Perché l'accesso remoto è il requisito più critic della NIS2

Una guida alla conformità per le infrastrutture critiche, la difesa e le organizzazioni governative che operano ai sensi della Direttiva NIS2 dell'UE

Di Netop | Aprile 2026

Sintesi esecutiva

La direttiva NIS2 dell'UE è la normativa sulla sicurezza informatica più importante nella storia europea. Si applica a circa 160.000 entità in 18 settori critici, ritiene i vertici aziendali personalmente responsabili in caso di non conformità e impone multe fino a 10 milioni di euro o al 2% del fatturato annuo globale. Per gli operatori di infrastrutture critiche, le organizzazioni di difesa e gli enti governativi, non si tratta di un semplice esercizio di conformità, ma di un cambiamento fondamentale nel modo in cui devono essere gestite le operazioni digitali.

Tra tutti i requisiti introdotti dalla NIS2, l'accesso remoto è quello che presenta la posta in gioco più alta. L'accesso remoto si trova all'intersezione di cinque distinti obblighi NIS2 contemporaneamente: sicurezza della catena di fornitura digitale, controllo degli accessi, crittografia, segnalazione degli incidenti e certificazione di sicurezza informatica. È il punto di ingresso più sfruttato dagli aggressori, l'ambito più frequentemente escluso dai framework di sicurezza legacy e l'area con la più alta concentrazione di rischi legati a terze parti. Un'organizzazione che soddisfa tutti gli altri requisiti NIS2 ma non riesce a gestire correttamente l'accesso remoto rimane pericolosamente esposta, in più articoli contemporaneamente.

Questo white paper spiega perché l'accesso remoto richiede un'attenzione prioritaria nell'ambito della NIS2, mappa i requisiti di conformità specifici ai controlli operativi e mostra come l'accesso remoto sicuro di Netop consenta alle organizzazioni di soddisfare tali requisiti. Netop non si limita a soddisfare i requisiti della NIS2, ma offre ciò che gli auditor devono vedere: prove documentate e a prova di manomissione di un accesso controllato, autenticato e supervisionato a ogni endpoint nell'ambito di applicazione.

Il panorama normativo NIS2 nel 2026

Dalla direttiva all'applicazione

La NIS2, ufficialmente nota come Direttiva (UE) 2022/2555, è entrata in vigore nel gennaio 2023. Gli Stati membri erano tenuti a recepirla nelle loro leggi nazionali entro il 17 ottobre 2024. Tale scadenza è stata ampiamente disattesa: all'inizio del 2026, il recepimento è ancora in corso in tutta l'UE e i quadri di applicazione sono in fase di finalizzazione a livello nazionale.

Le organizzazioni che consideravano la scadenza di ottobre 2024 un evento lontano si trovano ora ad affrontare un periodo di conformità ridotto, poiché le autorità di regolamentazione nazionali stanno attivando i poteri di supervisione e applicazione.

> **Situazione normativa: marzo 2026**
> *Il recepimento della NIS2 sta accelerando in tutti gli Stati membri dell'UE a seguito del mancato rispetto della scadenza di ottobre 2024. I quadri normativi nazionali sono in fase di finalizzazione e si prevede che l'attività di applicazione aumenti in modo significativo nel corso del 2026 e fino al 2027 .*

Responsabilità personale dei vertici aziendali

La NIS2 introduce un requisito che non era presente nella versione precedente: la responsabilità personale dei vertici aziendali. Ai sensi dell'articolo 20, gli organi di gestione sono tenuti ad approvare le misure di gestione dei rischi di sicurezza informatica e a supervisionarne l'attuazione. La mancata conformità può comportare la sospensione dei dirigenti, nonché sanzioni pecuniarie a carico dell'organizzazione. La direttiva porta esplicitamente la sicurezza informatica a livello di consiglio di amministrazione.

Per i CISO, i CTO e i CIO delle organizzazioni regolamentate dalla NIS2, ciò stabilisce una responsabilità personale diretta nel garantire che i controlli di accesso remoto siano adeguati. L'attenzione si sposta dal semplice possesso di una politica alla dimostrazione (con prove) che la politica sia effettivamente applicata.

Ambito di applicazione: chi è interessato

La NIS2 si applica alle entità di medie e grandi dimensioni in 18 settori critici e importanti: energia, trasporti, settore bancario, sanità, infrastrutture digitali, gestione dei servizi ICT, pubblica amministrazione, settore spaziale, produzione manifatturiera, prodotti chimici, produzione alimentare, servizi postali, gestione dei rifiuti, fornitori di servizi digitali e organizzazioni di ricerca.

La direttiva ha anche portata extraterritoriale: le organizzazioni non UE che forniscono servizi a entità con sede nell'UE o operano all'interno del mercato UE devono conformarsi. Per gli appaltatori della difesa globali, gli operatori di infrastrutture multinazionali e i fornitori di tecnologia internazionali con clienti nell'UE, la conformità alla NIS2 è obbligatoria.

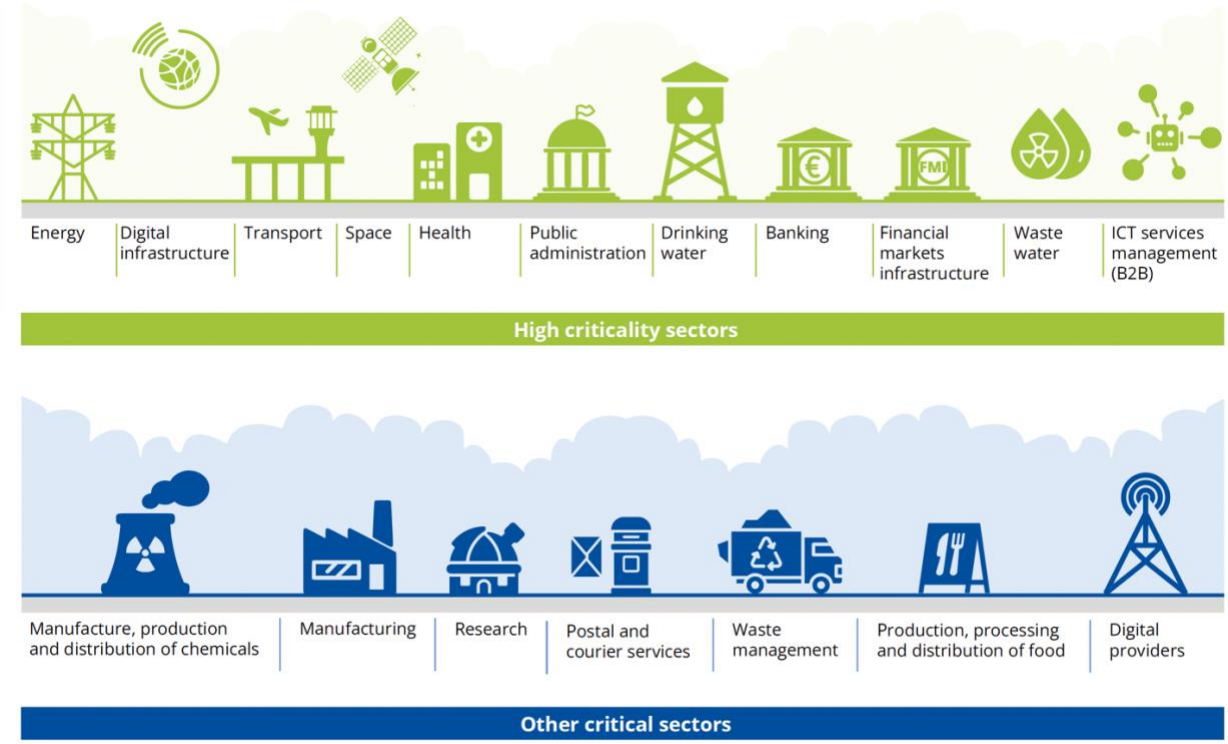


Grafico elaborato dall'ENISA, nell'ambito della campagna informativa sulla NIS2. Maggiori informazioni su www.enisa.europa.eu

Perché l'accesso remoto è il requisito più importante della direttiva NIS2

Il punto di convergenza

La maggior parte degli obblighi NIS2 può essere affrontata in modo relativamente isolato: i processi di segnalazione degli incidenti possono essere definiti indipendentemente dagli standard di crittografia, oppure le politiche di controllo degli accessi possono essere sviluppate separatamente dalle procedure di gestione delle vulnerabilità. L'accesso remoto è l'eccezione. È l'unico ambito in cui tutti i seguenti requisiti NIS2 convergono simultaneamente:

- **Sicurezza della catena di approvvigionamento** (articolo 21, paragrafo 2, lettera d) — poiché l'accesso remoto è il modo in cui fornitori, appaltatori e terze parti accedono ai vostri sistemi
- **Sicurezza della rete e gestione delle vulnerabilità** (articolo 21, paragrafo 2, lettera e) — poiché i protocolli di accesso remoto sono tra i vettori di attacco più sfruttati
- **Crittografia** (Articolo 21 §2.h) — poiché ogni sessione remota trasmette dati sensibili attraverso reti che potrebbero non essere sotto il vostro controllo
- **Controllo degli accessi e gestione delle risorse** (Articolo 21 §2.i) — poiché l'accesso remoto è il punto in cui l'identità, l'autenticazione e i privilegi devono essere applicati al momento dell'ingresso
- **Segnalazione degli incidenti** (Articolo 23) — poiché le sessioni di accesso remoto generano le prove di audit a supporto degli obblighi di segnalazione entro 24 e 72 ore
- **Certificazione della sicurezza informatica** (Articolo 24) — poiché gli strumenti che gestiscono l'accesso remoto devono a loro volta essere certificati e verificabili
- **Funzionalità CSIRT** (Articolo 11) — poiché la visibilità in tempo reale sulle sessioni remote è essenziale per il rilevamento delle minacce e la risposta agli incidenti

Nessun'altra singola funzionalità copre così tanti articoli della normativa NIS2. Ecco perché l'accesso remoto non è solo una voce nella checklist di conformità NIS2.

La realtà della superficie di attacco

L'accesso remoto è il principale vettore di ingresso per gli attacchi alla catena di approvvigionamento contro le infrastrutture critiche. I meccanismi sono ben documentati: credenziali dei fornitori compromesse, accesso VPN non controllato, connessioni RDP non governate e account anonimi o condivisi utilizzati dagli appaltatori. Ognuno di questi rappresenta un percorso diretto verso i sistemi che la NIS2 designa come essenziali.

Il rischio è aggravato da ciò che la NIS2 definisce "catena di approvvigionamento digitale". Qualsiasi organizzazione che disponga di un dispositivo dotato di chip accessibile da remoto, dai laptop e dai server ai robot di produzione, ai sensori della rete elettrica, alle apparecchiature mediche, ai sistemi di trasporto autonomi e alle infrastrutture satellitari, presenta una superficie di attacco per l'accesso remoto che richiede una governance. Per le organizzazioni nei settori essenziali della NIS2, tale superficie è in genere molto più ampia di quanto credano.

L'ambito delle "apparecchiature digitali" ai sensi della NIS2

Gli obblighi della catena di approvvigionamento NIS2 si applicano a qualsiasi dispositivo dotato di un microcontrollore o di capacità di elaborazione a cui è possibile accedere da remoto. Ciò include non solo l'infrastruttura IT ma anche la tecnologia operativa (OT): sistemi di controllo industriale, dispositivi medici, sistemi di gestione dei trasporti, sensori della rete energetica e apparecchiature di difesa. Se ha un chip ed è accessibile da remoto, rientra nell'ambito di applicazione.

Il problema delle VPN

Molte organizzazioni gestiscono ancora l'accesso di terze parti e fornitori attraverso soluzioni punto-rete, come le VPN o architetture equivalenti alle VPN, che garantiscono un ampio accesso alla rete agli utenti autenticati. Questo approccio è strutturalmente incompatibile con i requisiti di sicurezza della catena di approvvigionamento della NIS2.

Una VPN garantisce a un utente connesso l'accesso a un segmento di rete, non a un dispositivo o a un'applicazione specifica. Non è in grado di applicare i principi di accesso "need-to-know" o "need-to-perform" al livello granulare richiesto dalla NIS2. Non può limitare l'accesso in base a una finestra temporale, certificare l'autorizzazione dell'individuo per un'attività specifica o generare le prove di sessione a prova di manomissione richieste per la segnalazione degli incidenti. Ai sensi della NIS2, l'accesso basato su VPN ai sistemi critici costituisce un percorso di accesso non controllato.

L'accesso remoto conforme alla NIS2 richiede un'architettura punto a punto: una connessione controllata, autenticata, supervisionata e completamente registrata tra un individuo autorizzato e un dispositivo specifico, senza capacità di movimento laterale e senza un punto d'appoggio persistente nella rete.

Vulnerabilità nelle catene di fornitura digitali – Accesso sicuro di terze parti

L'accesso di terze parti è una vostra responsabilità

Ai sensi della direttiva NIS2, un'organizzazione è responsabile del livello di sicurezza informatica di ogni fornitore o appaltatore che abbia accesso ai propri sistemi. L'obbligo di conformità non si limita al perimetro dell'organizzazione, ma si estende a ogni soggetto terzo in grado di accedervi dall'esterno. Si consideri la gamma di accessi remoti di terze parti che sono di routine in un'organizzazione soggetta alla NIS2: tecnici di supporto IT che accedono in remoto ai dispositivi degli utenti finali; fornitori di BPO che accedono a sistemi finanziari ed ERP; ingegneri OT che riconfigurano apparecchiature industriali; produttori di dispositivi medici che aggiornano il firmware nei sistemi ospedalieri; appaltatori della difesa che accedono alle infrastrutture di comunicazione; consulenti energetici che leggono i dati dei sensori dalle strutture della rete. Ciascuna di queste interazioni deve essere controllata, autenticata, registrata e suscettibile di revisione forense.

Chi ha accesso alla vostra catena di fornitura digitale?

Il primo passo per la conformità all'accesso remoto NIS2 è capire chi ha accesso remoto a quali sistemi. Per la maggior parte delle grandi organizzazioni, questo non è così semplice come sembra. I rapporti con i fornitori sono documentati nei sistemi di approvvigionamento, ma i privilegi di accesso remoto sono spesso gestiti separatamente, a volte da singoli reparti o team di sede, senza una supervisione centralizzata. Il risultato è un panorama di accessi che si è sviluppato organicamente nel corso degli anni, con autorizzazioni che sopravvivono ai progetti e alle persone.

L'articolo 22 della NIS2 impone valutazioni coordinate dei rischi di sicurezza per le catene di fornitura critiche. Ciò richiede alle organizzazioni di identificare la propria catena di fornitura, mappare quali fornitori dispongono di accesso remoto e valutare i rischi associati. Senza prove documentate per rispondere alla domanda "chi ha accesso remoto a quali sistemi?", non è possibile ottenere la conformità all'articolo 22.

Requisiti di conformità NIS2: mappatura dell'accesso remoto

Temi relativi alle funzionalità e copertura degli articoli

La tabella sottostante mappa le funzionalità di accesso remoto di Netop agli articoli specifici della NIS2 a cui si riferiscono. Questa struttura è progettata per supportare sia le valutazioni di conformità che la documentazione di audit, dimostrando la connessione tra i controlli operativi e gli obblighi normativi.

Tema relativo alle funzionalità	Articolo NIS2	Requisito trattato
Controllo degli accessi e autenticazione	Art. 21 §2.d, §2.i	Accesso con privilegi minimi, MFA, identità federata, eliminazione dell'accesso anonimo
Monitoraggio e registrazione delle sessioni	Art. 21 §2.e, Art. 23	Audit trail audio-video a prova di manomissione, registrazione di tastiera/mouse, prove forensi per la segnalazione di incidenti
Governance della catena di fornitura digitale	Art. 21 §2.d, Art. 22	Raggruppamento degli accessi dei fornitori, IP-fencing, restrizioni temporali, controllo a quattro occhi, whitelist geografica
Crittografia e integrità dei dati	Art. 21 §2.h	Crittografia end-to-end AES-256 per le sessioni in transito e le registrazioni inattive; scambio di chiavi Diffie-Hellman / RSA
Risposta alle minacce in tempo reale	Art. 11 §3.a	Pannello di controllo live degli endpoint, kill-switch per sessioni non autorizzate, disattivazione dei permessi, supporto alla visibilità CSIRT
Infrastruttura certificata	Art. 24	ISO 27001, SOC 2, PCI-DSS, FIPS, HIPAA; residenza dei dati nell'UE su AWS; opzioni di implementazione on-premise e ibrida
Supporto alla segnalazione degli incidenti	Art. 23	Registrazione centralizzata a livello di entità, integrazione con AWS CloudTrail, registrazioni crittografate a prova di manomissione per gli obblighi di segnalazione 24h/72h

Articolo 21: Misure di gestione del rischio in dettaglio

§2.d — Sicurezza della catena di fornitura

Le organizzazioni devono controllare e limitare ciò a cui i fornitori possono accedere, quando possono accedervi e cosa possono fare una volta connessi. Ciò richiede una gestione degli accessi a un livello di granularità che gli strumenti generici di accesso alla rete non sono in grado di fornire.

- Le autorizzazioni di accesso devono essere definite in base a principi di raggruppamento: livello di criticità, area geografica, certificazioni possedute e necessità di eseguire operazioni
- Le restrizioni relative alle finestre temporali devono essere applicabili: un appaltatore autorizzato per una specifica finestra di manutenzione non dovrebbe essere in grado di connettersi al di fuori di tale finestra
- Devono essere disponibili meccanismi di supervisione umana (il principio dei quattro occhi) per le sessioni ad alto rischio, che richiedono che un supervisore designato accetti o monitori la connessione
- L'IP-fencing deve limitare l'accesso a intervalli geografici inseriti nella whitelist e a indirizzi di appaltatori specifici
- Le autorizzazioni di accesso a livello di applicazione devono essere applicabili, limitando ciò che un utente connesso può vedere e con cui può interagire

§2.e — Sicurezza di rete e gestione delle vulnerabilità

I protocolli di accesso remoto sono tra i vettori di attacco più frequentemente sfruttati nelle infrastrutture critiche. Il blocco dei protocolli aperti non sicuri — RDP, VNC, Telnet e SSH — riduce in modo significativo la superficie di attacco. La sostituzione dell'accesso punto-rete con un'architettura punto-punto elimina la capacità di movimento laterale che rende così dannose le compromissioni della catena di approvvigionamento.

- La registrazione delle sessioni deve catturare tutti gli eventi relativi a tastiera, video e mouse, fornendo prove di livello forense di ogni azione intrapresa durante una sessione remota
- I protocolli di sessione remota aperti devono essere bloccati al perimetro della rete
- L'accesso punto-rete basato su VPN o equivalente per i fornitori esterni dovrebbe essere sostituito con un accesso controllato punto-punto
- Tutta la registrazione dei dati deve avvenire a livello di entità, non solo a livello dei dispositivi dei fornitori o degli appaltatori: l'organizzazione deve essere responsabile della tracciabilità

§2.h — Crittografia

Tutti i dati trasmessi in una sessione remota e tutte le registrazioni delle sessioni archiviate devono essere crittografati secondo uno standard riconosciuto. La crittografia AES a 256 bit per le sessioni in transito, combinata con lo scambio di chiavi Diffie-Hellman o RSA, costituisce lo standard riconosciuto per le implementazioni di accesso remoto conformi.

§2.i — Controllo degli accessi e sicurezza delle risorse umane

L'accesso anonimo, comprese le sessioni in sola lettura, deve essere eliminato. Ogni individuo con accesso remoto, sia esso un dipendente o un appaltatore esterno, deve essere identificato e autenticato in modo univoco prima che venga stabilita una sessione. L'autenticazione a più fattori è obbligatoria per i sistemi connessi a Internet. La gestione federata delle identità garantisce che i diritti di accesso del personale dimesso o degli appaltatori il cui contratto è scaduto vengano revocati tempestivamente.

- L'integrazione federata delle directory degli utenti garantisce la governance delle identità su larga scala
- L'autenticazione a più fattori (MFA) deve essere applicata prima dell'avvio di qualsiasi sessione, non come livello opzionale
- L'accesso alle sessioni anonimo, condiviso o non autorizzato deve essere bloccato per tutte le categorie di utenti

Articolo 23: Segnalazione degli incidenti

La NIS2 richiede che la notifica iniziale alle autorità nazionali venga effettuata entro 24 ore da un incidente significativo, con un rapporto completo da presentare entro 72 ore. Per le organizzazioni che affrontano un incidente che coinvolge l'accesso remoto, come credenziali di un appaltatore compromesse, una sessione non autorizzata o un movimento laterale, la capacità di produrre prove documentate entro questi tempi dipende interamente dalla qualità dell'infrastruttura di audit messa in atto prima che l'incidente si verifichi.

Le registrazioni delle sessioni, i registri delle connessioni e i dati relativi agli eventi di accesso devono essere a prova di manomissione, archiviati in più sedi e accessibili a livello di entità. Senza questa infrastruttura in atto prima di un incidente, i requisiti di segnalazione entro 24 e 72 ore non possono essere soddisfatti con lo standard probatorio richiesto.

Articolo 11: Capacità del CSIRT

I team di risposta agli incidenti di sicurezza informatica (CSIRT) richiedono una visibilità in tempo reale sulla rete e sui sistemi informativi che proteggono. Per l'accesso remoto, ciò significa un dashboard in tempo reale che mostri tutti gli endpoint online e offline, tutte le sessioni attive, tutte le connessioni in corso e tutte le autorizzazioni attualmente implementate. La funzionalità kill-switch (la capacità di terminare istantaneamente una sessione sospetta) non è una funzione di comodità, ma un requisito operativo dell'articolo 11.

Come Netop supporta la conformità

L'infrastruttura di conformità di cui i vostri revisori hanno bisogno

Soddisfare i requisiti di accesso remoto NIS2 non è principalmente una sfida di policy, ma una sfida di infrastruttura. Le policy senza meccanismi di applicazione sono insufficienti. Ciò che i revisori NIS2 richiedono sono prove: prove documentate che i controlli siano in atto, applicati in modo coerente e che producano registrazioni di livello di audit. Netop è l'infrastruttura che genera tali prove.

Controllo degli accessi e autenticazione

Netop applica un accesso granulare e basato sui ruoli a livello di singoli audit NIS2. Le autorizzazioni sono definite per utente, per gruppo di dispositivi, per applicazione e per finestra temporale. Ogni sessione richiede un'identificazione positiva. L'accesso anonimo non è consentito per nessuna categoria di utenti. L'autenticazione a più fattori viene applicata in modo nativo o tramite l'integrazione con le soluzioni di identità aziendali esistenti. Il supporto delle directory federate garantisce che i diritti di accesso riflettano lo stato attuale dei rapporti tra appaltatori e dipendenti piuttosto che istantanee storiche.

Controllo a quattro occhi e supervisione umana

Per le sessioni remote ad alto rischio, in particolare quelle condotte da fornitori esterni su apparecchiature critiche, Netop supporta meccanismi di controllo di qualità umano. L'accettazione della sessione può essere delegata a un supervisore della sicurezza designato: la sessione non procede fino a quando una persona autorizzata non la approva, tramite un pop-up sullo schermo o una conferma via e-mail. Questo principio del doppio controllo risponde direttamente ai requisiti di sicurezza della catena di fornitura della NIS2 e fornisce una registrazione documentata dell'approvazione per ogni sessione supervisionata.

Registrazione delle sessioni a prova di manomissione

Ogni sessione remota sulla piattaforma Netop può essere registrata con piena fedeltà audio-video, inclusi tutti gli eventi della tastiera, i movimenti del mouse e l'attività dello schermo, catturati in sequenza. Le registrazioni sono archiviate in un formato crittografato e a prova di manomissione con controlli di accesso in sola lettura, garantendo la conservazione della catena probatoria. In caso di incidente, queste registrazioni forniscono la documentazione di livello forense richiesta per la segnalazione ai sensi dell'articolo 23 e per le interazioni con i CSIRT nazionali e le autorità di vigilanza.

Le registrazioni utilizzano codec non standard o crittografati per impedire la manipolazione esterna. Le sessioni vengono automaticamente interrotte in caso di errore di registrazione, garantendo che nessuna sessione proceda senza che la funzionalità di audit sia attiva.

Governance dell'accesso alla catena di fornitura

L'architettura di Netop è stata progettata specificamente per risolvere il problema dell'accesso alla catena di fornitura a cui si riferisce la direttiva NIS2. I fornitori esterni, gli appaltatori e i fornitori di servizi accedono solo ai dispositivi e alle applicazioni specifici per i quali sono autorizzati, durante le fasce orarie per cui hanno ricevuto l'approvazione, e solo dagli intervalli IP autorizzati/registrati per il loro utilizzo che sono stati registrati per il loro utilizzo. L'accesso non può essere esteso oltre questi parametri senza una nuova autorizzazione esplicita.

- L'IP-fencing limita le sessioni a intervalli geografici inseriti nella whitelist e a indirizzi di fornitori specifici
- I controlli delle finestre temporali garantiscono che l'accesso degli appaltatori scada automaticamente al termine dei periodi di incarico
- L'accesso "need-to-perform" limita ciò che può essere visualizzato ed eseguito durante una sessione, a livello di applicazione
- I meccanismi di accettazione delle sessioni richiedono l'approvazione umana per le connessioni sensibili

Visibilità in tempo reale e kill-switch

Netop fornisce un dashboard in tempo reale che offre al personale addetto alle operazioni di sicurezza e al CSIRT piena visibilità sull'ambiente di accesso remoto: quali endpoint sono online o offline, quali sessioni sono attive, quali connessioni sono in esecuzione e quali autorizzazioni sono attualmente in uso. Le sessioni sospette possono essere interrotte all'istante. Le autorizzazioni possono essere disattivate in tempo reale senza richiedere alcun intervento sull'endpoint.

Standard di crittografia

Tutte le sessioni remote di Netop sono crittografate end-to-end utilizzando AES-256. Sono protetti sia i dati delle sessioni in transito che le registrazioni archiviate. Lo scambio di chiavi utilizza algoritmi di esponenziazione modulare Diffie-Hellman o RSA, soddisfacendo gli standard riconosciuti di cui all'articolo 21 §2.h del NIS2.

Controllo a livello hardware: integrazione con Intel AMT

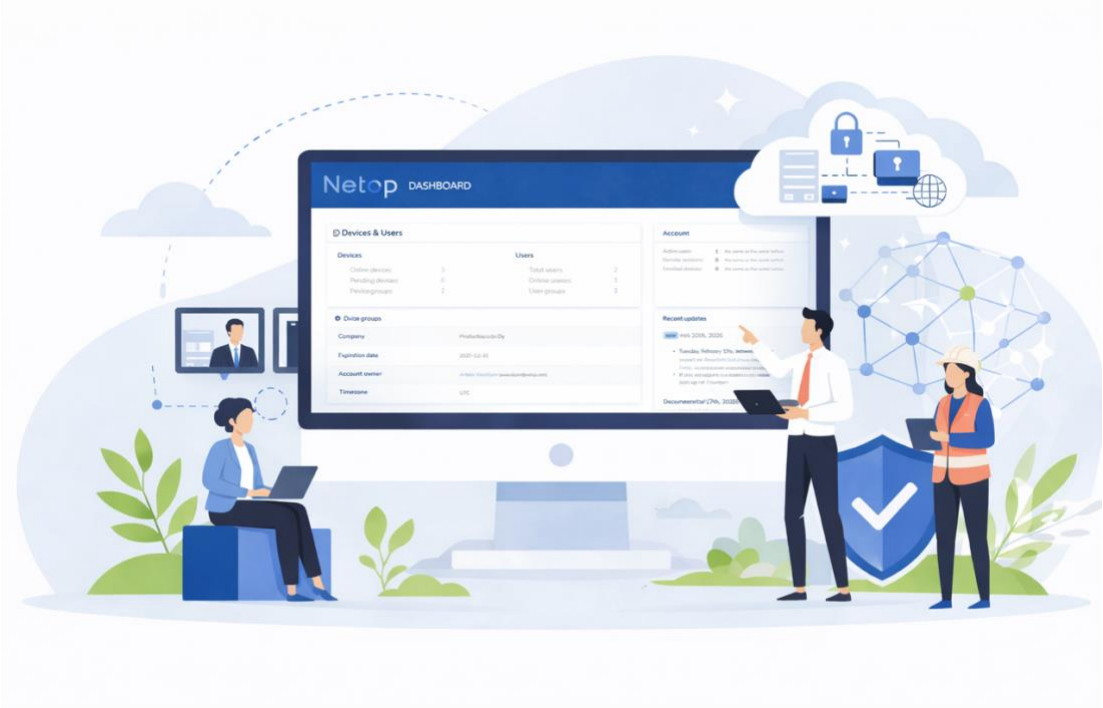
Per le organizzazioni con infrastrutture abilitate per Intel vPro, l'integrazione di Netop con Intel AMT estende l'accesso remoto sicuro fino al livello hardware. Ciò include One-Click Recovery: un processo remoto sicuro, controllato da autorizzazioni e completamente verificato per il ripristino di un dispositivo critico per l'azienda senza intervento fisico. Per gli operatori di infrastrutture critiche che gestiscono risorse distribuite geograficamente, come nodi della rete energetica, sistemi di gestione dei trasporti o apparecchiature di comunicazione per la difesa, questa funzionalità riduce il rischio operativo associato agli scenari di ripristino remoto, mantenendo al contempo la traccia di audit richiesta dalla NIS2.

Blocco dei vettori di attacco dei protocolli aperti

Netop raccomanda e supporta il blocco dei protocolli di sessione remota aperti, come RDP, VNC, Telnet e SSH, al perimetro della rete. Questi protocolli rappresentano una superficie di

attacco significativa e ben documentata. Sostituirli con un'architettura di accesso remoto punto a punto, controllata e autenticata, riduce sostanzialmente la superficie di attacco ed elimina la capacità di movimento laterale che caratterizza gli attacchi alla catena di approvvigionamento delle infrastrutture critiche.

Informazioni su Netop



Accesso remoto sicuro per ambienti critici

Netop è un fornitore globale di software di accesso remoto sicuro per infrastrutture critiche, con oltre 40 anni di esperienza al servizio di settori critici per le aziende. Netop è utilizzato da centinaia di organizzazioni in tutto il mondo, consentendo a tecnici, dipendenti, ingegneri, appaltatori e subappaltatori di accedere in modo controllato da remoto a dispositivi critici per le operazioni quotidiane e la risoluzione dei problemi.

Settori serviti

Netop opera in tutti i settori essenziali e importanti della NIS2, con particolare attenzione ai settori in cui il rischio di accesso remoto è più elevato:

- Difesa — accesso remoto sicuro per appaltatori della difesa, infrastrutture di comunicazione e apparecchiature mission-critical
- Energia — operazioni remote per infrastrutture di rete, sistemi di condutture e impianti di energia rinnovabile
- Governo e pubblica amministrazione — accesso sicuro per enti della pubblica amministrazione centrale e regionale
- Sanità — accesso remoto per apparecchiature mediche, sistemi di laboratorio e infrastrutture cliniche
- Trasporti — gestione remota dei sistemi di controllo dei trasporti, delle attrezzature della flotta e delle infrastrutture logistiche
- Servizi finanziari — accesso sicuro per sistemi di trading, reti di bancomat e operazioni finanziarie

- Produzione e servizi pubblici — accesso remoto a sistemi di controllo industriale, linee di produzione e tecnologia operativa

Netop supporta e garantisce la conformità ai principali standard di sicurezza quali ISO 27001, SOC 2, PCI-DSS, FIPS e HIPAA grazie alla propria architettura di sicurezza, ai controlli e alla flessibilità di implementazione.

Prodotto realizzato per sistemi critici conformi

Il mercato degli strumenti di accesso remoto è ampio, ma la conformità NIS2 pone requisiti elevati e specifici. La maggior parte dei prodotti di accesso remoto è stata progettata per garantire praticità operativa: facilità di connessione, supporto multipiattaforma e bassa latenza. Netop è stato progettato per ambienti controllati in cui sicurezza, verificabilità e governance sono requisiti imprescindibili. È proprio questa differenza di progettazione che fa la differenza ai fini della conformità NIS2.

1. Copertura dei controlli NIS2 per progettazione, non per adeguamento

Netop è direttamente allineato alle misure tecniche richieste dalla NIS2: crittografia, controllo degli accessi basato sui ruoli, MFA, registrazione delle sessioni, integrazione SIEM e governance degli accessi alla catena di fornitura, poiché queste funzionalità sono state integrate nell'architettura della piattaforma sin dall'inizio. Non si tratta semplicemente di componenti aggiuntivi di conformità realizzati in risposta alla normativa.

Netop è in grado di dimostrare la copertura dei controlli allineando specifiche funzionalità della piattaforma a particolari articoli della NIS2. Questa distinzione è importante in un audit: i revisori valutano ciò che un sistema fa effettivamente, non ciò che un fornitore sostiene di supportare.

2. Architettura Zero Trust by Design

L'architettura di Netop incorpora naturalmente i principi Zero Trust in tre aree chiave richieste dalla NIS2: verifica esplicita (MFA, SSO, autenticazione tramite smart card), applicazione del principio del privilegio minimo (controllo degli accessi granulare basato sui ruoli, autorizzazioni basate sulla sessione) e ipotesi di violazione (registrazione continua, segmentazione della rete, monitoraggio in tempo reale). Questo approccio differisce fondamentalmente dai prodotti che si limitano a sovrapporre lo Zero Trust come configurazione su un'architettura non originariamente progettata per esso.

3. Approfondimento dell'audit forense

L'articolo 23 della direttiva NIS2 impone alle organizzazioni di segnalare gli incidenti significativi, corredandoli di prove documentate, entro un termine compreso tra 24 e 72 ore. Lo standard probatorio è rigoroso: non è sufficiente dimostrare che si è verificato un accesso; le organizzazioni devono essere in grado di dimostrare con precisione cosa è successo, quando e da parte di chi. Netop offre funzionalità complete di riproduzione forense: registrazioni delle sessioni a prova di manomissione che includono tutti gli eventi della tastiera, i movimenti del mouse e l'attività dello schermo catturati in sequenza, con conservazione configurabile e archiviazione crittografata dei log su più destinazioni quali archiviazione locale, SIEM e cloud.

> **Il test forense**
>
> *Il vostro attuale strumento di accesso remoto è in grado di dimostrare esattamente cosa ha fatto un fornitore su un sistema in un momento specifico in una data specifica? Se la risposta è "abbiamo i log ma non la riproduzione della sessione", ciò non è sufficiente per i requisiti di segnalazione e di indagine forense previsti dall'articolo 23 della NIS2.*

4. Controllo degli accessi alla catena di fornitura

La sicurezza della catena di fornitura ai sensi dell'articolo 21, paragrafo 2, lettera d) della direttiva NIS2 richiede che l'accesso di terze parti e fornitori sia regolato con un livello di specificità che gli strumenti di accesso remoto generici non sono in grado di fornire. I controlli di accesso alla catena di fornitura di Netop sono tra i suoi principali elementi di differenziazione per i casi d'uso NIS2:

- **Politiche di accesso specifiche per fornitore**: definiscono chi può accedere a cosa, quando, da dove e per quanto tempo
- **Accesso a tempo determinato e just-in-time**: accesso dei collaboratori esterni che scade automaticamente al termine di una finestra autorizzata
- **Restrizioni a livello di applicazione** — limitando ciò con cui un fornitore connesso può interagire durante una sessione, non solo a quali dispositivi può accedere
- **Principio del doppio controllo** — che richiede che un supervisore designato accetti le sessioni ad alto rischio prima che procedano
- **Raggruppamento di dispositivi e utenti in base al livello di rischio, all'area geografica e alla certificazione**: consente la governance degli accessi su larga scala in vaste reti di fornitori

La maggior parte degli strumenti di accesso remoto utilizza politiche di accesso uniformi per tutti gli utenti. Offrono una separazione minima tra l'accesso dei dipendenti interni e quello dei collaboratori esterni e forniscono controlli minimi su ciò che un fornitore connesso può fare durante una sessione. Secondo le regole di sicurezza della catena di fornitura della NIS2, si tratta di una lacuna strutturale in materia di conformità.

5. Flessibilità di implementazione e sovranità dei dati

Le organizzazioni regolamentate dalla NIS2, specialmente nei settori della difesa, della pubblica amministrazione e delle infrastrutture critiche, devono spesso far fronte a requisiti di residenza dei dati o a vincoli infrastrutturali che impediscono opzioni di implementazione esclusivamente SaaS. Netop supporta implementazioni on-premise, cloud e ibride, inclusi portali self-hosted e configurazioni VPC. Netop Cloud opera su infrastruttura AWS all'interno dell'Unione Europea, garantendo la residenza dei dati nell'UE per tutti i dati di sessione, i log e le registrazioni.

Le architetture esclusivamente cloud o cloud-primary non sono adatte alle organizzazioni con requisiti di sovranità. Il principio fondamentale è chiaro: la NIS2 pone l'accento sul controllo. Le organizzazioni non possono rivendicare il pieno controllo sulla propria infrastruttura di accesso remoto se tale infrastruttura è ospitata in un cloud di terze parti che non gestiscono.

6. Architettura a connessione inversa (solo in uscita): nessuna superficie di attacco esposta

Netop utilizza un'architettura a connessione inversa: nessuna porta in entrata aperta, nessuna dipendenza da RDP o VNC esposti, nessuna infrastruttura condivisa che crei percorsi di attacco laterali. Tutte le sessioni utilizzano TLS con crittografia AES-256. Questa architettura risponde direttamente ai requisiti di riduzione del rischio di NIS2 ai sensi dell'articolo 21, paragrafo 2, lettera e), ed elimina i vettori di attacco più comunemente sfruttati nelle compromissioni della catena di approvvigionamento contro le infrastrutture critiche.

Le VPN combinate con RDP rimangono un vettore primario per gli attacchi alle infrastrutture critiche. Gli strumenti di accesso remoto che dipendono da porte in entrata aperte o da infrastrutture di relay condivise introducono una superficie di attacco che l'architettura di Netop non presenta.

7. Supporto per ambienti legacy e OT

NIS2 copre un'ampia gamma di apparecchiature digitali, non solo endpoint IT moderni ma anche tecnologia operativa: sistemi di controllo industriale, bancomat, dispositivi medici, sensori della rete energetica, sistemi di gestione dei trasporti e infrastrutture embedded che potrebbero avere decenni di vita. Netop è progettato per operare in questi ambienti, supportando sistemi legacy, condizioni di bassa larghezza di banda e alta latenza, nonché scenari con isolamento fisico o reti limitate.

La maggior parte degli strumenti di accesso remoto è progettata per i moderni endpoint IT e non funziona bene o non funziona affatto in ambienti OT e legacy. Per le organizzazioni che rientrano nell'ambito di applicazione della NIS2 e che includono sistemi industriali o embedded (che costituiscono la maggior parte delle entità essenziali nei settori dell'energia, dei trasporti e della produzione), ciò rappresenta una limitazione significativa alla loro idoneità.

Una nota sulla certificazione NIS2

Nessun fornitore di accesso remoto detiene attualmente una "certificazione NIS2" formale: tale certificazione non esiste ancora nel quadro normativo dell'UE. La base corretta per il confronto è la copertura delle funzionalità: quale piattaforma implementa i controlli tecnici richiesti dalla NIS2, con la profondità di audit richiesta da tali requisiti, nei modelli di implementazione accettati dalle organizzazioni regolamentate. Sulla base di questi criteri, l'architettura e il set di funzionalità di Netop sono più direttamente allineati ai requisiti della NIS2 rispetto alle altre alternative disponibili sul mercato.

Roadmap passo dopo passo per l'implementazione dell'accesso remoto NIS2

Il seguente quadro in quattro fasi fornisce un approccio strutturato alla conformità dell'accesso remoto NIS2. È progettato per produrre la documentazione richiesta sia per il progetto di implementazione di Netop che per i futuri audit NIS2.

Fase 1: Mappare la catena di fornitura digitale

Compilare un elenco completo di tutti i fornitori, appaltatori e fornitori di servizi con cui si intrattiene qualsiasi forma di rapporto di servizio digitale. Attingere dai registri contabili, dai sistemi di approvvigionamento e di gestione dei rapporti con i fornitori e dai contratti attivi degli ultimi 12-36 mesi. L'obiettivo è un registro completo dei fornitori, non limitato ai fornitori IT, ma che includa qualsiasi organizzazione che fornisca servizi che comportano l'accesso digitale ai propri sistemi.

In questa fase, i fornitori che non offrono servizi digitali (come la gestione delle strutture, i trasporti fisici o le forniture per ufficio) possono essere esclusi dall'ambito dell'accesso remoto. Le voci rimanenti dell'elenco costituiscono la base della valutazione della catena di approvvigionamento.

Fase 2: Inventario delle apparecchiature digitali

Qualsiasi dispositivo dotato di chip, microcontrollore o capacità di elaborazione a cui è possibile accedere da remoto rientra nell'ambito di applicazione. Ciò va ben oltre le risorse IT convenzionali. Le fonti per questo inventario includono:

- **Risorse IT e di comunicazione:** laptop, computer desktop, server, apparecchiature di rete, infrastrutture di comunicazione
- **Automazione di edifici e strutture:** sistemi di controllo degli accessi, videosorveglianza, piattaforme di gestione degli edifici
- **Tecnologia operativa specifica del settore:** robot industriali, sensori, apparecchiature mediche, bancomat, terminali POS, linee di produzione, veicoli di trasporto, apparecchiature per i servizi cittadini, controlli degli impianti energetici

I dispositivi accessibili solo fisicamente — mai in remoto — possono essere esclusi in questa fase. Il risultato è un registro completo delle apparecchiature, con lo stato di accesso remoto confermato per ogni articolo.

Fase 3: Mappare l'accesso dei fornitori alle apparecchiature

Con a disposizione sia il registro dei fornitori che l'inventario delle apparecchiature, il team di progetto mappa chi accede a cosa, in quali condizioni e da dove. Ciò presenta due dimensioni:

- Incentrato sul fornitore: per ciascun fornitore, a quali dispositivi accede da remoto, per quali servizi, da quali luoghi e con quale frequenza?

- Incentrato sui dispositivi: per ogni apparecchiatura, quali utenti o fornitori vi accedono da remoto, da quali reti (aziendale, esterna, domestica, Internet) e in base a quale controllo degli accessi è attualmente in vigore?

Il risultato di questa fase è la mappa di accesso remoto sicuro: una matrice documentata di utenti, dispositivi, condizioni di accesso e stato attuale dei controlli. Questo documento diventa la definizione dell'ambito del progetto di conformità NIS2 e la linea di base di riferimento per i futuri audit.

Fase 4: Implementazione con Netop

La documentazione prodotta nelle fasi da 1 a 3 fornisce tutti gli input necessari per l'implementazione di Netop. Ogni percorso di accesso dei fornitori identificato nella mappa viene configurato all'interno di Netop con i controlli di accesso, le finestre temporali, le restrizioni IP, le impostazioni di registrazione e i requisiti di supervisione appropriati. L'implementazione sostituisce i percorsi di accesso non controllati con connessioni regolate, verificabili e conformi alla NIS2.

Dopo l'implementazione, la piattaforma Netop genera le prove di audit continue (registrazioni delle sessioni, registri delle connessioni, registrazioni degli eventi di accesso) che la conformità NIS2 richiede di conservare e di poter produrre su richiesta.

Quali sono i costi della non conformità

Sanzioni pecuniarie

L'articolo 34 della NIS2 prevede sanzioni amministrative per la violazione degli articoli 21 e 23, ovvero gli obblighi di gestione del rischio e di segnalazione che supportano direttamente la governance dell'accesso remoto. La struttura delle multe applica il valore più alto tra un massimo fisso e un limite basato sul fatturato.

Tipo di entità	Sanzione massima	Limite basato sul fatturato	Articoli che determinano le sanzioni
Entità essenziali	10.000.000	2% del fatturato annuo globale	Art. 21 e 23
Enti rilevanti	7.000.000	1,4% del fatturato annuo globale	Art. 21 e 23

Per i grandi soggetti essenziali nei settori dell'energia, delle catene di approvvigionamento della difesa, delle infrastrutture finanziarie o della pubblica amministrazione, una sanzione pari al 2% del fatturato globale non è un rischio teorico, ma un'esposizione finanziaria concreta. Per un'azienda con un fatturato globale di 5 miliardi di euro, l'esposizione massima ai sensi dei soli articoli 21 e 23 è pari a 100 milioni di euro.

Responsabilità del management

Oltre alle sanzioni a carico dell'organizzazione, la NIS2 introduce conseguenze personali dirette per l'alta dirigenza. Ai sensi dell'articolo 20, gli organi di gestione sono tenuti a supervisionare la gestione dei rischi di sicurezza informatica e possono essere ritenuti personalmente responsabili in caso di inadempienze. Nei casi più gravi, ciò può comportare la sospensione dalle funzioni esecutive. La dimensione della responsabilità personale modifica il calcolo della governance: le decisioni in materia di sicurezza informatica, compresa la governance dell'accesso remoto, sono ora prese dal consiglio di amministrazione con responsabilità individuale.

Conseguenze operative e reputazionali

Le conseguenze di un fallimento della sicurezza dell'accesso remoto in un settore essenziale ai sensi della NIS2 vanno ben oltre le multe normative. Un operatore di rete energetica la cui infrastruttura di accesso remoto è compromessa deve affrontare l'interruzione operativa dei servizi essenziali. Un operatore sanitario le cui apparecchiature mediche sono accessibili da terzi non autorizzati deve affrontare rischi per la sicurezza dei pazienti. Un appaltatore della difesa il cui accesso remoto a sistemi sensibili è violato deve affrontare implicazioni per la sicurezza nazionale.

Il costo dell'inazione

Per le organizzazioni che non hanno ancora affrontato la questione della governance dell'accesso remoto ai sensi della NIS2: ogni mese senza controlli conformi è un mese di non conformità documentata a cui le autorità di vigilanza nazionali possono fare riferimento. La NIS2 non richiede che si verifichi una violazione per dare avvio all'applicazione della normativa. Le revisioni e gli audit di vigilanza possono identificare controlli inadeguati prima che si verifichi un incidente.

Conclusione

L'accesso remoto non è solo uno dei tanti elementi del quadro di conformità NIS2. È il requisito che abbraccia la maggior parte degli obblighi, presenta il rischio operativo più elevato ed è più comunemente inadeguato nelle organizzazioni che si sono affidate ad architetture legacy basate su VPN o ad accesso non controllato.

Per gli operatori di infrastrutture critiche, le organizzazioni di difesa e le agenzie governative, il percorso verso la conformità NIS2 per l'accesso remoto prevede quattro passaggi chiave: sapere chi ha accesso a cosa, applicare controlli dettagliati su tale accesso, creare prove a prova di manomissione di ogni sessione ed essere in grado di rispondere e segnalare gli incidenti con prove documentate. Netop è il software progettato per fornire tutti e quattro questi elementi.

Le organizzazioni che si muoveranno per prime per implementare una governance dell'accesso remoto conforme non solo soddisferanno i revisori NIS2, ma elimineranno anche una classe di rischio della catena di approvvigionamento che rappresenta uno dei vettori di attacco più sfruttati contro le infrastrutture critiche in Europa oggi.

Contatta Netop per la conformità alla normativa NIS2

Richiedi una demo del software di accesso remoto sicuro di Netop e discuti i tuoi requisiti di conformità NIS2 con uno specialista.

www.netop.com | info@netop.com

Appendice: Settori essenziali e importanti ai sensi della NIS2

I seguenti settori sono definiti nella Direttiva (UE) 2022/2555 come entità essenziali o importanti soggette agli obblighi NIS2. Fonte: Commissione Europea / ENISA.

Settori essenziali (ad alta criticità)

1. Energia — imprese elettriche, operatori di distribuzione e trasmissione, oleodotti e gasdotti, produzione e stoccaggio di idrogeno
2. Trasporti — vettori aerei, infrastrutture ferroviarie, trasporto marittimo, gestione del traffico stradale, sistemi di trasporto intelligenti
3. Istituzioni bancarie e di credito
4. Infrastrutture dei mercati finanziari — sedi di negoziazione, controparti centrali
5. Sanità — fornitori di assistenza sanitaria, laboratori di riferimento dell'UE, produttori farmaceutici, produttori di dispositivi medici
6. Acqua potabile — fornitori e distributori di acqua destinata al consumo umano
7. Acque reflue — imprese che raccolgono, smaltiscono o trattano le acque reflue
8. Infrastrutture digitali — punti di interscambio Internet, fornitori di DNS, registri TLD, cloud computing, centri dati, reti di distribuzione dei contenuti, fornitori di servizi fiduciari, comunicazioni elettroniche pubbliche
9. Gestione dei servizi TIC (B2B) — fornitori di servizi gestiti, fornitori di servizi di sicurezza gestiti
10. Pubblica amministrazione — enti governativi centrali e regionali come definiti dagli Stati membri
11. Settore spaziale — operatori di infrastrutture terrestri a supporto di servizi spaziali

Altri settori critici (importanti)

12. Servizi postali e di corriere
13. Gestione dei rifiuti
14. Fabbricazione, produzione e distribuzione di sostanze chimiche
15. Produzione, trasformazione e distribuzione di prodotti alimentari
16. Produzione — dispositivi medici, prodotti informatici ed elettronici, apparecchiature elettriche, macchinari, veicoli a motore, mezzi di trasporto
17. Fornitori di servizi digitali — mercati online, motori di ricerca online, piattaforme di social network
18. Organizzazioni di ricerca

Fonte: Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio (Direttiva NIS2). Testo ufficiale disponibile all'indirizzo: eur-lex.europa.eu/eli/dir/2022/2555

Pagina della Commissione europea dedicata alla direttiva NIS2: digital-strategy.ec.europa.eu/en/policies/nis2-directive