uniqkey

Direttiva NIS2: ottenere la conformità con una migliore sicurezza degli accessi

Questa guida fornisce una breve ripartizione della direttiva NIS2 dal punto di vista della sicurezza dell'accesso e offre consigli concreti su come soddisfare i requisiti NIS2 utilizzando una semplice soluzione di sicurezza informatica.

Made in Denmark

www.uniqkey.eu

uniqkey

La direttiva NIS2

L'ultima versione della direttiva sulle reti e sui sistemi informativi (NIS2), adottata dagli Stati membri dell'UE, impone un'applicazione più rigorosa dei requisiti di cibersicurezza in tutta l'Unione e garantisce sanzioni uniformi. **La direttiva entrerà in vigore nel 2024, il che significa che sarà obbligatorio per le organizzazioni degli Stati membri, conformarsi ai nuovi requisiti.**

uniqkey

Sommario

01 Cos'è NIS2?

NIS2 è l'acronimo di **"Network and Information Security Directive"** ed è una continuazione e un'espansione della precedente direttiva UE sulla sicurezza informatica, NIS1. L'obiettivo di NIS2 è quello di rafforzare il livello collettivo di cibersicurezza degli Stati membri dell'UE, aumentando i requisiti di applicazione della cibersicurezza per i settori delle infrastrutture critiche.

La direttiva NIS2, che disciplina le imprese e le agenzie governative nel settore cybersecurity, si manifesterà come legge nazionale, il che significa che ogni organizzazione inclusa nella direttiva sarà tenuta a soddisfare i propri requisiti.

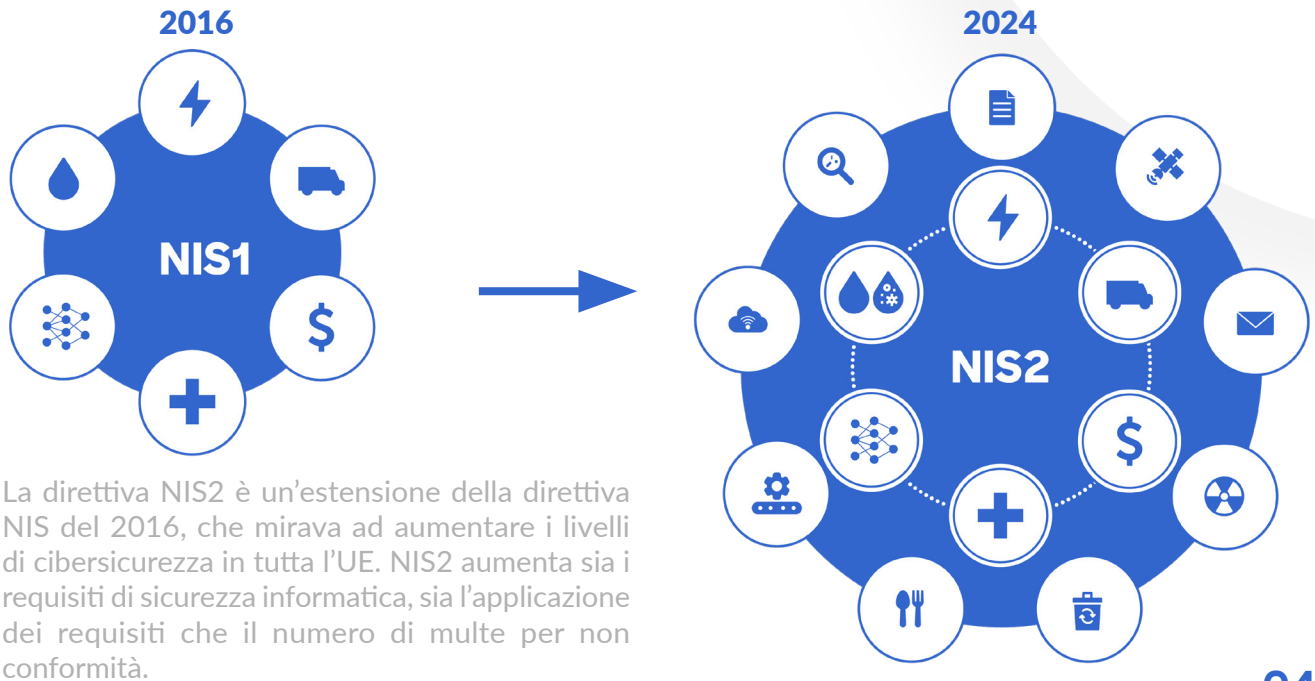
NIS2 espande sia i requisiti che le sanzioni di sicurezza informatica a livello europeo per armonizzare e semplificare il livello di sicurezza in tutti gli Stati membri dell'UE, fatto che per le organizzazioni significa definire piani più chiari su come gestire il rischio, controllare e supervisionare.

Qual è la differenza tra GDPR e NIS2?

NIS2 è per la sicurezza informatica europea ciò che il GDPR è stato per la protezione dei dati europei.

Mentre il GDPR ha rafforzato i requisiti su come gli Stati membri dell'UE gestiscono i dati personali, l'obiettivo di NIS2 è garantire che tutte le aziende e le organizzazioni europee, considerate parti di infrastrutture essenziali, mantengano un livello adeguato di sicurezza informatica.

NIS2 amplia l'ambito e rafforza i requisiti di sicurezza



La direttiva NIS2 è un'estensione della direttiva NIS del 2016, che mirava ad aumentare i livelli di cibersicurezza in tutta l'UE. NIS2 aumenta sia i requisiti di sicurezza informatica, sia l'applicazione dei requisiti che il numero di multe per non conformità.

02 Quali settori copre NIS2?

Il numero di settori coperti dalla direttiva è in aumento, in quanto la Commissione NIS2 vuole che tutte le organizzazioni che occupino una posizione critica nella società siano incluse nella direttiva, al fine di rafforzare la resilienza informatica dell'Europa. Ciò significa che NIS2 ora coprirà anche settori come la produzione alimentare, la gestione dei rifiuti e l'intera catena di approvvigionamento.

Ecco i settori coperti da NIS2:

- Energia
- Transporti
- Infrastrutture Bancarie e del Mercato Finanziario
- Salute
- Acqua Potabile e Acque Reflue
- Infrastrutture Digitali
- Pubblica Amministrazione
- Spazio
- Servizio Postale
- Gestione dei Rifiuti
- Prodotti Chimici
- Alimenti
- Produzione
- Fornitori Digitali
- Ricerca

uniqkey

03 Quali organizzazioni sono interessate da NIS2?

NIS2 espande notevolmente le organizzazioni interessate dai suoi requisiti e distingue tra **“aziende essenziali”** e **“aziende importanti”.**

Aziende Essenziali

- **Energia**- fornitura, distribuzione, trasmissione e vendita
- **Transporti**- aerei, ferroviari, stradali e marittimi
- **Finanza** - credito, commercio, mercato e infrastrutture
- **Salute** – ricerca, produzione, fornitori e produttori
- **Acqua potabile e acque reflue**
- **Infrastruttura digitale** – DNS, servizi fiduciari, servizi di data center, cloud computing, servizi di comunicazione, fornitori di servizi gestiti e fornitori di sicurezza gestiti.
- **Pubblica amministrazione**, comuni e regioni
- **Spazio** – software e servizi

Aziende importanti:

- **Servizio postale** e pacchi
- **Gestione dei rifiuti**
- **Chemical products** – production and distribution
- **Foods** - production and distribution
- **Production** of pharmaceutical, electronic and optical equipment and machinery and vehicles
- **Digital providers** of online marketplaces, search engines, social platforms
- **Research**

Quando entrerà in vigore NIS2?

La direttiva è stata approvata dal Parlamento europeo il 10 novembre 2022 e tutte le organizzazioni e le aziende applicabili avranno tempo fino al 2024 per conformarsi ai nuovi requisiti legali, dopodiché saranno passibili di eventuali multe.

Secondo la direttiva, le aziende nei settori applicabili sono obbligate a comprendere e affrontare le nuove regole, requisiti e linee guida.

04 Quali requisiti pone NIS2 alla tua organizzazione?

La direttiva NIS2 aggiunge nuovi requisiti per 4 aree delle varie organizzazioni: gestione, reporting alle autorità, gestione del rischio e continuità operativa. Lo scopo è aumentare la capacità dell'Europa di resistere alle minacce informatiche attuali e future.

1. Gestione

È necessario che la direzione sia consapevole e comprenda i requisiti della direttiva e gli sforzi di gestione del rischio, in quanto hanno la responsabilità diretta di identificare e affrontare i rischi informatici per conformarsi ad essi.

2. Segnalazione alle autorità

Le organizzazioni devono disporre di processi stabiliti per garantire una corretta segnalazione alle autorità, come la segnalazione di incidenti gravi entro 24 ore.

3. Gestione del rischio

Per soddisfare i nuovi requisiti, le organizzazioni devono implementare misure che possano ridurre il rischio al minimo. Ciò include la gestione degli incidenti, una migliore sicurezza della catena di approvvigionamento, la sicurezza della rete, il controllo degli accessi e l'encryption.

4. Continuità operativa

Le organizzazioni devono considerare come garantire la continuità aziendale in caso di gravi incidenti informatici. Ciò include, ad esempio, il ripristino del sistema, le procedure di emergenza e la creazione di un'organizzazione di crisi.

05 Misure minime da attuare

Non finiscono però qui i requisiti applicabili ad imprese ed organizzazioni. A seconda delle dimensioni dell'azienda infatti, della funzione sociale o dell'esposizione dell'organizzazione, il livello dei requisiti varia. Ciò al fine di garantire che i requisiti rimangano proporzionati, alle piccole imprese in modo che non siano colpite con gravi incidenti e che per le imprese più grandi essi riflettano il loro ruolo nella società. **Detto questo, ci sono una serie di misure minime che NIS2 richiede a tutte le indipendentemente dalle dimensioni.**

Come nel caso dei 4 aspetti specifici sopracitati, le seguenti misure minime (cfr. pagina successiva) sono sintesi generali delle aree della direttiva, non definitive. Per garantire che la tua azienda sia pienamente conforme alla direttiva NIS2, dovresti sempre verificare quindi tali punti con la tua offerta di conformità.

Misure minime NIS2:

**Il testo blu indica quali misure minime Uniqkey può aiutare a coprire.*

1. Valutazione dei rischi e politiche di sicurezza per i sistemi informativi

2. Un piano per la gestione degli incidenti di sicurezza

3. **Un piano per la gestione delle operazioni aziendali durante e dopo un incidente di sicurezza, che comporta l'aggiornamento dei backup e un piano per garantire l'accesso ai sistemi IT e alle loro funzioni operative, durante e dopo un incidente di sicurezza.**

4. Sicurezza intorno alle catene di approvvigionamento e nel rapporto tra azienda e fornitore diretto. In altre parole le aziende devono scegliere misure di sicurezza che si adattino alle vulnerabilità di ciascun fornitore diretto, valutando comunque anche livello di sicurezza complessivo per tutti i fornitori..

5. Politiche e procedure per valutare l'efficacia delle misure di sicurezza.

6. **Sicurezza intorno all'approvvigionamento allo sviluppo e al funzionamento dei sistemi. Ciò significa disporre di criteri per la gestione e la segnalazione delle vulnerabilità.**

7. **Formazione sulla sicurezza informatica e sulla "Computer Hygiene" di base.**

8. **Politiche e procedure per l'uso della crittografia e, se necessario, dell'encryption.**

9. **Procedure di sicurezza per i dipendenti con accesso a dati sensibili o importanti, comprese le politiche per l'accesso ai dati. La società deve anche avere una panoramica di tutte le risorse rilevanti e garantire che siano correttamente utilizzate e gestite.**

10. **L'uso dell'autenticazione a più fattori, delle soluzioni di autenticazione continua, della crittografia vocale, video e testuale e delle comunicazioni di emergenza interne crittografate, quando appropriato.**

Queste descrizioni sono sintesi generali dei settori coperti dalla direttiva e non sono quindi complete. Per garantire quindi che la tua azienda sia conforme alla direttiva NIS2, dovresti sempre chiedere consiglio al tuo responsabile della compliance.

06

Come Uniqkey può aiutarvi a rispettare NIS2

Sulla base delle descrizioni della direttiva, è possibile coprire una serie di nuovi requisiti e aspettative NIS2 implementando Uniqkey.

Informazioni su Uniqkey

Uniqkey è il fornitore danese di una soluzione user-friendly per la gestione delle password aziendali e degli accessi, che aiuta le aziende a usare le password in sicurezza e a semplificare la gestione degli accessi.

Uniqkey può aiutare a coprire queste misure minime

Sulla base delle descrizioni della direttiva, **è possibile coprire una serie di nuovi requisiti e aspettative NIS2 implementando Uniqkey.**

NIS2 Misure minime:	Uniqkey copre questo aspetto:
Pt 3: **Proteggere l'accesso ai sistemi IT**	✔ **Managing, storing and saving all user logins securely.** And can be used without internet access. ✔ **Securing access to IT systems** and company services during operation with strong, unique passwords and two-factor authentication ✔ **Enabling admins to access a detailed audit log in** case of an incident
Pt 6: **Politiche e procedure per la valutazione dell'efficacia delle misure di sicurezzavulnerabilities.**	✔ **Offrendo punteggi di sicurezza basati sui dati** peri singoli dipendenti, servizi e gruppi di lavoro. ✔ Includendo una funzionalità per **produrre facilmente rapporti sugli incidenti.**
Pt 7: **Formazione sulla sicurezza informatica e pratica per la "Computer Hygiene" di base**	✔ **Aumentando la consapevolezza della sicurezza dell'utente** , informandolo su password deboli, riutilizzate o compromesse. ✔ **Facilitando la "Computer Hygien" di base** dando supporto per l'accesso sicuro ai sistemi, sostituendo le abitudini di archiviazione delle password non sicure e riducendo al minimo gli incidenti di utilizzo non autorizzato del software (Shadow IT). ✔ **Fornendo agli amministratori una panoramica** e delle informazioni dettagliate su quanto sia realmente al sicuro ogni dipendente, servizio e gruppo di lavoro. ✔ **Offrendo formazione diretta sulla sicurezza tramite** pannello di controllo con guide per la configurazione 2FA e l'aggiornamento delle password compromesse.

NIS2 Misure minime:	Uniqkey copre questo aspetto:
Pt 8: **Politiche e procedure per l'uso della crittografia e, se necessario, dell'encryption**	✔ **Crittografando dei dati della password** del singolo utente offline e localmente sul proprio dispositivo. ✔ **Archiviando in sicurezza** tutti gli accessi rilevanti per l'azienda.
Pt 9: **Procedure di sicurezza per i dipendenti con accesso a dati sensibili o importanti, comprese le politiche per l'accesso ai dati. L'azienda deve anche avere una visione d'insieme di tutte le risorse rilevanti e garantire che siano correttamente utilizzate e gestite**	✔ **Fornendo una panoramica automatica di tutte le risorse IT,** , degli accessi dei dipendenti e supportandone l'onboarding e l'offboarding in modo semplice e sicuro. ✔ **Supportando laconfigurazione di livelli di sicurezza aggiuntivi** aggiuntivi e restrizioni su sistemi e servizi business-critical.
Pt 10: **L'uso dell'autenticazione a più fattori, soluzioni di autenticazione continua, crittografia vocale, video e testuale e comunicazione di emergenza interna crittografata, quando appropriato.**	✔ **Offrendo TOTP e autenticazione continua** tramite misure di sicurezza ad accesso biometrico. ✔ **Garantendo che tutte le comunicazioni e i dati siano crittografati** utilizzando TLS e chiavi pubbliche / private.

07 Cosa succede se non si rispetta NIS2?

Multe

Le aziende che non si conformeranno a NIS2 una volta che la direttiva sarà entrata in vigore nel 2024, saranno soggette a multe significative a seconda che siano classificate come aziende essenziali o importanti.

Aziende essenziali

Le società classificate come essenziali, saranno sanzionate con multe di rischio essenziale fino a 10 milioni di euro o il 2% del loro fatturato annuo globale.

Aziende importanti

Le società classificate come importanti rischiano multe fino a 7 milioni di euro o l'1,4% del loro fatturato annuo globale.

Conseguenze legali

Le conseguenze derivanti dall'incapacità di raggiungere la conformità NIS2 ora includono più della sola ammissibilità a multe. Infatti, i team di gestione dell'azienda ora, possono essere ritenuti responsabili per qualsiasi incapacità di soddisfare i nuovi requisiti. In altre parole, la nuova direttiva ora sottolinea che la gestione può affrontare conseguenze legali se non si rispettano le nuove regole.

Infine, il management deve seguire corsi per migliorare la propria capacità di valutare i rischi di sicurezza informatica e incoraggiare la propria organizzazione a offrire corsi simili a tutti i dipendenti su base regolare.

08

Scopri come Uniqkey protegge le infrastrutture critiche

Scopri come le aziende che gestiscono infrastrutture critiche utilizzano Uniqkey per migliorare la resilienza informatica.

Testimonianza della difesa danese

Sei curioso di conoscere Uniqkey? Guarda l'ex CIO della Difesa danese, Kristian VengsGaard, parlare del loro test completo Uniqkey.

Casi di studio


BUSINESS CASE Security Ease-of-use

BORNHOLMS ENERGI & FORSYNING

Our employees' passwords were the weakest link in our security. Uniqkey solved that immediately.

- Kristoffer Munch, Head of IT at Beof

Heavy responsibility, heavy requirements

Bornholms Energy & Supply, also referred to as Beof, is a Danish utility company. Responsible for the entire energy infrastructure on the island of Bornholm, including energy, water, and electricity, Beof is considered a cornerstone of Denmark's critical infrastructure.

To minimize the risk of security breaches, Beof has to follow strict security standards set by the government. A task that puts a heavy load on Beof's IT department.

Customer: Bornholms Energy & Supply www.beof.dk

Industry: Energy & Supply

The Challenge:

To comply with government requirements and protect critical national infrastructure, Beof wanted an easy-to-implement security solution that would help them minimize human-related security risks in their company.

Before implementing Uniqkey:

- Employees weak or reused passwords jeopardized security.
- Admins lacked overview and control over employee access.
- IT department was forced to manually reset employees' passwords to maintain high levels of security.
- Employees access flow was inconvenient and disorganized.

After implementing Uniqkey:

- Built-in password generator helps employees use more complex passwords.
- Uniqkey's Admin Dashboard gives admins a detailed overview over all employee access and login activity.
- Employees have access to own password manager, eliminating the need for manual password resets.
- With Uniqkey's intuitive auto-login feature, employees now have a streamlined, convenient and exceptionally safe login flow.

Beof's goal: eliminate human-related security risks.

According to Verizon, 80% of company security breaches are caused by human-related errors like using weak or compromised passwords on a daily basis.

Aware of this risk, Beof sought a solution that would give each employee a secure, simple and convenient way to handle logins to critical systems, reducing this risk dramatically. And that's what they found in Uniqkey.

From the initial implementation phase, Beof prioritized password and cloud security to reduce employees use of re-used and weak passwords while gaining overview of company services and employee access.

Because of the rising threat of phishing attacks, passwords breaches and social engineering, Kristoffer knew that their employees were the weakest link in their companys security.

Kristoffer explains that Beof chose Uniqkey "because they help us minimize human-related security risks." "With Uniqkey's user-friendly platform and intuitive, auto-login app, it is now easy for us to onboard employees and we have increased our general access security" - Kristoffer Munch, Head of IT.

Forced to make decisions "in the dark"

Prior to the implementation of Uniqkey, Beof had no tools to monitor employee access outside their Active Directory or any insight into the complexity of their user's passwords. This reduced their security management to guesses and general awareness training rather than data-driven decisions.

"Before Uniqkey, we had no overview of our users and their passwords. Our primary focus was awareness training and educating our employees to steer them towards more secure behaviour. But we had no tool to measure the actual impact." - Kristoffer Munch.

Want to know more?

uniqkey

- Bornholms Energi - og Forsyning
- Vejle Brand Forsikring

Uniqkey protegge le infrastrutture critiche europee

RISMA · energi ikast hele din forsyning · skanderborg forsyning a/s · REJSEKORT · ADmire · AARHUS TECH · JF · BORNHOLMS ENERGI & FORSYNING · ODSHERRED KOMMUNE · expdigital · TRelation · COPENHAGEN MEDICAL

uniqkey

Lascia che Uniqkey ti aiuti a rispettare NIS2

NIS2 è pronto? Lascia che i nostri esperti di prodotto ti facciano scoprire come Uniqkey copre i requisiti essenziali NIS2, facilitando al contempo la sicurezza immediatamente misurabile per le aziende europee che gestiscono infrastrutture critiche. Agisci su NIS2 e contattaci oggi stesso.

Contatta il nostro team su:

Email: nis2@uniqkey.eu
Telefono: +45 71 96 99 67