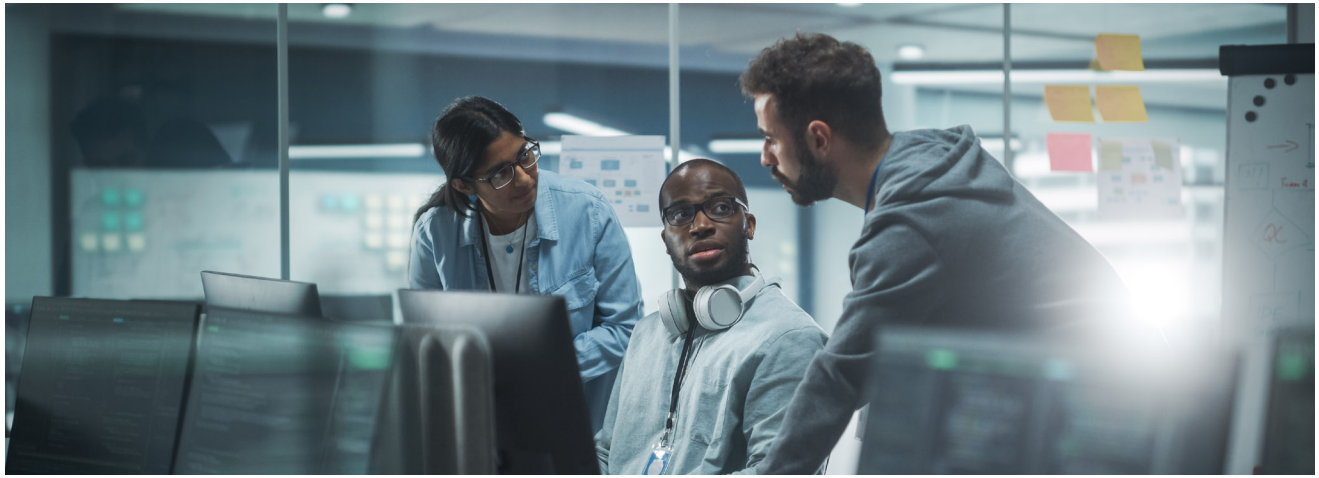
Direttiva NIS2: requisiti più severi per la sicurezza informatica

La direttiva NIS2 è una normativa europea che mira ad aumentare il livello di sicurezza informatica all'interno dell'Unione Europea. Lo fa, tra le altre cose, rivolgendosi ad un'ampia gamma di settori, imponendo misure di cybersecurity più rigorose (comprese le minacce nelle catene di approvvigionamento) e creando requisiti più rigorosi per la segnalazione degli incidenti.

Gli Stati membri dell'Unione Europea (UE) hanno tempo fino a settembre 2024 per trasporre la direttiva NIS2 in atti esecutivi nazionali. Questi saranno vincolanti per legge, il che significa che la tua organizzazione (se interessata) dovrà conformarsi ai suoi requisiti.



Organizzazioni interessate

La direttiva NIS2 è rivolta alle organizzazioni di medie e grandi dimensioni, e, ora, fornisce un elenco esteso di settori soggetti alla regolamentazione.

Le organizzazioni sono classificate (in base alle dimensioni e al settore) come "enti essenziali" o "enti importanti". La classificazione incide sulle responsabilità che le organizzazioni avranno quando la NIS2 entrerà in vigore.

Nota: la direttiva NIS2 elenca eccezioni alla regola sulle dimensioni e sulla classificazione di settore.
Vedi Capo I - Articoli 2 e 3

Settore	Sottosettore	**Di grandi dimensioni** 250+ dipendenti o più di 50 milioni di fatturato	**Di medie dimensioni** 50-250 dipendenti o 10-50 milioni di fatturato
Energia	elettricità, gas, petrolio, riscaldamento/raffreddamento, idrogeno, operatori di punti di ricarica EV	Essenziale	Importante*
Trasporti	aereo, ferroviario, stradale e marittimo (incl. compagnie di navigazione e strutture portuali)	Essenziale	Importante*
Bancario e finanziario	istituti di credito, infrastrutture del mercato finanziario, sedi di negoziazione, controparti centrali (attenzione: DORA)	Essenziale	Importante*
Salute	operatori sanitari, laboratori di ricerca, prodotti farmaceutici, produzione di dispositivi medici	Essenziale	Importante*
Acqua	fornitori di acqua potabile, operatori delle acque reflue (solo se è parte essenziale della loro attività generale)	Essenziale	Importante*
Infrastrutture digitali e servizi IT	servizi fiduciari, DNS, registri dei nomi TLD, reti pubbliche di comunicazioni elettroniche	Essenziale	Essenziale
	scambi internet, centri dati, cloud computing, servizi gestiti (di sicurezza).	Essenziale	Importante*
Pubblica amministrazione	governo centrale (escl. magistratura, parlamento, banca centrale; difesa, sicurezza nazionale/pubblica)	Essenziale	Essenziale
	governo regionale: basato sul rischio, governo locale: facoltativo	Importante*	Importante*
Spazio	operatori di infrastrutture a terra	Essenziale	Importante*
Servizi postali e corrieri		Importante*	Importante*
Gestione dei rifiuti	(solo se attività economica principale)	Importante*	Importante*
Prodotti chimici	manifattura, produzione, distribuzione	Importante*	Importante*
Alimentare	produzione, trasformazione, distribuzione	Importante*	Importante*
Manifatturiero	dispositivi medici; computer, elettronica, ottica, macchinari, veicoli a motore, rimorchi, altri mezzi di trasporto	Importante*	Importante*
Provider digitali	marketplace online, motori di ricerca, piattaforme social	Importante*	Importante*
Istituti di ricerca	(esclusi gli istituti scolastici)	Important*	Important*

Gestione dei rischi di cybersecurity

Una volta attuata, la NIS2 aumenterà lo sforzo (minimo) che le organizzazioni dovrebbero dedicare alla cybersecurity. In sintesi, la direttiva NIS2 stabilisce i requisiti per:

Risk Ownership

Al management viene affidata la responsabilità diretta di garantire che i rischi informatici vengano identificati, affrontati e che i requisiti siano soddisfatti.
Capo IV - Articolo 20

Controllo del rischio

La tua organizzazione deve implementare misure di prevenzione e mitigazione che riducano i rischi e gli impatti. Ad esempio, misure adeguate in materia di gestione degli incidenti, cybersecurity nelle catene di approvvigionamento, sicurezza della rete, controllo degli accessi e crittografia.

Continuità operativa

La tua organizzazione dovrebbe considerare come garantire la continuità operativa aziendale in caso di grave incidente informatico. Ad esempio, ripristino del sistema, procedure di emergenza e creazione di un organismo di crisi.

Segnalazione degli incidenti

Le organizzazioni devono garantire un'adeguata segnalazione alle autorità. Tra le altre cose, vige il rigido requisito che gli incidenti gravi vengano segnalati entro 24 ore e che venga eseguita una valutazione iniziale entro 72 ore. Capo IV - Articolo 23

Nello specifico, l'Articolo 21 della direttiva NIS2 elenca esplicitamente le seguenti misure tecniche, operative e organizzative per gestire i rischi legati alla sicurezza delle reti e dei sistemi informativi e per prevenire o ridurre al minimo l'impatto degli incidenti: Capo IV - Articolo 21

a. policy sull'analisi del rischio e sulla sicurezza dei sistemi informativi;

b. gestione degli incidenti;

c. business continuity, tra cui backup management, disaster recovery e crisis management;

d. sicurezza della catena di approvvigionamento, compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascuna entità e i suoi fornitori diretti o prestatori di servizi;

e. sicurezza nell'acquisizione, sviluppo e manutenzione di reti e sistemi informativi, compresa la gestione e la divulgazione delle vulnerabilità;

f. policy e procedure per valutare l'efficacia delle misure di gestione dei rischi della sicurezza informatica;

g. pratiche di igiene informatica di base e formazione sulla cybersecurity;

h. policy e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;

i. sicurezza delle risorse umane, policy di controllo degli accessi e gestione delle risorse;

j. l'uso dell'autenticazione a più fattori o di soluzioni di autenticazione continua, comunicazioni vocali, video e testuali sicure e sistemi di comunicazione d'emergenza protetti all'interno dell'entità, se necessario

Supervisione ed esecuzione

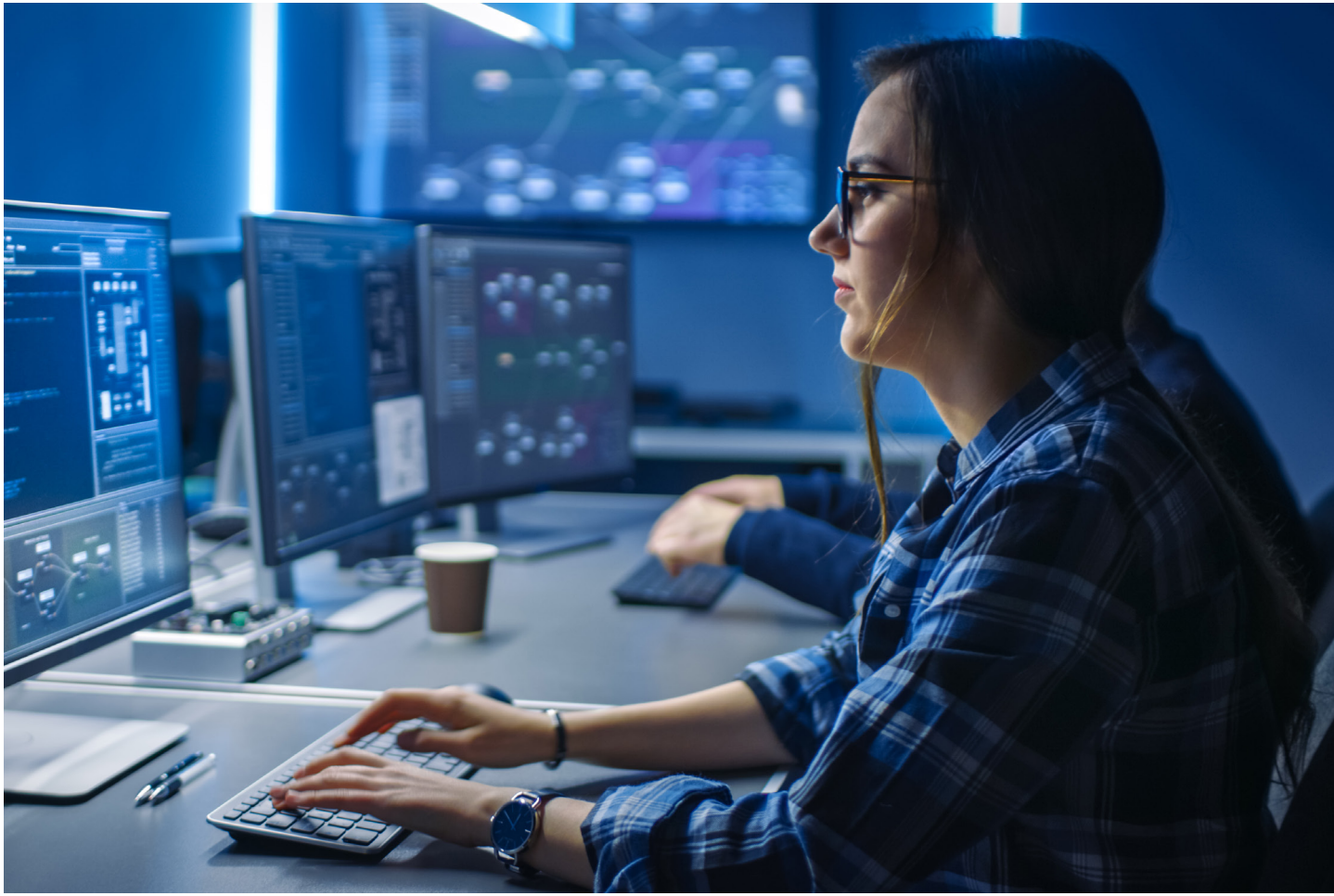
Le organizzazioni classificate come Entità Essenziali possono aspettarsi di essere soggette a supervisione in sede e fuori sede, compresi controlli a campione. Inoltre, audit annuali e mirati, basati sui risultati della valutazione del rischio o sulle informazioni disponibili relative al rischio.

Ai sensi della direttiva NIS2, le autorità hanno il potere di ritenere il management personalmente responsabile in caso di comprovata negligenza grave dopo un incidente informatico. Per quanto concerne le entità Essenziali, le autorità sono autorizzate sospendere temporaneamente una persona dal ricoprire posizioni manageriali, in caso di negligenza ripetuta.
Capo VII - Articolo 32

Le organizzazioni classificate come Entità Importanti saranno soggette a una supervisione reattiva da parte delle autorità, a differenza della supervisione proattiva riservata alle Entità Essenziali. Ciò significa che, a meno che non vi sia una ragione specifica, come un incidente informatico o delle segnalazioni provenienti da organizzazioni esterne, quali revisori o altre parti della catena di approvvigionamento, un'Entità Importante non sarà soggetta alla supervisione diretta da parte di regolatori e autorità.
Capo VII - Articolo 33

La direttiva NIS2 estende le sanzioni fino a includere quelle basate sul fatturato globale. Queste sanzioni differiscono a seconda che le organizzazioni facciano parte di un'Entità Essenziale o di un'Entità Importante. Per quelle Essenziali, si basano su un minimo di dieci milioni di euro o sul 2% del fatturato annuo globale, a seconda di quale valore sia superiore.

Per le Entità Importanti, le sanzioni si basano su un minimo di sette milioni di euro o sull'1,4% del fatturato.
Capo VII - Articolo 34



Informazioni su Ivanti

Ivanti si impegna a elevare e proteggere l'Everywhere Work per far sì che persone e aziende possano crescere e prosperare. Mettiamo la tecnologia al servizio delle persone, non viceversa. I dipendenti di oggi utilizzano una vasta gamma di dispositivi aziendali e personali per accedere alle applicazioni e ai dati IT su più reti ed essere sempre produttivi, ovunque e comunque. Ivanti è l'unica azienda tecnologica che individua, gestisce e protegge ogni asset ed endpoint IT di un'organizzazione. Oltre 40.000 clienti, tra cui 88 delle aziende Fortune 100, hanno scelto Ivanti per aiutarle ad offrire un'eccellente esperienza digitale ai propri dipendenti e migliorare la produttività e l'efficienza dei team IT e di sicurezza. In Ivanti, ci impegniamo a creare un ambiente in cui tutte le prospettive vengano ascoltate, rispettate e valorizzate e ci impegniamo per un futuro più sostenibile per i nostri clienti, partner, dipendenti e per il pianeta. Per maggiori informazioni, visita ivanti.com

ivanti

Per maggiori informazioni, per favore visita ivanti.com.