Allegato NIS2

TIM ENTERPRISE

L'importanza dell'innovazione per l'adeguamento alla NIS2

Le opportunità dell'innovazione nella sicurezza

La nascita della Direttiva NIS2 rappresenta un'opportunità preziosa per le aziende e le organizzazioni alle quali si rivolge. Infatti, se da un lato impone obblighi da rispettare e sanzioni, anche piuttosto salate, dall'altro mira a colmare un disavanzo, dal punto di vista normativo e innovativo, da troppi anni presente nel nostro continente.

Questo disavanzo nel tempo ha creato un gap competitivo, almeno in termini di sicurezza, non indifferente per il tessuto imprenditoriale italiano ed europeo. Si pensi, ad esempio, al tema della protezione dei dati personali degli utenti conservati nei sistemi di un'azienda colpita. Dal punto di vista dell'utente, affidarsi ad un'organizzazione cyber-resiliente è un chiaro elemento valoriale nell'atto della scelta: l'utente sceglierà, idealmente, l'azienda che percepisce come più sicura, proprio per limitare questo tipo di rischi. Ecco appunto che un vincolo normativo, anche se imposto, può rivelarsi un'opportunità per la reputazione aziendale.

Troppo spesso iniziative normative come la Direttiva NIS2 sono viste, dai soggetti interessati, principalmente come meri vincoli ed obblighi che, se non rispettati, minacciano di erodere guadagni e fatturato, oltre a complicare le attività operative. È perciò essenziale comprendere effettivamente ogni aspetto di questo importante aggiornamento normativo, capire di cosa si tratta e conoscere i doveri e le opportunità che ne scaturiscono.

Innanzitutto, è fondamentale chiarire il tema centrale che contraddistingue la Direttiva NIS2: semplificando, parliamo di governance della propria sicurezza cyber e delle soluzioni tecnologiche alle quali ci si affida. Questi aspetti concorrono a pieno titolo nella valutazione dell'affidabilità organizzativa e della supply chain di riferimento. Si pensi infatti al tema della fornitura di componenti – di ogni genere – per le infrastrutture critiche, per la difesa, e per altri elementi nevralgici della nostra società. Affidarsi a soluzioni di sicurezza

prodotte da fornitori non certificati, o peggio, dei quali non conosciamo nel dettaglio i processi produttivi e gli standard di sicurezza in uso, ci espone a una moltitudine di rischi, dalle più varie vulnerabilità cyber fino allo spionaggio doloso.

La Direttiva NIS2 ci fornisce dieci importanti punti di intervento riportati nell'infografica sotto, sui quali convogliare gli sforzi innovativi e di investimento dei soggetti ai quali si rivolge.

A primo sguardo emerge chiaramente lo sforzo atto a rendere sicuri innanzitutto gli utenti della sicurezza, ovvero tanto il manager quanto il dipendente o il cliente finale. Dalla consapevolezza dei rischi cyber ai quali siamo esposti fino alla sicurezza proattiva dei propri dispositivi e della connettività, l'elemento innovativo è centrale. È importante, in questo senso, iniziare da subito a formare ed informare utenti e operatori circa il

complesso panorama cyber in costante evoluzione, mettendoli al riparo da un uso incauto degli strumenti digitali a loro disposizione.

Tradurre un obbligo normativo in un'opportunità di innovazione tecnologica e crescita della competitività sul mercato è un passo apparentemente complesso, ma assolutamente realizzabile. Tuttavia, come spesso accade, la conditio sine qua non è la scelta del partner di sicurezza al quale affidarsi.

Importanza dell'adozione di soluzioni tecnologiche avanzate e di approcci innovativi alla sicurezza informatica

Secondo il "Rapporto CLUSIT 2024 sulla sicurezza ICT in Italia" nel solo primo trimestre del 2023 sono stati rilevati 1.382 incidenti gravi, +11% rispetto allo stesso periodo 2023. L'Italia è al terzo posto in Europa e al sesto nel mondo per attacchi ransomware, ben il 74% delle grandi organizzazioni nazionali ha rilevato un incremento dei tentativi di attacco subìti e il 12% ha registrato conseguenze tangibili derivanti da un incidente informatico.

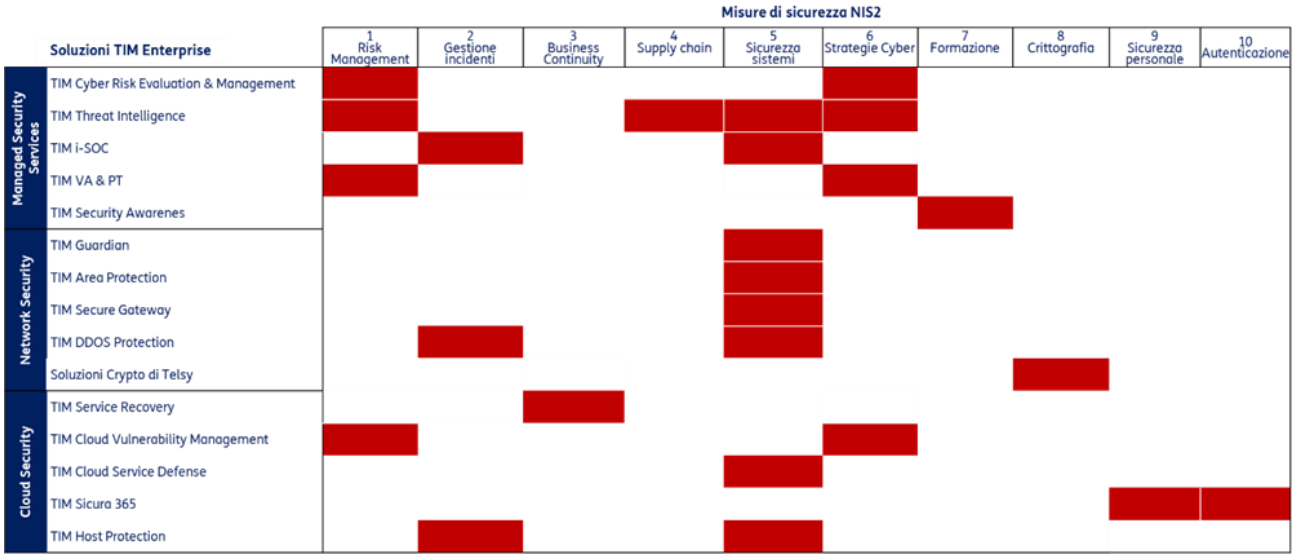
È chiaro che gli attacchi informatici, dalle violazioni dei dati alle minacce ransomware, mettono in grave rischio la sicurezza delle informazioni sensibili. Inoltre, l'evoluzione informatica, l'intelligenza artificiale, richiedono soluzioni tecnologiche più evolute con un monitoraggio proattivo da parte di personale e analisti esperti.

In questo contesto, TIM si propone, come un partner affidabile per accompagnare le aziende e le organizzazioni in un percorso che le porti a diventare cyber resilienti e conformi alla direttiva NIS2.

TIM ha infatti maturato una pluriennale esperienza nella gestione della sicurezza dei suoi importanti asset di telecomunicazione, dalle reti nazionali e internazionali ai datacenter di ultima generazione. Infrastrutture altamente critiche che TIM ha dovuto adeguatamente proteggere adottando opportune soluzioni tecnologiche, stringenti requisiti di conformità e sviluppando forti competenze al proprio interno. Esperienze e competenze che poi sono state ulteriormente rafforzate con l'acquisizione di Telsy, Centro di Competenza specializzata nella Cybersecurity, e sviluppando partnership con i principali vendor mondiali di Cybersicurezza.

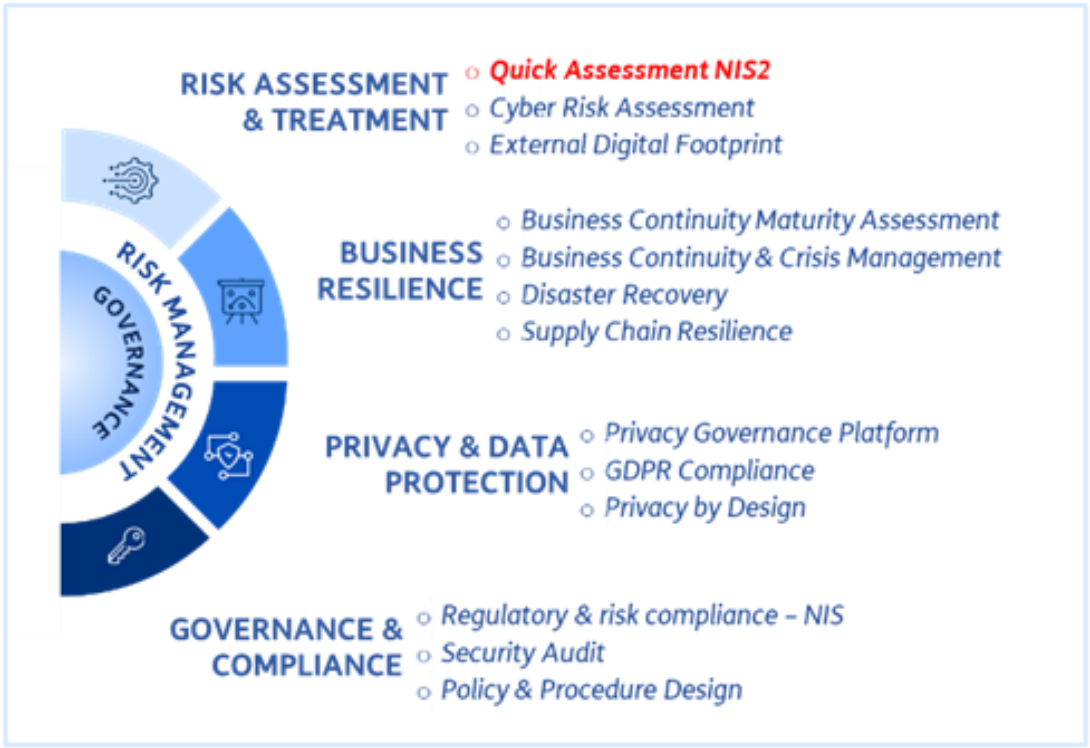
Tutto questo ha portato TIM a diventare uno dei principali attori nazionali in ambito cybersicurezza con un portafoglio di soluzioni completo che aiutano le aziende e le istituzioni a prevenire, proteggere e mitigare i rischi informatici. Portafoglio di soluzioni che quindi può supportare le aziende e le organizzazioni

nell'adeguamento alla direttiva stessa come si può vedere dalla tabella seguente, dove viene mostrato come ogni soluzione aiuta a soddisfare i 10 punti della Direttiva NIS2.



Le soluzioni sono raggruppate in tre principali macroaree:

- Managed Security Services: soluzioni e servizi di consulenza che, tramite tecnologie avanzate e personale altamente qualificato, permettono di valutare e migliorare la postura di sicurezza delle aziende, monitorare le infrastrutture IT dei clienti e di garantire una protezione completa e continuativa.
    - TIM Cyber Risk Evaluation & Management offre un framework di servizi di consulenza finalizzati a valutare il grado di esposizione al rischio del patrimonio informativo e tecnologico dell'azienda ed a supportarla nell'implementare piani di rientro sostenibili ed efficaci.



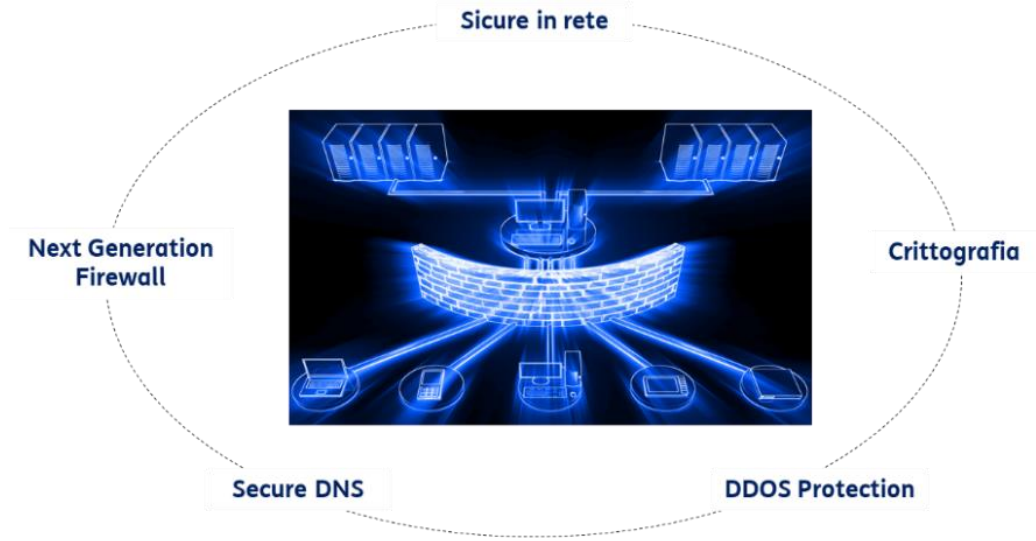
In particolare, all'interno di quest'offerta è presente il servizio Quick Assesment NIS2 che può essere considerato il punto di partenza per un'azienda che vuole adeguarsi alla direttiva NIS2 perché permette di effettuare una gap-analysis rispetto ai requisiti richiesti dalla direttiva, permette di identificare le principali criticità e aree di miglioramento e fornisce raccomandazioni per migliorare il livello di adeguatezza alla direttiva stessa.

Una volta effettuato l'assesment e quindi una volta che le aziende conoscono quali azioni devono prevedere per adeguarsi alla NIS2, possono successivamente utilizzare gli altri moduli del framework per essere supportati nell'implementazione di piani e procedure necessarie per introdurre una strategia di Cyber Risk management a 360 gradi che permetta di essere conformi alle principali normative e standard di sicurezza mondiali.

- Per effettuare un assesment esaustivo ed implementare un'efficacie strategia cyber è necessario analizzare anche le minacce, sia interne che esterne, a cui sono sottoposti i sistemi e le procedure

aziendali. Per fare questo è necessario dotarsi di “intelligence”, cioè raccogliere, analizzare e interpretare le informazioni sulle minacce informatiche, come malware, attacchi DDoS, attività di hacking e altre minacce emergenti, al fine di prevedere e mitigare gli incidenti prima che possano verificarsi danni significativi. La soluzione TIM Threat Intelligence mette a disposizione le competenze tecniche e investigative della società TS-WAY, da maggio 2023 parte del gruppo Telsy, che si occupa esclusivamente di Cyber Threat Intelligence e si configura come Information Provider, cioè fornisce informazioni tempestive e validate a livello umano e tecnologico sia di natura OSINT, provenienti da fonti aperte, che CLOSINT, cioè da fonti riservate, esclusive e non accessibili pubblicamente. Informazioni di tipo strategico, tattico, operativo che possono essere utilizzate per effettuare analisi mirate, one shot, oppure fruite tramite la piattaforma proprietaria “TS-Intelligence” che permette di tracciare informazioni e dati tecnici, correlarli e migliorare la postura delle organizzazioni evolvendo l’approccio da reattivo a predittivo.

- Una volta effettuato l’assesment e analizzata la postura di sicurezza aziendale, è necessario implementare delle azioni che permettano di monitorare costantemente i sistemi e le reti aziendali al fine di prevenire, rilevare e rispondere nel più breve tempo possibile ad eventuali incidenti informatici. Per far questo è possibile utilizzare l’iSOC Telsy, un Security Operation Center che tramite piattaforme tecnologiche avanzate e una squadra di professionisti specializzati permette di monitorare, analizzare gli eventi e rilevare gli attacchi più avanzati.
  Team di professionisti che può essere utilizzato anche per effettuare Vulnerability assessment e Penetration test, cioè per identificare le vulnerabilità dei sistemi aziendali e simulare attacchi al



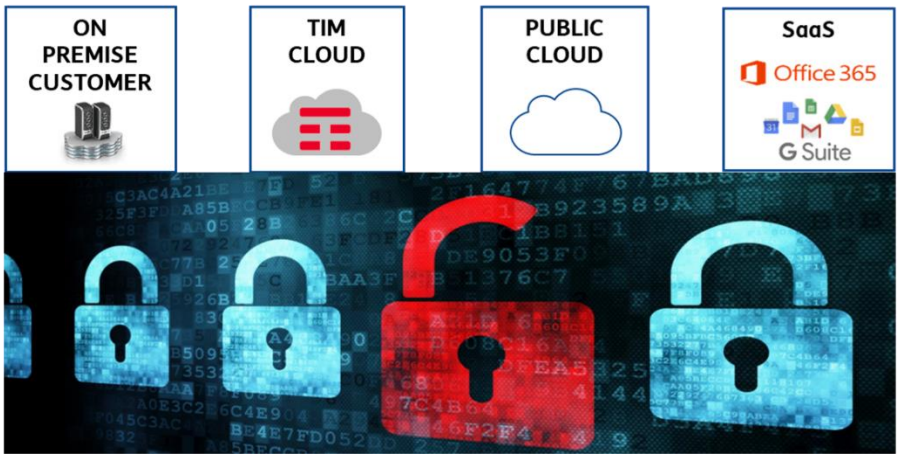
fine di individuare le falle e le debolezze della sicurezza che potrebbero essere sfruttate da un hacker.

- Altra azione fondamentale, su cui la direttiva NIS2 pone un particolare accento, è la formazione dei dipendenti. Recenti studi mostrano infatti che l'82% degli incidenti è causato proprio da errori umani. Quindi formare i dipendenti affinché questi adottino corrette pratiche di cyber igiene, come ad esempio utilizzare password sicure o installare senza indugio gli aggiornamenti software, e addestrarli al riconoscimento del phishing può trasformare i dipendenti nella prima linea di difesa dagli attacchi informatici. Da questo punto di vista la soluzione TIM Security Awareness mette a disposizione la piattaforma TelsySkills, che, tramite moduli di e-learning interattivi e campagne di addestramento anti-phishing, permette di sviluppare una chiara consapevolezza del rischio cyber nei propri dipendenti.

- Network Security: un insieme di tecnologie, servizi professionali e metodologie pensate per proteggere le reti aziendali e i dati sensibili da attacchi informatici e minacce avanzate su ogni tipologia di rete e infrastruttura.

  - Con la diffusione del Cloud e dello Smart Working diventa sempre più difficile proteggere il traffico internet dei dipendenti perché le aziende sono costrette a raccogliere sulla sede principale tutto il traffico della periferia per applicare le opportune policy di sicurezza, con un sensibile incremento dei costi di gestione. Per questo motivo Tim, forte dell'esperienza maturata nella sicurezza delle reti, ha sviluppato la soluzione TIM Guardian che protegge nativamente le proprie connessioni di rete. In altre parole, TIM fornisce connessioni di rete, fisse e mobili, già "sicurizzate" dove cioè sono state implementate centralmente, direttamente nella rete, tutte le funzionalità di sicurezza che servono a proteggere e controllare il traffico e la navigazione Internet e che quindi permettono alle aziende di mettere al sicuro le proprie infrastrutture evitando inutili investimenti.
  - Aziende con esigenze più specifiche possono invece utilizzare TIM Area Protection che permette di implementare un'avanzata sicurezza perimetrale tramite il noleggio di Next Generation Firewall gestiti centralmente da personale specializzato del Security Operation Center di TIM. Oppure possono utilizzare TIM Secure Gateway che offre sicurezza gestita e centralizzata, senza necessità di installazione di tecnologia apposita in sede, per proteggere l'accesso e il traffico internet effettuato dai propri dipendenti.

- Per proteggere le proprie risorse online dagli attacchi DDOS, che mirano ad interrompere il normale funzionamento di un sito web o di una rete sovraccaricandoli con un'eccessiva quantità di richieste proveniente da più fonti distribuite, è invece possibile utilizzare TIM DDOS Protection. Il servizio, erogato centralmente da personale specializzato TIM, si attiva automaticamente e tempestivamente in caso di attacco deviando il traffico dati, ripulendolo e successivamente reinstradandolo verso l'azienda, tutelando in questo modo la continuità dei servizi online erogati dall'azienda.
- Infine, è fondamentale per le aziende mantenere il pieno controllo delle proprie informazioni proteggendo le comunicazioni che sono sempre più a rischio violazioni visto il dilagare di dispositivi connessi a Internet e delle reti digitali. TIM e in particolare Telsy, che da oltre 50 anni rappresenta un punto di riferimento nazionale nella sicurezza delle comunicazioni, forniscono tutte le soluzioni che permettono di comunicare e condividere i dati in sicurezza grazie all'utilizzo della crittografia e dei più elevati standard di sicurezza.



Sistemi di crittografia che Telsy sta rafforzando e rendendo "a prova di futuro" grazie all'utilizzo della Quantum Key Distribution (QKD), tecnologia nata per superare la minaccia degli attacchi dei prossimi computer quantistici, e alle competenze e tecnologia di QTI, azienda italiana leader nel campo di cui Telsy è azionista.

- Cloud Security: soluzioni che consentono di proteggere e garantire l'integrità, disponibilità e riservatezza dei dati e delle risorse aziendali che risiedono in ambiente cloud sia pubblico che privato o fornito da TIM stessa.

- Tra le principali misure da implementare richieste dalla Direttiva NIS2 c'è assicurare la continuità operativa (Business Continuity) e quindi garantire che un'organizzazione possa continuare a operare o riprendersi rapidamente da interruzioni impreviste o catastrofiche. Questo permette infatti di ridurre al minimo l'impatto di eventi inaspettati che possono causare perdita di dati sensibili, danni legali, finanziari e reputazionali con conseguenti perdita di fiducia da parte dei clienti.
  Una delle soluzioni che può essere utilizzata per assolvere questa misura è TIM Service Recovery che permette di ripristinare i sistemi, i dati e le infrastrutture in caso di emergenze che ne interrompono l'attività. Infatti, permette di effettuare backup dei dati nei datacenter TIM da utilizzare come ripristino in caso di eventi malevoli. Oppure permette di replica nei datacenter TIM le risorse informatiche (server, storage, connettività) del sito cliente, per il ripristino del servizio IT nel caso di eventi di fault.
- TIM Cloud Vulnerability Management invece consente una protezione completa delle infrastrutture cloud, offrendo una visibilità completa delle risorse cloud e dei rischi associati ad esse, identificando eventuali vulnerabilità e configurazioni errate, e automatizzando le attività di sicurezza come, ad esempio, l'applicazione di "patch" ai sistemi o software per risolvere le vulnerabilità.
- Altre soluzioni che consentono di proteggere le risorse cloud dell'azienda sono TIM Host Protection, che difende le applicazioni ed i siti web da attacchi DDOS applicativi o basati su BOT e API Manipolation, o TIM Cloud Defense che fornisce una protezione avanzata delle suite cloud Office 365, Google Workspace, DropBox da tentativi di phishing, malware e violazioni dei dati.
- Infine, TIM Sicura 365 fornisce consulenza per implementare la gestione delle identità degli utenti digitali che accedono al cloud Microsoft e permette di verificarne l'identità in modalità sicura tramite l'utilizzo della "Autenticazione Multi Fattore".

In conclusione, per adeguarsi alla direttiva NIS2 è necessario affrontare un percorso olistico che analizzi l'intero ambiente tecnologico, organizzativo e di contesto in cui un'azienda opera e pervada tutte le aree dell'azienda, a partire dalla consapevolezza del management. Gli esperti di **TIM e Telsy** sono a disposizione delle aziende che vogliono cominciare questo cammino e che vogliono essere accompagnate passo dopo passo, dall'inizio alla fine, in questo percorso di adeguamento.

Tim inoltre è socio del **Competence Center Cyber 4.0** e ha incluso nel portafoglio del Competence Center i propri servizi professionali cyber atti a garantire livelli di sicurezza ottimali e che permettano alle imprese che utilizzano suddetti servizi di usufruire di agevolazioni economiche significative.

Ruolo Competence Center Cyber 4.0

Il Centro di Competenza Cyber 4.0, oltre ad essere affermato centro di eccellenza e conoscenza dei temi di cybersicurezza, ricopre anche un ruolo di abilitatore per conto del Governo dei finanziamenti previsti per guidare le imprese verso il processo di trasformazione digitale e di messa in sicurezza secondo normativa NIS2.

Avviato nel contesto del piano Industria 4.0, il Centro è oggi riconosciuto come polo di trasferimento tecnologico nazionale ed è soggetto attuatore del PNRR per conto del MIMIT.

Cyber 4.0 è costituito nella forma di un'Associazione di diritto privato, che esprime un partenariato pubblico-privato largamente rappresentativo del contesto di cyber security nazionale, cui partecipano oltre 40 attori di rilevanza nazionale, rappresentanti di università ed enti di ricerca, istituzioni pubbliche, grandi aziende, fondazioni e PMI altamente specializzate.

La missione di Cyber 4.0 è accompagnare policy maker, imprese e PA in un percorso di crescita verso una digitalizzazione sicura, grazie a soluzioni concrete, strategiche e sostenibili basate su conoscenze, tecnologie innovative e servizi abilitanti sviluppati con le competenze del proprio network, che valorizzino le eccellenze del Paese nel contesto europeo e internazionale e che rispondano ai requisiti della direttiva europea NIS2.

Per mandato istituzionale, il Centro offre a Imprese e Pubblica Amministrazione servizi di advisory e formazione, assesment e test-before-invest in ambito cybersecurity, e finanzia progetti di ricerca e innovazione.

Il Centro rappresenta oggi un canale di accesso semplificato a fondi PNRR, erogabili in forma di incentivi alle imprese per l'acquisto dei servizi offerti e di co-finanziamento di progetti di ricerca e innovazione.

- I Servizi possono essere erogati con percentuali di co-finanziamento erogabili nella modalità dello sconto in fattura e variabili a seconda della tipologia di servizio e della dimensione aziendale, secondo la seguente tabella riportata nel Decreto.

Categorie di servizi	Intensità massima di aiuto		
	Micro Piccole	Medie	Grandi
Audit tecnico, valutazione maturità tecnologica – **Assessment**	100%	80%	30%
Prova prima dell'investimento – **Demo Lab e Test-before-invest**	100%	90%	40%
Formazione (<=24h)	100%	80%	60%
Formazione (>24h)	70%	60%	50%
Consulenza su proprietà intellettuale	70%	60%	50%
Consulenza su **accesso ai finanziamenti**	70%	60%	50%
Consulenza su **innovazione tecnologica di processo e di prodotto, sensibilizzazione e networking**	80%	70%	50%
Progettazione dell'intervento di innovazione	50%	40%	30%

- I bandi di ricerca vengono emanati periodicamente e prevedono percentuali di co-finanziamento variabile in considerazione della dimensione aziendale.

  Ultimo Bando emesso:

  Codice: 01/2024

  Importo stanziato: 2,735 mln

  Settore: Aerospace, Automotive, Healthcare, Core Cyber Security

  Intensità: fino a 400K per singolo progetto variabile sulla base della dimensione aziendale

  Durata:12 mesi

  Scadenza: 31/05/2024