

Kit Software Documentale Procedure Adempimenti Direttiva NIS2

Questo PDF contiene un esempio dei materiali Winple. Per verificare la versione, i contenuti completi, gli altri dimostrativi e la disponibilità, visita la scheda del prodotto.

APRI LA SCHEDA DEL PRODOTTO



www.wingle.it/kit-procedure-modulistica-politiche-adempimenti-direttiva-nis-2/

Analizzare la probabilità e l'impatto

Siccome le minacce insistono sugli asset strategici, nella fase di identificazione del rischio l'organizzazione provvede a stimare la "rilevanza" di ciascun asset rispetto alla tenuta generale del servizio reso dall'organizzazione ai suoi destinatari.

Analisi dell'impatto

Quanto maggiore risulta la rilevanza del singolo asset (nel funzionamento complessivo dell'organizzazione) tanto maggiore risulterà l'impatto complessivo in termini di sicurezza, resilienza e continuità operativa nel caso l'asset subisse sottrazione, alterazione, distruzione e cioè l'evento negativo.

Nel modulo **MOD-01-Rischio Cyber** alla scheda **Rischio**, in corrispondenza di ciascun asset strategico individuato l'organizzazione stima la rilevanza attraverso i seguenti fattori da valutare:

Criticità		
	Livello	Descrizione
La criticità rappresenta il grado di importanza dell'asset per il raggiungimento degli obiettivi dell'organizzazione. Un asset è più critico quanto più la sua compromissione può impattare negativamente su operatività, sicurezza, reputazione o servizi erogati	1	Impatto importante, ma limitato a specifiche aree/servizi dell'organizzazione
	2	Impatto significativo su un singolo processo critico, senza però causare disservizi diffusi
	3	Impatto rilevante su più processi o su un servizio essenziale, con effetti temporanei ma gestibili
	4	Impatto molto rilevante, causa disservizi gravi e/o perdita di continuità operativa estesa
	5	Impatto critico su vasta scala: blocco generalizzato di attività core, danni molto gravi e diffusi

Peso		
	Livello	Descrizione
Il peso rappresenta la rilevanza specifica dell'asset all'interno dell'insieme degli asset strategici dell'organizzazione. Un asset con un peso maggiore è maggiormente trasversale, centrale o insostituibile nei processi core rispetto agli altri asset strategici	1	Asset importante per un singolo processo strategico, ma non trasversale ad altri processi core
	2	Asset rilevante per più processi strategici, con impatto significativo ma non determinante
	3	Asset centrale per uno o più servizi chiave, il cui funzionamento regolare è essenziale
	4	Asset strategico e trasversale, fondamentale per la maggior parte delle attività core dell'organizzazione
	5	Asset insostituibile da cui dipende la continuità operativa dell'intera organizzazione

Piano di gestione delle vulnerabilità

Scopo del piano

Il presente Piano ha lo scopo di descrivere la modalità con cui l'organizzazione procede a gestire le vulnerabilità in maniera efficace e tempestiva allo scopo di ridurre il rischio cyber a cui è esposta.

Struttura

Il piano è strutturato dalle seguenti fasi operative:

- a) Identificazione delle Vulnerabilità
- b) Pianificazione delle Attività
- c) Modalità di Monitoraggio
- d) Analisi e Risposta alle Informazioni sulle Vulnerabilità

Fasi operative

a) Identificazione delle Vulnerabilità

Il processo di identificazione delle vulnerabilità non si limita a un'unica attività, ma si basa su un approccio multi-livello che combina test proattivi con il monitoraggio continuo.

- **Identificazione Proattiva:**

- **Scansioni e Penetration Test:** Il **Security Engineer** e il **Penetration Tester** eseguono scansioni periodiche delle reti e delle applicazioni per individuare vulnerabilità note e configurazioni errate. I risultati vengono registrati e analizzati per stabilire la criticità
- **Code Review:** L'**Application Security Specialist** esegue revisioni del codice per identificare potenziali vulnerabilità nelle applicazioni sviluppate internamente, garantendo la sicurezza del software fin dalle prime fasi di sviluppo
- **Vulnerability assessment:** Tutto il personale ricerca attivamente eventuali vulnerabilità (fisiche, organizzative, ecc) in tutti gli elementi dell'organizzazione

- **Identificazione Reattiva:**

- **Monitoraggio dei Log:** Il **Security Analyst** monitora costantemente i log di sistema e di rete per rilevare anomalie o tentativi di accesso non autorizzato che potrebbero indicare una vulnerabilità

6. Condizioni di attivazione

Il piano viene attivato in caso di un'interruzione di servizio o di un incidente che non è considerato catastrofico, ma che ha un **impatto significativo o alto** sul business.

Casi di esempio per l'attivazione del piano	
1. Attacco Ransomware non diffuso	Un attacco ransomware colpisce il Sistema di ticketing tecnico, rendendolo inutilizzabile. Sebbene l'attacco non si sia diffuso ad altri sistemi critici, l'interruzione del processo di assistenza tecnica è considerata un impatto significativo sul business, che richiede l'attivazione del piano
2. Interruzione del Software di un fornitore	Il servizio fornito da un fornitore strategico, ad esempio il Software di configurazione e gestione reti LAN, subisce un'interruzione a causa di una vulnerabilità non gestita. L'impossibilità di configurare la rete compromette il funzionamento di numerosi asset, come la Centrale Servizi, con un impatto significativo
3. Degrado del Sistema di Controllo Fluviale	Un errore nel Sistema di gestione flussi idrici compromette l'accuratezza dei dati, causando un degrado del servizio piuttosto che un'interruzione totale. Questo degrado, pur non bloccando le operazioni, ha un impatto significativo sulla qualità del servizio fornito alla collettività e giustifica l'attivazione del piano
4. Violazione del Portale dei Contratti	Un attacco informatico sfrutta una vulnerabilità del Portale contratti e capitolati compromettendone l'integrità. Anche se i sistemi operativi rimangono in funzione, la compromissione di documenti contrattuali ha un impatto alto e richiede l'attivazione immediata del piano
5. Violazione delle Credenziali di un Dipendente	Le credenziali di un membro del personale con accesso a sistemi non critici vengono rubate tramite un attacco di phishing. Sebbene l'accesso iniziale non sia critico, la potenziale escalation dell'attacco rappresenta un rischio significativo, richiedendo l'attivazione delle procedure di continuità per contenere la minaccia

7. Condizioni di disattivazione

La disattivazione del piano avviene quando i servizi essenziali sono stati completamente ripristinati e il rischio è stato riportato a un **livello accettabile**. La chiusura formale è documentata, spesso con una relazione che ne attesta l'esito.

Condizioni da verificare per la disattivazione del piano	
Contenimento della minaccia	La causa principale dell'interruzione, che si tratti di un attacco informatico, un guasto hardware o un'altra minaccia, deve essere stata completamente identificata, contenuta e neutralizzata. Questo assicura che il ripristino dei servizi non porti a una nuova interruzione
Ripristino completo dei servizi	Tutti i processi di business critici e i sistemi che li supportano devono essere stati ripristinati e devono funzionare a un livello di servizio normale. Prima della disattivazione, deve essere condotta una verifica formale per confermare il pieno ripristino delle operazioni
Approvazione formale e documentazione della chiusura	La decisione di disattivare il piano non è automatica. Deve essere approvata da un'autorità designata, come il team di gestione della crisi o il responsabile della continuità operativa. La chiusura del piano deve essere documentata in un rapporto che riassume gli esiti dell'evento

2. Ruoli e responsabilità

Il piano assegna ruoli e responsabilità specifiche in caso di disastro, in linea con l'organizzazione per la sicurezza informatica definita nei tuoi documenti. I responsabili sono:

- Comitato di gestione della continuità operativa: Ha la responsabilità generale del piano e ne coordina l'attivazione e la disattivazione
- CSIRT: È il team principale incaricato del ripristino tecnico dei sistemi compromessi, con l'obiettivo di limitare l'impatto e ripristinare le normali operazioni
- Security Engineer: Collabora con il CSIRT per implementare le soluzioni tecniche di ripristino, come l'attivazione dei backup e dei sistemi ridondanti
- Amministratore di Sistema: È responsabile del ripristino operativo dei sistemi informativi e di rete

3. Contatti principali e canali di comunicazione (interni ed esterni)

Il piano prevede l'uso di canali di comunicazione dedicati e alternativi per garantire il coordinamento in caso di disastro.

- Interni: I contatti del personale chiave sono documentati nel modulo **MOD-03-Personale** e utilizzati per coordinare il team di ripristino
- Esterni: I contatti dei fornitori strategici sono riportati nel modulo **MOD-08-Supply chain**. Il Punto di Contatto NIS è il responsabile per le comunicazioni ufficiali con le autorità competenti, come il CSIRT Italia

4. Condizioni per l'attivazione e la disattivazione del piano

Attivazione: Il piano viene attivato solo in caso di un incidente che provoca un'interruzione totale dei servizi con un impatto catastrofico, valutato a un livello superiore a 14 sulla scala di rischio.

Disattivazione: La disattivazione avviene solo dopo una verifica completa del ripristino, con la conferma che tutti i sistemi funzionano correttamente e che l'organizzazione è tornata a uno stato di normalità operativa.

4. Comunicazioni

La comunicazione durante una crisi è gestita a livello strategico per controllare la narrativa e mantenere la fiducia degli stakeholder.

- Comunicazione interna: Il Comitato di Gestione della Crisi deve stabilire canali sicuri per comunicare con il personale, fornendo aggiornamenti tempestivi e istruzioni chiare per evitare la diffusione di informazioni non verificate
- Comunicazione esterna: La comunicazione con le autorità competenti, come il CSIRT Italia, è gestita esclusivamente dal Punto di Contatto NIS. Per il pubblico e i media, il comitato designa un unico portavoce ufficiale per garantire un messaggio coerente e trasparente

5. Procedura di esecuzione

La procedura di gestione della crisi è suddivisa in fasi chiare, che guidano il Comitato attraverso l'evento.

Fase	Descrizione
Rilevazione e Allerta	La crisi viene identificata attraverso la segnalazione di un incidente significativo. Il Security Analyst e l'Incident Response Team (CSIRT) forniscono un rapporto preliminare al Comitato
Attivazione del piano	Il Comitato di Gestione delle Crisi si riunisce immediatamente per valutare la gravità della situazione e dichiarare l'attivazione del piano di crisi
Gestione strategica	Il comitato si concentra sulla gestione delle conseguenze non tecniche della crisi. Le azioni includono la valutazione dell'impatto reputazionale, la comunicazione con gli stakeholder e le autorità, e la definizione di una strategia per il ritorno alla normalità
Chiusura e Valutazione	Una volta che l'evento è stato risolto e l'organizzazione è tornata a uno stato stabile, il piano viene formalmente chiuso. Viene condotta un'analisi post-crisi per identificare le lezioni apprese e per aggiornare i piani e le procedure per il futuro

Contenuti

Formazione per il personale di business

Per tutto il personale impiegato nei processi di business, in ragione del contesto, l'organizzazione ritiene necessaria la formazione inerente ai seguenti moduli formativi:

- Phishing e ingegneria sociale
- Sicurezza delle password e autenticazione
- Uso sicuro di email, web e dispositivi
- Policy aziendali di sicurezza e ruoli
- Gestione delle vulnerabilità
- Configurazione sicura dei sistemi
- Incident response
- Protezione dei dati e crittografia
- Minacce informatiche e scenari di attacco
- Governance della sicurezza e responsabilità

Formazione per il personale tecnico

Per il personale tecnico, in ragione del contesto, l'organizzazione ritiene necessaria la formazione inerente ai seguenti moduli formativi:

Ruolo	Modulo Formativo Specialistico
Chief Information Security Officer	Strategia e governance della sicurezza
	Normative (NIS2, GDPR, DORA, ISO 27001)
	Gestione del rischio cyber
Security Officer / Information Security Manager	Compliance framework (ISO, NIS2)
	Incident management avanzato
	Monitoraggio dei controlli
Security Analyst	Analisi dei log e tecniche SIEM
	Threat detection e intelligence
	Tecniche di triage degli eventi
Security Engineer	Hardening sistemi e reti
	Patch management
	Sicurezza cloud e container
Incident Response Team (CSIRT)	Tecniche di contenimento e risposta
	Analisi forense base
	Simulazioni tabletop
Penetration Tester / Ethical Hacker	Tecniche di penetration testing (OWASP, OSSTMM)
	Uso di strumenti (Burp, Metasploit, Nmap, etc.)

4. Attività operative e responsabilità

g) Comunicazione

Entro un mese dalla trasmissione della notifica dell'incidente, il responsabile del punto di contatto NIS2 provvede a comunicare al CSIRT Italia:

1. Una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto
2. Il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente
3. Le misure di attenuazione adottate e in corso
4. Ove noto, l'impatto transfrontaliero dell'incidente

La relazione è documentata nel modulo **MOD-24-Relazione finale CSIRT**.

Le informazioni per la redazione della relazione sono già presenti, in parte nel modulo **MOD-22-Registro incidenti**.

h) Documentazione

L'organizzazione rileva e registra tutte le fasi che caratterizzano l'incidente e lo descrivono nel suo divenire dalla genesi fino al ripristino.

Nel modulo **MOD-22-Registro incidenti** l'organizzazione raccoglie le informazioni che le permettono di comprendere come è avvenuto l'incidente e come prevenirlo.

Le informazioni sono:

- Chi ha rilevato l'incidente
- Quali vulnerabilità sono state registrate e a quale livello
- Quali asset strategici (Reti e sistemi) sono stati interessati dall'incidente
- Quali asset operativi sono stati interessati dall'incidente
- Com'è aumentata la probabilità del rischio cyber
- Quale valore ha assunto il rischio
- Qual è stato l'impatto sui dati
- Qual è stato l'impatto sulle persone fisiche
- Qual è stato l'impatto sugli asset
- Quali sono le cause dell'incidente significativo
- Cosa ha reso l'incidente significativo
- Quali controlli di sicurezza non hanno funzionato
- Com'è stato ripristinato il regolare funzionamento

Il registro incidenti è reso disponibile alle parti interne al punto di contatto NIS 2 per comunicare all'interno dell'organizzazione il ripristino dei servizi