BeeProd
Sweet productivity.

360consulenza

WHITE PAPER

SOLUZIONI PER LA DIRETTIVA NIS2

beeprod.it
360consulenza.com

COS'È LA NORMATIVA NIS2?

Nel gennaio 2023, i Paesi membri dell'UE hanno ufficialmente approvato una revisione della Direttiva sulla sicurezza delle reti e dei sistemi informatici (NIS) del 2016. Questa nuova versione, nota come Direttiva NIS2, è stata sviluppata in risposta a numerosi cyber attacchi di grande rilievo e dannosi. La Direttiva NIS2 innalza gli standard di sicurezza, semplifica gli obblighi di segnalazione, e introduce misure di sorveglianza più stringenti, oltre a requisiti di applicazione più severi. L'obiettivo principale della nuova Direttiva è rafforzare le difese delle infrastrutture critiche contro le vulnerabilità della catena di fornitura, gli attacchi ransomware e altre minacce informatiche. **Tutti i 27 Stati membri dell'UE dovranno recepire la Direttiva NIS2 entro il 17 ottobre 2024.**

Questo documento fornisce una breve panoramica della Direttiva NIS2, spiegando come essa potrebbe impattare la tua attività e come prepararti al meglio.

A CHI SI RIVOLGE?

La normativa è rivolta alle **medie e grandi imprese che operano nei seguenti settori**

Settori ad alta criticità	Energia	Salute	Trasporti	Finanza
	Infrastrutture digitali	Pubblica amministrazione	Spazio	Fornitura di acqua
Altri settori critici	Servizi digitali	Servizi postali	Gestione rifiuti	Ricerca
	Cibo	Fabbricazione	Sostanze chimiche	

COME PUÒ AIUTARTI LA NIS2?

Requisito	Come supporta la sicurezza delle identità
Paragrafo 49: Norme di cyber-igiene per le infrastrutture	
La sicurezza delle identità contribuisce a implementare buone pratiche di cyber-igiene, come la gestione delle password e la limitazione degli accessi amministrativi.	• Gestione degli accessi privilegiati per proteggere e controllare gli account amministrativi. • Gestione delle identità per proteggere le password e gli accessi degli utenti. • Rimozione dei diritti amministrativi locali sui dispositivi per prevenire l'escalation dei privilegi.
Paragrafo 53: Sicurezza per i settori delle utenze	
Protezione delle infrastrutture digitalizzate e delle città intelligenti da attacchi informatici.	• Gestione degli accessi privilegiati per isolare le sessioni e gestire le credenziali. • Rilevazione di comportamenti anomali che indicano potenziali attacchi. • Rimozione dei privilegi amministrativi permanenti per proteggere da attacchi informatici.
Paragrafo 54: Protezione contro il ransomware	
Difesa delle infrastrutture critiche da attacchi ransomware.	• Rimozione dei privilegi amministrativi sui dispositivi per limitare la diffusione del ransomware. • Isolamento e monitoraggio delle sessioni privilegiate per prevenire l'escalation dei privilegi.
Paragrafo 85: Sicurezza della supply chain	
Risoluzione delle vulnerabilità di sicurezza nella supply chain.	• Gestione dei segreti per monitorare e proteggere password, chiavi e certificati utilizzati da applicazioni e altre identità non umane. • Accesso remoto sicuro e registrazione delle sessioni per i fornitori esterni per applicare il principio del privilegio minimo.

Requisito	Come supporta la sicurezza delle identità
Paragrafo 89: Cyber-igiene per gli utenti	
Implementazione di buone pratiche di cyber-igiene, inclusi i principi Zero Trust e l'uso di tecnologie avanzate come l'intelligenza artificiale (IA) e il machine learning (ML).	• Autenticazione multifattoriale (MFA) per garantire l'identità degli utenti. • Limitazione degli accessi a finestre temporali specifiche per rafforzare i principi Zero Trust. • Utilizzo di MFA adattiva con analisi comportamentale basata sull'IA per determinare i fattori di autenticazione appropriati.
Paragrafo 98: Sicurezza della rete di comunicazioni elettroniche pubbliche	
Utilizzo della crittografia end-to-end e di concetti di sicurezza incentrati sui dati.	• Uso di tecnologie di crittografia per proteggere le credenziali e i segreti utilizzati da persone, applicazioni e macchine. • Isolamento delle sessioni privilegiate per ridurre la diffusione del malware. • Controllo degli accessi basato su policy e decisioni di accesso automatizzate.
Paragrafo 102: Comunicazione obbligatoria degli incidenti	
Le entità critiche devono notificare tempestivamente qualsiasi incidente.	• Audit e registrazione delle sessioni privilegiate per documentare gli incidenti. • Rilevazione automatica di comportamenti anomali che segnalano una violazione. • Uso di IA e ML per identificare attività sospette degli utenti.

COME ESSERE A NORMA?

Rischio	Soluzioni
1 - Procedure di analisi del rischio e di sicurezza del sistema informatico	
Senza procedure efficaci di analisi del rischio, le aziende potrebbero non identificare vulnerabilità critiche nei loro sistemi informativi. Questo potrebbe portare a esposizioni non mitigate che possono essere sfruttate da attori malevoli, causando violazioni di dati, interruzioni dei servizi e perdite finanziarie significative.	• **Strategia e governance della sicurezza informatica:** Implementare una governance solida per la sicurezza informatica che comprenda una chiara assegnazione di ruoli e responsabilità, allineata ai principali framework di settore (ISO/IEC 27001, NIST CSF). • **Assessment del rischio e maturità della cybersecurity:** Condurre regolarmente assessment approfonditi per valutare la maturità delle misure di sicurezza rispetto agli standard internazionali, identificando lacune e aree di miglioramento. • **Gap Analysis e supporto all'implementazione:** Effettuare analisi delle discrepanze rispetto alle normative e implementare le azioni correttive necessarie (ad es. implementazione di ISO/IEC 27001, SOC 2). • **Strumenti di gestione del rischio:** Utilizzare strumenti di gestione del rischio come GRC (Governance, Risk Management, Compliance) per monitorare i rischi in tempo reale e prendere decisioni informate.
2 - Procedure di gestione degli incidenti	
La mancanza di procedure strutturate di gestione degli incidenti può rallentare la risposta a eventi di sicurezza, aumentando il danno potenziale. Senza un piano chiaro, gli incidenti possono degenerare in crisi più ampie, causando danni reputazionali, perdite finanziarie e possibili sanzioni legali.	• **Pianificazione e implementazione della risposta agli incidenti (ISO/IEC 27035):** Sviluppare piani dettagliati di risposta agli incidenti che comprendano protocolli per l'identificazione, la risposta e il recupero in caso di incidente. • **Test di risposta agli incidenti:** Condurre regolarmente esercitazioni pratiche di simulazione di incidenti per valutare l'efficacia della risposta e migliorare la prontezza operativa. • **Penetration test mirati:** Implementare test di penetrazione regolari e simulazioni di attacco (red team/blue team) per identificare potenziali vulnerabilità prima che possano essere sfruttate. • **Intelligence sulle minacce:** Utilizzare intelligence avanzata (OSINT) per monitorare le minacce emergenti e migliorare la capacità di rilevamento proattivo.

Rischio	Soluzioni
3 - Gestione delle crisi e continuità operativa	
Se un'azienda non dispone di un piano di continuità operativa e di gestione delle crisi, un evento catastrofico potrebbe interrompere le operazioni aziendali per un periodo prolungato. Questo potrebbe comportare perdite finanziarie gravi, perdita di fiducia dei clienti e danni irreparabili alla reputazione.	• **Business Continuity Planning (ISO 22301):** Sviluppare e mantenere aggiornati i piani di continuità operativa che garantiscano la resilienza in caso di interruzione significativa delle operazioni. • **Business Impact Analysis (BIA):** Condurre analisi dettagliate degli impatti aziendali per identificare le priorità e le risorse critiche necessarie per mantenere l'operatività. • **Disaster Recovery Planning:** Implementare piani di disaster recovery che includano backup sicuri e test periodici per garantire la rapidità di recupero delle operazioni IT. • **Crisis Management:** Creare team dedicati alla gestione delle crisi con una formazione specifica per la gestione di eventi critici e l'adozione di procedure rapide e standardizzate, con obbligo di **notificare ai rispettivi CSIRT o all'autorità nazionale competente**.
4 - Sicurezza della supply chain	
La mancata sicurezza nella supply chain può esporre l'azienda a vulnerabilità attraverso fornitori o partner commerciali. Un attacco che sfrutta una debolezza nella supply chain può compromettere l'integrità dei dati aziendali, portando a interruzioni significative e potenziali violazioni di dati sensibili.	• **Gestione del rischio di terze parti (ISO/IEC 27036-2):** Stabilire procedure per valutare e monitorare costantemente la sicurezza dei fornitori e delle terze parti, con particolare attenzione alle vulnerabilità della supply chain. • **Framework di gestione dei fornitori:** Creare un quadro di gestione end-to-end per i fornitori, che includa valutazioni iniziali, monitoraggio continuo e audit periodici. • **Certificazione dei fornitori:** Richiedere ai fornitori di ottenere certificazioni di sicurezza riconosciute a livello internazionale (es. ISO 27001) come condizione per la partnership. • **Piattaforme di gestione della supply chain:** Utilizzare soluzioni tecnologiche avanzate per il monitoraggio e la gestione della supply chain in tempo reale, rilevando e mitigando potenziali rischi.

Rischio	Soluzioni
5 - Sicurezza della rete e dei sistemi informativi	
Senza adeguate misure di sicurezza della rete, i sistemi informativi possono essere compromessi da attacchi come ransomware, DDoS o intrusioni non autorizzate. Questo può portare a interruzioni dei servizi, perdita di dati critici e un impatto diretto sulle operazioni aziendali.	• **Implementazione di tecnologie Zero Trust**: Adottare un approccio Zero Trust per proteggere la rete, riducendo al minimo i privilegi e verificando costantemente ogni accesso. • **Segmentazione della rete:** Implementare la segmentazione della rete per isolare i sistemi critici e limitare il movimento laterale degli attacchi. • **Sicurezza fisica:** Integrare la sicurezza fisica con quella informatica, eseguendo assessment regolari e simulazioni di attacco per testare la resilienza. • **Automazione della sicurezza:** Implementare soluzioni di automazione per monitorare e rispondere alle minacce in tempo reale, riducendo al minimo i tempi di reazione.
6 - Gestione del rischio di cybersecurity	
L'assenza di una gestione proattiva del rischio di cybersecurity espone l'azienda a minacce che potrebbero non essere rilevate tempestivamente. Un rischio non gestito può materializzarsi in un attacco devastante che potrebbe essere prevenuto con un'adeguata valutazione e mitigazione dei rischi.	• **Sviluppo e implementazione di un framework di gestione del rischio IT (ISO/IEC 27005):** Integrare un framework di gestione del rischio che identifichi, valuti e mitighi i rischi legati alla sicurezza informatica in modo sistematico. • **Valutazione delle minacce:** Implementare un processo continuo di modellazione e valutazione delle minacce per comprendere e anticipare le potenziali minacce alla sicurezza. • **Reporting del rischio:** Creare un sistema di reporting chiaro e tempestivo per informare la leadership aziendale sui rischi emergenti e le misure di mitigazione adottate. • **Assessment della gestione del rischio di terze parti:** Valutare lo stato attuale della gestione del ciclo di vita delle terze parti e implementare soluzioni per migliorare il controllo sui fornitori.

Rischio	Soluzioni
7 - Pratiche di igiene informatica e corsi di formazione sulla cybersecurity	
La mancanza di pratiche di igiene informatica e di formazione adeguata rende il personale vulnerabile a phishing, social engineering e altre tecniche di attacco che sfruttano errori umani. Questo può portare a violazioni di sicurezza, diffusione di malware all'interno della rete e compromissione dei sistemi aziendali.	• **Programmi di sensibilizzazione sulla sicurezza informatica:** Implementare campagne di sensibilizzazione continue per educare il personale sulle migliori pratiche di sicurezza e sull'importanza dell'igiene informatica. • **Formazione specifica sulla Business Continuity:** Fornire corsi di formazione sulla continuità operativa e sulla gestione delle crisi per assicurare che tutti i dipendenti siano preparati. • **Simulazioni di attacco (team rosso/blu/viola):** Condurre simulazioni di attacco interne per verificare la preparazione dei dipendenti e migliorare la loro reattività agli incidenti di sicurezza. • **Gamification della formazione:** Utilizzare tecniche di gamification per rendere la formazione sulla sicurezza più coinvolgente e migliorare la retention delle informazioni.
8 - Sicurezza dei dati mediante crittografia e cifratura	
Senza un'adeguata crittografia dei dati, le informazioni sensibili possono essere intercettate o esfiltrate durante la trasmissione o l'archiviazione. Questo espone l'azienda al rischio di violazioni dei dati, furto di proprietà intellettuale e violazioni delle normative sulla protezione dei dati, con conseguenti sanzioni legali e danni reputazionali.	• **Implementazione di soluzioni avanzate di crittografia:** Utilizzare algoritmi di crittografia robusti per proteggere i dati sensibili sia in transito che a riposo, garantendo l'integrità e la riservatezza dei dati. • **Gestione delle chiavi crittografiche:** Implementare soluzioni sicure per la gestione delle chiavi crittografiche, assicurando che solo personale autorizzato possa accedere alle chiavi. • **Cifratura end-to-end delle comunicazioni:** Adottare soluzioni di cifratura end-to-end per tutte le comunicazioni interne, riducendo il rischio di intercettazioni. • **Soluzioni di crittografia omomorfica:** Per ambienti ad alta sicurezza, considerare l'implementazione di crittografia omomorfica per elaborare i dati crittografati senza doverli decrittografare.

Rischio	Soluzioni
9 - Sicurezza delle risorse umane	
La mancanza di misure di sicurezza per le risorse umane può portare a insider threats, dove dipendenti o ex-dipendenti con accesso non autorizzato possono compromettere i dati aziendali o causare danni intenzionali. Inoltre, l'accesso inappropriato ai sistemi aziendali da parte di personale non autorizzato rappresenta un rischio significativo.	• **Policy di sicurezza delle risorse umane:** Implementare policy che coprano l'intero ciclo di vita dei dipendenti, dalla selezione alla cessazione, includendo controlli di sicurezza pre-assunzione e la gestione sicura degli accessi post-cessazione. • **Controlli di accesso basati sui ruoli:** Implementare controlli di accesso basati sui ruoli (RBAC) per garantire che i dipendenti abbiano accesso solo alle informazioni necessarie per il loro lavoro. • **Monitoraggio continuo delle attività:** Utilizzare sistemi di monitoraggio delle attività dei dipendenti per rilevare comportamenti anomali o sospetti. • **Formazione e sensibilizzazione:** Integrare la sicurezza delle risorse umane con programmi di formazione che rafforzino la consapevolezza delle minacce interne.
10 - Sistemi di identificazione e autenticazione avanzati	
L'uso di sistemi di autenticazione deboli aumenta il rischio di accessi non autorizzati ai sistemi aziendali, facilitando l'attività di attori malevoli. Questo può portare a compromissioni di sistema, furto di dati e attacchi mirati che sfruttano credenziali rubate o deboli.	• **Implementazione di un approccio Zero Trust:** Configurare l'accesso ai sistemi e alle reti aziendali secondo i principi Zero Trust, dove ogni accesso è considerato una potenziale minaccia fino a prova contraria. • **Autenticazione a più fattori (MFA):** Utilizzare l'autenticazione a più fattori per proteggere l'accesso ai sistemi critici, combinando diversi metodi di verifica (es. password, token, biometria). • **Autenticazione continua:** Implementare sistemi che monitorano e verificano costantemente l'identità dell'utente durante la sessione, rilevando comportamenti anomali. • **Sistemi di comunicazione di emergenza protetti:** Adottare soluzioni di comunicazione protette per scenari di emergenza, assicurando la disponibilità e la sicurezza delle comunicazioni critiche anche in situazioni di crisi.

QUALI SONO LE DIFFERENZE TRA LA NORMATIVA NIS2 E LA ISO-27001?

Di seguito una tabella di confronto tra NIS2 e ISO 27001

NIS2 Measures	ISO/IEC 27001	
Article 20: Governance		
	Annex A	
	A.5.1	Policies for information security
	A.5.31	Legal, statutory, regulatory and contractual requirements
	A.5.34	Privacy and protection of personal Identifiable information (PII)
	A.5.35	Independent review of information security
	A.5.36	Compliance with policies, rules and standards for information security
	A.6.3	Information security awareness, education and training
Article 21: Cyber security risk management measures		
(A) Policies on risk analysis and information system security	5.2	Information security policy
	6.1.2	Information security risk assessment process
	6.1.3	Information security risk treatment process
	8.2	Information security risk assessment
	8.3	Information security risk treatment
	Annex A	
	A.5.1	Policies for information security
(B) Incident handling	**Annex A**	
	A.5.24	Information security incident management planning and preparation
	A.5.25	Assessment and decision on information security events
	A.5.26	Response to information security incidents
	A.5.27	Learning from information security incidents
	A.5.28	Collection of evidence
	A.6.8	Information security event reporting
	A.8.16	Monitoring activities

NIS2 Measures	ISO/IEC 27001	
Article 21: Cyber security risk management measures (cont.)		
(C) Business continuity, such as backup managemen and disaster recovery, and crisis management	**Annex A**	
	A.5.29	Information security during disruption
	A.5.30	ICT readiness for business continuity
	A.8.13	Information backup
	A.8.14	Information backup
	A.8.15	Logging
	A.8.16	Monitoring activities
(D) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	**Annex A**	
	A.5.19	Information security in supplier relationships
	A.5.20	Addressing information security within supplier agreements
	A.5.21	Managing information security in the ICT supply chain
	A.5.22	Monitoring, review and change management of supplier services
	A.5.23	Information security for use of cloud services
(E) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	**Annex A**	
	A.5.20	Addressing information security within supplier agreements
	A.5.24	Information security incident management planning and preparation
	A.5.37	Documented operating procedures
	A.6.8	Information security event reporting
	A.8.8	Management of technical vulnerabilities
	A.8.9	Configuration management
	A.8.20	Network security
	A.8.21	Security of network services
(F) Policies and procedures to assess the effectiveness of cybersecurity risk- management measures	9.1	Monitoring, measurement, analysis and evaluation
	9.2	Internal audit
	9.3	Management review
	Annex A	
	A.5.35	Independent review of information security
	A.5.36	Compliance with policies, rules and standards for information security

NIS2 Measures	ISO/IEC 27001	
Article 21: Cyber security risk management measures (cont.)		
(G) Basic cyber hygiene practices and cybersecurity training	7.3	Awareness
	7.4	Communication
	Annex A	
	A.5.15	Access control
	A.5.16	Identity management
	A.5.18	Access rights
	A.5.24	Information security incident management planning and preparation
	A.6.3	Information security awareness, education and training
	A.6.5	Responsibilities after termination of change of employment
	A.6.8	Information security event reporting
	A.8.2	Privileged access rights
	A.8.3	Information access restriction
	A.8.5	Secure authentication
	A.8.7	Protection against malware
	A.8.9	Configuration management
	A.8.13	Information backup
	A.8.15	Logging
	A.8.19	Installation of software on operational systems
	A.8.22	Segregation of networks
(H) Policies and procedures regarding the use of cryptography and, where appropriate, encryption	**Annex A**	
	A.8.24	Use of cryptography

NIS2 Measures	ISO/IEC 27001	
Article 21: Cyber security risk management measures (cont.)		
(I) Human resources security, access control policies and asset management	**Annex A**	
	A.5.9	Inventory of information and other associated assets
	A.5.10	Acceptable use of information and other associated assets
	A.5.11	Return of assets
	A.5.15	Access control
	A.5.16	Identity management
	A.5.17	Authentication information
	A.5.18	Access rights
	A.6.1	Screening
	A.6.2	Terms and conditions of employment
	A.6.4	Disciplinary process
	A.6.5	Responsibilities after termination or change of employment
	A.6.6	Confidentiality or non-disclosure agreements
(J) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications 5and secured emergency communication systems within the entity, where appropriate	**Annex A**	
	A.5.14	Information transfer
	A.5.16	Identity management
	A.5.17	Authentication information
Article 23: Reporting obligations		
	Annex A	
	A.5.14	Information transfer
	A.6.8	Information security event reporting
Article 24: Use of European cybersecurity certification schemes		
	Annex A	
	A.5.20	Addressing information security within supplier agreements

Non restare indietro: con noi al tuo fianco, l'adeguamento alla NIS2 sarà semplice e vantaggioso. Siamo qui per rendere il tuo business più sicuro, efficiente e pronto al futuro.

Contattaci

commerciale@beeprod.it

+39 080 987 7791