KINGSTON IRONKEY™

Direttiva NIS2

Questa scheda informativa fornisce informazioni sulla Direttiva NIS2, spiegando di cosa si tratta, quale impatto avrà sulle organizzazioni e quali sono le attività che le aziende dovranno compiere per risultare conformi a questa nuova direttiva.

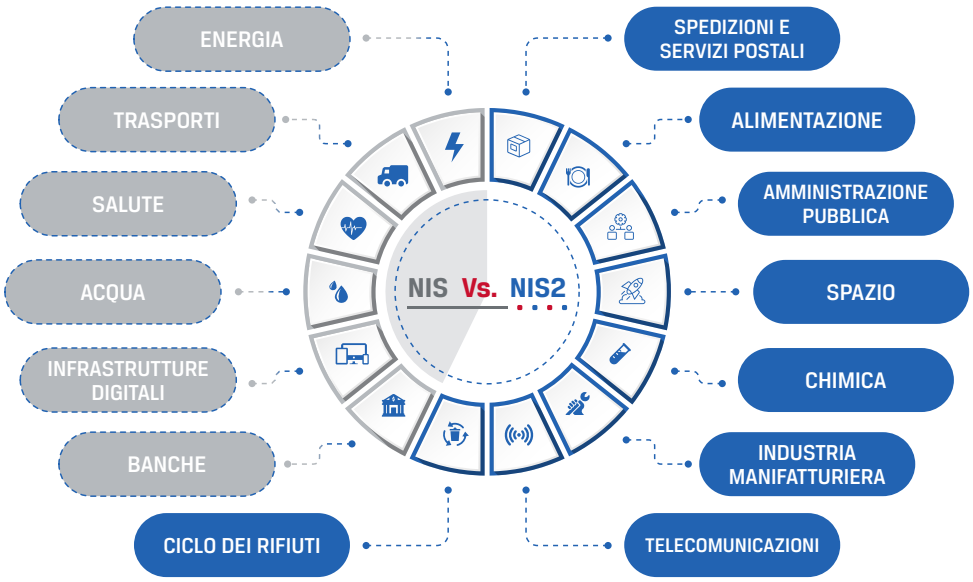
Di cosa si tratta?

- La NIS2 (Network and Information Security Directive 2) è una direttiva UE che amplia e migliora la precedente direttiva NIS. La direttiva NIS2 ha l'obiettivo di rafforzare la sicurezza informatica delle infrastrutture critiche in tutta l'UE, garantendo una maggiore resilienza e una protezione più efficace contro le violazioni dei dati e le interferenze attuate da criminali o malintenzionati.
- La direttiva è in vigore dal 17 ottobre 2024.

Differenze principali tra NIS e NIS2

L'Unione Europea ha adottato la Direttiva NIS2, che riforma in modo significativo la precedente Direttiva NIS (Network and Information Systems) del 2016, ampliando il campo di applicazione, che arriva ora ad interessare un maggior numero di infrastrutture critiche e di fornitori di servizi essenziali.

- **Requisiti di sicurezza:** la direttiva NIS2 impone misure più severe come la gestione del rischio, le valutazioni periodiche sulla sicurezza, le strategie di risposta agli incidenti e l'uso della crittografia e dei controlli di accesso per la protezione dei dati.
- **Segnalazione degli incidenti: l**a precedente versione della direttiva NIS obbligava gli enti a rendere noti gli incidenti di significativa importanza, senza ritardi ingiustificati. La nuova versione NIS2 rende più incisivo questo obbligo, stabilendo che gli incidenti debbano essere segnalati entro 24 ore dal rilevamento e che venga data risposta più rapidamente agli attacchi e alle relative intrusioni.
- **Sicurezza della catena di approvvigionamento:** La direttiva NIS2 specifica che le aziende saranno responsabili anche dei loro fornitori e fornitori di servizi.



Chi sarà interessato?

L'ampliamento del campo di applicazione della direttiva NIS2 comporta un'estensione dei settori interessati, che includono energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile, infrastrutture digitali, governi e settore aerospaziale. Se l'organizzazione opera in UE o con un qualsiasi ente dell'UE – è tenuta a rispettare questa normativa e a sopportare le conseguenti sanzioni nel caso di mancata conformità.

Perché ai vostri clienti conviene informarsi sulla NIS2?

- "Entro il 2025 i costi legati alla criminalità informatica sono destinati a raggiungere i 10,5 trilioni di dollari annui, rispetto ai 3 trilioni di dollari del 2015.1. Questa impennata è causata da attacchi informatici sempre più sofisticati, con una frequenza e una gravità crescente di minacce ransomware ed episodi di violazione dei dati." - Cybersecurity Ventures
- Il Global Risk Report 2023 del World Economic Forum2 mette in risalto la pericolosità delle minacce informatiche, considerandole uno fra i principali rischi globali.

Per far fronte all'aumento delle minacce, l'Unione Europea ha introdotto questa nuova direttiva, rafforzando il potere di controllo delle autorità nazionali: il mancato rispetto della normativa può comportare sanzioni fino a 10 milioni di euro o al 2% del fatturato annuo globale della società (si applica il valore maggiore).

In che modo le soluzioni dotate di crittografia Kingston IronKey possono contribuire alla conformità NIS2 delle aziende?

I drive USB e SSD esterni dotati di crittografia hardware Kingston IronKey offrono funzioni avanzate di protezione dei dati, grazie alle quali le aziende possono soddisfare i requisiti imposti della direttiva:

- **Protezione dei dati:** conforme ai requisiti di crittografia e controllo degli accessi previsti dalla NIS2.
- **Compliance:** aiuta le organizzazioni a rispettare e dimostrare la conformità agli standard NIS2.
- **Reazione agli incidenti:** agevola il recupero e il ripristino rapido dei servizi in caso di attacco o violazione.
- **Sicurezza della catena di approvvigionamento:** mitiga i rischi ricorrendo all'uso di storage portatile sicuri.

Conclusioni

Considerati i livelli senza precedenti raggiunti dalla criminalità informatica, l'adozione della nuova direttiva NIS2 costituisce un importante passo avanti nel miglioramento della sicurezza informatica delle infrastrutture critiche nell'UE. Le organizzazioni sono chiamate ad adottare soluzioni concrete per conformarsi alla direttiva NIS2 e proteggere così i dati sensibili. I dispositivi Kingston IronKey utilizzano crittografia hardware, così da offrire una soluzione scalabile e affidabile per conseguire la conformità e proteggere le informazioni critiche, aiutando le aziende a navigare nelle complessità dell'attuale panorama della cybersecurity.

Domande che i rivenditori possono rivolgere ai loro clienti/utenti finali

- Conoscete la direttiva NIS2, entrata in vigore il 17 ottobre 2024?
- Che strategia avete previsto per risultare conformi alla direttiva NIS2?
- Conoscete le conseguenze a cui potreste andare incontro non rispettando la NIS2? Le sanzioni possono arrivare fino al 2% del fatturato annuo globale.
- Eseguite backup realmente sicuri dei vostri dati sensibili, usando la crittografia di tipo hardware?

Descrizione riportata	IronKey Vault Privacy 50 Series	IronKey Vault Privacy 80 ES	IronKey Keypad 200 Series	IronKey D500S	IronKey S1000
Livello di sicurezza	Aziendale, mainstream	Aziendale, mainstream	Specifiche militari	Specifiche militari/Leader di settore	Specifiche militari/Leader di settore
Capacità[4]	8-512GB	480-7,680GB	16-256GB USB-A 8-512GB USB-C	8-512GB	8-128GB
Crittografia hardware con protocollo AES 256-bit	XTS	XTS	XTS	XTS	Cryptochip integrato + XTS
Certificazione FIPS[5]	FIPS 197	FIPS 197	FIPS 140-3 di Livello 3 (in corso di approvazione)	FIPS 140-3 di Livello 3 (in corso di approvazione)	PS 140-2 di livello 3

Per sapere come Kingston può aiutarvi a trovare la soluzione più adatta ai vostri clienti, scansionate il codice QR e compilate il nostro modulo Ask an Expert.

www.kingston.com

1. www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime
2. www.weforum.org/publications/global-risks-report-2023
3 I nomi USB Type-C® e USB-C® sono marchi commerciali registrati di USB Implementers Forum.
4. Parte della capacità totale indicata per i dispositivi di storage Flash viene in realtà utilizzata per le funzioni di formattazione e per altre funzioni e tale spazio non è disponibile per la memorizzazione dei dati. Per ulteriori informazioni, consultare la Guida alle Memorie Flash di Kingston, all'indirizzo web: kingston.com/flashguide.
5. Conformità allo standard FIPS (Federal Information Processing Standards) 140-2: "Requisiti di sicurezza per i moduli crittografici". Per ulteriori informazioni, visitare il sito http://csrc.nist.gov/publications/PubsFIPS.html.

© 2025 Kingston Technology Europe Co LLP e Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Regno Unito. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469
Tutti i diritti riservati. Tutti i marchi e i marchi registrati sono proprietà dei rispettivi titolari.