WHITE PAPER

Verso la conformità alla NIS2: perché lo zero trust è un elemento fondamentale del percorso

Indice

Riepilogo

La direttiva NIS2 e il ruolo di un modello zero trust nel migliorare la resilienza informatica

L'emanazione della Direttiva sulla sicurezza delle reti e dei sistemi informativi 2 (Network and Information Security Directive 2, NIS2) segna un'evoluzione significativa nell'impegno dell'Unione europea (UE) nel rafforzare la sicurezza informatica in tutti i suoi Stati membri. La direttiva NIS2 sostituisce la precedente direttiva NIS e ne amplia l'ambito di applicazione a una gamma più estesa di settori e sottosettori, rafforzando al contempo i requisiti di sicurezza, tra cui l'elevazione della sicurezza informatica a imperativo negli ambiti della gestione e della governance. Sebbene la NIS2 sia entrata in vigore nel 2023, la scadenza chiave era ottobre 2024, data entro cui gli Stati membri dell'UE avrebbero dovuto disporre di leggi nazionali vincolanti per la relativa implementazione. Dato che l'attuazione della NIS2 può variare leggermente da uno stato membro all'altro, questo whitepaper si concentrerà sui requisiti e i principi generali della Direttiva.

Nessuna soluzione o fornitore di software può garantire da solo la conformità alla direttiva NIS2. Tuttavia, l'adesione ai principi dello zero trust (che la Direttiva stessa suggerisce alle entità di adottare come pratica di base di igiene informatica) risponde a diversi dei criteri imposti dalla Direttiva. L'implementazione di un'architettura zero trust nell'ambiente di un'organizzazione, negli elementi distribuiti di una rete e in quelli di terze parti di un'organizzazione può contribuire a ridurre drasticamente le superfici di attacco e a eliminare una serie di variabili tecniche che possono ostacolare i progressi verso la conformità alla NIS2. Lo zero trust dovrebbe essere lo strumento primario utilizzato dalle organizzazioni per potenziare la resilienza e un fornitore affidabile nel campo dello zero trust può supportare i percorsi di conformità delle organizzazioni.

Il percorso verso la conformità deve essere strutturato e comunicato in tutte le organizzazioni interessate dalla nuova Direttiva. Recenti indagini condotte da Zscaler sui team IT europei hanno analizzato il livello di preparazione delle organizzazioni a essere conformi. Il 71% dei responsabili IT intervistati ritiene che la modernizzazione della sicurezza richieda un significativo cambiamento di mentalità, non solo un esercizio di conformità.

Tuttavia, le posizioni assunte dai vari stakeholder, che saranno determinanti per la conformità, differiscono considerevolmente. Se da un lato l'80% dei responsabili IT intervistati è sicuro che le proprie organizzazioni saranno conformi entro la scadenza, solo il 53% ritiene che i propri team comprendano appieno la portata degli obblighi previsti dalla NIS2. Quando si chiede se i vertici aziendali sono effettivamente a conoscenza degli obblighi previsti dalla Direttiva, quella percentuale scende a 49%. Oltre il 60% degli intervistati ritiene che la NIS2 richiederà un cambiamento radicale, rispetto all'attuale strategia di sicurezza.

Grazie alla nostra competenza nel campo della sicurezza sul cloud, Zscaler riveste un ruolo chiave nell'aiutare le organizzazioni a gestire i cambiamenti introdotti dalla NIS2. Adottando l'architettura zero trust di Zscaler, le organizzazioni di tutte le dimensioni possono soddisfare i requisiti fondamentali previsti dalla Direttiva, potenziando i propri meccanismi difensivi, riducendo l'esposizione ai rischi informatici e semplificando le attività per raggiungere la conformità. I principi dello zero trust sono strettamente allineati agli obiettivi della NIS2, in quanto prevedono l'eliminazione sistematica dei diritti di accesso non necessari, la verifica rigorosa di tutte le connessioni e la mitigazione dell'impatto dei potenziali incidenti di sicurezza. Zscaler fornisce una serie di funzionalità e strumenti che supportano le iniziative volte a uniformarsi a specifiche disposizioni della NIS2, tra cui l'applicazione delle policy, il rilevamento degli incidenti e i processi di risposta.

Una panoramica sulla direttiva NIS2 e sul suo ambito di applicazione

La direttiva NIS2 è entrata in vigore nel 2023 e la scadenza per la relativa attuazione da parte degli Stati membri dell'UE era a ottobre 2024. I responsabili politici dell'Unione europea hanno emanato questa nuova legislazione fondamentale in risposta alla necessità dell'UE di accrescere la propria resilienza informatica, in un'epoca in cui gli attacchi informatici rivolti ai cittadini, alle imprese e alle economie europee continuano a crescere. La NIS2 sottolinea la responsabilità delle entità nel garantire la sicurezza delle reti e dei sistemi informativi, invitandole ad adottare una cultura di governance e framework completi per la gestione del rischio. La NIS2 è in linea con la crescente tendenza dell'UE verso una regolamentazione più diretta delle iniziative di resilienza informatica (ad esempio, il Digital Operational Resilience Act (DORA), che è entrato in vigore a gennaio 2025, è un quadro normativo separato per la gestione e la mitigazione del rischio ICT nel settore finanziario).

La NIS2 aggiunge nuovi settori industriali, oltre a nuove tipologie di entità, ai settori già inclusi nella direttiva NIS originale. Questa espansione risponde alla crescente consapevolezza che un'ampia gamma di attività economiche e sociali dipende in modo critico dalle infrastrutture IT, che le minacce informatiche dirette a questi settori sono in aumento e che le interruzioni possono avere effetti a cascata in tutta l'UE.

I settori industriali indicati nella NIS2 sono classificati come "essenziali" o "importanti", per riflettere la loro criticità o il servizio che forniscono. Sebbene i requisiti di sicurezza informatica e di segnalazione degli incidenti siano gli stessi per entrambi i gruppi, queste due categorie di entità saranno soggette a regimi di supervisione e applicazione leggermente diversi, tra cui l'ammontare delle potenziali sanzioni per inosservanza (maggiori dettagli di seguito).

> “Con la scadenza ormai alle porte, le organizzazioni si trovano a dover accelerare le attività rivolte alla conformità, a scapito però di altri aspetti vitali della sicurezza informatica. Il 60% dei partecipanti all'indagine teme infatti che concentrando gli sforzi solamente sulla conformità alla NIS2 si possano trascurare altre aree critiche della sicurezza. Di conseguenza, è fondamentale che i leader aziendali forniscano il massimo supporto ai reparti IT, garantendo un approccio olistico alla conformità che mitighi i rischi correlati alle vulnerabilità e ai rallentamenti operativi.”
>
> **James Tucker,** responsabile dei CISO in Residence EMEA presso Zscaler

Settori e sottosettori inclusi nella NIS2[1]

Entità essenziali ("settori a elevata criticità")	
Energia	Rientrano elettricità, petrolio, gas, teleriscaldamento e raffrescamento e idrogeno.
Trasporti	Rientrano il trasporto aereo, ferroviario, marittimo/fluviale e su strada
Banche (istituti di credito)	
Infrastrutture del mercato finanziario	
Salute	Rientrano assistenza sanitaria, settore farmaceutico
Acqua potabile	
Acque reflue	
Infrastruttura digitale	Rientrano i fornitori di Internet Exchange Point (IXP), i fornitori di servizi DNS, i registri dei nomi TLD, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione di contenuti, i fornitori di servizi fiduciari, i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica disponibili al pubblico
Gestione dei servizi ICT (business-to-business)	Rientrano i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestita
Pubblica amministrazione	Enti della pubblica amministrazione dei governi centrali e regionali come definiti dalle leggi nazionali degli Stati membri
Spazio (operatori di infrastrutture terrestri)	
Entità importanti ("altri settori critici")	
Servizi postali e di corrieri	
Gestione dei rifiuti	
Manifattura, produzione e distribuzione di prodotti chimici	
Produzione, trasformazione e distribuzione di alimenti	
Settore manifatturiero	Rientra un'ampia gamma di produzioni manifatturiere, quali dispositivi medici, computer ed elettronica, apparecchiature elettriche, macchinari e attrezzature, veicoli a motore, attrezzature di trasporto
Fornitori digitali	Rientrano i fornitori di marketplace online, i fornitori di motori di ricerca online e i fornitori di piattaforme di servizi di social network
Organizzazioni di ricerca	

1. Esistono alcune eccezioni a queste categorie; per maggiori dettagli puoi consultare gli allegati I e II della Direttiva. Sono esclusi anche gli enti della pubblica amministrazione le cui attività sono prevalentemente rivolte alla sicurezza nazionale, alla sicurezza pubblica, alla difesa o all'applicazione della legge. Inoltre, la Direttiva si applica solo alle entità che nell'UE sono considerate "medie imprese" (imprese con più di 250 dipendenti e un fatturato annuo superiore a 50 milioni di euro). Allo stesso tempo, alcune eccezioni applicano a loro volta la NIS2 ad alcune entità più piccole.

L'approccio zero trust di Zscaler supporta la direttiva NIS2

La piattaforma Zero Trust Exchange™ di Zscaler riduce la complessità associata alla sicurezza della rete tradizionale, rendendo più semplice per le organizzazioni uniformarsi ai requisiti della direttiva NIS2. Zero Trust Exchange™ è un'architettura nativa del cloud, basata sul modello SASE, appositamente progettata per soddisfare le esigenze delle operazioni aziendali globali, caratterizzate da bisogni tecnologici e operativi eterogenei. L'utilizzo di una segmentazione granulare per compartimentare una rete, l'applicazione di un accesso con privilegi minimi per limitare le autorizzazioni degli utenti e il monitoraggio continuo del traffico sono misure proattive che aiutano a identificare e rispondere agli aggressori, riducendo al minimo i potenziali danni e l'impatto degli attacchi.

Zero Trust Exchange™ consente inoltre alle organizzazioni di ridurre la superficie di attacco, prevenire il movimento laterale e mitigare i rischi di subire violazioni, astraendo la sicurezza dall'infrastruttura di rete. Ciò garantisce che gli utenti si connettano in modo sicuro alle applicazioni senza esporre le reti a Internet, riducendo significativamente il rischio di attacchi. Le funzionalità della piattaforma supportano le attività rivolte alla conformità previste dalla NIS2 negli ambiti della gestione sicura dei dati, dei controlli dell'accesso e della gestione degli incidenti.

La piattaforma potenzia la sicurezza proteggendo tutto il traffico, gli utenti e i dispositivi, garantendo il blocco delle minacce in tempo reale e offrendo un'ispezione completa del traffico. Zscaler incrementa inoltre la produttività degli amministratori, grazie a una gestione globale unificata e all'amministrazione delle policy, eliminando la necessità di manutenere l'hardware e consentendogli di concentrarsi sulle attività di maggior valore per il business. La piattaforma Zscaler ottimizza le prestazioni di Internet riscontrate dagli utenti finali e le connessioni dirette a Internet; inoltre, la nostra conformità ai principali framework di sicurezza, quali ISO 27001 e SOC2 Type II, contribuisce a migliorare ulteriormente l'esperienza utente complessiva e il livello di sicurezza aziendale. Ulteriori dettagli sullo zero trust e sull'approccio di Zscaler all'architettura zero trust sono disponibili sul portale Zpedia di Zscaler.

L'allineamento di Zscaler con la NIS2

L'approccio completo di Zscaler alla sicurezza e alla conformità ci consente di reagire rapidamente e di allinearci alle normative esistenti, nuove ed emergenti come la NIS2. Il programma interno di gestione del rischio di sicurezza informatica di Zscaler garantisce l'aderenza a standard riconosciuti a livello internazionale, quali ISO 27001 e SOC 2. L'allineamento a questi standard fondamentali consente a Zscaler di integrare efficacemente una serie diversificata di controlli di sicurezza per identificare, prevenire, rilevare, rispondere e ripristinare i sistemi dalle minacce associate all'interno dei nostri prodotti e servizi. Zscaler sfrutta un framework strutturato di controlli comuni, che si concentra su competenze chiave in materia di sicurezza informatica, quali l'istituzione di un programma di gestione del rischio per la sicurezza delle informazioni, l'adozione di pratiche di sicurezza rivolte alla catena di approvvigionamento, la gestione del rischio di terze parti, l'introduzione di valutazioni continue del rischio, la segnalazione degli incidenti, la divulgazione delle vulnerabilità e molto altro ancora. Un elenco aggiornato degli standard di sicurezza e conformità adottati da Zscaler è disponibile nella **pagina** dedicata alla conformità di Zscaler.

Inoltre, Zscaler gestisce lo Zscaler Trust **Portal** per fornire ai clienti informazioni strategiche in tempo reale sulle operazioni di Zscaler, fungendo da forum di riferimento sulle comunicazioni relative a **incidenti** e **avvisi** correlati a Zscaler.

Aspetti chiave della conformità alla NIS2 e come Zscaler può aiutare

La NIS2 delinea la responsabilità delle entità nel garantire la sicurezza delle reti e dei sistemi informativi, invitandole a implementare una cultura di governance e framework per la gestione del rischio che siano consolidati, completi e ben integrati. Per raggiungere questi obiettivi, la NIS2 include misure di gestione del rischio di sicurezza informatica, misure di governance, requisiti sulla segnalazione degli incidenti, nonché misure di supervisione e applicazione, tutti elementi che verranno descritti di seguito.

Nell'indagine condotta sui responsabili IT europei citata in precedenza, il 56% degli intervistati ha riferito a Zscaler che i propri team ritengono di non disporre del supporto necessario da parte della dirigenza per riuscire a rispettare la scadenza di conformità prevista dalla NIS2. Per supportare i percorsi di conformità, i responsabili IT intervistati hanno affermato che i cambiamenti più significativi richiesti dalle loro organizzazioni erano i seguenti:

- Aggiornamento dell'assetto tecnologico e delle soluzioni di sicurezza informatica: 34%
- Formazione dei dipendenti: 20%
- Formazione della leadership: 17%

Le misure per la gestione del rischio informatico previste dalla NIS2

Le entità che rientrano nell'ambito di applicazione della Direttiva devono adottare misure tecniche, operative e organizzative proattive per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi che tali realtà utilizzano per le loro operazioni o per l'erogazione dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi che le organizzazioni possono fornire.

L'articolo 21 della Direttiva elenca le misure minime di gestione del rischio informatico che le organizzazioni devono adottare, mentre i considerando 78 e 89 forniscono maggiori informazioni sulle aspettative degli autori della legge.

- **L'articolo 21 (misure minime di gestione del rischio di sicurezza informatica)** specifica che le entità devono implementare policy sull'analisi del rischio e sulla sicurezza dei sistemi informativi; sulla continuità aziendale e sulla gestione delle crisi; sulla sicurezza della catena di approvvigionamento, che include le procedure di sviluppo dei prodotti di qualità e sicure e le pratiche di sicurezza informatica dei loro fornitori e provider di servizi; le pratiche di base di igiene informatica e la formazione sulla sicurezza informatica; policy e procedure relative all'uso di crittografia/cifratura; sicurezza delle risorse umane, policy di controllo dell'accesso e gestione delle risorse; e utilizzo di soluzioni di autenticazione a più fattori o di autenticazione continua.
- **Ai sensi del considerando 78**, le misure di gestione del rischio di sicurezza informatica attuate dalle entità rientranti nell'ambito di applicazione della Direttiva dovrebbero tenere conto del grado di dipendenza dell'entità dalla rete e dai sistemi informativi; identificare eventuali rischi di incidenti; prevenire, rilevare, rispondere e ripristinare i sistemi dagli incidenti e mitigarne l'impatto; coprire i dati archiviati, trasmessi ed elaborati; e prevedere un'analisi sistemica, tenendo conto del fattore umano.
- **Il considerando 89** esorta le entità ad attuare una serie di pratiche di base raccomandate in materia di igiene informatica, ovvero i principi dello zero trust, gli aggiornamenti software, la configurazione dei dispositivi, la segmentazione della rete, la gestione delle identità e degli accessi o la sensibilizzazione degli utenti, nonché formare e sensibilizzare il personale in merito alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale. Il considerando 89 esorta inoltre le entità a implementare tecnologie volte a migliorare la sicurezza informatica, come i sistemi di intelligenza artificiale (IA) o di machine learning (ML), per potenziare le proprie capacità e la sicurezza delle reti e dei sistemi informativi.

Come può aiutare Zscaler: di seguito descriviamo in generale come Zscaler può aiutare le entità ad allinearsi a specifici aspetti di queste disposizioni. Per una mappatura dettagliata delle soluzioni e degli strumenti di Zscaler che supportano queste disposizioni, puoi rivolgerti al tuo rappresentante Zscaler di zona. Contenuti generali e whitepaper sulle soluzioni di Zscaler sono disponibili all'indirizzo https://www.zscaler.com/it/resources?type=white-papers.

Governance e gestione del rischio secondo la NIS2

La NIS2 attribuisce la responsabilità massima alla dirigenza aziendale. Quest'ultima deve approvare e supervisionare l'attuazione delle misure di gestione del rischio informatico dell'entità. La dirigenza deve inoltre seguire corsi di formazione sulla sicurezza informatica e offrire regolarmente corsi analoghi ai propri dipendenti, in modo che acquisiscano conoscenze e competenze sufficienti per identificare i rischi, nonché valutare le pratiche di gestione dei rischi di sicurezza informatica e il relativo impatto sui servizi dell'entità.

In che modo Zscaler può aiutare: Zscaler offre funzionalità di sicurezza complete attraverso tutta la sua suite di servizi, progettate per aiutare le organizzazioni a ridurre al minimo la superficie di attacco e a garantire l'efficacia dei controlli di sicurezza applicati nel programma di governance e gestione del rischio del cliente.

Zscaler Resilience™ è un set completo di funzionalità che garantisce la continuità operativa senza interruzioni durante blackout, abbassamenti di tensione o eventi catastrofici imprevisti.

Zscaler Internet Access (ZIA) e Zscaler Private Access (ZPA) gestiscono i flussi di traffico e forniscono log di eventi e transazioni di sicurezza per la correlazione e la gestione, consentendo alle organizzazioni di monitorare e mitigare efficacemente le potenziali minacce.

Zero Trust Exchange™ di Zscaler garantisce che gli utenti non vengano collocati sulla rete e che le applicazioni non vengano mai esposte a Internet, riducendo significativamente la superficie di attacco. Questa soluzione consente inoltre alle organizzazioni di creare e applicare policy relative ai siti di IA generativa con cui gli utenti possono interagire, per garantire la protezione dei dati sensibili.

Le funzionalità di ispezione SSL di Zscaler migliorano ulteriormente la sicurezza, decrittografando il traffico HTTPS per rilevare e bloccare i contenuti dannosi.

Le soluzioni Risk360™ e Zscaler Posture Control (ZPC) di Zscaler consentono il monitoraggio continuo e il rilevamento delle vulnerabilità, permettendo alle organizzazioni di affrontare in modo proattivo i rischi per la sicurezza.

Zscaler Digital Experience (ZDX) fornisce il monitoraggio dell'inventario dei dispositivi, garantendo che i componenti del servizio siano identificati in modo appropriato e ritirati in modo sicuro quando necessario, contribuendo a ridurre al minimo la superficie di attacco.

Il servizio Nanolog Streaming Service (NSS) di Zscaler semplifica la comunicazione tra il cloud di Zscaler e le soluzioni di sicurezza di terze parti, consentendo la trasmissione in tempo reale dei log ai sistemi SIEM dei clienti tramite opzioni basate su VM o Cloud NSS.

Zscaler Cloud Intrusion Prevention Service (IPS), integrato con tecnologie quali firewall e sandbox, fornisce una protezione completa dalle minacce contro vari attacchi, sfruttando firme personalizzate e leader del settore per il monitoraggio in tempo reale e l'applicazione delle policy. Inoltre, le organizzazioni possono identificare e correggere in modo proattivo le vulnerabilità utilizzando le funzionalità di Zscaler, quali le policy Advanced Threats Protection e Mobile Malware Protection di ZIA, mentre Risk360 offre informazioni utili sulla superficie di attacco esterna e sul rischio di propagazione laterale, consentendo decisioni informate per migliorare la sicurezza di un'organizzazione e ridurre il tempo medio di risposta (MTTR).

Infine, tutti i clienti possono registrarsi per utilizzare lo ZScaler Trust Portal per segnalare gli incidenti effettivi e sospetti.

I requisiti di segnalazione degli incidenti previsti dalla NIS2

Le entità devono notificare alle autorità qualsiasi incidente che abbia un impatto significativo sull'erogazione dei loro servizi. Se del caso, devono inoltre informare i destinatari dei loro servizi di incidenti significativi che potrebbero influire negativamente sulla fornitura dei servizi. La NIS2 definisce "incidente significativo" come un incidente che ha causato o è in grado di causare gravi interruzioni operative dei servizi o perdite finanziarie per l'entità interessata, oppure ha colpito o è in grado di colpire altre persone fisiche o giuridiche causando ingenti danni materiali o immateriali.

La cronologia della segnalazione degli incidenti è la seguente:

- Un "allarme precoce" entro 24 ore da quando si viene a conoscenza di un incidente significativo;
- Una notifica formale dell'incidente entro 72 ore dal momento in cui si è venuti a conoscenza di un incidente significativo, che fornisca una valutazione iniziale dell'incidente, inclusa la relativa gravità e impatto, nonché (ove disponibili) degli indicatori di compromissione;
- Una relazione finale entro un mese che descriva dettagliatamente l'incidente, compresa la relativa gravità e impatto; il tipo di minaccia o la causa principale che ha verosimilmente innescato l'incidente; le misure di mitigazione applicate e in corso; e (ove applicabili) le implicazioni transfrontaliere.
- Durante questo processo le autorità possono richiedere una relazione intermedia con aggiornamenti rilevanti sullo stato.

Come può aiutare Zscaler: le soluzioni di sicurezza con base cloud di Zscaler offrono funzionalità di rilevamento e mitigazione delle minacce in tempo reale, garantendo alle organizzazioni la possibilità di identificare e mitigare rapidamente gli attacchi. Inoltre, spostando il focus dalle difese tradizionali basate sul perimetro a favore della verifica e dell'autorizzazione continuative delle identità, l'architettura zero trust di Zscaler contribuisce a prevenire il movimento laterale che potrebbe peggiorare la gravità in caso di violazione. Valutando ogni richiesta di accesso in base all'identità, all'autorizzazione e al contesto correlato, l'intero ambiente risulta protetto in modo ottimale dagli incidenti informatici.

Supervisione e applicazione della NIS2 (articoli 32 e 33)

Gli Stati membri dell'UE possono esercitare poteri di vigilanza e di controllo sulle entità che violano le misure di gestione del rischio di sicurezza informatica e gli obblighi di segnalazione previsti dalla NIS2. I regimi di vigilanza e di applicazione per le entità essenziali e importanti divergono leggermente: per le entità essenziali la vigilanza è ex ante, mentre per le entità importanti è ex post (quando vi sono prove, indicazioni o informazioni che un'entità non rispetta la NIS2).
In generale, le autorità possono sottoporre le entità interessate di entrambe le categorie a:

- Ispezioni in loco e supervisione fuori sede
- Audit di sicurezza mirati, effettuati da un organismo indipendente o da un'autorità competente
- Scansioni della sicurezza
- Richiesta di informazioni necessarie per valutare le misure di gestione del rischio di sicurezza informatica adottate, comprese le policy di sicurezza informatica documentate
- Richiesta di accesso a informazioni, dati e documenti necessari alla vigilanza
- Richiesta di prova dell'attuazione delle policy di sicurezza informatica

La Direttiva stabilisce inoltre che la dirigenza può essere ritenuta personalmente responsabile per le violazioni della NIS2, prevedendo ad esempio potenziali divieti temporanei dal ricoprire posizioni dirigenziali e, come ultima risorsa, le autorità hanno il potere di sospendere temporaneamente una certificazione o un'autorizzazione relativa ai servizi pertinenti forniti dall'entità o alle attività svolte.

Gli Stati membri dell'UE possono inoltre imporre sanzioni amministrative in caso di inosservanza delle disposizioni della NIS. Per le entità essenziali, le sanzioni amministrative possono raggiungere i 10 milioni di euro o 2% del fatturato annuo totale globale dell'esercizio finanziario precedente, a seconda di quale sia il valore più alto. Per le entità importanti, le sanzioni possono raggiungere i 7 milioni di euro o l'1,4% del fatturato annuo totale globale dell'esercizio finanziario precedente, a seconda di quale sia il valore più alto.

Come può aiutare Zscaler: Zscaler supporta le organizzazioni a prepararsi e a rispondere agli audit e ai controlli normativi, attraverso una rendicontazione completa, un'applicazione coerente delle policy e una reportistica dettagliata.

Per maggiori informazioni sulla NIS2 e sulle funzionalità offerte da Zscaler, rivolgersi al proprio rappresentante Zscaler di zona.

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su **X (precedentemente Twitter) @zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/it