuo >43 ML) e **Soggetti Importanti** (con <250 dipendenti o un fatturato annuo <50 milioni di Euro o il totale di bilancio annuo <43 ML) dei *seguenti settori*:

- ✔ **Settori ad Alta Criticità** (All. 1 Dlgs 138/2024): Energia, Trasporti, Bancario, Sanità, Acqua, Infrastruttura digitale, Servizi ICT, Pubblica amministrazione, Spazio
- ✔ **Settori Critici** (All. 2 Dlgs 138/2024): Posta e corrieri, Gestione dei rifiuti, Prodotti chimici, Alimentare, Manifatturiero, Servizi digitali, Ricerca
- ✔ **Pubbliche amministrazioni** indipendentemente dalle dimensioni (All. 3 Dlgs 138/2024): amministrazioni centrali, amministrazioni regionali, amministrazioni locali, altri soggetti pubblici.
- ✔ **Ulteriori Soggetti** indipendentemente dalle dimensioni (All. 4 Dlgs 138/2024): fornitori di servizi di trasporto pubblico locale; Istituti di istruzione che svolgono attività di ricerca; Soggetti che svolgono attività di interesse culturale; Società in house, società partecipate e società a controllo pubblico.

NIS 2

D.Lgs. 138/2024 di recepimento nell'ordinamento Italiano

dinova

GRUPPO Maggioli

Misure di sicurezza obbligatorie

- **Politiche** di **analisi dei rischi** e di **sicurezza dei sistemi informatici**
- Gestione efficace degli **incidenti di sicurezza**
- **Garanzia di Continuità operativa**, **backup, disaster recovery**, e **gestione delle crisi**
- Sicurezza della **catena di fornitura**
- Sicurezza nell'**acquisizione**, **sviluppo**, **manutenzione** dei **sistemi informatici** e di **rete**, gestione e divulgazione delle **vulnerabilità**
- **Strategie** e **procedure** di gestione efficace dei **rischi cyber**
- Pratiche di "**igiene informatica**" di base e **formazione** in materia di cybersicurezza;
- **Politiche** e **procedure** di **crittografia** e **cifratura**
- Sicurezza delle **risorse umane**, strategie di **controllo accessi**, utilizzo di soluzioni che prevedano l'autenticazione a più fattori di comunicazioni protette vocali/video/testuali

NIS 2

D.Lgs. 138/2024 di recepimento nell'ordinamento Italiano

dinova

GRUPPO Maggioli

Sanzioni

Sanzioni: di natura pecuniaria con carattere interdittivo con divieti temporanei nei riguardi degli apicali (amministratori delegati, ecc.), di esercitare funzioni dirigenziali. In termini di ammontare, sono previsti:

- Per i **soggetti essenziali**, **sanzioni amministrative pecuniarie fino a 10 milioni di euro o il 2% del fatturato totale annuo**
- Per i **soggetti importanti**, **sanzioni amministrative pecuniarie fino a 7 milioni di euro o 1,4% del fatturato totale annuo**
- Per le **pubbliche amministrazioni** di cui **all'allegato III del Dlgs.138/2024**, nonché per i **soggetti** rientranti fra le tipologie di cui **all'allegato IV**, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti essenziali, **sanzioni amministrative pecuniarie da euro 25.000 a euro 125.000**

Principali scadenze DLGS 138/2024

- *Entro il 31.12.24* – Verifica di applicabilità NIS 2
- *01.01.25 - 28.02.25* - Registrazione sulla piattaforma digitale di ACN
- *01.04.25 -15.04.25* – Comunicazione ai soggetti registrati del loro inserimento nell'elenco ACN.
- *Entro il 15.04.25* – Nomina interna del soggetto responsabile dell'adempimento degli obblighi normativi.
- *15.04.25 - 31.05.25* – Fornitura a ACN di ulteriori informazioni richieste dalla normativa.
- *Dal 01.01.26* - Obbligo di notifica degli incidenti.
- *Entro il 01.09.26* – Adempimento:
  - agli obblighi degli organi di amministrazione e direttivi.
  - agli obblighi in materia di misure di sicurezza.
  - all'obbligo di raccolta e mantenimento di una banca dei dati.
  - di registrazione dei nomi di dominio, laddove applicabile.

NIS 2

D.Lgs. 138/2024 di recepimento nell'ordinamento Italiano

Fabio Mario Bernardino

Referente Interacta area PA

dinova

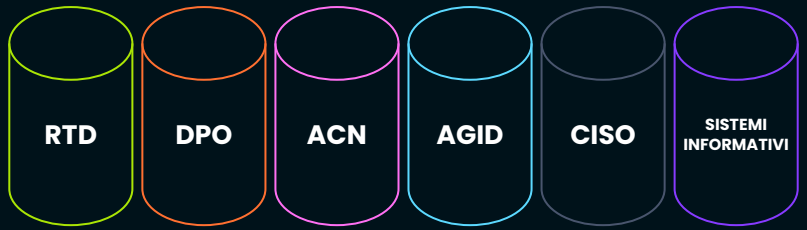
GRUPPO Maggioli

Non esiste un approccio universale alla cybersecurity

*Per questo motivo, adottiamo un approccio **olistico** che abbraccia **governance**, **tecnologie** e **fattore umano***

Come è gestita la cybersecurity oggi?

La governance della cybersecurity inerente privacy, normative, regolamenti, politiche e procedure all'interno di un'organizzazione è sovente divisa in **SILOS** complicando la gestione delle informazioni e la comunicazione tra gli attori del processo.



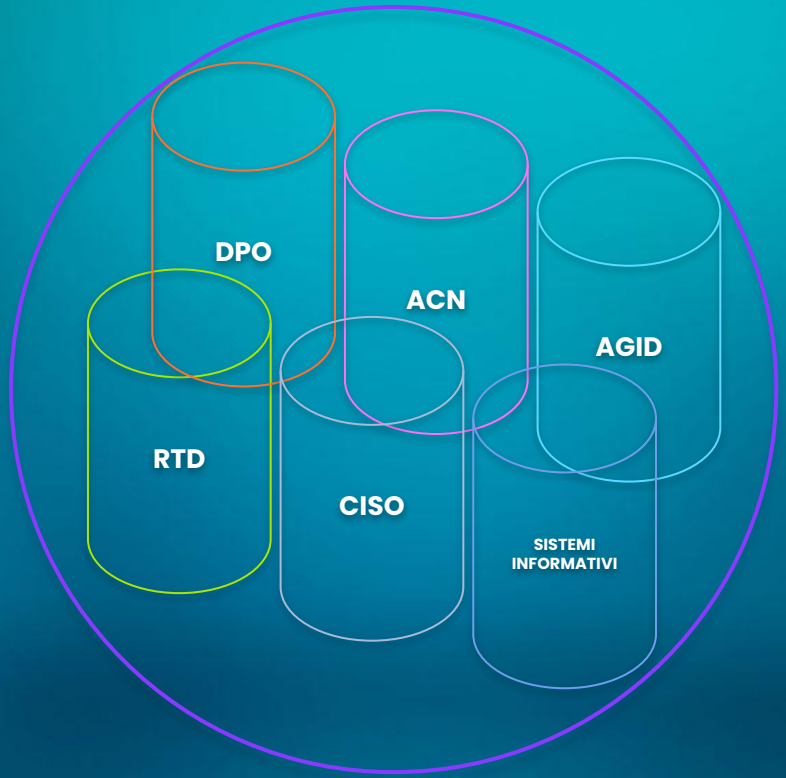
dinova

GRUPPO Maggioli

Tecnologie, Governance e Fattore Umano

Definire ruoli, responsabilità, processi e procedure per assicurare che la sicurezza sia **integrata** in ogni aspetto del Business, garantendo la conformità a leggi e normative e aumentando la cultura delle persone.

...e gestire tutto con uno strumento unico



dinova

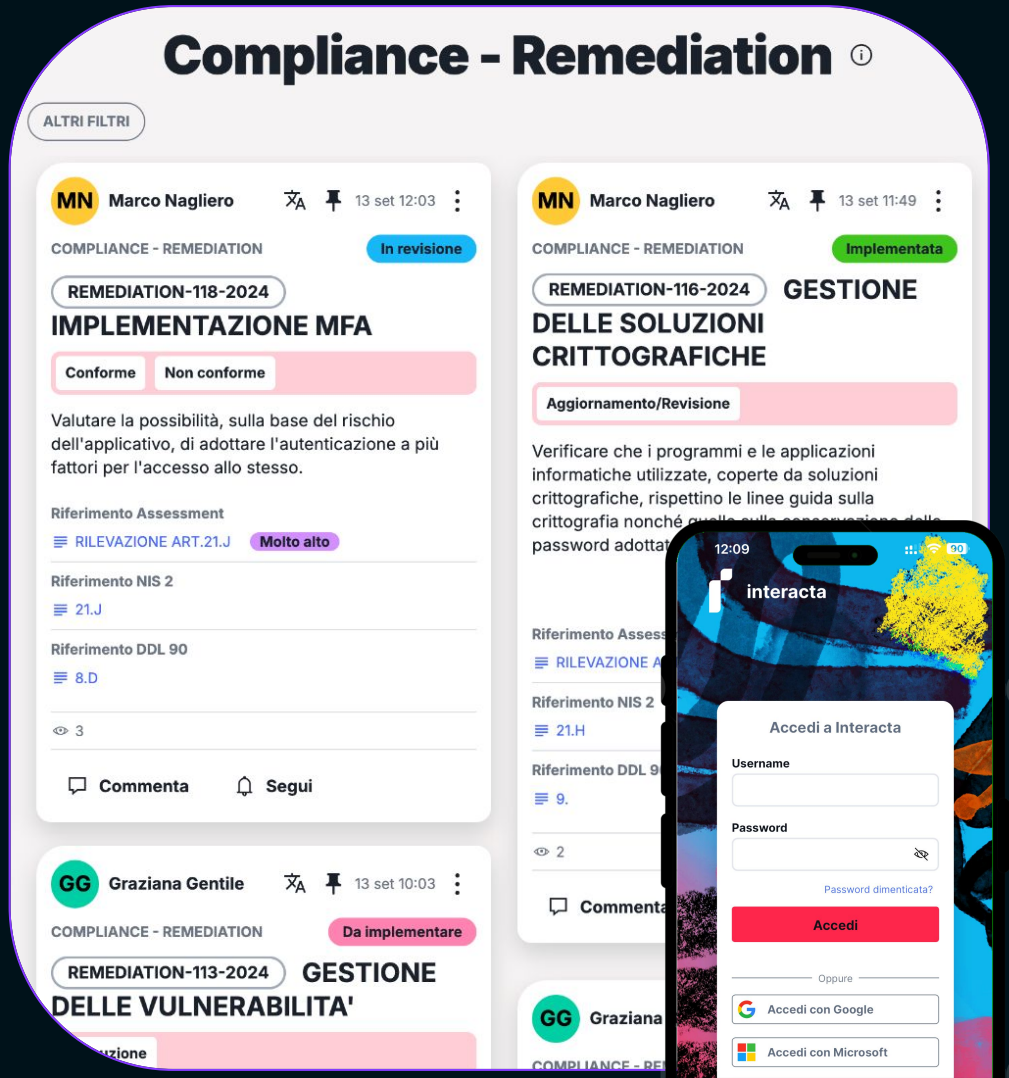
GRUPPO Maggioli

Interacta

Per una governance omnicomprensiva e dinamica della cybersecurity, **Interacta** è lo strumento perfetto di gestione di strategie, processi, comunicazioni e conoscenza.

Interacta è già pronta all'uso per i processi di:

- Compliance misure minime ICT
- Compliance DDL 90
- Compliance NIS 2
- Risk management
- Information & Asset inventory
- Gestione vulnerabilità/minacce
- Incident management
- Referente cyber / CISO as a Service



Francesco Schifilliti

Responsabile Cyber Defense

dinova

GRUPPO Maggioli

BUSINESS UNIT DEEPCYBER – CYBER DEFENSE

Services Overview

ATTACK SURFACE MANAGEMENT

L'**Attack Surface Management** è un approccio proattivo e continuo per proteggere le risorse IT di un'organizzazione.

Gestire efficacemente la superficie di attacco richiede una combinazione di tecnologie avanzate, processi ben definiti e una forte cultura della sicurezza all'interno dell'organizzazione, ma consente alle organizzazioni di ridurre significativamente il rischio di compromissione e migliorare la loro resilienza contro le minacce informatiche.

Principali attività compongono il servizio

- **Monitoraggio delle Minacce:** Implementare soluzioni di monitoraggio per rilevare attività sospette e potenziali attacchi in tempo reale.
- **Analisi delle Vulnerabilità:** Utilizzare strumenti di scansione delle vulnerabilità per identificare debolezze e punti di ingresso sfruttabili.
- **Prioritizzazione dei Rischi:** Valutare l'impatto e la probabilità delle vulnerabilità identificate e prioritizzare le azioni di mitigazione.

ATTACK SURFACE MANAGEMENT

- **Improved Visibility** - Discovery di tutte le risorse esterne, infrastrutture dimenticate, conferma le risorse della tua organizzazione per generare un inventario degli asset IT aggiornato, automatizza il rilevamento delle risorse IT e mappa continuamente la superficie esterna di attacco dell'organizzazione
- **Threat Intelligence Data** - Ottieni informazioni dettagliate sui rischi nascosti come i credential dumps, dark web mention, botnet, malware, etc.
- **Risk Assessment** - Controlla le risorse confermate per vulnerabilità comuni e assegna ad ognuna un punteggio di rischio per ottimizzare il piano di remediation
- **Stronger Security Posture** - Riduce i rischi e risolvi i problemi che forniscono risultati misurabili per il tuo programma di sicurezza

dinova

GRUPPO Maggioli

EARLY WARNING

L'**Early Warning** è essenziale per proteggere le risorse informatiche e ridurre il rischio di attacchi informatici.

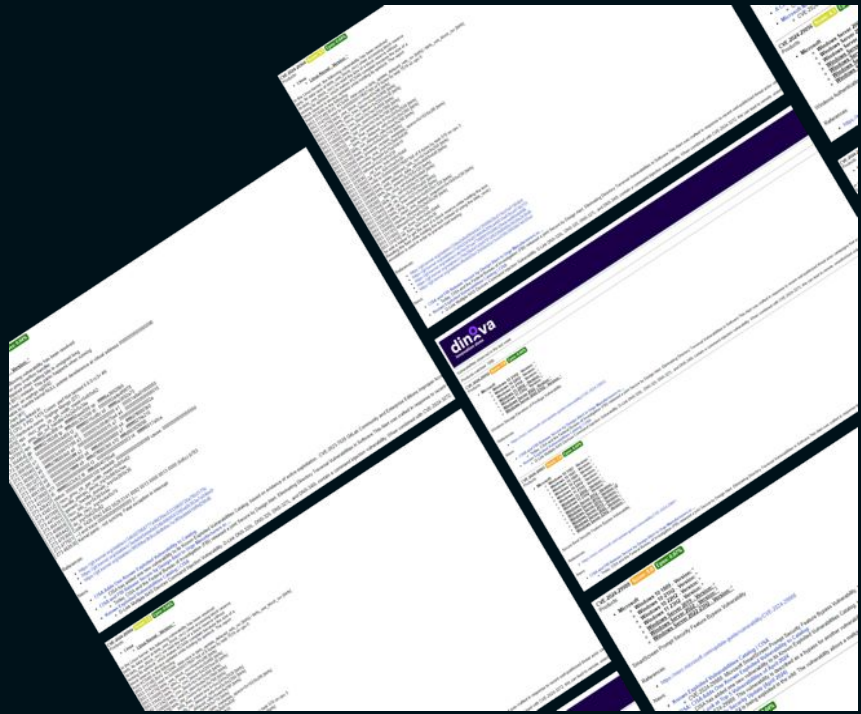
Implementare un processo sistematico e continuo di identificazione, valutazione, trattamento e monitoraggio delle vulnerabilità aiuta le organizzazioni a mantenere un elevato livello di sicurezza e a rispondere rapidamente alle minacce emergenti

Principali attività compongono il servizio

- **Monitoraggio Continuo**: implementazione di un monitoraggio continuo per rilevare nuove vulnerabilità e verificare l'efficacia delle misure di mitigazione applicate.
- **Classificazione e Prioritizzazione**: valutazione delle vulnerabilità in base alla loro gravità, impatto potenziale e probabilità di sfruttamento. Le metriche comuni utilizzate includono il CVSS (Common Vulnerability Scoring System).
- **Valutazione del Rischio**: considerazione del contesto specifico dell'organizzazione, inclusi fattori come l'esposizione del sistema, la criticità dei dati e la presenza di misure di mitigazione esistenti.

EARLY WARNING

- Il servizio Early Warning è una soluzione proattiva progettato per mantenere i nostri clienti informati relativamente alle minacce emergenti.
- Utilizzando tecnologie avanzate e informazioni sulle minacce, il nostro sistema monitora continuamente tutte le nuove vulnerabilità.
- Manteniamo un database completo e aggiornato delle vulnerabilità conosciute, comprese le Common Vulnerabilities and Exposures (CVE)
- Ogni volta vengano identificate nuove CVE che possono avere un impatto sui prodotti dei nostri clienti, il nostro sistema verifica automaticamente le corrispondenze e avvisa le parti interessate.



THIRD-PARTY MONITORING

Il **Monitoraggio delle Terze Parti** è il processo di valutazione che persegue due obiettivi:

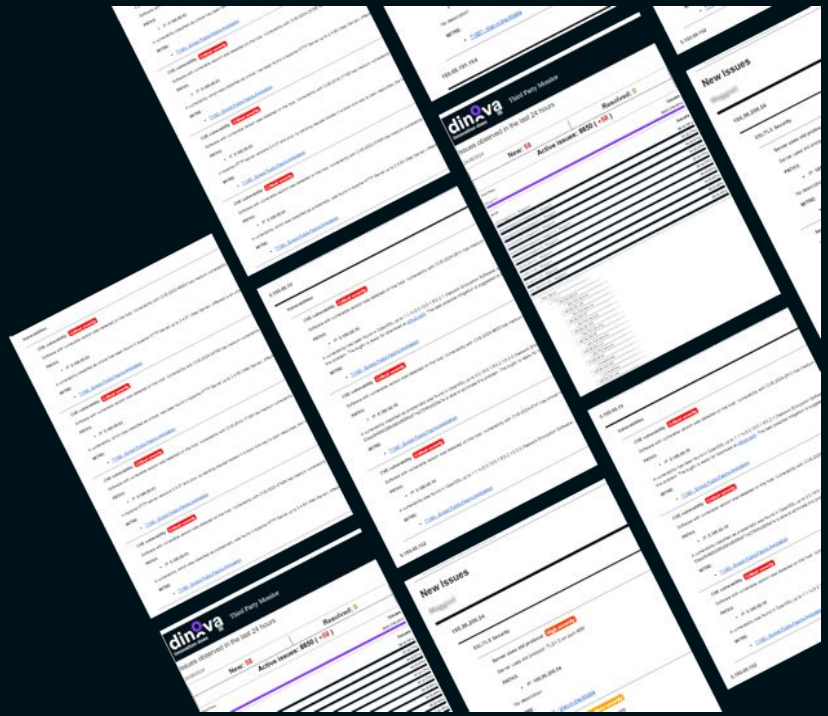
1. gestione del Rischio: Identificare e mitigare i rischi di sicurezza legati alle terze parti per proteggere i dati sensibili e le risorse IT.
2. conformità: Assicurarsi che le terze parti aderiscano alle normative di sicurezza e ai requisiti di conformità applicabili.

Principali attività compongono il servizio

- **Catalogare e Classificare le 3P**: mantenere un inventario aggiornato di tutte le terze parti con cui l'organizzazione interagisce, classificandole in base al livello di rischio associato.
- **Valutazioni di Rischio Periodiche**: eseguire valutazioni di rischio periodiche per tutte le terze parti, aggiornando le valutazioni in base ai cambiamenti nel contesto operativo o nelle minacce.
- **Implementare piattaforme e strumenti di monitoraggio dedicati**: che possano automatizzare la raccolta dei dati, l'analisi delle minacce e la gestione delle vulnerabilità per le terze parti.

THIRD-PARTY MONITORING

- Il monitoraggio di terze parti comporta l'analisi e la valutazione di fornitori, partner e altre entità esterne che interagiscono con i sistemi, i dati o le reti di un'organizzazione.
- Il monitoring dell 3P è un aspetto cruciale, poiché queste entità possono introdurre rischi significativi per la sicurezza.
- Questo processo comprende il monitoraggio continuo degli asset di terze parti, la valutazione del rischio di ogni problema per valutare la proattività e la consapevolezza dei partner rispetto al rischio informatico.



VULNERABILITY ASSESSMENT & PENTESTING

I servizi di **Vulnerability Assessment & Penetration Testing** sono i processi di valutazione di sicurezza necessari a verificare lo stato di sicurezza di due tipologie di asset:

1. Le infrastrutture, ovvero gli apparati (server, PdL, network device, etc.) che sono presenti nelle reti interne/esterne per contribuire all'erogazione dei servizi e alla produzione
2. Le applicazioni, ovvero il software scritto ad-hoc o commerciale utilizzato per erogare i servizi verso gli utenti

Principali attività compongono il servizio

- **Identifying & Evaluating Vulnerabilities**: identificare il perimetro e ricercare le vulnerabilità e valutare gli esiti della ricerca delle vulnerabilità.
- **Treating Vulnerabilities**: sviluppare e realizzare dei piani di remediation per le vulnerabilità «risolvibili» o, in alternativa, predisporre delle azioni di mitigazione ovvero formalizzare l'accettazione del rischio.
- **Reporting Vulnerabilities**: a seguito delle attività di remediation verificare la corretta esecuzione delle correzioni ed introdurre misure migliorative nella gestione delle configurazioni e nelle operazioni di sicurezza.

VULNERABILITY ASSESSMENT & PENTESTING

- Il VAPT Infrastrutturale si compone di varie fasi di approfondimento modulate anche a seconda della tipologia dei target e sono una sintesi della metodologia OSSTMM. Le fasi eseguite permettono di emulare pienamente il comportamento di un attacco reale.

- Il Web Application Testing si basa sui principi della metodologia OWASP e delle procedure di Vulnerability Assessment applicativo sviluppate autonomamente e affinate nel tempo in base all'esperienza accumulata. Le fasi seguite nel WAT sono pienamente compatibili con le linee guida proposte dall'Agid per la verifica delle web application.

Managed Detection and Response

Il **Managed Detection and Response (MDR)** è un servizio di sicurezza che combina la tecnologia avanzata di rilevamento delle minacce con il monitoraggio continuo e la risposta gestita da un team di esperti di sicurezza.

Principali attività compongono il servizio

- **Monitoring**: monitoraggio continuativo H24 effettuato da un Security Operation Center
- **Response**: Intervento degli analisti del Security Operation Center in caso di incidente o tentativo di attacco. Un esempio di response è l'isolamento della macchina (client o server) dal resto dell'infrastruttura per impedire l'attacco
- **Reporting**: Report periodici e incontri con i referenti dell'organizzazione per approfondimenti sulle attività del SOC e dei possibili miglioramenti

Per info e contatti:
marketing@maggioli.it

dinova

interacta

GRUPPO Maggioli