La protezione cibernetica e la sicurezza informatica nazionale
Il quadro strategico nazionale per la sicurezza dello spazio cibernetico

Il quadro strategico nazionale per la sicurezza dello spazio cibernetico

In questa lezione analizzeremo i seguenti punti:

- Infrastrutture critiche;
- Quadro Strategico Nazionale;
- Piano Nazionale per la protezione cibernetica e la sicurezza informatica.

Infrastruttura critica

Il decreto legislativo 61/2011 relativo alla individuazione di IC Europee definisce:

infrastruttura: un elemento, un sistema o parte di questo, che contribuisce al mantenimento delle funzioni della società, della salute, della sicurezza e del benessere economico e sociale della popolazione.

infrastruttura critica (IC): infrastruttura, ubicata in uno Stato membro dell'Unione europea, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni.

Infrastruttura critica

INFRASTRUTTURE CRITICHE: DIRETTIVA 2008/114/CE

Stabilisce una procedura per **identificare** e **designare le infrastrutture critiche europee** (ICE) e un approccio comune per valutare la necessità di migliorare la loro protezione. La direttiva ha uno scopo settoriale, applicabile solo ai settori dell'energia e dei trasporti.

Infrastruttura critica

Fra le infrastrutture identificate come critiche per una nazione si annoverano:

- Le reti per la trasmissione e la distribuzione dell'Energia (elettrica, gas, ecc.);
- Le reti di telecomunicazioni;
- I trasporti (merci e passeggeri);
- I servizi di emergenza;
- Le infrastrutture a servizio della Difesa;
- I circuiti bancari e finanziari;
- Il sistema sanitario nazionale;
- I sistemi per il trasporto, distribuzione e trattamento delle Acque;
- I media ed il settore dell'informazione pubblica;
- Le filiere agro-alimentari;
- Le reti governative.

Lo spazio cibernetico

Con il DPCM del 24 Gennaio 2013 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale» si è avviato un percorso di strutturazione della protezione dello "spazio cibernetico" Italiano. Elementi chiave del Decreto sono:

- il Quadro Strategico Nazionale;
- il Piano Nazionale per la protezione cibernetica e la sicurezza informatica.

Il quadro strategico nazionale per la sicurezza dello spazio cibernetico

Indirizzi Strategici

1. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese;
2. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali;
4. Promozione e diffusione della cultura della sicurezza cibernetica;
5. Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica;
6. Rafforzamento delle capacità di contrasto alle attività e contenuti illegali on-line.

Piano Nazionale per la protezione cibernetica e la sicurezza informatica nazionali

Il Piano Nazionale mira a sviluppare gli indirizzi individuati dal Quadro Strategico Nazionale.

Esso non costituisce un mero aggiornamento del precedente Piano, ma si pone l'obiettivo di imprimere un immediato impulso all'ulteriore fase di sviluppo dell'architettura nazionale cyber.

Il Piano prevede undici indirizzi operativi, con obiettivi specifici e conseguenti linee d'azione, così come previsto dal DPCM 17 febbraio 2017, recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". Il Piano Nazionale stabilisce, dunque, la roadmap per l'adozione, da parte dei soggetti pubblici e privati di cui alla Direttiva NIS, delle misure prioritarie per l'implementazione del Quadro Strategico.

indirizzi operativi

1. Potenziamento capacità di intelligence, di polizia e di difesa civile e militare (La protezione cibernetica e la sicurezza informatica nazionali, per essere efficacemente perseguite, presuppongono un'approfondita conoscenza delle vulnerabilità e delle minacce cibernetiche);
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati (l'obiettivo di potenziare il coordinamento e la cooperazione non solo tra i diversi soggetti pubblici, ma anche tra questi e i soggetti privati, considerato che questi ultimi gestiscono le infrastrutture critiche nazionali. l'esigenza di assicurare l'interoperabilità);

indirizzi operativi

3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento (l'esigenza di un'attività di promozione della cultura della sicurezza informatica diretta ad un ampio pubblico, che includa privati cittadini e personale, sia delle imprese che della Pubblica Amministrazione);
4. Cooperazione internazionale ed esercitazioni (Il carattere per definizione transnazionale della minaccia cibernetica e la sua pervasività richiedono un approccio internazionale alla tematica, posto che i singoli Stati devono necessariamente agire sinergicamente per far fronte alla stessa. Ciò presuppone, necessariamente, un comune livello di preparazione e di interoperabilità.);

indirizzi operativi

5. Operatività delle strutture nazionali di incident prevention, response e remediation (sviluppo di Computer Emergency Response Team (CERT) quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e/o privati. La Direttiva NIS prevede la costituzione dei Computer Security Incident Response Team (CSIRT), una nuova tipologia di organismo intesa quale evoluzione dei CERT in grado di assicurare una effettiva capacità di assistenza e supporto attivo alla propria constituency in caso di evento cibernetico. Nelle more del recepimento della direttiva NIS, sarà avviato un processo di progressiva unificazione dei CERT pubblici.);

CSIRT

Il CSIRT italiano sarà istituito presso la Presidenza del Consiglio dei ministri mediante unificazione del Computer Emergency Response Team (CERT) Nazionale e del CERT-PA, assumendone i compiti.

Nelle more della definizione di funzionamento e organizzazione della nuova struttura:

- le funzioni del CSIRT italiano sono svolte dal CERT-N unitamente al CERT-PA, con una ripartizione di ruoli e responsabilità secondo le attuali constituency (Pubblica Amministrazione per il CERT-PA, settore privato per il CERT-N) e con l'introduzione di uno scambio informativo rafforzato e di specifiche procedure di gestione delle notifiche;
- il CERT-N garantisce la cooperazione a livello europeo, anche nell'ambito della rete di CSIRT, in stretto raccordo con il CERT-PA.

indirizzi operativi

6. Interventi legislativi e compliance con obblighi internazionali (La rapida evoluzione tecnologico-informatica comporta un altrettanto veloce obsolescenza delle norme, pertanto, esse necessitano di periodiche revisioni e aggiornamenti);
7. Compliance a standard e protocolli di sicurezza (La compliance a standard e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune ed elevato livello qualitativo nell'assicurare la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti.) ;
8. Supporto allo sviluppo industriale e tecnologico (La garanzia dell'affidabilità e della sicurezza di componenti HW e SW prodotte nell'Unione Europea e nei Paesi terzi rappresenta un obiettivo conseguibile solo se tutti gli attori della catena del valore faranno della sicurezza una priorità.);

indirizzi operativi

9. Comunicazione strategica e operativa (La comunicazione circa un evento cibernetico occorso e le relative conseguenze assume un'importanza strategica, in quanto le singole Amministrazioni interessate ed i soggetti privati gestori di servizi essenziali devono essere in grado di fornire, ove necessario o opportuno, un'informazione completa, corretta, veritiera e trasparente);
10. Risorse (Punto di partenza per un'oculata pianificazione finanziaria e per la ripartizione delle risorse è l'analisi dei costi di eventi cibernetici occorsi o potenziali, in quanto la rilevanza del rischio è direttamente proporzionale alla probabilità ed all'entità del danno.);

indirizzi operativi

11. Implementazione di un sistema di cyber risk management nazionale (La protezione dei dati da minacce che ne pregiudicano l'autenticità, l'integrità, la riservatezza e la disponibilità è parte integrante del presente PN in quanto le informazioni costituiscono un valore intrinseco all'organizzazione, pubblica o privata, e imprescindibile obiettivo di ogni attacco cibernetico.).

Conclusioni

Nelle more delle misure legislative che saranno adottate in occasione del recepimento della direttiva Network and Information Systems (NIS) della UE, è stata operata una razionalizzazione dell'architettura delineata nel 2013 improntata, ad invarianza del quadro normativo primario vigente, alla:

- semplificazione delle procedure ordinarie e straordinarie di gestione delle attività di mantenimento e di implementazione dell'architettura nazionale;
- rimodulazione degli Organi che fanno parte del sistema di protezione cibernetica nazionale (soppressione nel NISP "cyber", revisione del ruolo del NSC, etc.);
- complessiva contrazione della "catena di comando" deputata alla gestione delle crisi, al fine di rendere tempestiva ed efficace l'azione degli organi chiamati a svolgere compiti di response e remediation in caso di eventi cibernetici di rilievo.

La protezione cibernetica e la sicurezza informatica nazionale
Cybersecurity, che cosa cambia con la Direttiva Nis

Cyber security, che cosa cambia con la Direttiva Nis

In questa lezione analizzeremo i seguenti punti:

- Modello del rischio;
- Analisi delle minacce e delle vulnerabilità;
- Trattamento del rischio;
- Direttiva NIS.

Cyber security

La raccolta di strumenti, politiche, concetti di sicurezza, tutele di sicurezza, linee guida, approcci di gestione del rischio, azioni, formazione, best practice e tecnologie che possono essere utilizzate per proteggere l'organizzazione e le risorse dell'utente nell'ambiente cibernetico. Le risorse dell'organizzazione e dell'utente comprendono dispositivi informatici connessi, personale, infrastrutture, applicazioni, servizi, sistemi di telecomunicazione e tutte le informazioni trasmesse o archiviate.

Si intende **l'insieme dei mezzi e delle tecnologie** volti alla **protezione** dei sistemi informatici in termini **di disponibilità, confidenzialità e integrità dei beni o asset informatici**

Risk management

Il **cyber security risk management** è un processo continuo e dinamico, da cui desumere le azioni da implementare per la gestione del rischio in modo consapevole, adeguato agli asset da proteggere e in linea con i mutamenti organizzativi, ambientali e tecnologici che coinvolgono l'azienda internamente ed esternamente.

La **gestione del rischio** consiste **nell'applicazione sistematica** di **politiche di gestione, procedure**, azioni, al compito di **identificare, analizzare, valutare, mitigare e controllare il rischio.**

L'obiettivo della gestione del rischio è quello di identificare, quantificare e gestire i rischi di sicurezza delle informazioni allo scopo di perseguire gli obiettivi di business dell'organizzazione applicando opportune metodologie e tecniche.

Il risk management è il processo con cui si assicura che gli impatti dovuti a minacce insistenti su vulnerabilità dei sistemi e dei processi rimangano all'interno di limiti accettabili e con costi accettabili

Attività

- Sviluppare un processo di gestione del rischio sistematico, analitico e continuo;
- Assicurare che le attività di identificazione, analisi e mitigazione dei rischi siano integrate nel ciclo di vita dei processi;
- Applicare metodi formalizzati per l'identificazione e l'analisi dei rischi;
- Definire strategie e prioritizzare le opzioni per la mitigazione dei rischi a livelli accettabili per l'azienda;
- Riportare ogni cambiamento significativo nei rischi agli appropriati livelli manageriali, sia su base periodica che secondo necessità.

Definizioni

Asset → qualunque cosa, materiale o immateriale, abbia valore all'interno dell'organizzazione:

- Persone;
- Beni materiali, mobili o immobili;
- Software;
- Informazioni, know-how;
- Reputazione.

Vulnerabilità → caratteristica intrinseca di un sistema o di un processo che, in particolari condizioni, può provocare o facilitare (o essere utilizzata per provocare o facilitare) il verificarsi di eventi indesiderati per l'organizzazione e/o comportare danni o perdite per l'organizzazione stessa

Definizioni

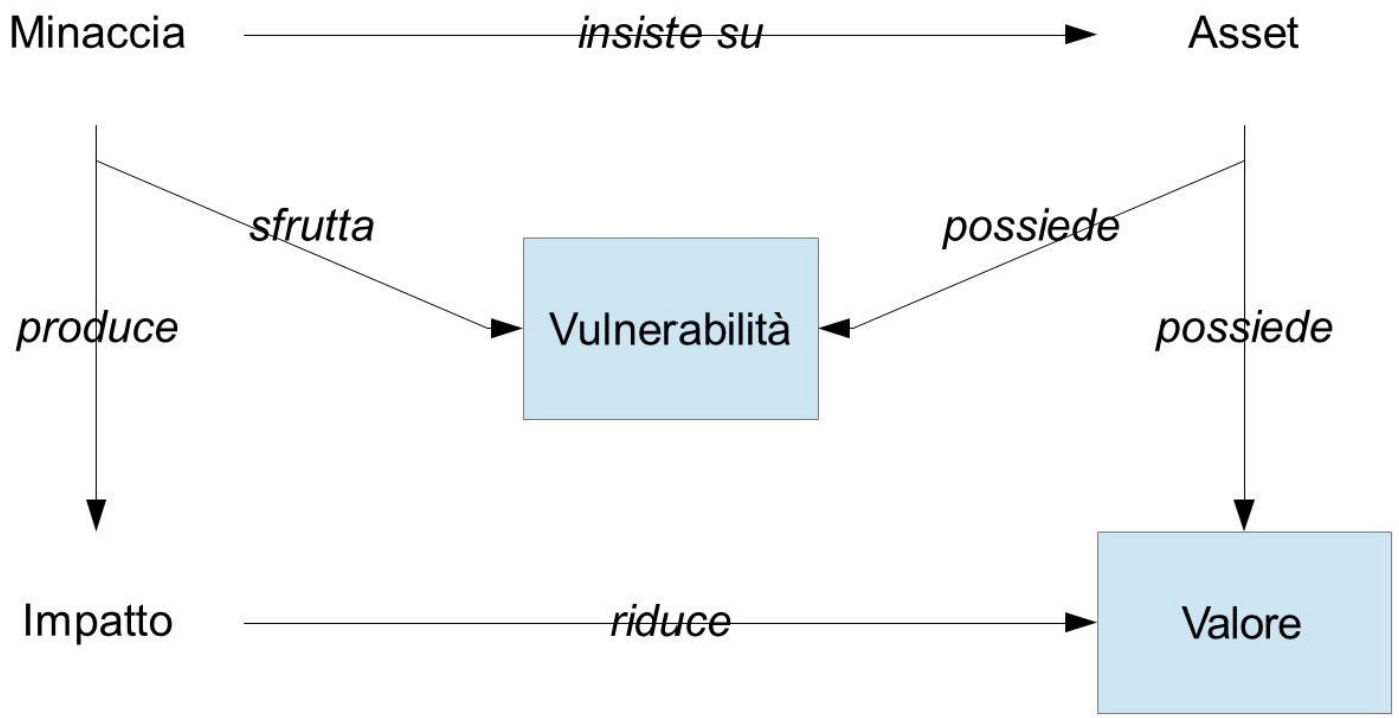
Minaccia → evento potenziale che, se attuato, comporta conseguenze indesiderate per l'organizzazione e/o danni o perdite per l'organizzazione.

Agente di minaccia → entità in grado di attuare una possibile minaccia, deliberatamente o meno.

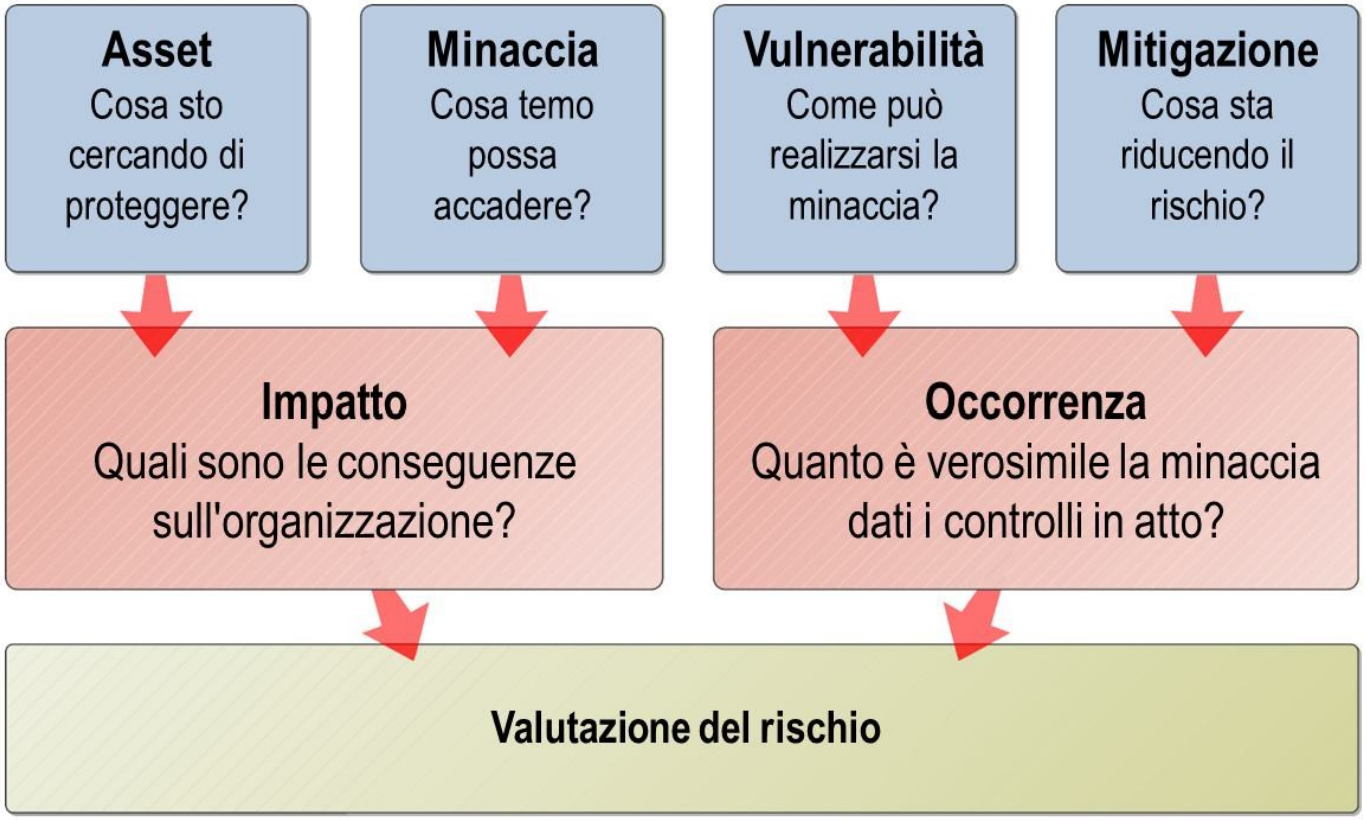
Rischio → la probabilità che una minaccia si attui sfruttando una vulnerabilità.

Impatto → la conseguenza indesiderata cui andrebbe soggetta l'organizzazione in seguito al verificarsi di un rischio.

Modello del rischio



Modello di valutazione del rischio



Come classificare i rischi?

- **Valore strategico dei processi informativi:**
  reputazione, perdita di clienti, fallimento di piani e deadline.

- **Perdite economiche dirette:**
  costi operativi aggiuntivi, mancati guadagni, perdite una tantum (sostituzione beni).

- **Perdite di produttività:**
  ore personale aggiuntive, spreco di risorse.

Definizioni

- **Aspetti legati alla safety:**
  perdite di vite umane, danni alla salute
- **Aspetti legali:**
  violazione di norme (multe) e contratti (cause)
- **Classificazione dei beni coinvolti:**
  tipologia, criticità, proprietà di sicurezza coinvolte (riservatezza, integrità, disponibilità, ...)

Analisi qualitativa o quantitativa

- **Alcuni impatti sono direttamente ed oggettivamente quantificabili in termini di:**
  - perdita di guadagni
  - costi di riparazione
  - lavoro necessario a correggere i problemi

- **Altri invece sono misurabili solo in termini qualitativi (es. impatto alto/medio/basso):**
  - perdita di credibilità
  - danni agli interessi di un'organizzazione
  - violazioni di segretezza

Analisi qualitativa o quantitativa

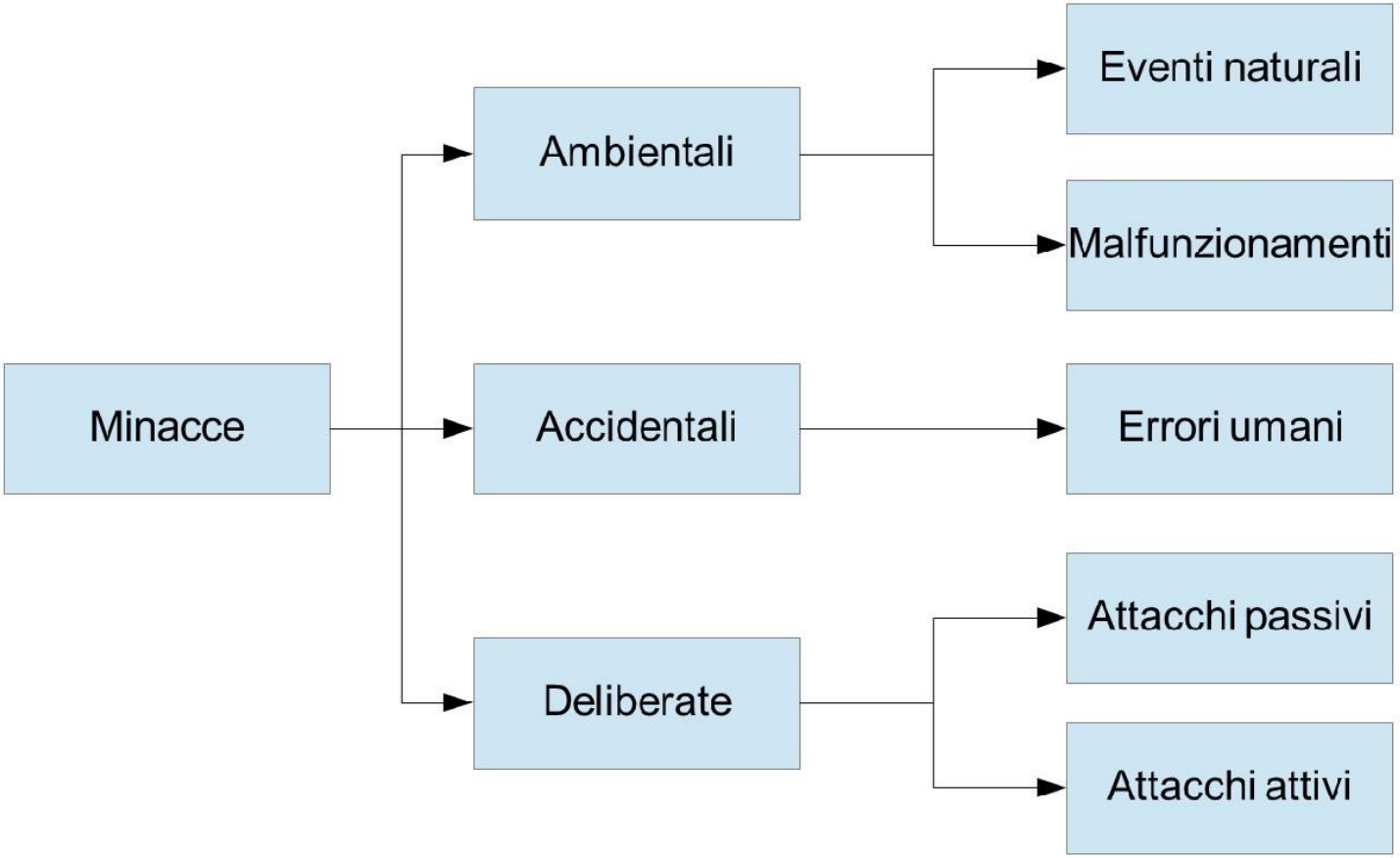
Approcci	Vantaggi	Svantaggi
Quantitativo	• Rischi prioritizzati secondo il loro impatto economico; asset secondo il loro valore economico • I risultati facilitano la gestione in termini di "ritorno sull'investimento" • I risultati sono espressi in termini comprensibili al management	• I valori degli impatti assegnati ai rischi si basano su opinioni soggettive degli intervistati • Può richiedere molto tempo • Può essere molto costoso • Non tutti i valori sono misurabili
Qualitativo	• Migliore comprensione della relativa importanza dei vari rischi • È più facile raggiungere il consenso • Non è necessario quantificare la frequenza delle minacce • Non è necessario determinare il valore economico degli asset	• Granularità insufficiente fra rischi importanti • Difficile giustificare investimenti in controlli in mancanza di un'analisi costi-benefici • Risultati dipendenti dalla qualità del team di analisi

Analisi e classificazione delle minacce

- **Per valutare correttamente i rischi è essenziale effettuare una completa ed esaustiva analisi delle minacce che insistono sugli asset presenti nel perimetro considerato.**

- **Le minacce vanno:**
  - identificate
  - classificate
  - quantificate in termini di “aggressività”.

Tipologia di minacce



Minacce alla sicurezza informatica

- perdita di confidenzialità (*confidentiality*)
- perdita di integrità (*integrity*)
- perdita di disponibilità (*availability*)
- perdita di tracciabilità (*accountability*)
- perdita di autenticità (*authenticity*)
- perdita di affidabilità (*reliability, dependability, survivability, assurance, resiliency, trustwothiness*)

Analisi delle vulnerabilità

Per valutare correttamente i rischi è inoltre essenziale effettuare un'analisi il più possibile completa ed esaustiva delle vulnerabilità, reali o presumibili, che affliggono gli asset presenti nel perimetro considerato.

Anche le vulnerabilità vanno:

- identificate
- classificate
- quantificate in termini di pericolosità

Analisi delle vulnerabilità

Sono dovute a difetti nella:

- progettazione
- implementazione
- configurazione
- gestione operativa

di parti o componenti del sistema informativo che rendono possibile il concretizzarsi di una o più minacce.

Trattamento del rischio

- **rifiuto** (avoidance): evitare il rischio eliminando causa e/o conseguenze della minaccia/vulnerabilità (es. eliminare funzioni o parti del sistema, rinunciare ad un'attività)
- **trasferimento** (transfer): trasferire il rischio a terze parti (es. assicurazioni, outsourcing)
- **riduzione** (reduction): limitare il rischio implementando controlli aggiuntivi che riducono/eliminano la minaccia o la vulnerabilità e/o ne limitano l'impatto
- **accettazione** (retention): accettare il rischio potenziale e le sue conseguenze

Rischio residuo

Il **rischio residuo** è quello che rimane dopo la fase di trattamento del rischio (adozione delle contromisure).

Se il rischio residuo è minore del livello di rischio accettabile stabilito a priori il processo termina con successo, altrimenti viene iterato nuovamente e si ripete finché necessario

Direttiva NIS

La **Direttiva (UE) 2016/1148** del 6 luglio 2016 recante **le misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione** ha come obiettivo quello di raggiungere un elevato livello di sicurezza dei sistemi, delle reti e delle infrastrutture comuni agli Stati membri.

La Direttiva NIS :

1. Impone a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;
2. Istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi;
3. Crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace.

Direttiva NIS

Ogni Stato membro dovrà:

- **Disporre di una strategia nazionale** in materia di sicurezza della rete e dei sistemi informativi che definisca gli obiettivi strategici e gli interventi strategici concreti da attuare;
- **Individuare più di un'autorità nazionale** competente responsabile di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi degli operatori di servizi essenziali e dei fornitori di servizi digitali;
- **assicurare la disponibilità di CSIRT** ben funzionanti e rispondenti a determinati requisiti essenziali, in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione;
- **Prevedere una cooperazione internazionale** più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti della sicurezza.

Attuazione NIS

Con il **Decreto Legislativo 18 maggio 2018, n.65**, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, alla NIS, **intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi**.

Il decreto si applica agli **Operatori di Servizi Essenziali** (OSE) e ai **Fornitori di Servizi Digitali** (FSD).

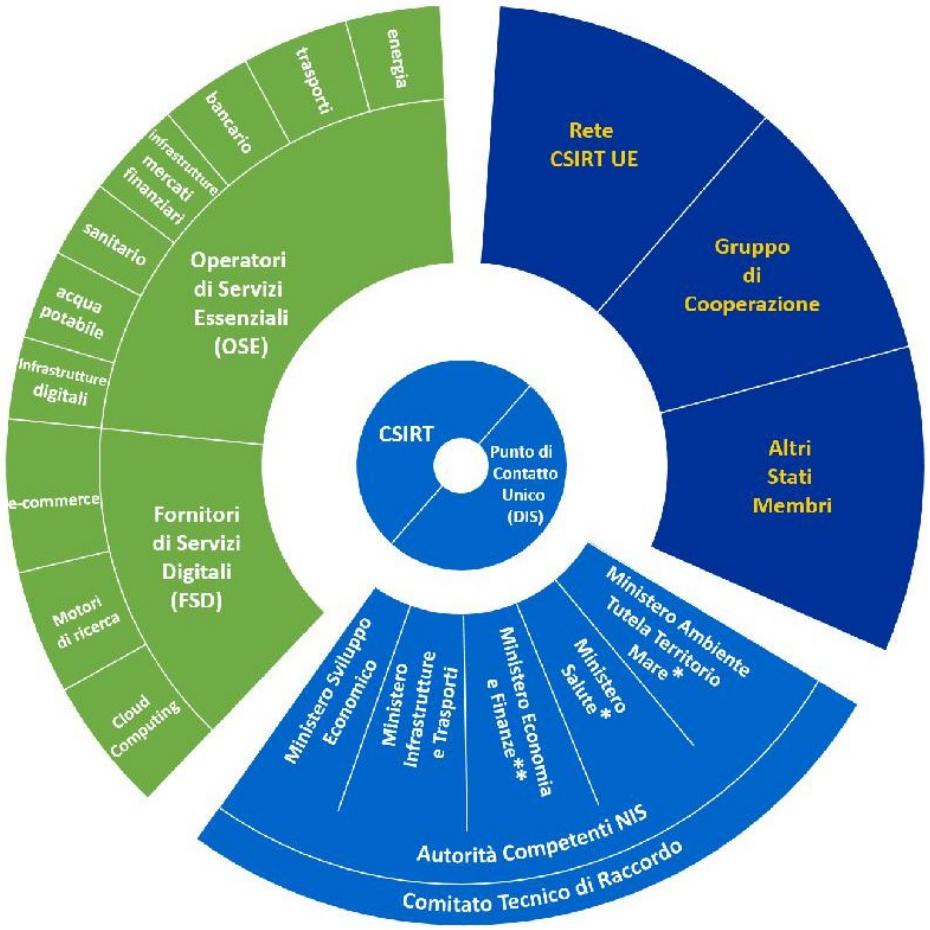
L'elenco nazionale degli OSE è istituito presso il Ministero dello sviluppo economico e viene aggiornato, almeno ogni due anni, a cura delle Autorità competenti NIS.

OSE e FSD

Gli OSE sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

Gli FSD sono le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle imprese che la normativa europea definisce "piccole" e "micro", quelle cioè che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro.

Panoramica



Servizi interessati

Attori governativi NIS

Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

Obblighi OSE e FSD

Tanto gli OSE che gli FSD:

- sono chiamati ad **adottare misure tecniche e organizzative** adeguate e proporzionate alla **gestione dei rischi** e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l'obbligo di **notificare**, senza ingiustificato ritardo, **gli incidenti che hanno un impatto rilevante,** rispettivamente sulla continuità e sulla fornitura del servizio, al Computer Security Incident Response Team (**CSIRT**) italiano, **informandone anche l'Autorità competente NIS di riferimento**.
- soggetti giuridici non identificati come OSE e che non sono FSD possono inoltrare al CSIRT notifiche volontarie degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati.

CSIRT

Il Computer Security Incident Response Team (CSIRT) italiano:

definisce le procedure per la prevenzione e la gestione degli incidenti informatici;

- **riceve le notifiche di incidente**, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica;
- **fornisce** al soggetto che ha effettuato la notifica le **informazioni** che possono **facilitare la gestione** efficace dell'evento;
- **informa gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente,** tutelando la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite;
- **garantisce la collaborazione nella rete di CSIRT**, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di best practices.

Incidenti

Un incidente a carico di un FSD è rilevante se si verifica almeno una delle seguenti condizioni
Indisponibilità del servizio fornito per oltre 5.000.000 di ore utente
Perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE
Rischio per la sicurezza e/o l'incolumità pubblica, o in termini di perdite di vite umane
Danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'UE

Grazie

Vincenzo Calabrò

www.vincenzocalabro.it