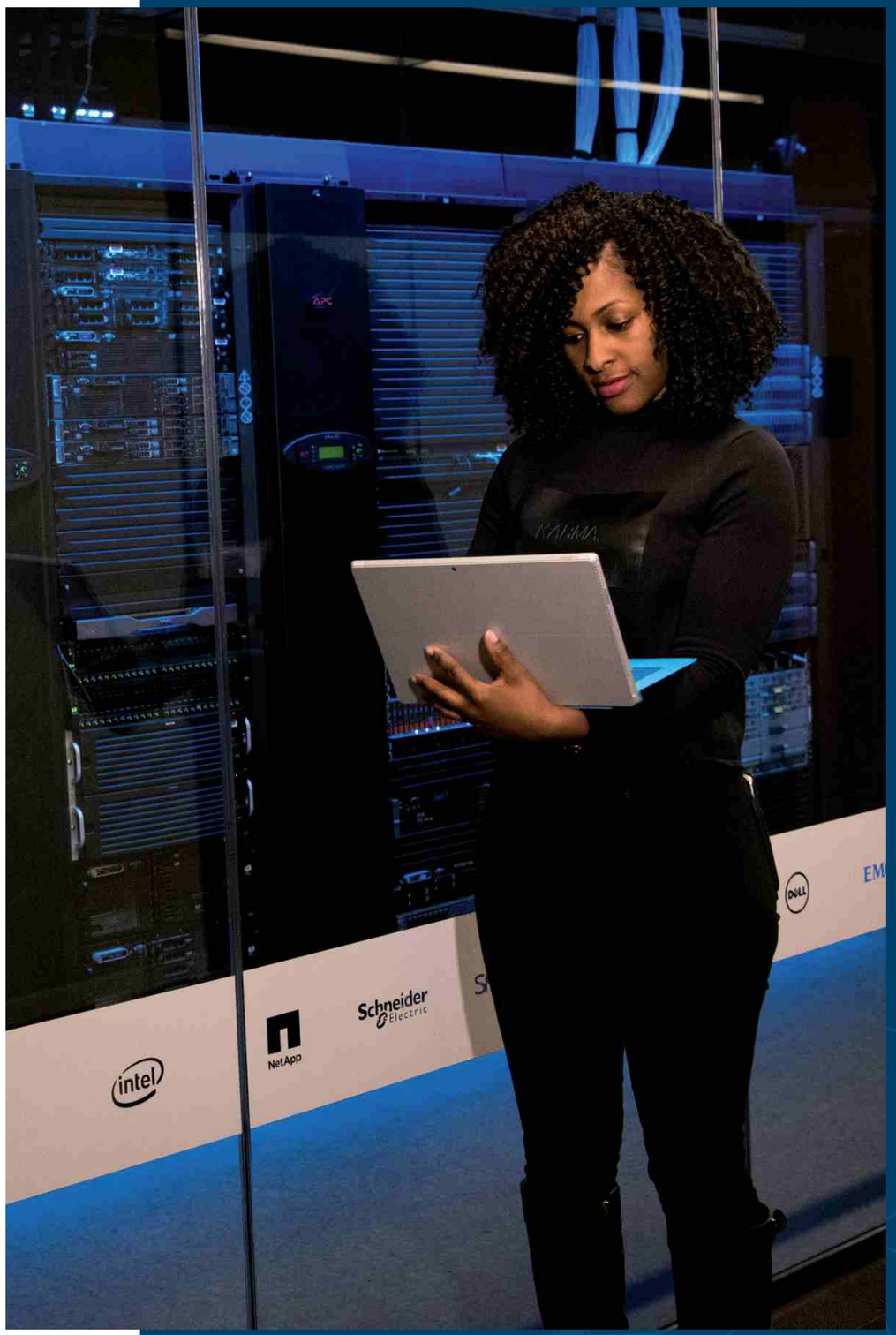
RAFFORZARE LA SICUREZZA FISICA DELLA TUA AZIENDA

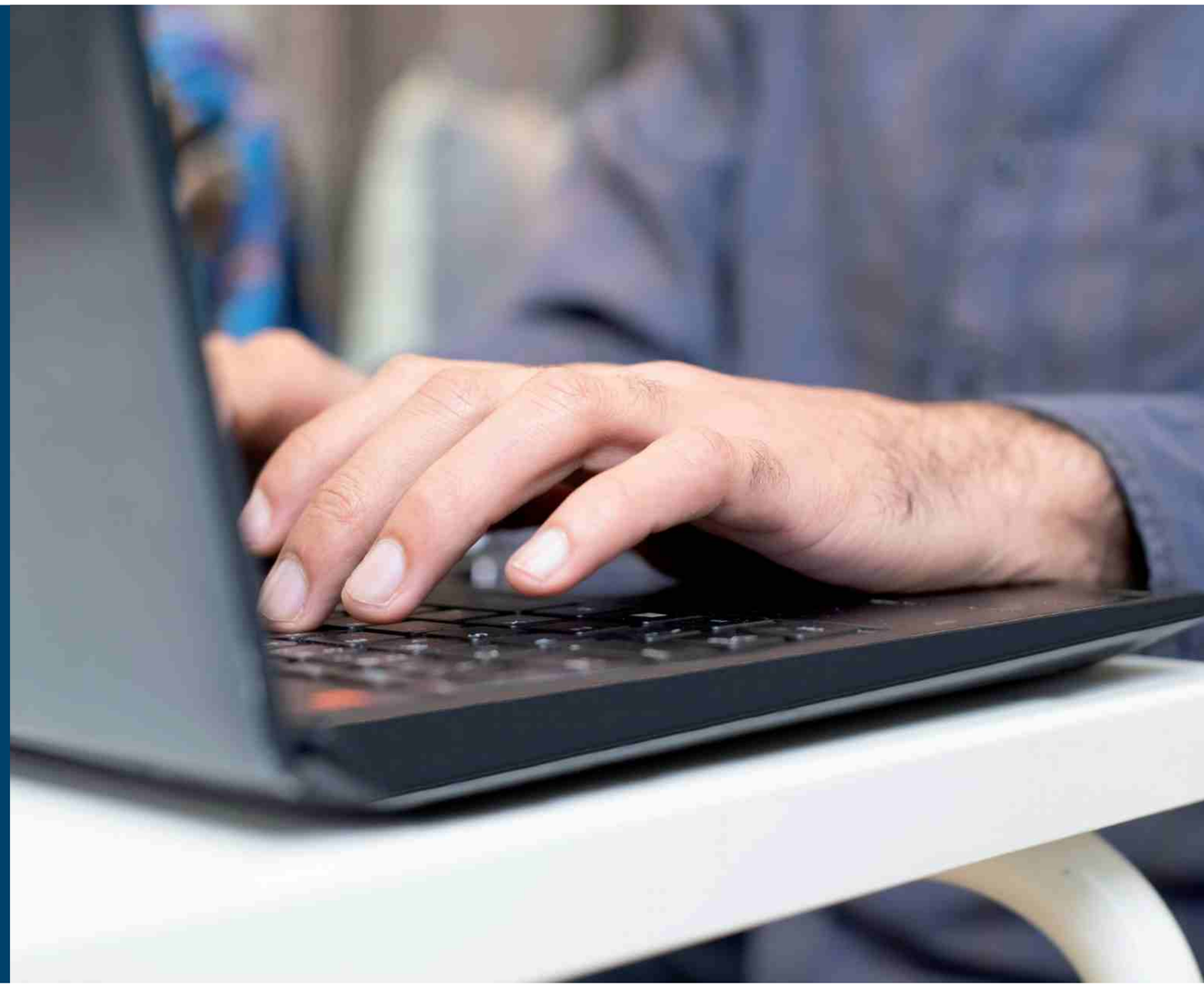


EXA SYS
IT & SYSTEM INTEGRATOR

Utilizza la nostra checklist per assicurarti di soddisfare i requisiti e migliorare la resilienza informatica.

Le aziende che operano nell'Unione europea si stanno preparando alla Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS2).
La Direttiva, già Legge in Italia dal 16 ottobre 2024 con decreto legislativo n. 138 del 4 settembre 2024, ha l'obiettivo di affrontare le sfide attuali ed emergenti per rafforzare la cybersecurity e migliorare il funzionamento del mercato interno.

Questa checklist aiuterà il tuo team a prepararsi alla Direttiva NIS2, nello specifico per quanto riguarda le soluzioni di sicurezza.
Non si tratta di un elenco esaustivo, ma ti aiuterà a capire come affrontare i rischi, gestire il tuo ecosistema di partner e segnalare eventuali incidenti.



Maggiore consapevolezza e preparazione

La Direttiva NIS2 introduce nuovi obblighi che richiedono cambiamenti in svariati ambienti di sicurezza e le aziende che non li rispettano rischiano multe salate, la perdita della propria certificazione e la responsabilità personale del senior management.

È importante che i programmi di compliance alla Direttiva NIS2 abbiano la massima priorità e coinvolgano tutti i principali stakeholder.

Priorità

- Comprendi a fondo le implicazioni della Direttiva NIS2 per la tua azienda?
- La Direttiva riceve l'attenzione e la priorità necessarie all'interno della tua azienda?
- Il consiglio di amministrazione e il top management sono consapevoli delle sanzioni previste e della propria responsabilità in caso di mancata compliance per quanto riguarda la sicurezza?
- Con la Direttiva NIS2, l'Unione europea si aspetta che la leadership assuma un ruolo attivo. Il consiglio di amministrazione e le posizioni apicali della tua azienda lo stanno facendo?

Preparazione

- Hai definito un programma di preparazione alla Direttiva NIS2 con obiettivi e tempistiche chiari?
- Il team che gestisce il programma include il direttore del dipartimento IT, i responsabili di procedure, sicurezza, strutture e compliance, i rappresentanti legali e qualsiasi altro ruolo rilevante?
- Hai verificato che i tuoi fornitori principali abbiano un programma in vista della Direttiva NIS2?

Capire dove è necessario rafforzare la sicurezza

La Direttiva NIS2 dà particolare importanza al modo in cui i beni, le persone e le aziende vengono protetti dalle minacce fisiche e di cybersecurity.

È essenziale poter contare su una tecnologia che permetta solo alle persone autorizzate di accedere in modo sicuro alle aree e alle risorse critiche. Queste domande ti aiuteranno a valutare meglio la tua posizione dal punto di vista della compliance.

Valutazione

- ☐ La tua azienda ha effettuato una valutazione dei rischi alla luce dei requisiti della Direttiva NIS2?

La valutazione ha coperto le aree seguenti?

Sedi

- ☐ Sicurezza in prossimità degli edifici
- ☐ Sicurezza nei punti di accesso agli edifici Gestione di aree critiche (come data center, camere bianche e apparecchiature)
- ☐ Gestione dei visitatori
- ☐ Procedure in caso di disastri naturali

Sistemi

- ☐ La tua tecnologia di cybersecurity è all'avanguardia o utilizzi sistemi datati?
- ☐ Disponi di tecnologie di crittografia e controllo accessi avanzate per proteggere i sistemi fondamentali?
- ☐ Il firmware viene aggiornato automaticamente?
- ☐ Il sistema di controllo accessi si integra con i sistemi di gestione degli incidenti?

Criteri

- ☐ Hai predisposto criteri e procedure aggiornati per gestire i rischi di cybersecurity?
- ☐ Le tue soluzioni di controllo accessi si basano su modelli, credenziali e ruoli utente?
- ☐ I diritti di accesso dei dipendenti vengono sempre forniti e gestiti in modo sicuro?
- ☐ Le approvazioni sono vengono gestite dai responsabili preposti?
- ☐ Dai la massima priorità alla sicurezza nella fase di offboarding dei dipendenti?
- ☐ L'accesso dato al personale autorizzato dei tuoi partner di fiducia è limitato e monitorato?

Assicurarsi di poter soddisfare gli obblighi di risposta agli incidenti

La Direttiva NIS2 è allineata con i nuovi meccanismi di supervisione e applicazione come il Centro europeo di competenza per la cibersicurezza e il Quadro dell'UE per la certificazione della cibersicurezza.

La cooperazione e il coordinamento sono temi chiave del nuovo regolamento UE, che prevede l'obbligo, per le aziende interessate, di informare le autorità competenti in merito agli incidenti di cybersecurity con un impatto significativo sulla fornitura dei servizi.

Procedure

- Hai previsto misure di risposta agli incidenti e piani di continuità aziendale aggiornati per affrontare i rischi di cybersecurity?
- Utilizzi strumenti di gestione delle decisioni per supportare la collaborazione e rispondere in modo efficace agli incidenti di cybersecurity?
- Hai predisposto procedure operative standard e persone di riferimento?

Sistemi

Se si verifica un incidente di sicurezza:

- Puoi ottenere un quadro completo dell'evento? Ad esempio, il tuo sistema di sicurezza integra il controllo accessi, la videosorveglianza e altre funzionalità di sicurezza avanzate in modo rapido ed efficiente?
- Sei in grado di identificare i prodotti o i servizi ICT interessati, la gravità della vulnerabilità e la disponibilità delle relative patch o indicazioni?
- Disponi di sistemi per la gestione degli incidenti?
- La tua infrastruttura di sicurezza si integra perfettamente con questi sistemi?

Informazioni

- Puoi contare su un metodo efficace per la gestione dei registri di controllo degli eventi?
- Disponi di strumenti per collaborare e condividere le informazioni in modo sicuro con gli le parti interessate?
- I tuoi sistemi sono in grado di notificare alle autorità competenti eventuali minacce, vulnerabilità e incidenti di cybersecurity significativi?
- Queste notifiche possono essere inviate in modo automatico?
- Se si verifica un incidente, sei in grado di rispettare le scadenze previste dalla Direttiva NIS2 e segnalare l'incidente entro 24 ore, 72 ore e 30 giorni dalla sua scoperta?
- I tuoi metodi di segnalazione sono allineati con il database stabilito dall'Unione europea?
- I tuoi addetti alla risposta agli incidenti informatici hanno un referente presso le autorità competenti?
- È semplice fornire informazioni accurate sulla natura e sulla gravità degli incidenti?
- Puoi fornire dettagli sul numero di utenti interessati?
- Saresti in grado di fornire una prova delle tue misure di mitigazione?

Garantire un approccio condiviso alla sicurezza con i propri partner

La sicurezza di un'azienda può essere compromessa dalla vulnerabilità dei partner commerciali.

Di conseguenza, la Direttiva NIS2 richiede alle aziende di garantire la sicurezza della propria supply chain implementando misure che includono la due diligence e gli accordi contrattuali con i fornitori.

Contratti

- Hai previsto misure per garantire la sicurezza di strutture, persone e dati associati ai servizi esternalizzati?
- Hai stabilito accordi contrattuali e di due diligence con i tuoi fornitori di servizi in materia di sicurezza?

Fornitori

- I tuoi fornitori offrono hardware e software sicuri e affidabili, sia on-premise che sul cloud?
- Le loro soluzioni sono sviluppate con sistemi avanzati di autenticazione e crittografia?
- Sono a conoscenza della Direttiva NIS2 e delle sue implicazioni?
- Implementano una propria strategia per identificare e colmare lacune e vulnerabilità della sicurezza?
- Aderiscono agli standard per la sicurezza, come ISO 27001?
- I loro addetti dichiarano apertamente le vulnerabilità note e le correzioni per rimediare in tempi brevi?
- I fornitori mantengono rigorosamente aggiornata la propria sicurezza?

Raggiungere gli obiettivi NIS2 in modo tempestivo

Ogni azienda deve prepararsi in modo efficace alla Direttiva NIS2 per prevenire problemi di sicurezza e gravi conseguenze. Valutare in anticipo le esigenze, le spese e la formazione ti permetterà di alleggerire la pressione in futuro e di raggiungere i tuoi obiettivi. Un modello di sicurezza software multilivello può aiutarti a ridurre i rischi e a favorire la compliance in materia di sicurezza.

Il nuovo regolamento UE andrebbe anche considerato nel contesto più ampio della tua strategia di sicurezza. Sebbene soddisfare i requisiti della Direttiva sia importante, ampliare ulteriormente i tuoi sistemi in un'ottica lungimirante potrebbe offrire molto più valore e aumentarne radicalmente l'efficienza. Potresti ottenere risparmi significativi e dati importanti, oltre a scoprire metodi lavorativi migliori e in grado di rafforzare la tua azienda e il suo ecosistema.

Passaggi fondamentali per il tuo progetto di compliance alla Direttiva NIS2

Alla luce delle domande che abbiamo posto finora:

- Sei in grado di rispettare le tempistiche che hai previsto per i tuoi obiettivi di preparazione alla Direttiva NIS2?
- Tutte le parti interessate sono informate e stanno svolgendo il proprio ruolo?
- Disponi di un meccanismo di reporting affidabile per tenere tutti aggiornati?
- Hai bisogno di soluzioni di sicurezza fisiche aggiuntive, che potrebbero prevedere recinzioni e illuminazione automatica, oltre a telecamere di sorveglianza, rilevatori di movimento e sistemi di controllo accessi?
- Dovresti forse prendere in considerazione l'aggiunta di soluzioni all'avanguardia per integrare la sicurezza, rispondere meglio agli eventi e generare rapidamente rapporti?
- Devi rivedere i criteri di sicurezza o collaborare più strettamente con i fornitori?
- Hai a disposizione un budget adeguato per gli investimenti necessari a soddisfare gli obblighi della Direttiva NIS2 in termini di tecnologia, servizi e formazione? Hai bisogno di costruire un business case?

EXA SYS
IT & SYSTEM INTEGRATOR

ULTERIORI INFORMAZIONI

VISITA OGGI STESSO IL NOSTRO SITO EXASYS.IT PER SAPERNE DI PIÙ SUL NOSTRO APPROCCIO ALLA CYBERSECURITY NELL'ERA DELLA DIRETTIVA NIS2 E OLTRE.

ISO 9001 2015 CERTIFIED
EXASYS SERVICE S.r.l.
P.Iva: 08844400724
www.exasys.it
info@exasys.it
S.S. 96 KM. 118+0,50
70026 - Modugno (BA)
+39 080 2148012
ISO 27001:2022 CERTIFIED