ARITECH

ARITECH CYBERSECURITY NOVEMBRE 2025

Cybersecurity

una panoramica dinamica di strategie, processi e tecnologie

Chi siamo

La nostra visione

Con oltre mezzo secolo di competenza e passione, Aritech continua a fornire tecnologie all'avanguardia e integrate per una nuova era di prodotti che rendono il mondo un posto più sicuro.

La nostra missione

Creiamo un ecosistema di sicurezza integrato che protegge la tua azienda e si evolve per soddisfare le esigenze future. Guidati da agilità e capacità di anticipazione, combiniamo la sicurezza on-premise con funzionalità di gestione remota e una forte attenzione alla sicurezza informatica. Pronti ad affrontare qualsiasi sfida di sicurezza, sempre e ovunque. Bring it on!

Aritech e la cybersecurity

In Aritech, la cybersecurity è al centro di tutto ciò che facciamo. Integrando un'ampia gamma di prodotti del nostro portfolio, oltre a sistemi di protezione antincendio, serrature wireless e soluzioni di terze parti per il controllo degli accessi e antintrusione, offriamo maggiore efficienza, maggiore praticità e una maggiore sicurezza per persone, proprietà e beni.

Con la crescente connettività dei sistemi di sicurezza tramite reti IP a banda larga e cellulari, la necessità di una solida protezione informatica non è mai stata così elevata. Aritech si impegna a essere leader nella cybersecurity, garantendo che le nostre soluzioni offrano resilienza contro le minacce in continua evoluzione; **perché nel mondo di oggi la sicurezza è tanto robusta quanto il suo anello più debole.**

Sommario

L'importanza della cybersecurity

La cybersecurity è un panorama dinamico di strategie, processi e tecnologie che proteggono reti, sistemi informativi e dati riservati da attacchi informatici e accessi non autorizzati nel mondo digitale in continua evoluzione. La cybersecurity comprende un'ampia varietà di procedure e tattiche utilizzate per proteggere i dati protetti, comprese le informazioni di identificazione personale (PII), dai crimini informatici.

Attacchi informatici

Nell'ultimo anno, i criminali informatici hanno scatenato un'ondata di attacchi informatici non solo altamente coordinati, ma anche molto più frequenti e avanzati di quanto mai visto prima, con un costo in termini economici e di reputazione che ha avuto un impatto su tutti i tipi di aziende.

Secondo Cybersecurity Ventures, dal 2015, il costo degli attacchi informatici è continuamente cresciuto, da 3,000 miliardi di dollari fino a 6,000 miliardi nel 2021, e la previsione per il 2025 è di oltre 10,000 miliardi (Cybercrime Magazine). Ciò rappresenta poco più del 10% del PIL globale, l'equivalente della terza economia più grande del mondo!

Oggi, tutte le aziende sono consapevoli dei rischi e la cybersecurity non è più un "optional", ma un requisito imprescindibile. Qualsiasi violazione, per quanto piccola, può avere un impatto negativo sull'azienda non solo in termini di reputazione, ma anche attraverso costi aggiuntivi come:

- Interruzione dell'attività per un periodo di tempo sconosciuto, a seconda della gravità dell'attacco.
- Perdita di proprietà intellettuale o di competitività se vengono esposti dati sensibili, come progetti di ricerca e sviluppo o piani strategici.
- Spese legali se sei ritenuto responsabile del furto di dati a causa di una protezione inadeguata.
- Aumento dei costi assicurativi per migliorare la protezione dai rischi a seguito di un incidente informatico.

Enormi perdite di dati

I semplici attacchi agli endpoint diventano operazioni complesse e articolate in più fasi. Gli attacchi ransomware colpiscono sia le piccole imprese che le grandi aziende. Gli attacchi malware di cryptomining offrono ai criminali informatici un facile accesso alle reti aziendali. Sono anni di massicce fughe di dati, costosi risarcimenti per ransomware e un panorama delle minacce vasto, nuovo e complesso.

I rischi informatici aziendali di oggi

Vari tipi di attacchi

Un attacco informatico si riferisce a un'azione progettata per colpire un computer o qualsiasi elemento di un sistema informatico per modificare, distruggere o rubare dati, nonché sfruttare o danneggiare una rete.

Nel corso della sua storia, la sicurezza informatica ha dovuto adattarsi a minacce nuove e in continua evoluzione. Inizialmente, semplici precauzioni di sicurezza hanno funzionato, ma con il progressivo perfezionamento degli autori di attacchi, si è resa necessaria l'adozione di nuove tecnologie di sicurezza informatica. I pericoli informatici si sono evoluti dal phishing ad attacchi dannosi avanzati.

Gli esperti di sicurezza classificano le minacce informatiche in base alle loro caratteristiche e al danno. Tra le categorie più diffuse figurano le minacce interne, in cui i dipendenti rubano dati sensibili, e gli attacchi alla catena di approvvigionamento, che prendono di mira i punti deboli della rete. L'esposizione dei dati è una preoccupazione costante che richiede soluzioni di sicurezza efficaci per difendersi da minacce note e impreviste.

Sebbene ne esistano decine di tipi diversi, possiamo identificare i principali tipi di attacchi informatici:

- **Malware** (software dannoso) sono programmi informatici dannosi che includono virus e worm. Questi software pericolosi possono rubare dati o danneggiare i computer.
- **Phishing attacks** i criminali informatici impersonano organizzazioni affidabili nelle conversazioni elettroniche per ottenere dati.
- **Ransomware attacks**,gli hacker chiedono un pagamento per decifrare i dati.
- **Denial-of-service attacks**, gli hacker alimentano le reti con traffico dati interrompendo, in questo modo, le operazioni e i servizi aziendali.
- **Man-in-the-middle (MITM) attacks** si riferiscono a violazioni della sicurezza informatica che consentono a un aggressore di intercettare i dati scambiati tra due persone, reti o computer.

Gli specialisti della sicurezza informatica sviluppano costantemente nuove misure di sicurezza per salvaguardare i dati sensibili e preservare la sicurezza man mano che queste minacce si evolvono.

La cybersecurity nelle nostre mani

Le aziende sono consapevoli del rischio aziendale rappresentato dalla sicurezza informatica e stanno implementando programmi di governance e gestione del rischio, adattati alle dimensioni dell'organizzazione.

Esistono quadri volontari che possono essere utilizzati per considerare la valutazione del rischio e le relative migliori pratiche.
Per esempio, il National Institute of Standards and Technology (NIST) include cinque funzioni simultanee e continue:

1. **Identificare:** Sviluppare una comprensione organizzativa per gestire il rischio di sicurezza informatica per sistemi, persone, risorse, dati e capacità.
2. **Proteggere:** Sviluppare e attuare misure di sicurezza adeguate a garantire la fornitura di servizi critici.
3. **Rilevare:** Sviluppare e implementare attività appropriate per identificare il verificarsi di un evento di sicurezza informatica.
4. **Rispondere:** Sviluppare e implementare attività appropriate per intervenire in caso di incidente di sicurezza informatica rilevato.
5. **Recuperare:** Sviluppare e implementare attività appropriate per mantenere piani di resilienza e ripristinare capacità o servizi compromessi a causa di un incidente di sicurezza informatica.

Responsabilità

Non è sufficiente che le aziende implementino misure di sicurezza informatica solo per mantenere agilità e reattività alle minacce in continua evoluzione. Ecco alcuni dei **malintesi** che possono portare a violazioni dei sistemi informatici:

- **La sicurezza informatica è responsabilità del reparto IT.**
- **Le reti Wi-Fi pubbliche sono sicure:** i criminali informatici possono intercettare i dati trasmessi tramite reti Wi-Fi pubbliche, compromettendo potenzialmente informazioni sensibili. Evitate di accedere ad account sensibili o di effettuare transazioni finanziarie su tali reti.
- **Le e-mail di phishing sono facili da riconoscere:** sebbene alcuni tentativi di phishing siano facili da riconoscere, i criminali informatici sono diventati abili nel creare e-mail e messaggi convincenti. Spesso utilizzano tecniche di ingegneria sociale, sfruttando la psicologia umana per ingannare anche gli utenti più attenti.
- **L'antivirus è sufficiente per proteggere i miei dispositivi:** avere un antivirus aggiornato è fondamentale, ma non è una soluzione definitiva. Le minacce informatiche si sono evolute e i malware più sofisticati possono aggirare i programmi antivirus tradizionali.
- **Le password robuste mi mantengono al sicuro:** le password complesse sono un buon punto di partenza, ma affidarsi esclusivamente a esse è rischioso. Con l'aumento degli attacchi brute-force e degli strumenti di cracking delle password, anche le password più complesse possono essere compromesse.
- **Non sono un bersaglio:** i criminali informatici spesso tessono una rete molto ampia, sfruttando le vulnerabilità ovunque le trovino. Chiunque può essere un bersaglio, anche un singolo individuo o un piccolo imprenditore.

La cybersecurity nelle nostre mani

Ogni utente svolge un ruolo chiave nel supportare i programmi di governance della cybersecurity e di gestione del rischio nella organizzazione. I seguenti 5 suggerimenti possono aiutarti a mantenere il controllo sulla tua cybersecurity:

1. **Utilizzo dell'autenticazione a più fattori:** fornisce un ulteriore livello di sicurezza, garantendo che anche se la tua password viene rubata, un aggressore non può accedere ai tuoi account senza il secondo metodo di autenticazione.
2. **Esecuzione di audit di sicurezza e aggiornamenti software regolari.** Gli sviluppatori rilasciano aggiornamenti per correggere le vulnerabilità di sicurezza e migliorare la stabilità del sistema. Abilita gli aggiornamenti automatici quando possibile per garantire la protezione dalle minacce più recenti.
3. **Rimani aggiornato sugli ultimi sviluppi tecnologici** e sii consapevole dei requisiti aggiuntivi e di come questi interagiranno con la tua attuale infrastruttura di sicurezza.
4. **Impara a riconoscere le truffe di phishing:** Verifica sempre l'identità del mittente, ricontrolla gli indirizzi e-mail ed evita di cliccare su link sospetti o di scaricare allegati da fonti sconosciute.
5. **Rimani aggiornato** con corsi di formazione sulla sicurezza.

Quadro normativo europeo

Oggi la cybersecurity è un tema in fase di sviluppo, integrato in diverse normative a livello europeo e locale. Il panorama legislativo dell'UE in materia di cybersecurity è in continua evoluzione e sta diventando sempre più complesso. Solo per citare alcuni esempi (elenco non esaustivo):

Panorama delle leggi UE sulla cybersecurity

- Digital Operational Resilience Act (DORA): regolamento UE entrato in vigore il 16 gennaio 2023 e applicabile dal 17 gennaio 2025. Mira a rafforzare la **sicurezza informatica delle entità finanziarie** come banche, compagnie assicurative e società di investimento e a garantire che il settore finanziario in Europa sia in grado di rimanere resiliente in caso di grave interruzione operativa.
- Critical Entities Resilience (CER): direttiva UE entrata in vigore il 16 gennaio 2023. Gli Stati membri dell'UE avevano tempo fino al 17 ottobre 2024 per adottare la legislazione nazionale di recepimento della direttiva. Mira a rafforzare la resilienza delle entità critiche contro una serie di minacce, tra cui calamità naturali, attacchi terroristici, minacce interne o sabotaggi, nonché emergenze di sanità pubblica. Si noti che le entità coperte dal CER dovranno anche conformarsi al NIS2.
- Cybersecurity Act (CSA): regolamento UE entrato in vigore nel giugno 2019. Mira a raggiungere un elevato livello di cybersecurity, resilienza informatica e fiducia nell'Unione europea (UE), definendo obiettivi, compiti e aspetti organizzativi per un'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) rafforzata e rinominata, con un nuovo mandato permanente e definendo un quadro per i sistemi volontari europei di certificazione della cybersecurity per prodotti, servizi e processi delle tecnologie dell'informazione e della comunicazione (TIC).
- Cyber Resilience Act (CRA): è una legge dell'UE entrata in vigore il 12 aprile 2024. Nella prima metà del 2026 entreranno in vigore gli obblighi di segnalazione degli incidenti e di divulgazione delle vulnerabilità. I nuovi requisiti entreranno in vigore nella prima metà del 2027. Il loro scopo è colmare le lacune, chiarire i collegamenti e rendere più coerente il quadro legislativo esistente in materia di sicurezza informatica, garantendo che i prodotti con componenti digitali, ad esempio i prodotti "Internet of Things" (IoT), **sono resi sicuri lungo tutta la catena di fornitura e durante tutto il loro ciclo di vita**.
- Network and Information Security (NIS/NIS2): si tratta di una direttiva UE entrata in vigore nel gennaio 2023 e tutti i 27 Stati membri dovevano predisporre le proprie leggi adottando NIS2 entro il 17 ottobre 2024. Mira a definire **misure per un elevato livello comune di sicurezza informatica in tutta l'Unione**.

Le **5 normative** coprono ambiti diversi e sono collegate nel contesto della sicurezza informatica.

Quadro normativo europeo

Il Cybersecurity Act (Regolamento (UE) 2019/881) (e Regolamento di esecuzione (UE) 2024/482 della Commissione) ha l'obiettivo di istituire un sistema europeo di certificazione della sicurezza informatica. Il Cyber Resilience Act è nato per completare il quadro normativo UE sulla sicurezza informatica esistente: la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS), la direttiva sulle misure per un elevato livello di sicurezza informatica nell'Unione (direttiva NIS2) e il Cybersecurity Act dell'UE.

Oltre al quadro europeo in alcuni paesi, gli enti locali hanno sviluppato normative locali come il regolamento KRITIS (Kritische Infrastrukturen) in Germania o ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) in Francia.

In questo documento analizzeremo la direttiva NIS2 per comprendere le implicazioni per i diversi tipi di attività e come prepararsi ai requisiti della direttiva.

NIS2 e DORA

NIS2 e DORA sono stati adottati lo stesso giorno ed entrambi i testi si completano a vicenda, pur non condividendo gli stessi obiettivi: NIS2 mira a rafforzare il livello globale di sicurezza informatica all'interno dell'UE, mentre DORA mira a garantire l'integrità e la disponibilità del settore finanziario. Inoltre, NIS2 e DORA non si rivolgono alle stesse entità: NIS2 riguarda le entità essenziali (EE) e le entità importanti (IE), mentre DORA copre il settore finanziario, attraverso 21 tipologie specifiche di entità.

- Il DORA è la "lex specialis" del NIS2 per il settore finanziario, un principio secondo cui una legge specifica prevale su una legge generale. Per le entità soggette al DORA, il presente testo prevale quindi sul NIS2.
- Ciò non significa che gli obblighi NIS2 non siano più applicabili alle entità interessate da entrambi i testi.

Zoom su NIS2

La Direttiva europea NIS2 fornisce strumenti legali per migliorare il livello complessivo di sicurezza informatica nell'UE e la resilienza delle infrastrutture critiche e dei servizi digitali in Europa. Stabilisce obblighi di sicurezza informatica, vigilanza e applicazione per gli Stati membri dell'UE, obblighi di gestione del rischio e di segnalazione per le entità rientranti nel suo ambito di applicazione (Allegati I e II della Direttiva NIS2) e obblighi di scambio di informazioni sulla sicurezza informatica.

La Direttiva NIS2 si applicherà solo in una fase successiva, una volta che i Paesi avranno istituito le autorità competenti e le regole di ingaggio locali. **Gli obiettivi principali dichiarati nella Direttiva sono:**

- Costringere gli Stati membri dell'UE a redigere leggi sulla sicurezza informatica in linea con la strategia dell'UE in materia di sicurezza informatica.
- Richiedere agli Stati membri dell'UE di istituire un Computer Security Incident Response Team (CSIRT), autorità competenti e punti di contatto unici.
- Garantire che gli Stati membri dell'UE forniscano ai propri CSIRT tutte le capacità necessarie per monitorare e difendere i sistemi informativi essenziali e importanti.
- Stabilire un quadro solido per la collaborazione tra tutti i CISRT e le autorità competenti istituite dagli Stati membri dell'UE.
- Definire gli obblighi di gestione del rischio di sicurezza informatica e di segnalazione degli incidenti per le entità essenziali e importanti.

Dovere di diligenza

Monitoraggio proattivo

Obbligo di segnalazione

Essenziale o importante

La Direttiva NIS2 definisce la classificazione delle attività in essenziali o importanti e, in base a tale classificazione, si applica la Direttiva. Ampliando la precedente, la Direttiva NIS2 dichiara che il suo obiettivo è rafforzare i quadri di sicurezza informatica in un più ampio spettro di settori considerati essenziali per il benessere sociale ed economico.

La direttiva aggiornata include settori critici come l'energia, i trasporti, la sanità e le infrastrutture digitali, riflettendo il crescente riconoscimento della natura interconnessa delle minacce informatiche in diversi settori.

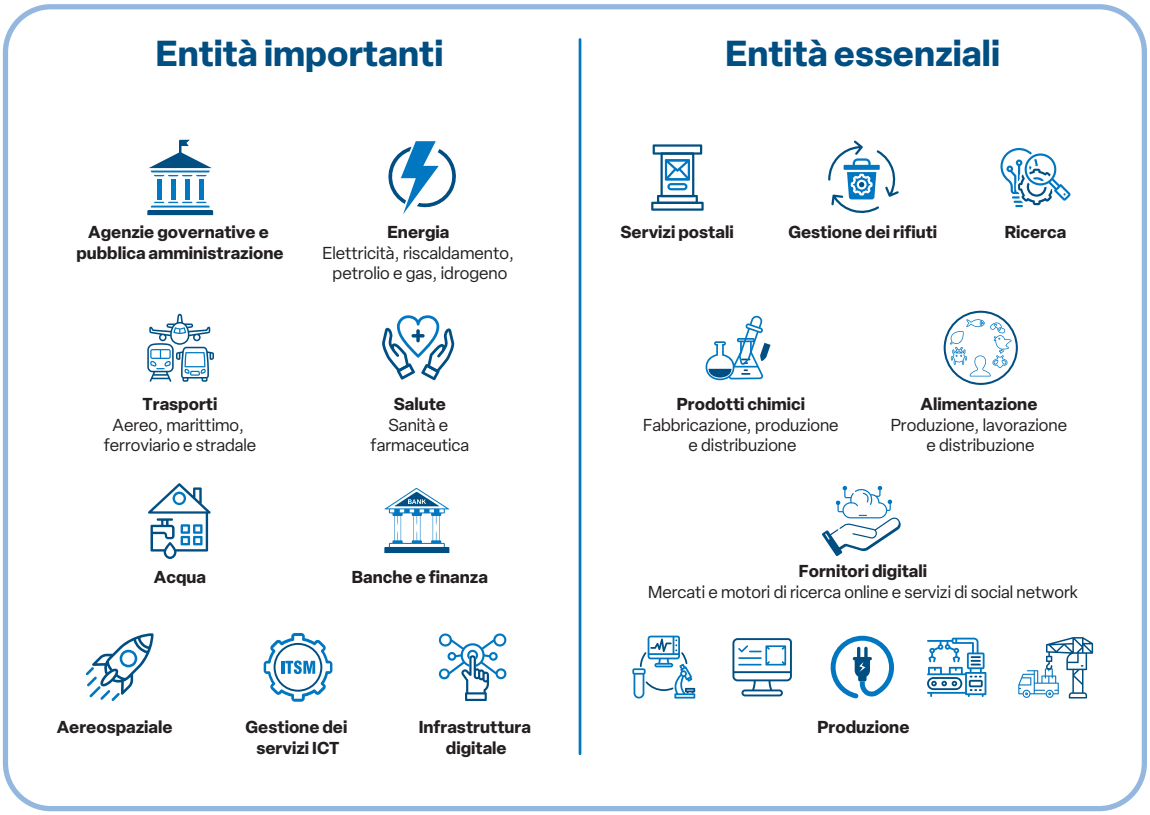
Sono interessate tutte le entità essenziali e importanti e i settori interessati sono classificati nella Direttiva come segue:

Aziende essenziali:

Agenzie governative, enti privati e pubblici che operano nei settori critici dell'energia, dei trasporti, delle banche, della finanza, della sanità, dell'acqua, delle infrastrutture digitali, della gestione dei servizi ICT, della pubblica amministrazione, dello spazio.

Aziende importanti:

Enti che operano in altri settori critici: servizi postali, gestione dei rifiuti, prodotti chimici, alimenti, produzione, fornitori digitali, ricerca.



Secondo la direttiva NIS2, le aziende sono designate come entità essenziali se:

- La società è stata definita come Operatore di Servizi Essenziali secondo NIS a partire dal 16 gennaio 2023.
- L'azienda opera in uno degli 11 settori altamente critici sopra indicati ed è considerata grande azienda (fatturato > 50 milioni di euro o utile > 43 milioni di euro o più di 250 dipendenti).

Le aziende saranno (possibilmente) designate come entità importanti se:

- Le aziende operano in uno degli 11 settori altamente critici o 7 settori critici indicati sopra.
- Le aziende hanno un fatturato o un utile superiore a 10 milioni di euro o più di 50 dipendenti

Secondo il principio della catena di responsabilità, qualunque sia la dimensione dell'azienda, questa può essere designata come EE o IE se:

- TL'azienda è l'unico fornitore di un servizio essenziale.
- L'azienda fa parte della catena di fornitura di un'entità classificata come essenziale o importante, il che significa che una violazione della sicurezza informatica in questa azienda potrebbe avere un impatto su tale entità.

Le entità designate come entità critiche dal CER devono inoltre conformarsi alla NIS2 e dovrebbero essere prese in considerazione quando si valuta l'intera portata delle entità interessate dalla NIS2.

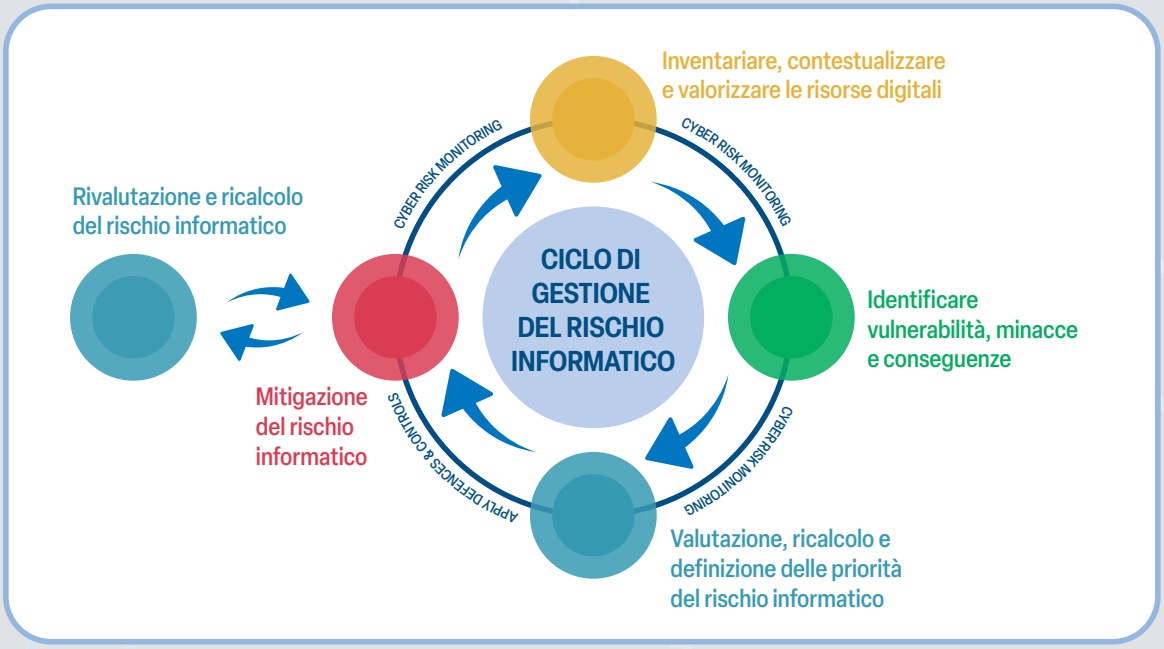
Zooming on NIS2

Settori altamente critici (NIS2 + CER)	Tipo di entità			Elenco dei settori critici (NIS2)	Tipo di entità
	Alta criticità	Fatturato			
		<50M€	>50M€		
Energia	CE	IE	EE	Servizi postali e di corriere	IE
Trasporti	CE	IE	EE	Gestione dei rifiuti	IE
Infrastrutture del mercato finanziario	CE	IE	EE	Produzione, fabbricazione e distribuzione di prodotti chimici	IE
Sanità	CE	IE	EE	Produzione, lavorazione & distribuzione di alimenti	IE
Acqua potabile	CE	IE	EE	Produzione	IE
Acque reflue	CE	IE	EE	Fornitore digitale	IE
Infrastruttura digitale	CE	IE	EE	Ricerca	IE
Gestione dei servizi informatici e della telecomunicazione	CE	IE	EE	CE: Entità critiche (definite dal CER) IE: Entità importanti (definite dalla NIS2)	
Pubblica amministrazione	CE	EE	EE		
Aerospaziale	CE	IE	EE		
Produzione, lavorazione & distribuzione di alimenti	CE				

Secondo la classificazione di cui sopra, **Aritech** è designata come un'entità importante a causa della sua partecipazione nel settore manifatturiero, in particolare nel sottosettore della produzione di computer, prodotti elettronici e ottici.

E se la mia attività fosse critica?

Se un'azienda, secondo la classificazione NIS2, è un'entità critica, essenziale o importante, deve essere pronta per la NIS2 e, secondo il Capitolo IV, deve essere allineata a determinate misure di gestione del rischio di sicurezza informatica e obblighi di segnalazione secondo i seguenti passaggi definiti nella direttiva:



Articolo 20 – Governance: Gli organi di gestione delle entità essenziali e importanti approvano le **misure di gestione del rischio di sicurezza informatica** adottate da tali entità al fine di conformarsi all'articolo 21, supervisionarne l'attuazione e può essere ritenuta responsabile per le violazioni di tale articolo da parte delle entità. Inoltre, i membri degli organi di gestione sono tenuti a seguire **la formazione** e incoraggiare le entità essenziali e importanti a offrire regolarmente una formazione simile ai propri dipendenti, in modo che acquisiscano conoscenze e competenze sufficienti per consentire loro di identificare i rischi e valutare le pratiche di gestione del rischio di sicurezza informatica e il loro impatto sui servizi forniti dall'entità.

- **Aritech** ha istituito un Consiglio per la sicurezza informatica digitale per definire le misure di gestione del rischio e un Comitato di audit per supervisionare il ciclo di vita di queste misure.
- **Aritech** ha istituito una formazione obbligatoria sulla politica digitale e un'attestazione annuale.

E se la mia attività fosse critica?

Articolo 21 – Misure di gestione del rischio di sicurezza informatica: le entità essenziali e importanti adottano misure tecniche, operative e organizzative appropriate e proporzionate per gestire i rischi posti alla sicurezza di sistemi di reti informatiche che tali entità utilizzano per le loro operazioni o per la fornitura dei loro servizi, e per prevenire o ridurre al minimo l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi.

Il Digital Cybersecurity Council di **Aritech** ha creato una politica aziendale sulla tecnologia digitale e la sicurezza delle informazioni. La politica definisce le misure di gestione del rischio, dettagliate nell'Aritech Digital Policy Framework, tra cui:

- Valutazione dell'analisi del rischio per comprendere il punto di partenza delle risorse digitali.
- Piano di gestione degli incidenti, che include un team specifico da coordinare e processi da eseguire in caso di violazione della sicurezza.
- Piano di continuità operativa per reagire e ridurre al minimo l'impatto di qualsiasi violazione della sicurezza.
- Piano di sicurezza della supply chain per proteggere la produzione, in quanto siamo un'entità importante.
- Acquisizione di reti e sistemi per avere il pieno controllo della nostra rete e dei nostri sistemi informativi e gestione delle vulnerabilità per ridurre al minimo il rischio.
- Come azienda, abbiamo definito politiche di gestione del rischio.
- Tutti nell'organizzazione, dal top management all'ultimo dipendente, devono seguire misure di igiene informatica e seguire la formazione obbligatoria sulla politica digitale, inclusa l'attestazione annuale.
- Le nostre reti e i nostri sistemi informativi includono crittografia e regole di crittografia.
- Gli edifici sono protetti da sistemi di controllo degli accessi e disponiamo di un sistema di sicurezza delle risorse umane e di gestione delle risorse.
- Tutti gli accessi alla rete e digitali sono protetti con autenticazione a più fattori.

E se la mia attività fosse critica?

Articolo 22 – Valutazioni coordinate dei rischi per la sicurezza a livello sindacale delle catene di approvvigionamento critiche: effettuare valutazioni coordinate dei rischi, per la sicurezza per specifici dei servizi, dei sistemi o prodotti critici di tecnologie dell'informazione e della comunicazione (ICT).

Aritech in quanto entità importante, è pronta a rispondere ad audit da parte del gruppo di cooperazione una volta che sarà istituito.

Articolo 23 – Obblighi di segnalazione: garantire che le entità essenziali e importanti notifichino, senza indebito ritardo, al proprio CSIRT o all'autorità competente, qualsiasi incidente che abbia un impatto significativo (incidente significativo) sulla fornitura dei propri servizi ai destinatari dei servizi ed all'autorità competente per determinare l'eventuale impatto transfrontaliero dell'incidente. Le tempistiche indicate nell'articolo sono: 24 ore per l'allerta precoce, 72 ore per la notifica dell'incidente e 1 mese dopo la presentazione della notifica dell'incidente per un rapporto finale.

Aritech has established a Cybersecurity Incident Response plan with the following process:

- Aritech notificherà al CSIRT gli incidenti significativi che hanno causato gravi interruzioni operative o perdite finanziarie, o che hanno colpito o sono in grado di colpire altre persone fisiche o giuridiche.
- Inoltre, Aritech notificherà ai destinatari dei servizi potenzialmente interessati da una minaccia informatica significativa qualsiasi misura che possa essere adottata in risposta a tale minaccia.
- Aritech notificherà al CSIRT senza indebito ritardo ed entro 24 ore dalla conoscenza dell'incidente significativo.
- Aritech fornirà aggiornamenti al CSIRT entro 72 ore dalla conoscenza dell'incidente significativo, con una valutazione iniziale che includa gravità e impatto.
- Aritech fornirà rapporti intermedi su richiesta del CSIRT.
- Aritech fornirà un rapporto finale al CSIRT entro un mese dalla presentazione dell'incidente.
- Aritech fornirà un rapporto sullo stato di avanzamento se l'evento è in corso alla data di scadenza del rapporto finale.

E se la mia attività fosse critica?

Articolo 24 – Utilizzo di schemi europei di certificazione della sicurezza informatica: al momento non esiste alcuno schema europeo pubblicato.

Articolo 25 – Standardizzazione: che incoraggia l'uso di standard e specifiche tecniche europee e internazionali rilevanti per la sicurezza delle reti e dei sistemi informativi.

Aritech tiene traccia degli aggiornamenti forniti dall'ENISA.

In sintesi, **Aritech** In quanto entità importante, è già allineata ai requisiti minimi definiti in NIS2. Tuttavia, ogni Stato membro dell'UE può andare oltre i requisiti minimi e ciò richiederà ulteriori convalide quando le leggi saranno in vigore.

Implicazioni per la conformità NIS2

Emergeranno delle sfumature tra le diverse implementazioni. Alcuni Paesi definiranno più requisiti di altri, ecco perché dobbiamo comprendere gli sviluppi che saranno implementati in ciascun Paese per essere completamente in linea con la Direttiva recepita.

Le procedure di comunicazione degli incidenti saranno definite per Paese e per CSIRT; sarà quindi fondamentale essere in contatto con le autorità locali per allinearsi alle tempistiche e alle procedure implementate a livello locale. Gli Stati membri dell'UE garantiscono che le sanzioni amministrative imposte alle entità essenziali e importanti ai sensi del presente articolo in relazione alle violazioni della presente direttiva siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

In caso di non conformità o ritardi nell'attuazione di azioni correttive sulle carenze identificate, verranno applicate sanzioni amministrative che potrebbero variare da paese a paese, ma per le entità importanti NIS2 stabilisce un massimo "minimo":

- Per le entità importanti almeno 7.000.000€ o l'1.4% del fatturato totale mondiale
- Per le entità essenziali almeno 10.000.000€ o il 2% del fatturato totale mondiale

Aritech e la conformità alla NIS2

I prodotti e i servizi supportati da Aritech sono soggetti a rigorosi requisiti di sviluppo sicuro e controllo dei processi, conformi agli standard di sicurezza informatica commercialmente appropriati.

Aritech applica politiche interne di sicurezza informatica dei prodotti, il che significa attenzione proattiva, best practice, supporto completo e competenza per rafforzare e garantire la resilienza e la stabilità delle nostre offerte. La nostra missione è garantire i seguenti risultati strategici fondamentali:

- Prodotti e servizi "sicuri per progettazione"
- Governance e conformità della sicurezza informatica basate su standard
- Vigilanza persistente e miglioramento continuo
- Missione del cliente Success

Leadership di pensiero

Aritech lavora in modo proattivo per garantire le proprie offerte e garantire i migliori risultati per i clienti. Ciò richiede di contribuire e trarre vantaggio dalla nostra comunità professionale nell'ambito di alleanze strategiche reciprocamente vantaggiose e di assumere posizioni di leadership di pensiero nel settore presso le principali organizzazioni di sicurezza informatica. Aritech è orgogliosa di ricoprire il ruolo di:

Founding Member of the ISA Global Cybersecurity Alliance

CVE Numbering Authority (CNA)

Il nostro Focus

In Aritech, la sicurezza dei sistemi e delle operazioni è fondamentale. Per garantire i risultati, i team di ricerca e sviluppo sfruttano le politiche di sicurezza informatica dei prodotti Aritech: un team di veterani altamente qualificati ed esperti del settore della sicurezza informatica diversificati e dinamici che hanno ricoperto ruoli e responsabilità di rilievo nella progettazione, costruzione e gestione di sistemi complessi altamente sicuri.

Le politiche di sicurezza informatica dei prodotti Aritech supportano e soddisfano le richieste strategiche, produttive, operative e commerciali relative alla sicurezza informatica dei nostri stakeholder, soddisfacendo tre aree operative fondamentali della missione:

- Sviluppo sicuro dei prodotti
- Operazioni di sicurezza dei prodotti
- Innovazione nella sicurezza informatica

Aritech e la conformità alla NIS2

Sviluppo sicuro dei prodotti

L'architettura di sicurezza informatica globale dei prodotti garantisce il successo della missione progettando proattivamente i sistemi per la sicurezza, valutando, gestendo e migliorando costantemente il posizionamento di Aritech in tutte le fasi appropriate del ciclo di sviluppo e supporto del prodotto.

Caratteristiche chiave:

- Governance, Conformità e Formazione
- Progettazione, requisiti e architettura della sicurezza
- Sviluppo di funzionalità e sistemi di sicurezza informatica
- Modellazione e garanzia della sicurezza
- Valutazione del rischio informatico

Operazioni di sicurezza del prodotto

Le operazioni di sicurezza informatica dei prodotti globali assicurano e consentono il successo della missione post-sviluppo fornendo test avanzati di sicurezza informatica, integrazione, pianificazione di implementazione sicura, intelligence sulle minacce, risposta agli incidenti, pubblicazione delle vulnerabilità e supporto del ciclo di vita.

Caratteristiche chiave:

- Test di penetrazione e regressione
- Distribuzione sicura
- Gestione minaccia sui prodotti
- Consulenza e Comunicazione
- Integrazione sicura sinergica
- Risposta agli incidenti di sicurezza del prodotto

Innovazione nella sicurezza informatica

Global Product Cybersecurity Innovation ricerca e sviluppa soluzioni innovative, promuove la leadership di pensiero, differenzia le offerte e fornisce vantaggi competitivi nel settore della sicurezza informatica per i clienti Aritech risolvendo problemi complessi, promuovendo la sicurezza informatica come caratteristica e stimolando una trasformazione tecnologica avanzata e sicura.

Caratteristiche chiave:

- Ricerca e sviluppo informatico avanzato
- Innovazione informatica, innovazione e offerte di servizi/prodotti
- Conformità e certificazione degli standard di sicurezza informatica dei prodotti
- Analisi competitiva
- Supporto e coinvolgimento del mercato

Siete pronti per la NIS2?

L'integrità del prodotto può essere garantita quando l'hardware e il firmware sono protetti efficacemente da qualsiasi modifica o manipolazione non autorizzata durante tutto il percorso del prodotto lungo la catena di fornitura. Il processo di sviluppo del prodotto Aritech include controlli di qualità e verifiche sviluppati dal Product Cybersecurity Operations Team per verificare l'integrità delle soluzioni che sviluppiamo.

Le soluzioni Aritech aiutano la tua azienda a essere pronta per NIS2

Nell'ambito di tale processo, il team di sviluppo convalida la nostra soluzione dal punto di vista della sicurezza informatica, esaminando l'elenco delle potenziali minacce e i requisiti di sicurezza nell'architettura e nella progettazione della soluzione. Eseguiamo scansioni periodiche dei componenti dell'applicazione (incluse le librerie di terze parti) per rilevare eventuali vulnerabilità di sicurezza, problemi di conformità o rischi per la qualità. In Aritech, eseguiamo valutazioni della sicurezza utilizzando analisi automatizzate delle vulnerabilità, strumenti di scansione e penetration test manuali su tutti i nostri nuovi prodotti in fase di sviluppo per convalidare la resistenza del sistema agli attacchi informatici. I test sono in conformità con metodologie generalmente accettate, tra cui OWASP Top 10 Web, OWASP IoT Security Verification Standards e SANS Top Issues. Includiamo le best practice interne per la conduzione di test di sicurezza sviluppate dal team Aritech Global Product Cybersecurity, con diversi anni di esperienza nell'esecuzione di penetration test.

Are you ready for NIS2?

Le soluzioni Aritech includono diverse misure di sicurezza per garantire il nostro contributo all'allineamento con la direttiva NIS2 una volta adottata:

- Con le piattaforme ATS Advisor Advanced ed Everon, **Aritech offre** un sistema di rilevamento delle intrusioni fisiche per impedire a persone non autorizzate di accedere alle proprie infrastrutture critiche (server/IT/data room, produzione, dati IP, stock critici...). Qualsiasi rilevamento di persone non autorizzate verrà notificato tramite i percorsi programmati agli istituti di vigilanza o alla sala di controllo.
- **Aritech offre** soluzioni di controllo degli accessi fisici per impedire a persone non autorizzate di accedere alle proprie infrastrutture critiche. Il controllore di controllo accessi CDC4, integrato con il sistema di intrusione Everon, crea un ecosistema per rilevare e comunicare qualsiasi tentativo di accesso non autorizzato ai locali protetti. La soluzione include diversi livelli di sicurezza (canale sicuro/crittografia, autenticazione a due fattori...) in conformità con l'articolo 21 della Direttiva NIS2. Anche Axon, come sistema di controllo degli accessi autonomo, include diversi livelli di sicurezza (canale sicuro/crittografia, autenticazione a due fattori...) in conformità con l'articolo 21 della Direttiva NIS2.
- **Aritech offre** soluzioni di videosorveglianza fisica per monitorare le infrastrutture critiche. L'ecosistema utilizza comunicazioni crittografate HTTPS con certificati SSL e crittografia TLS 1.2, a seconda della composizione dell'ecosistema.
- **Aritech offre** protezione perimetrale per proteggere le infrastrutture critiche come primo anello di protezione nel sistema di controllo accessi.
- **Aritech offre** soluzioni per la gestione dei visitatori come parte della sua soluzione software di integrazione ATS8600.
- Naturalmente, **Aritech garantisce** che i prodotti siano conformi agli standard di settore come EN e altre certificazioni

Are you ready for NIS2?

Ecco alcuni suggerimenti su come i prodotti Aritech possono aiutarti con NIS2:

- **App UltraSync per cellulari:** Le comunicazioni tra le app e il cloud UltraSync sono crittografate con HTTPS.
- **Portale UltraSync:** Le comunicazioni tra il portale UltraSync e il cloud UltraSync sono crittografate con HTTPS.
- **TruVision Navigator:** Tra client e server, tramite comunicazione HTTPS con certificato autofirmato (impostazione predefinita). Il cliente può caricare i propri certificati SSL. Tra client e dispositivo, la comunicazione è crittografata. Utilizza la crittografia TLS 1.2 sulla trasmissione TCP.
- **TruVision Cloud:** Tra App e cloud, utilizzando la comunicazione HTTPS con certificati SSL. Tra servizi cloud e cellulari (per le notifiche), utilizzando la comunicazione protetta secondo le API più recenti di APNS (iOS) e Firebase (Android).
- La centrale antintrusione Advisor Advanced utilizza un protocollo di comunicazione proprietario, crittografato con AES a 128 bit, tra i diversi elementi collegati al bus. Advisor Advanced è inoltre certificata RTC Livello 3 dal CNPP (Ente Nazionale di Certificazione Francese), che è lo schema di certificazione proprietario specifico per la sicurezza informatica.
- La centrale antintrusione Everon utilizza un protocollo di comunicazione proprietario, crittografato con AES a 128 bit e HTTP e HTTPS tra i diversi elementi collegati al bus. La centrale Everon è in fase di ottenimento delle certificazioni RTC e ANSII per la sicurezza informatica.
- La centrale di controllo accessi CDC4 utilizza un protocollo di comunicazione proprietario, crittografato con AES a 128 bit, tra il controller e i lettori collegati al bus.

Inoltre, è importante sottolineare che il portfolio prodotti di Aritech rispetta gli standard GDPR. Le valutazioni pertinenti per il nostro portfolio sono disponibili sul nostro sito web.

Conclusioni

Le pubblicazioni NIS e NIS2 rappresentano traguardi importanti nel riconoscimento dell'importanza della sicurezza informatica in settori specifici e nella definizione di misure per un elevato livello comune di sicurezza informatica in tutta l'Unione europea.

La Direttiva NIS2 è entrata ufficialmente a far parte del diritto dell'UE il 16 gennaio 2023 e il 17 ottobre 2024 è scaduto il termine ultimo per il recepimento da parte degli Stati membri dell'UE, che dovevano adeguare le proprie legislazioni nazionali per conformarsi alla Direttiva NIS2.
La data di entrata in vigore sarà 18 mesi dopo la scadenza del termine di recepimento. Tale data potrebbe variare da uno Stato membro all'altro; infatti, Belgio, Ungheria, Croazia, Italia, Lettonia e Lituania sono stati i primi Paesi a recepire la Direttiva nelle proprie legislazioni nazionali e la maggior parte inizierà ad applicare la Direttiva NIS2 verso la metà del 2025.

Per aiutare i nostri clienti a conformarsi a NIS2, l'ecosistema di soluzioni Aritech è progettato per migliorare la sicurezza informatica come parte della valutazione delle risorse digitali richieste per essere conformi a NIS2.

Per domande tecniche, inviare un'e-mail al nostro sistema di ticket di assistenza:
Per l'Italia: support.italy@kgsolutions.com

La tua domanda verrà registrata e il follow-up è garantito.