www.rbrverona.it

RBR

RENOVATING BUSINESS REALITY

CYBERSECURITY

DIRETTIVA NIS2

L'EVOLUZIONE DELLA CYBERSECURITY: L'IMPATTO DELLA DIRETTIVA NIS2 SULLE AZIENDE

Scoprite come la Direttiva NIS2 sta ridefinendo il panorama della sicurezza informatica in Europa.

Con un'analisi dettagliata, questo white paper esplora le nuove normative che ampliano l'ambito di applicazione della sicurezza cibernetica, introducendo standard più rigorosi e obblighi di segnalazione per un'ampia gamma di settori critici.

AFFRONTARE LE COMPLESSITÀ E I RISCHI DELLA DIRETTIVA NIS2

Un focus particolare verrà posto sulle difficoltà operative e sui costi associati all'aggiornamento delle infrastrutture e delle procedure per soddisfare le esigenze di questa normativa critica.

NIS2 METTE A RISCHIO LA SICUREZZA AZIENDALE?

Discuteremo l'importanza di adottare un approccio proattivo alla cybersecurity e come l'adeguamento a NIS2 può trasformarsi da un onere in un vantaggio competitivo, aumentando la fiducia e la sicurezza nelle operazioni aziendali.

La Direttiva NIS2 e la Nuova Era della Cybersecurity

In un'era digitale in cui la sicurezza informatica è diventata una priorità imprescindibile, la Direttiva NIS2 emerge come una pietra miliare nel panorama legislativo dell'Unione Europea. Questo documento è stato concepito per rispondere alle sfide sempre più complesse poste dalle minacce cyber, con l'obiettivo di rafforzare la resilienza e la sicurezza delle reti e dei sistemi informativi degli Stati membri.

Dalla NIS1 alla NIS2

La Direttiva NIS (Network and Information Systems), introdotta nel 2016, è stata il primo passo verso una maggiore sicurezza informatica a livello europeo.

Tuttavia, l'evoluzione rapida e continua delle minacce cyber ha reso necessario un aggiornamento significativo.

La Direttiva NIS2, quindi, non solo amplia il campo d'azione della legislazione precedente ma introduce anche requisiti più stringenti e dettagliati per le aziende e le organizzazioni.

Quali responsabilità?

Un aspetto fondamentale della NIS2 è l'enfasi sulla responsabilità e sull'accountability delle organizzazioni. L'adeguamento alla direttiva richiede un impegno significativo in termini di risorse e competenze, ponendo la cybersecurity al centro della strategia aziendale.

La direttiva incentiva le aziende a sviluppare una comprensione approfondita delle proprie infrastrutture IT, dei dati gestiti e dei rischi associati, favorendo un approccio proattivo alla gestione della sicurezza informatica.

Direttiva NIS2 segna un passo avanti decisivo nel rafforzamento delle capacità di resilienza e di risposta alle minacce cyber in Europa.

Con la sua implementazione, si prevede un notevole incremento nel livello di sicurezza delle reti e dei sistemi informativi, una maggiore consapevolezza dei rischi cyber e un impegno rinnovato nella protezione delle infrastrutture critiche e dei dati sensibili.

Settori Critici Inclusi:

La Direttiva NIS2 estende significativamente l'ambito di applicazione della sua predecessora, includendo una gamma più ampia di settori e servizi essenziali. Questa espansione riflette la crescente comprensione che la sicurezza delle reti e dei sistemi informativi è vitale non solo per alcuni settori critici ma per l'economia e la società nel suo complesso.

Energia:	Inclusi elettricità, gas e petrolio, dove un attacco informatico potrebbe avere conseguenze catastrofiche sulla distribuzione e l'approvvigionamento.
Trasporti:	Aviazione, ferrovie, trasporto marittimo e su strada, infrastrutture critiche per la mobilità delle persone e delle merci.
Sanità:	Ospedali, laboratori di ricerca e produttori di farmaci, settori resi ancora più critici dalla pandemia di COVID-19.
Acqua e Rifiuti:	Gestione delle risorse idriche e trattamento dei rifiuti, fondamentali per la salute pubblica e l'ambiente.
Fornitori di Servizi Digitali:	Compresi provider di cloud, piattaforme online e motori di ricerca, essenziali per il funzionamento dell'economia digitale.
Settore Pubblico:	In particolare, amministrazioni che forniscono servizi essenziali come la sicurezza sociale.
Alimentari:	Produzione, trasformazione e distribuzione di alimenti, settore critico per la sicurezza alimentare.
Servizi Pubblici e Amministrativi:	Enti che offrono servizi essenziali alla cittadinanza, come l'istruzione e la gestione delle emergenze.

A differenza della NIS originale, la NIS2 si applica anche a enti di medie dimensioni che operano in questi settori critici. Questa estensione riconosce che la catena di approvvigionamento e la rete di servizi essenziali sono spesso interconnesse e che anche le entità più piccole possono essere un anello importante nella sicurezza complessiva del sistema.

Implicazioni per le Aziende

Le aziende operanti in questi settori devono adottare misure di sicurezza rafforzate e sono soggette a requisiti di segnalazione più rigorosi. Devono anche partecipare attivamente alla condivisione di informazioni e pratiche relative alla cybersecurity, contribuendo a un sistema di difesa collettivo.

L'Impatto Quantitativo della Direttiva NIS2 sulle Aziende: Una Panoramica Numerica

Nel dettaglio numerico della Direttiva NIS2, emerge un quadro chiaro dell'impatto profondo che questa normativa avrà sulle aziende in Europa.

Con l'espansione a più di 16 settori critici, la direttiva coinvolge migliaia di aziende, spingendole a rivedere e potenziare significativamente le loro strategie di cybersecurity. L'aumento previsto delle spese in sicurezza informatica, che potrebbe raggiungere il 70% nei prossimi anni, sottolinea l'importanza e l'urgenza di investire in robuste misure di protezione.

L'incremento delle segnalazioni di incidenti di sicurezza, stimato attorno al 40%, riflette una maggiore enfasi sulla trasparenza e la responsabilità. Le sanzioni per la non conformità, che possono raggiungere il 2% del fatturato annuo globale, evidenziano la severità delle conseguenze in caso di mancato adeguamento.

Questo aspetto, unito all'aumento del costo medio di un data breach per le aziende non conformi, rende evidente che la non conformità è un rischio troppo elevato da correre, sia in termini finanziari che reputazionali.

Personale dedicato alla sicurezza

Aumento previsto del 25%, insieme al tempo medio necessario per un adeguamento completo, stimato tra 18 e 24 mesi, indica la scala e la complessità dell'impegno richiesto.

Numeri in breve

Investimenti
€ 500K

Si stima che le spese per la cybersecurity aumenteranno del 70% nei prossimi 5 anni, in risposta ai requisiti della NIS2, con un investimento medio per azienda che potrebbe superare i 500.000 euro.

Obblighi
40%

Con la NIS2, si prevede un aumento del 40% nelle segnalazioni di incidenti di sicurezza, richiedendo alle aziende una maggiore trasparenza e capacità di risposta rapida.

Sanzioni
2%

Le aziende non conformi possono affrontare sanzioni fino al 2% del loro fatturato annuo globale, una cifra significativa soprattutto per grandi corporazioni.

Costi
30%

Nonostante l'impatto economico, questi investimenti sono cruciali per proteggere l'azienda dalle crescenti minacce informatiche.

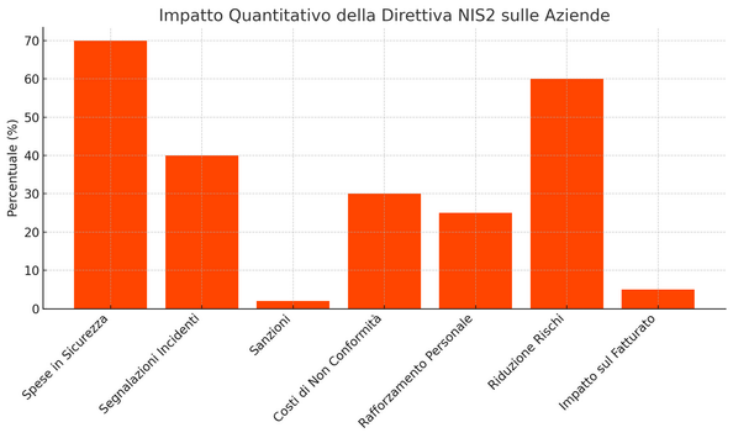
Personale
25%

Le aziende dovranno aumentare il personale dedicato alla sicurezza informatica di almeno il 25%, investendo in formazione e competenze specialistiche.

Tempo medio
24 mesi

Le organizzazioni avranno bisogno in media di 18-24 mesi per adeguarsi pienamente agli standard imposti dalla NIS2, includendo l'aggiornamento delle infrastrutture e delle politiche.

Effetti della direttiva



RBR RENOVATING BUSINESS REALITY

Business performance e continuity senza compromessi

Contattaci subito

Sito web	www.rbrgroup.com
Telefono	045 8403665
E-mail	info@rbrgroup.it
Social Media	@rbr_verona
Indirizzo	Via Monsignor Gentilin, 62 37132 Verona (VR)