CYBERSICUREZZA & NIS2

L’effetto domino della NIS2: adeguarsi per restare nel mercato.

26 giugno 2025

CORSO DI FORMAZIONE

Nell’incontro di oggi verranno trattati i seguenti temi:

- Universalità dei principi della Direttiva NIS2
- Focus sulla Direttiva NIS2 e sulla sua importanza strategica
- L’adeguamento proattivo ai principi della NIS2 non è solo raccomandato, ma è una necessità urgente per le aziende
- Pressione sulla Supply Chain
- Rischi di esclusione dal mercato
- Miglioramento della resilienza e della sicurezza complessiva

LA CYBERSICUREZZA (O CYBERSECURITY)

La cybersicurezza è l'insieme delle azioni che si devono mettere in pratica per proteggere i computer, le reti, i programmi e in generale **tutti i dispositivi connessi a internet** che utilizziamo in ufficio o a casa, dagli attacchi informatici.

LA CYBERSICUREZZA: DISPOSITIVI

Quando si parla di dispositivi si intendono oggetti che hanno una parte elettronica, un programma che li fa funzionare e sono connessi ad internet. Per questo non ci si riferisce solo ai computer fissi, portatili o ai tablet che usiamo per lavorare ma anche, e specialmente, alle smart TV, agli smartphone, agli elettrodomestici che si connettono a internet, ai sistemi di allarme, alle consolle per i videogiochi e a tutti gli altri apparecchi "intelligenti" che fanno parte della nostra vita quotidiana.

Gli attacchi informatici hanno lo scopo di entrare nei nostri dispositivi per entrare nella rete e rubare o sottrarre informazioni importanti, bloccarne il normale funzionamento oppure paralizzare l'azienda per creare un danno economico e richiedere un riscatto.

È quindi fondamentale fare attenzione e seguire le indicazioni per proteggere al meglio tutti i nostri dispositivi e le informazioni che contengono.

UNIVERSALITÀ DEI PRINCIPI DELLA DIRETTIVA NIS2

COSA PROTEGGE LA NIS2: I DATI AZIENDALI

Un’azienda non è fatta solo di persone, muri, scrivanie o macchinari, ma di un tessuto connettivo molto più intimo e potente: i suoi dati.

Pensiamo ai clienti: ogni nome che compare nei vostri archivi, ogni preferenza espressa, ogni singolo acquisto che hanno effettuato, non è un semplice dato. È un frammento di una relazione che è stata costruita con cura, un segno di fiducia che è stato accordato alla vostra impresa.
Questi dati non sono semplici numeri in un database, sono la voce dei clienti, il significato delle loro scelte e della loro fedeltà.

Pensiamo alle idee più brillanti, alle intuizioni che hanno portato l’azienda a dove siete oggi: le formule innovative che distinguono dalla concorrenza, i segreti che rappresentano l’unicità. Questi dati sono l'essenza più profonda dell’identità aziendale, il risultato tangibile di anni di impegno, di tentativi, di lavoro, di pura passione.

Consideriamo ora i bilanci, le proiezioni tracciate per il futuro, i numeri che raccontano la storia della crescita, le sfide superate, i successi che sono stati celebrati.
Questi dati sono come fotografie impresse nella memoria della vostra azienda, la testimonianza tangibile del lavoro, la promessa concreta di ciò che si potrà ancora creare ed ottenere.

COSA INTENDIAMO PER DATI AZIENDALI

Quando si parla di tesoro aziendale, a cosa ci si riferisce concretamente? Quali sono questi dati così preziosi che devono essere protetti? Ecco alcuni esempi:

- **Dati relativi ai clienti:**
  - Informazioni di contatto e demografiche (nomi, indirizzi email, numeri di telefono, età, posizione geografica)
  - Preferenze e interessi (desideri, bisogni espressi, feedback)
  - Storico degli acquisti e delle interazioni (prodotti/servizi acquistati, date, frequenza, canali di contatto)
- **Dati Operativi:**
  - Dati relativi alla produzione e all'inventario (livelli di stock, movimentazioni, previsioni)
  - Dati di logistica e spedizione (tempi di consegna, costi di trasporto)
- **Dati Finanziari:**
  - Registri contabili (entrate, uscite, profitti e perdite)
  - Dati di budget e previsioni finanziarie
- **Dati di Marketing e Vendite:**
  - Dati delle campagne di marketing (ROI)
  - Dati sulle vendite (volumi, valori, margini) e sul comportamento online (visite al sito web, social media)
- **Dati di Ricerca e Sviluppo:**
  - Risultati di test e sperimentazioni e dati relativi a nuovi prodotti o servizi in fase di sviluppo
  - Dati provenienti da ricerche di mercato o dalla Business Intelligence interna
- **Dati di Fornitori:**
  - Informazioni relative ai fornitori e alle loro performance
  - Dati relativi alla catena di fornitura (supply chain).

PERCHÉ PROTEGGERE I DATI

Con la crescita della digitalizzazione, la cybersecurity ha assunto un ruolo fondamentale per la sicurezza di individui e organizzazioni, proteggendoli delle minacce informatiche.

La protezione dei dati aziendali e personali è essenziale per:

- **proteggere le informazioni**: prevenire l'accesso non autorizzato a dati aziendali (dati relativi a clienti, fornitori, contratti ecc.) o personali (ad esempio dati biometrici, dati relativi alla salute, alla posizione, al comportamento online o sensibili come la fede religiosa, l'appartenenza sindacale, le opinioni politiche, l'origine, o di orientamento sessuale);
- **assicurare la continuità operativa aziendale**: garantire che i servizi e le operazioni aziendali non siano interrotti da attacchi informatici. Il blocco dei sistemi può creare danni operativi come la disabilitazione dei servizi web di siti B2B e B2C o di tipo logistico con ritardi nell'evasione degli ordini e possibili cancellazioni degli stessi, ecc.;
- **evitare perdite finanziarie**: prevenire frodi e furti dovuti ad attacchi informatici. Le comunicazioni con clienti e fornitori possono essere falsate creando pagamenti verso soggetti estranei all'ecosistema aziendale;
- **mantenere la fiducia dei clienti nell'impresa**: quando un'azienda subisce un attacco informatico, la sua immagine pubblica viene danneggiata seriamente, vengono sollevati dubbi sulla sicurezza dei dati affidatigli dai clienti e di conseguenza la reputazione del suo marchio (brand awareness) viene minata.

GRUPPO DI LAVORO MULTIDISCIPLINARE

Se abbiamo compreso il valore intrinseco dei dati, allora diventa chiaro che la loro protezione non può essere relegata a un singolo reparto. Tutti i reparti dovranno partecipare a questo obiettivo.

La cybersicurezza è un filo conduttore che lega indissolubilmente diversi settori aziendali. Le risorse umane giocano un ruolo cruciale nella creazione di una cultura della sicurezza tra i dipendenti, il responsabile privacy è il garante della corretta gestione dei dati sensibili, e la Direzione deve essere il motore di questa consapevolezza, integrando la sicurezza informatica nelle strategie aziendali. **Per questo si parla di gruppo di lavoro multidisciplinare**.

Proviamo a immaginare la nostra azienda come un corpo umano.

Il reparto informatico (IT) rappresenta il sistema nervoso, fondamentale per la comunicazione e la difesa. Ma se il sistema immunitario (la direzione del personale, che lo forma e lo sensibilizza), la pelle (privacy che definisce i confini e le regole) e il cervello (la direzione che prende decisioni strategiche) non lavorano in sinergia, l'intero organismo è vulnerabile.

CARDINI DELLA SOCIETÀ E NON SOLO MERO OBBLIGO NORMATIVO

L’obiettivo di oggi è esplorare insieme come i principi cardine della NIS2 non siano solo un mero obbligo normativo, bensì una vera e propria bussola strategica, indispensabile per chiunque operi, a qualsiasi livello, nel mondo digitale odierno.

Basti pensare a come la nostra vita, personale e professionale, sia permeata dal digitale: dalle infrastrutture critiche che garantiscono energia e trasporti nelle nostre città, ai servizi essenziali come quelli sanitari, bancari e finanziari, fino ai servizi digitali che utilizziamo quotidianamente senza quasi farci caso. Parliamo dell'home banking per gestire le nostre finanze, degli acquisti tramite ecommerce o delle chat/videochiamate che ci tengono costantemente connessi con colleghi, amici e familiari.

Ogni aspetto, ogni settore, è ormai profondamente interconnesso in una rete globale.

OPPORTUNITÀ STRAORDINARIE

Questa interconnessione se da un lato ci offre opportunità straordinarie e ha rivoluzionato il nostro modo di vivere e lavorare, dall'altro ci espone a un panorama di minacce cibernetiche in continua evoluzione: sempre più complesse, sofisticate e purtroppo, persistenti.
Non parliamo più solo di singoli attacchi isolati, ma di vere e proprie campagne mirate che possono paralizzare interi settori vitali, causare danni economici ingenti e, non ultimo, compromettere la fiducia nelle istituzioni e nelle aziende.

RESILIENZA CYBER

Proprio in questo scenario, in questa "tempesta perfetta" digitale, si inserisce la **Direttiva NIS2**.

Nata dalla pressante esigenza di rafforzare e armonizzare la **resilienza cyber** a livello dell'Unione Europea, NIS2 espande significativamente l'ambito di applicazione rispetto alla sua predecessora, introduce requisiti di sicurezza molto più stringenti e, fondamentale, rafforza la **cooperazione** tra gli Stati membri.

Ma il suo vero potere, la sua vera "rivoluzione", risiede nell'aver codificato una serie di **principi universali di cybersicurezza**.
Parliamo di concetti come la **gestione del rischio**, la **notifica tempestiva degli incidenti**, la **sicurezza delle forniture** e una **cooperazione** profonda a tutti i livelli. Questi principi, cari partecipanti, trascendono il singolo settore o la dimensione specifica dell'organizzazione. Sono le fondamenta robuste su cui dobbiamo costruire una difesa cyber efficace, sia che siate un'azienda multinazionale, una piccola e media impresa dinamica, o un'infrastruttura critica essenziale per il nostro Paese.

INVESTIMENTO STRATEGICO

Oggi, dunque, scopriremo insieme come l'adozione consapevole e proattiva di questi principi non sia semplicemente una questione di conformità normativa, ma un investimento strategico irrinunciabile.

Un investimento per garantire la continuità operativa, per proteggere la reputazione delle nostre aziende e, in ultima analisi, per salvaguardare la sicurezza e la prosperità del nostro futuro digitale.

FOCUS SULLA DIRETTIVA NIS2 E LA SUA IMPORTANZA STRATEGICA

DECRETO LEGISLATIVO N. 138 DEL 4 SETTEMBRE 2024: DIRETTIVA NIS2

La Direttiva (UE) 2022/2555, nota come **Direttiva NIS2**, è stata recepita nell'ordinamento giuridico italiano attraverso il **Decreto Legislativo 4 settembre 2024, n. 138.**

Questo decreto è stato pubblicato nella Gazzetta Ufficiale n. 230 del 1° ottobre 2024 ed è entrato in vigore il **16 ottobre 2024.**
Si chiama Direttiva NIS2 (Network and Information Systems) perché segue la Direttiva NIS del 6 luglio 2016.

La NIS si concentrava principalmente sugli operatori di Servizi Essenziali (OSE) in settori specifici come energia, trasporti, sanità, infrastrutture digitali e fornitori di servizi digitali (come motori di ricerca, servizi cloud e mercati online).
La NIS2 invece espande significativamente il suo raggio d'azione, introducendo la distinzione tra Entità Essenziali ed Entità Importanti, include un numero maggiore di settori, come la pubblica amministrazione, lo spazio, la produzione di beni critici, la gestione dei rifiuti, la produzione alimentare e molti altri. Di conseguenza, abbassa le soglie dimensionali, includendo molte più medie e grandi imprese.

OBIETTIVO DELLA DIRETTIVA NIS2

L'obiettivo principale della Direttiva NIS2 è stabilire un livello elevato e comune di sicurezza in tutta l'Unione Europea, rafforzando la resilienza cibernetica delle aziende e degli Stati membri, armonizzando le normative tra i paesi e ampliando la portata della protezione a un numero maggiore di settori e imprese.

Si vuole migliorare la gestione del rischio digitale attraverso:

- un approccio proattivo
- rafforzando la sicurezza della catena di fornitura
- aumentando la responsabilità del management in materia di cybersecurity (la NIS2 introduce un elemento significativo riguardante la **responsabilità del management** all'interno delle entità essenziali e importanti. Questo significa che le persone che ricoprono ruoli di **alta dirigenza** hanno un ruolo attivo e diretto nel garantire l'applicazione di regole di cybersecurity all'interno della loro azienda)
- migliorando la segnalazione degli incidenti con procedure più chiare e tempestive
- promuovendo la cooperazione e la condivisione di informazioni tra gli Stati membri e le autorità competenti.

L'intento finale è quello di creare un ecosistema digitale più sicuro e resiliente per proteggere infrastrutture critiche, servizi essenziali e la società nella quale viviamo, dalle crescenti minacce cibernetiche.

SOGGETTI ESSENZIALI E IMPORTANTI (Allegato I e II)

I soggetti Essenziali comprendono settori che, se compromessi, avrebbero un impatto grave sulla sicurezza e sull'economia dello Stato:

- Energia (aziende e utility operanti nella generazione, distribuzione e fornitura di energia, incluse le reti elettriche intelligenti)
- Trasporti (infrastrutture ferroviarie, aeree, marittime e stradali)
- Banca e finanza
- Pubblica Amministrazione (enti governativi e istituzioni pubbliche che gestiscono dati sensibili)
- Sanità: ospedali, fornitori di servizi sanitari e aziende farmaceutiche
- Tecnologie spaziali (attività legate all'osservazione della Terra, alle telecomunicazioni satellitari e alla navigazione globale)
- Fornitura e distribuzione di acqua
- Infrastrutture digitali (ad es. fornitori di servizi di cloud computing e gestione ICT).

SOGGETTI ESSENZIALI E IMPORTANTI (Allegato I e II)

I soggetti Importanti sono le organizzazioni che, pur non essendo considerate "essenziali" (che operano nei settori più critici con un impatto potenzialmente più grave in caso di incidente), svolgono comunque un ruolo significativo e potrebbero causare interruzioni significative a causa di incidenti di cibersicurezza.
Questi i settori:

- Servizi Postali
- Gestione Rifiuti
- Fabbricazione, produzione e distribuzione di sostanze chimiche
- Produzione, trasformazione e distribuzione di alimenti
- Fabbricazione di dispositivi medici, computer e prodotti di elettronica, apparecchiature elettrice, macchinari, autoveicoli, rimorchi e semirimorchi, altri mezzi di trasporto
- Fornitori di servizi digitali tra cui di mercati online, motori di ricerca, social network e fornitori di registrazione di nomi di dominio
- Organizzazioni di ricerca

SANZIONI PREVISTE DALLA DIRETTIVA NIS2

Le sanzioni previste dalla direttiva NIS2 sono concepite per essere **efficaci, proporzionate e dissuasive** al fine di garantire che le entità designate prendano seriamente i propri obblighi di cybersecurity.
Il Decreto Legislativo n. 138/2024 stabilisce un sistema sanzionatorio che distingue tra entità essenziali ed entità importanti:

1) per le **entità essenziali:**
le sanzioni amministrative pecuniarie possono arrivare **fino a 10 milioni di euro o al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, a seconda di quale sia l'importo maggiore.

2) per le **entità Importanti:**
le sanzioni amministrative pecuniarie possono arrivare **fino a 7 milioni di euro o all'1,4% del fatturato mondiale totale annuo** dell'esercizio precedente, a seconda di quale sia l'importo maggiore.

Oltre alle sanzioni pecuniarie, la normativa prevede anche **sanzioni accessorie** che possono colpire direttamente l'Organo di Gestione delle organizzazioni inadempienti. L'ACN può disporre nei confronti delle persone fisiche responsabili (come amministratori e dirigenti) la **sospensione temporanea dall'esercizio delle funzioni dirigenziali** fino a quando l'azienda non adotta le misure necessarie per adeguarsi alla normativa.
Gli organi di vigilanza possono anche arrivare alla **rimozione dei dirigenti e manager ritenuti negligenti**.

RESPONSABILITÀ DELL'ORGANO DI GESTIONE AZIENDALE

Con la NIS2 la responsabilità della cybersecurity sale ai piani alti dell'azienda (art. 20 - Governance).

L'Organo di Gestione oltre ad assicurarsi che ci siano delle difese, diventa il garante che queste difese funzionino davvero e che l'azienda rispetti sempre le regole.
L'obiettivo della direttiva è far nascere una mentalità e una coscienza forte sui temi di cybersicurezza in tutta l'organizzazione, partendo dai responsabili, per creare consapevolezza sul tema.

OBBLIGHI CHIAVE

La Direttiva NIS2 impone una serie di obblighi chiave volti a migliorare la postura di cibersicurezza:

a) Responsabilità della Direzione
La direttiva impone una responsabilità diretta per gli organi di gestione (articolo 20). I leader aziendali devono approvare le misure di gestione del rischio di cibersicurezza e supervisionarne l'attuazione. Non è più solo una questione IT, ma una **questione di governance aziendale**.

Ecco cosa prevede l'articolo 20 della Direttiva NIS2:

1. gli organi di gestione delle entità essenziali e importanti devono approvare le misure di gestione dei rischi legati alla sicurezza dei sistemi informatici
2. devono supervisionare l'attuazione di tali misure.
3. sono tenuti a partecipare a programmi di formazione per acquisire conoscenze e competenze adeguate in materia di cybersecurity.
4. la responsabilità non è più delegabile: i dirigenti devono assumersi direttamente la responsabilità della sicurezza informatica dell'organizzazione.

OBBLIGHI CHIAVE

b) Misure di gestione del rischio
Non si tratta solo di avere un firewall o un antivirus non aggiornato. Le aziende dovranno implementare misure tecniche e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi di rete e informativi. Questo include la valutazione dei rischi, la gestione degli incidenti, la continuità operativa e la sicurezza della catena di fornitura.

c) Notifica degli Incidenti: In caso di un incidente di cibersicurezza significativo, ci sono requisiti rigorosi per la notifica alle autorità competenti entro scadenze specifiche. La rapidità e la trasparenza sono cruciali. Secondo l'articolo 23 della Direttiva NIS2, i soggetti essenziali e importanti sono obbligati a notificare al CSIRT (Computer Security Incident Response Team) nazionale qualsiasi incidente che abbia un impatto significativo sulla fornitura dei servizi.
I termini di notifica sono:

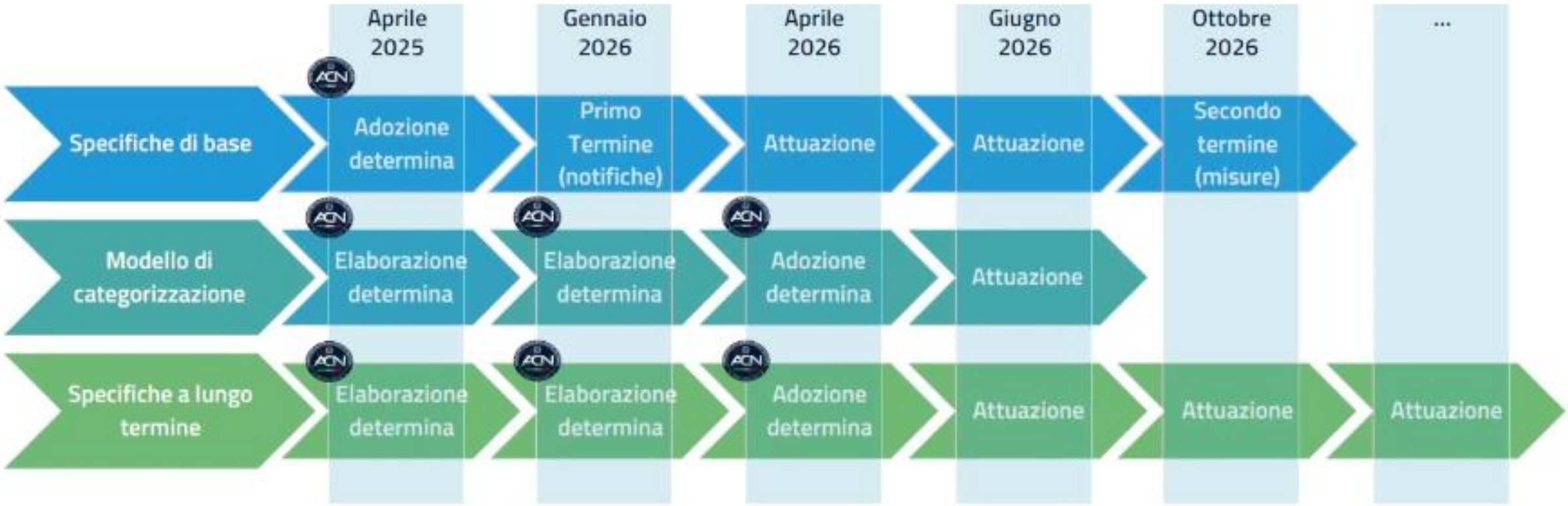
1. notifica preliminare (preallarme): entro 24 ore dalla conoscenza dell'incidente
2. notifica completa: entro 72 ore
3. relazione finale: entro 1 mese dalla notifica completa, con dettagli su cause, impatti e misure correttive adottate.

OBBLIGHI CHIAVE

d) Sicurezza della catena di fornitura
Le vulnerabilità nella catena di fornitura possono essere una porta d'ingresso per gli attaccanti. La NIS2 richiede che le organizzazioni considerino la cibersicurezza dei loro fornitori e subappaltatori.

La Direttiva NIS2 impone a tutte le entità classificate come essenziali o importanti di adottare un approccio sistemico alla gestione del rischio, che includa anche la catena di fornitura. Questo significa che la sicurezza informatica non può fermarsi ai confini dell’organizzazione, ma deve estendersi anche ai fornitori diretti e indiretti.

DIRETTIVA NIS2: PROSSIME SCADENZE



NIS2 E SUPPLY CHAIN

LA NIS2 IMPONE DI INDIVIDUARE I FORNITORI CRITICI

In ottica di sicurezza della catena di fornitura, la Direttiva NIS2 impone di:

1. Individuare i fornitori critici: ad esempio, chi fornisce servizi di hosting, software o gestione TIC, ma anche fornitori di prodotti che, se compromessi, possono introdurre vulnerabilità nella catena di approvvigionamento digitale
2. Qualificarli in modo strutturato attraverso due diligence documentale, questionari di valutazione e audit
3. Valutare il rischio associato perché ogni fornitore deve essere analizzato in base alla sua esposizione al rischio e alla sua capacità di garantire continuità e sicurezza
4. Integrare sicurezza e privacy in quanto la NIS2 si intreccia con il GDPR, richiedendo che i fornitori offrano “garanzie sufficienti” per proteggere i dati personali.

AMPLIFICAZIONE DEL PERIMETRO DI APPLICAZIONE

Le aziende soggette alla «NIS2» dovranno amplificare il perimetro di applicazione di sicurezza attraverso quella che viene definita «Responsabilità a Cascata». Questa attività identifica il cuore della pressione.

Queste aziende sono legalmente responsabili di valutare e gestire i rischi cyber associati ai loro fornitori e prestatori di servizi diretti.

NON è sufficiente un disclaimer contrattuale.

Le organizzazioni devono implementare solidi processi per valutare il rischio cyber dei loro fornitori. Questo include l'identificazione dei fornitori critici, l'analisi delle loro pratiche di sicurezza e l'identificazione di punti deboli.

Esempi: questionari di sicurezza, audit regolari, certificazioni richieste, monitoraggio continuo della postura di sicurezza di ogni fornitore.

OBBLIGHI CONTRATTUALI RAFFORZATI

I contratti con i fornitori includeranno clausole specifiche relative alla cybersecurity, come standard di sicurezza, protocolli di risposta agli incidenti, tempistiche di notifica delle violazioni e il diritto di audit.

Ricordiamo che la NIS2 prevede sanzioni significative per la non conformità (fino a 10 milioni di euro o il 2% del fatturato globale annuo per le entità essenziali, e 7 milioni di euro o l'1.4% per le entità importanti) e introduce la responsabilità personale per l'alta dirigenza (management) in caso di mancato rispetto degli obblighi di cybersecurity. Questo aumenta la pressione a livello esecutivo per garantire la conformità della supply chain.

SFIDE PER LE AZIENDE FORNITRICI DI SOGGETTI NIS2

La sfida si manifesterà attraverso diverse leve che i clienti soggetti NIS2 utilizzeranno per garantire la conformità della loro supply chain:

- Richieste di valutazione e audit:

1. I fornitori riceveranno domande sempre più specifiche e approfondite sulle loro misure di sicurezza, politiche, processi e controlli (**questionari di sicurezza dettagliati**)
2. I clienti potranno richiedere il diritto di effettuare audit di sicurezza direttamente presso le sedi dei fornitori o sui loro sistemi, per verificare l'effettiva implementazione delle misure dichiarate.
3. sarà sempre più comune che i clienti richiedano certificazioni riconosciute (es. ISO 27001, SOC 2 Type 2) come prova della maturità della sicurezza.
4. potrebbero essere richiesti report di test di sicurezza esterni o l'autorizzazione a condurne sui sistemi del fornitore.

SFIDE PER LE AZIENDE FORNITRICI DI SOGGETTI NIS2

- Revisione e rafforzamento dei vincoli contrattuali:

1. I nuovi contratti (e spesso anche quelli esistenti in fase di rinnovo) includeranno clausole stringenti che specificano standard di sicurezza minimi, requisiti di notifica degli incidenti, responsabilità in caso di violazione, e obblighi di collaborazione
2. I contratti rifletteranno la necessità per il fornitore di garantire che anche i *suoi* sub-fornitori siano allineati ai requisiti di sicurezza
3. L'inadempienza alle clausole di sicurezza potrebbe comportare penali contrattuali significative o la risoluzione del rapporto

- Obblighi di notifica degli incidenti:

1. I fornitori dovranno essere in grado di identificare e notificare incidenti di sicurezza ai loro clienti entro tempistiche molto strette, spesso in linea con gli obblighi di notifica NIS2 del cliente (es. 24/72 ore).
2. La notifica non sarà più generica, ma dovrà includere dettagli specifici sull'incidente, l'impatto potenziale e le misure correttive adottate.

SFIDE PER LE AZIENDE FORNITRICI DI SOGGETTI NIS2

- Investimenti necessari in sicurezza:

1. i fornitori devono investire in nuove tecnologie di sicurezza
2. è indispensabile formare il personale sulle best practice di cybersecurity e, in molti casi, assumere o consultare esperti di sicurezza
3. è necessario documentare e implementare processi chiari per la gestione degli incidenti, la gestione delle vulnerabilità, la continuità operativa, ecc.

RISCHI DI ESCLUSIONE DAL MERCATO

ESCLUSIONE DAL MERCATO

Anche se non direttamente sanzionabile dalla NIS2, le aziende che non si allineano agli standard di sicurezza richiesti dai loro clienti soggetti alla direttiva, rischiano di fatto un'**esclusione dal mercato.**
Potrebbero perdere contratti, reputazione e opportunità a causa dell'estensione della responsabilità e della maggiore attenzione alla sicurezza della supply chain da parte delle entità direttamente impattate dalla NIS2.

RISCHI PER LE AZIENDE NON SOGGETTE NIS2

Ecco i principali rischi di esclusione dal mercato per le aziende non NIS2 ma clienti di aziende soggette alla NIS2, se non si allineano:

1. Supply Chain Risk e quindi esclusione dalla catena di fornitura:

1. Le aziende soggette alla NIS2 dovranno assicurarsi che i loro partner, non direttamente rientranti nel perimetro NIS2, abbiano un livello adeguato di sicurezza informatica.
2. Per mitigare i propri rischi, le aziende soggette alla NIS2 includeranno probabilmente clausole contrattuali stringenti che richiederanno ai loro fornitori e clienti di dimostrare un certo livello di conformità o di adottare misure di sicurezza specifiche. Le aziende che non saranno in grado di soddisfare tali requisiti potrebbero essere escluse dai contratti esistenti o future opportunità commerciali.
3. Le aziende NIS2 dovranno condurre valutazioni più approfondite dei loro fornitori e clienti per assicurarsi che non introducano vulnerabilità nella loro catena di approvvigionamento. Questo potrebbe portare all'esclusione di partner che non dimostrano una robusta postura di cybersecurity.

RISCHI PER LE AZIENDE NON SOGGETTE NIS2

2. Vulnerabilità agli attacchi informatici e conseguenti impatti economici:

1. Le aziende non conformi alla NIS2 potrebbero essere anelli deboli nella catena di fornitura, rendendo l'intera rete vulnerabile ad attacchi. Se un attacco riesce a compromettere un fornitore non conforme, potrebbe poi propagarsi all'azienda NIS2, causando interruzioni operative, perdita di dati e danni finanziari significativi
2. Anche se non direttamente sanzionate dalla NIS2, le aziende non conformi che subiscono un attacco informatico possono affrontare costi elevati per il ripristino dei sistemi, la gestione degli incidenti, le indagini forensi e la possibile perdita di dati sensibili. Questi costi possono essere devastanti per le PMII

3. Mancanza di opportunità di business:

1. Molte aziende essenziali e importanti richiederanno, in maniera esplicita o implicita, che i loro partner adottino standard di sicurezza elevati. Non essere allineati alla NIS2 potrebbe significare la perdita di opportunità di collaborazione con attori chiave del mercato.
2. Le aziende che proattivamente adottano misure di sicurezza in linea con i principi della NIS2, anche se non direttamente soggette, possono ottenere un vantaggio competitivo, presentandosi come partner più affidabili e sicuri.

BENEFICI

Le aziende che trattano i dati in modo sicuro, attendendosi al framework consigliato dall'ACN, potranno:

- Proporsi a nuovi clienti (strutturati e importanti)
- Partecipare alle gare pubbliche nazionali e regionali
- Comunicare ai propri clienti di essere allineati con la direttiva

MIGLIORAMENTO DELLA RESILIENZA E DELLA SICUREZZA COMPLESSIVA

COME MIGLIORARSI DAL PUNTO DI VISTA DELLA SICUREZZA

Le aziende non soggette direttamente alla NIS2, ma che interagiscono con entità NIS2, dovrebbero considerare i seguenti passi:

a) **Confrontare le proprie pratiche di sicurezza** attuali con i requisiti impliciti o espliciti dei clienti NIS2, individuando le aree di miglioramento (**Gap Analysis)**
b) **Implementare framework di sicurezza riconosciuti** (adattamento nazionale del NIST CSF) che possano dimostrare un impegno verso la cybersecurity.
c) **Identificare** quali servizi e dati scambiano con i clienti NIS2 e quali rischi di cybersecurity sono associati a queste interazioni.
d) **Il fattore umano è spesso l'anello debole**. Formare regolarmente i dipendenti sulle best practice di sicurezza informatica è fondamentale.
e) **Sviluppare e testare piani dettagliati** su come gestire un incidente di sicurezza, dalla rilevazione alla ripristino, inclusa la comunicazione con i clienti.
f) **Lavorare a stretto contatto con i clienti soggetti alla NIS2** per capire le loro aspettative e i loro requisiti di sicurezza.


RECOVER
IDENTIFY
GOVERN
NIST
Cybersecurity
Framework
RESPOND
PROTECT
DETECT

BIBLIOGRAFIA & SALUTI

SITI UTILI PER APPROFONDIRE

Di seguito alcuni URL che possono essere utili per approfondire la tematica:

ACN: https://www.acn.gov.it/portale/home

Garante Privacy: https://www.garanteprivacy.it/temi/cybersecurity

Agenzia dell'Unione Europea per la cibersicurezza: https://www.enisa.europa.eu/

BRUCE SCHNEIER

Bruce Schneier è un crittografo americano, esperto di sicurezza informatica e autore di fama mondiale. È noto per le sue osservazioni e le sue frasi incisive sulla sicurezza, la tecnologia e la società.

La sicurezza (informatica) è un processo, non un prodotto!
Bruce Schneier

La sicurezza dei dati non è qualcosa che si può semplicemente acquistare e implementare una volta per tutte. Richiede un impegno continuo, aggiornamenti costanti, monitoraggio e adattamento alle nuove minacce.

DOMANDE & RICHIESTE DI APPROFONDIMENTO

Per informazioni o chiarimenti potete scrivere a:

c.fantinuoli@vbcgroup.it

Grazie per l’Attenzione