



NIS 2

ULTIMATE

SECUREBOX

La soluzione di Cyber Security
per le Micro e Piccole Aziende

■ Cos'è la Direttiva NIS2

La direttiva NIS2 (Network and Information Security Directive 2) è una normativa dell'Unione Europea che mira a rafforzare la sicurezza delle reti e delle informazioni nell'UE, introducendo requisiti più stringenti per la protezione dalle minacce cibernetiche all'interno della Supply Chain commerciale

SUPPLY CHAIN E CYBER SICUREZZA

■ Chi viene coinvolto dalla Direttiva

La direttiva è incentrata su tre criteri di valutazione circa il business di ogni azienda:

1. Settore di appartenenza
2. Dimensione
3. Ruolo

Sebbene la NIS2 si applica principalmente a organizzazioni di medie e grandi dimensioni, le Micro e Piccole Aziende sono incluse se operano in settori critici o forniscono servizi essenziali.

Inoltre, le Micro e Piccole Aziende che fanno parte della Supply Chain delle Medie e Grandi Imprese possono essere facilmente soggette agli obblighi della Direttiva, specialmente se la loro sicurezza influisce sulla resilienza complessiva del settore.





LE LINEE GUIDA INDICATE AGLI STATI DELL'EU PER LA CYBERSECURITY AZIENDALE

Richieste NIS2

Articolo 20, Governance

Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cybersicurezza e il loro impatto sui servizi offerti dal soggetto.

Articolo 21, Misure di gestione dei rischi di cibersicurezza

Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete... in base a:

- a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
- b) gestione degli incidenti;
- c) continuità operativa, come la gestione del backup e il

ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

COME ULTIMATE SECUREBOX RISPONDE CONCRETAMENTE ALLA NIS 2

Riassumiamo le richieste NIS2 in servizi e strumenti di Sicurezza

Formazione continua del personale:

La formazione deve riguardare le conoscenze base per una corretta postura di Sicurezza Informatica, al fine di prevenire comportamenti umani errati nei confronti della prevenzione e della gestione degli incidenti informatici.

RISPOSTA: Corso online di Cyber Security Awareness

Monitoraggio 24/7 dell'infrastruttura:

La rete deve essere monitorata e protetta 24/7 sia attraverso strumenti tecnologici, sia grazie alla competenza di personale esperto in Cybersecurity.

RISPOSTA: Deep Packet Inspection (DP); Intrusion Prevention System (IPS); Honeypot (trappola digitale), SOC 24/7

Rilevamento periodico delle Vulnerabilità:

L'infrastruttura di rete è un organismo in continuo movimento e cambiamento, per questo motivo è essenziale rilevare periodicamente vulnerabilità e bug di sistema che aprono a gravi vulnerabilità della rete.

RISPOSTA: Vulnerability Assessment (VA) continuo

Identificazione e gestione degli Incidenti:

Nonostante la tecnologia permetta l'implementazione di strumenti automatici di prevenzione e risposta alla minacce informatiche, l'attività dei Security Operation Center (SOC) con analisti certificati, che monitorano la rete in modalità 24/7 è tutt'ora indispensabile per una protezione reale ed efficace dell'infrastruttura di rete.

RISPOSTA: SOC 24/7; DPI; IPS; Honeypot

Rilevamento Dati e Credenziali nel darkweb:

Una minaccia in forte crescita è l'accesso non autorizzato agli account aziendali tramite credenziali rubate e inserite nel Darkweb, dove vengono rivendute ai cyber criminali.

RISPOSTA: Cyber Threat Intelligence (CTI) sulle più autorevoli fonti di Intelligence

Capacità di riferire all'Auditor le attività di Cybersecurity messe in atto dall'azienda:

In caso di controllo da parte delle Autorità, l'azienda è tenuta a presentare la documentazione delle misure intraprese per affrontare e mitigare il rischio informatico.

RISPOSTA: Dashboard con reportistica on demand su funzionalità e servizi della soluzione

