DIGITALCAMPUS
guidiamo l'innovazione

CSI
your digital partner

Corso NIS2 Mastering Compliance per Organi di Amministrazione e Direttivi

Enzo Veiluva – Cybersecurity e Business Continuity

11 giugno 2026

ASL AL
REGIONE PIEMONTE

Obiettivi del corso

- Comprendere l’importanza di adottare una strategia basata sull’analisi dei rischi e l’adozione di misure Cyber.
- Comprendere il contesto , motivazioni e obblighi alla base della Direttiva NIS2.
- Identificare e gestire le responsabilità di governance e supervisione legate alla sicurezza delle reti e dei sistemi informativi.
- Sviluppare strategie per l'implementazione di misure tecniche e organizzative adeguate per la gestione del rischio cyber.
- Approfondire le procedure di segnalazione degli incidenti e le responsabilità dei soggetti in perimetro.
- Valutare gli aspetti sanzionatori previsti dalla Direttiva.

Contenuti – Modulo 1

A) Conoscenze manageriali di base: Inquadramento del rischio Cyber, minacce e vulnerabilità

1. Il contesto odierno: Cyberspazio e Cybersecurity
2. La direttiva NIS 2: Figure chiave e responsabilità degli organi Direttivi
3. Le Competenze degli organi Direttivi

3a - l'evoluzione del rischio Cyber

- Qualche dato (il rapporto CLUSIT).
- I problemi ed i rischi nelle aziende e negli Enti Pubblici
- Quanto può costare alla mia azienda/Ente un attacco informatico

3b Vulnerabilità e tecniche di attacco

- Le principali vulnerabilità delle infrastrutture IT
- Gli attacchi interni ed esterni
- Misure tecniche ed organizzative

3c Il fattore umano

- L'errore umano come prima causa (fattore abilitante) di attacco Cyber
- Social Engineering: mezzo di attacco sempre più usato
- Gli attacchi attraverso la posta elettronica e cellulare: phishing/smishing
- I deepfake ed attacchi con l'IA
- Gli attacchi al CEO

1 Il contesto odierno: Cyberspazio e Cybersecurity

Mobilità PRESS AGENCY

NEWS VIDEO

Cyber: circa 60 gli attacchi informatici significativi al comparto trasporti nel 2024

Studio rileva un aumento annuo del 48%; nel settore aereo i danni possono superare i 580.000 Euro

Negli ultimi cinque anni il settore dei trasporti ha registrato un'escalation senza precedenti degli attacchi informatici. Secondo il nuovo report pubblicato dal Cyber Defense Center di Maticmind, nel 2024 si sono verificati quasi 60 attacchi significativi, rispetto ai 12 del 2020, con un tasso di crescita medio annuo del 48%. Il ransomware si conferma la minaccia principale (38% degli attacchi), seguito da DDoS (24%) e phishing (18%).

"Il settore dei trasporti sta vivendo un'escalation preoccupante di attacchi informatici. La digitalizzazione ha portato molti vantaggi, ma ha esposto il settore a rischi cyber anche di grandi portate. La protezione delle infrastrutture critiche richiede un cambio di paradigma: non basta più una difesa passiva, ma è essenziale adottare un approccio proattivo basato sul rischio e sull'adozione di soluzioni adeguate non solo per fronteggiare, ma per prevenire attacchi cyber, investendo in modo significativo nella protezione dei dati, delle infrastrutture e nei sistemi di sicurezza ", commenta Lorenzo Forina, ceo di Maticmind Group. "La cybersicurezza deve essere una priorità strategica fondamentale per la protezione dell'intero ecosistema aziendale"

Nel 2024, il 25% degli attacchi globali al settore trasporti ha avuto come obiettivo aziende italiane, che rappresentano da sole il 7,3% degli incidenti totali. Nonostante una crescita degli investimenti del 25% (contro il 15% della media nazionale), l'Italia resta fanalino di coda nel G7 per quota di spesa in cybersecurity rispetto al Pil (0,14%) e spende meno della media europea in percentuale sul budget IT (0,8% contro 1,5%). Il 53,8% delle aziende italiane del settore ha pianificato ulteriori investimenti nel biennio 2025-2026

SECURITYINFO
IL PUNTO DI RIFERIMENTO PER LA SICUREZZA IT IN ITALIA

NEWS RECENTI ı per l'Italia ■ Un dipendente ha venduto le proprie credenziali per un colpo da 120 milioni di eur

NEWS APPROFONDIMENTI OPINIONI TOP MALWARE MINACCE GUIDE ALLA SICUREZZA PODCAST STR

Le reti elettriche sono armi potenti al servizio dei cybercriminali

Mar 03, 2025 Marina Londei Approfondimenti, Attacchi, Attacchi, Campagne malware, Hacking, In evidenza, News 0

Negli ultimi anni gli **attacchi contro le reti elettriche si sono moltiplicati**, ma non le misure di sicurezza per proteggerle: hackerare pannelli solari e le cosiddette "smart grid" non è affatto difficile, per lo più a causa di errori degli utenti.

Quotidiano Nazionale • Tech • **Trasporti in tilt, internet do...**

Per continuare, goo
email e immagine de
sulla privacy e i tern

Trasporti in tilt, internet down e persino l'acqua a rischio. Così gli Usa potrebbero crollare sotto un attacco informatico

Ecco l'avvertimento della ex consigliera della National Security Agency (NSA): troppi tagli e tecnologi obsolete. "Non dobbiamo chiederci se succederà, ma quando"

I pericoli di un attacco informatico negli Stati Uniti

CHIARA CRESCENZI SECURITY 21.05.2024

L'acqua potabile nel mirino dei cybercriminali russi, cinesi e iraniani

I criminali informatici attaccano sempre più i sistemi idrici degli Stati Uniti

MENU

Regione del Veneto
Il portale della Regione del Veneto

Home page | la Regione | Servizi

> Attacco informatico ai siti della Regione del Veneto. Presidente Zaia, "Seguiamo con attenzione l'evolversi della situazione. Nessuna violazione segnalata di dati sensibili"

24 febbraio 2025

Comunicato n° 314

(AVN) – Venezia 24 febbraio 2025

TGCOM24 ULTIM'ORA CRONACA MONDO TV & SPETTACOLO DOSSIER

CRONACA | Abruzzo Basilicata Calabria Campania Emilia Romagna Friuli Venezia

OPERA DEL GRUPPO FILORUSSO "NONAME057(16)"

Cybersicurezza, nuovo attacco hacker: nel mirino Comuni e Regione Puglia

LE SANZIONI

Attacco Regione Lazio, il Garante Privacy conferma i gravi errori

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti > Ransomware

le sanzioni del Garante per i fatti cyber accaduti in pieno periodo anti Covid, a servizio sanitario di Regione Lazio. Un attacco are dagli impatti gravi e importanti per i cittadini che trovarono bilità delle strutture sensibili per giorni

.0 apr 2024

sec, fondatore Insicur

GENOVATODAY

braio 2025 14:15

la di

er

ne

stesso argomento

CRONACA

Nuovo attacco degli hacker russi: preso di mira il sito della Regione

L'ente ha spiegato che i disservizi sono durati pochi minuti, nei giorni scorsi attacco al sito sito dell'Autorità Portuale del Mar Ligure Occidentale per il quale è stata aperta un'inchiesta

INFORMATICA

Attacchi hacker: anche la Regione Emilia Romagna nel mirino dei filorussi

Gli hacker filorussi colpiscono il sito della Regione Emilia Romagna e altre istituzioni italiane con attacchi DDoS

ENZO VANNELLI
redazione@bolognacronaca.it

24 FEBBRAIO 2025 - 13:08

I casi ancora più gravi in sanità

SANITÀ SOTTO ATTACCO

Ransomware colpisce tre Asl di Modena: c'è la rivendicazione del gruppo Hunters, primi dati rubati online

SANITÀ SOTTO ATTACCO

Attacco all'Azienda Ospedaliera di Verona: dati in vendita, ma quelli sanitari sono una minima parte

MISURE D'URGENZA

Ospedali londinesi messi in ginocchio da un ransomware: cosa impariamo

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti > Ransomw

Sono diversi gli ospedali londinesi interessanti dall'attacco ransomwa in tutto, sono stati cancellati 800 interventi chirurgici. Notizie simili costringono a rivedere l'idea stessa di cyber security

Pubblicato il 4 lug 2024

RANSOMWARE

ASL di Torino colpita da attacco informatico, molti disagi per i pazienti

Home > Malware E Attacchi Hacker: Come Affrontare La Sicurez:

Sanità pubblica nuovamente sotto attacco informatico, si assiste alle difficoltà trascorse in questi giorni dalla Asl Città di Torino colpita da quello che potrebbe essere un tipico attacco ransomware. Computer degli ospedali bloccati, compare una nota di riscatto e le indagini proseguono

Pubblicato il 24 Ago 2022

RANSOMWARE

Attacco all'ASST Rhodense, online 1 TB di dati: c'è la rivendicazione del ransomware Cicada3301

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

I dati personali dei pazienti dell'ASST Rhodense sono stati pubblicati online e sono ora liberamente scaricabili. La rivendicazione è del gruppo ransomware Cicada3301. Ecco le implicazioni e le misure che servono per impedire che attacchi del genere si verifichino di nuovo

Pubblicato il 21 giu 2024

RANSOMWARE

Attacco al sistema sanitario lucano: unità di crisi attivata su ASP Basilicata

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

L’evoluzione del perimetro DI SICUREZZA…

Fino a qualche anno fa il perimetro di difesa era circoscritto

Ora invece lo scenario di accesso ai dati è cambiato!!!

I nuovi rischi nel contesto Cyber

Cloud

L'utilizzo del cloud introduce rischi di violazioni dei dati, in particolare attraverso configurazioni errate e accessi non autorizzati. Inoltre, il cloud è vulnerabile ad attacchi DoS e alla compromissione di credenziali da parte di cybercriminali.

Intelligenza Artificiale (AI)

L'AI può essere manipolata tramite attacchi adversarial, che alterano i dati per influenzare i modelli. Altri rischi includono la compromissione dei dati sensibili utilizzati per l'addestramento e la diffusione di bias nei sistemi decisionali.

Smart Working

Il lavoro remoto espone le reti aziendali a rischi di phishing, malware e accessi non autorizzati, soprattutto se i dispositivi personali non sono adeguatamente protetti o connessi a reti insicure.

I nuovi rischi nel contesto Cyber

Supply Chain

La supply chain è vulnerabile ad attacchi mirati contro fornitori terzi, che possono agire come punto di ingresso per malware. La mancanza di trasparenza nei processi aumenta i rischi di sabotaggi e compromissioni.

Internet of Things (IoT)

I dispositivi IoT sono spesso caratterizzati da scarsa sicurezza e sono bersagli facili per attacchi DDoS, manipolazione dei dati o violazione della privacy. La connessione a reti principali amplifica il rischio di infiltrazioni.

Social Network

I social network sono un terreno fertile per attacchi di ingegneria sociale, furto di identità e diffusione di malware tramite link malevoli. Inoltre, la raccolta e l'uso improprio di dati personali rappresentano un rischio significativo.

2.La direttiva NIS 2: Responsabilità degli organi Amministrativi e Direttivi

La Direttiva NIS2

Dal 16 ottobre 2024 è in vigore la nuova normativa Network and Information Security (direttiva NIS) di derivazione europea.

Il recepimento della direttiva con il decreto legislativo del 4 settembre 2024, n. 138 (decreto NIS: apre un link esterno), mira a garantire l'aumento del livello di sicurezza informatica del tessuto produttivo e delle Pubbliche Amministrazioni del Paese, in armonia con gli altri Stati membri dell'Unione Europea.

L'Agenzia per la cybersicurezza nazionale è l'Autorità competente NIS.

I Soggetti NIS2

Impatti sulla PA Italiana

Enti coinvolti a Livello Nazionale

Oltre le PA centrali , oggi sono circa una trentina i Comuni Italiani che saranno coinvolti dall'impatto della NIS 2, a cui si sommano le 20 Regioni e oltre 200 ASR e ASO

Ma le indicazioni della direttiva e le misure di sicurezza che dovranno essere attuate possono diventare degli elementi di analisi molto importanti per tutte le varie realtà, soprattutto perchè quanto definito dalla NIS 2 rappresenterà un modello di riferimento

IL CONFRONTO

NIS2, perché Italia, Francia e Germania seguono strade diverse

Home

Partecipa al dibattito

La Direttiva NIS2 nasce con obiettivi comuni, ma Italia, Francia e Germania la stanno applicando con logiche diverse. Il confronto mostra un modello italiano più amministrativo, uno francese più metodologico e uno tedesco più documentale, con effetti concreti su registrazione, misure, reporting e responsabilità

Pubblicato il 8 giu 2026

Marcello Filacchioni
ICT CISO e Cyber Security Manager

Paese	Modello prevalente	Autorità	Caratteristica dominante
Italia	Amministrativo-procedurale	ACN	Portale, elenchi, categorizzazioni, fornitori rilevanti
Francia	Dottrinale e di accompagnamento	ANSSI	Référentiel, autovalutazione, resilienza nazionale
Germania	Tecnico-industriale e documentale	BSI	Evidenze, obblighi tracciabili, responsabilità manageriale

FONTE: https://www.agendadigitale.eu/sicurezza/nis2-perche-italia-francia-e-germania-seguono-strade-diverse/

Ambito di applicazione nella PA

Nell'ambito della Pubblica amministrazione i Settori individuati includono:

1. **pubbliche amministrazioni centrali** incluse nell'elenco annuale ISTAT delle PA, previsto dall'art. 1, c. 3, della L. 196/2009
2. **regioni e province autonome di Trento e di Bolzano**
3. **città metropolitane**
4. **comuni con popolazione superiore a 100.000 abitanti e comunque i comuni capoluoghi di regione**
5. società di **trasporto pubblico urbano** con bacino di utenza non inferiore a 100.000 abitanti
6. società di **trasporto pubblico extraurbano** operanti nell'ambito delle città metropolitane
7. **aziende sanitarie locali**
8. **società in house degli** enti richiamati che siano fornitrici di servizi informatici, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali ovvero servizi di gestione dei rifiuti.

Il ruolo di ACN

Agenzia per la Cybersicurezza Nazionale
https://www.acn.gov.it/

L'**Agenzia per la Cybersicurezza Nazionale (ACN)** svolge un ruolo centrale e strategico nell'attuazione della Direttiva NIS2 in Italia, in quanto **autorità nazionale competente per la cybersicurezza**. La sua funzione è definita dal **Decreto Legislativo 4 settembre 2024, n. 138**, che ha recepito la Direttiva (UE) 2022/2555 (NIS2) nell'ordinamento italiano.

Il ruolo di ACN

Agenzia per la Cybersicurezza Nazionale
https://www.acn.gov.it/

Applicazione della Direttiva NIS2: elementi principali

1. la registrazione e l'aggiornamento delle informazioni (articolo 7);
2. **responsabilizzazione degli organi di amministrazione e direttivi (articolo 23);**
3. **gli obblighi in materia di misure di sicurezza informatica (articolo 24);**
4. **gli obblighi in materia di notifica di incidente (articolo 25);**
5. per alcune tipologie di soggetti, gli obblighi in materia di banca dei dati di registrazione dei nomi di dominio (articolo 29);
6. la categorizzazione delle attività e dei servizi (articolo 30).

Ovvero in sintesi

- **Formazione**
- **Gestione del rischio e prevenzione**
- **Obblighi di comunicazione: incidenti, flussi e dati**
- **Continuità del business**

Organi di Amministrazione e Direttivi

Sono individuate precise responsabilità in capo agli organi di amministrazione del soggetto, i quali approvano e sovraintendono all'implementazione delle misure oltre a essere responsabili delle eventuali violazioni.

ART. 23..
(Organi di amministrazione e direttivi)

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti:

   a) **approvano le modalità di implementazione** delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;
   b) **sovrintendono all'implementazione** degli obblighi di cui al presente capo e di cui all'articolo 7;
   c) **sono responsabili delle violazioni** di cui al presente decreto.

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti:

   a) sono tenuti a **seguire una formazione** in materia di sicurezza informatica;
   b) promuovono l'offerta periodica di una **formazione coerente** a quella di cui alla lettera a) **ai loro dipendenti**, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di **individuare i rischi e valutare le pratiche di gestione dei rischi** per la sicurezza informatica e **il loro impatto** sulle attività del soggetto e sui servizi

La Direttiva NIS2 – Focus Obblighi di base D.LGS 138/2024

Art. 25 – Obblighi in materia di notifica di incidente

I soggetti essenziali e i soggetti importanti devono notificare, senza ingiustificato ritardo, allo CSIRT **ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi**.

- senza ingiustificato ritardo, e comunque **entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo**, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli oppure possa avere un impatto transfrontaliero;

- senza ingiustificato ritardo, e comunque **entro 72 ore** (24 ore nel caso di un prestatore di servizi fiduciari) **da quando sono venuti a conoscenza dell'incidente significativo**, **una notifica dell'incidente** che, ove possibile, aggiorni le informazioni già trasmesse nella pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

- una **relazione finale entro un mese** dalla trasmissione della notifica di incidente.

Direttiva NIS2: sanzioni

Il trattamento sanzionatorio viene differenziato in base al tipo di violazione e alla qualifica del soggetto. In particolare, la violazione dei seguenti obblighi è sanzionata, in caso di soggetti essenziali:

- l'inosservanza degli obblighi imposti agli organi di amministrazione;
- la mancata implementazione delle misure tecniche, organizzative ed operative;
- l'assenza di notifica.

Per i soggetti Privati:

fino a 10 milioni o fino al 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, o, in caso di soggetti importanti, **fino a 7 milioni o fino al 1,4% del totale del fatturato mondiale:**

Per le pubbliche amministrazioni

sanzioni amministrative pecuniarie variano da **25.000 a 125.000** €.

Direttiva NIS2: sanzioni

Una novità introdotta dal Decreto Legislativo è la previsione di un minimo edittale delle sanzioni che è un ventesimo o di un trentesimo del massimo edittale rispettivamente per i soggetti essenziali e quelli importanti.

È prevista una sanzione fino al 0,1% o fino allo 0,07% del fatturato mondiale annuo per le violazioni considerate meno gravi, ossia:

- la mancata registrazione, comunicazione o aggiornamento delle informazioni sulla piattaforma dell'ACN;
- l'inosservanza delle modalità stabilite da ACN per la registrazione, comunicazione o aggiornamento dei dati;
- la mancata comunicazione o aggiornamento dell'elenco delle attività e servizi ai fini della loro categorizzazione;
- la mancata attuazione degli obblighi relativi agli schemi di certificazione;
- la mancata collaborazione con l'ACN nello svolgimento dei suoi compiti e nell'esercizio dei suoi poteri;
- la mancata collaborazione con il CSIRT Italia.
- In caso di reiterazione delle violazioni, le sanzioni possono essere aumentate fino al triplo.

Direttiva NIS2: sanzioni

Al di là delle sanzioni amministrative pecuniarie di cui può essere destinatario l'ente, il decreto di recepimento della Direttiva NIS 2 introduce sanzioni accessorie anche per:

- gli organi di amministrazione;
- le persone fisiche responsabili di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso;
- l'amministratore delegato;
- i legali rappresentanti del soggetto essenziale o importante.

Essi non potranno svolgere funzioni dirigenziali all'interno dell'ente, finché lo stesso non avrà adottato le **misure necessarie a porre rimedio alle carenze riscontrate dall'Agenzia per la Cybersicurezza Nazionale**, o finché non si sarà conformato alle prescrizioni indicate dalla stessa.

ART. 38 Commi 5,6 e 7

5 Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di **suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso**, assicura il rispetto delle disposizioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza.

6. Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, l'Autorità nazionale competente NIS può disporre nei confronti delle persone fisiche di cui al comma 5 del presente articolo, i**vi inclusi gli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante,** l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Tale **sospensione temporanea** è applicata finchè il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7.

7. Ai **dipendenti pubblici che esercitano i poteri di cui al comma 5**, si applicano le norme in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati. In particolare, la violazione degli obblighi di cui al presente decreto può costituire causa di responsabilità dirigenziale, disciplinare e amministrativo-contabile.

Circolare ASSONIME sulle responsabilità degli organi Direttivi

Cybersicurezza, impresa, hacker

Amministratori revocabili se non blindano la cybersicurezza delle imprese

Circolare di Assonime: scatta la responsabilità del manager per i danni a patrimonio e creditori frutto di attacchi in
Ecco quali misure vanno obbligatoriamente adottate

di Antonio Ciccia Messina 04/11/2025 | Aggiornato il 05/11/2025 10:26

Gli amministratori revocabili se non blindano la cybersicurezza delle imprese sono anche personalmente responsabili per i danni al patrimonio sociale e ai creditori conseguenti a un attacco informatico non fronteggiato a dovere. È quanto illustrato da Assonime, l'associazione delle imprese, con la circolare n. 23 del 4/11/2025, dedicata all'illustrazione del D.Lgs. 138/2024, che ha

Gli incidenti sono sempre più a rischio risarcimento per gli interessati

FEDERPRIVACY

Area Riservata

HOME | ASSOCIAZIONE | ATTIVITÀ | INFORMAZIONE | STRUMENTI | COMMUNI

NEWS > Data Breach in aumento del 22%

Home > Informazione > Privacy & Società > Attacco hacker alla Asl dell'Aquila, alcune delle vittime chiedono maxi

Tweet | Condividi | Condividi | Condividi

Attacco hacker alla Asl dell'Aquila, alcune delle vittime chiedono maxi risarcimento danni di 2,5 milioni di euro

Privacy & Società Mercoledì, 17 Dicembre 2025 18:18

Un maxi risarcimento da 2,5 milioni di euro. È questo il contenuto della diffida stragiudiziale presentata contro la Asl 1 abruzzese dagli avvocati Marco Colantoni, del foro dell'Aquila, e Pier Luigi D'Amore, del foro di Avezzano.

L'oggetto della controversia: la violazione dei dati personali di oltre 10mila persone tra pazienti, dipendenti e consulenti dell'azienda sanitaria locale, avvenuta a maggio 2023.

Responsabilità degli Organi di Amministrazione e Direttivi

Il decreto legislativo 138/2024 di recepimento della Direttiva NIS 2 precisa che a essere **responsabile della corretta implementazione della normativa** in questione **è qualsiasi persona fisica che sia in qualche modo responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni o di esercitare un controllo sul soggetto stesso**

Articolo 16
(Elencazione degli organi di amministrazione e direttivi)

1. *Ai fini dell'articolo 15, comma 3, lettera b), tramite il Servizio NIS/Aggiornamento annuale, gli utenti elencano i codici fiscali delle persone fisiche che compongono gli organi di amministrazione e direttivi, indicandone l'indirizzo di posta elettronica certificata.*
2. *Le informazioni di cui al comma 1 sono confermate dal punto di contatto.*
3. *Al fini dell'articolo 7, comma 4, lettera c), del decreto NIS, le persone fisiche appartenenti agli organi di amministrazione e direttivi del soggetto NIS accettano tale indicazione*

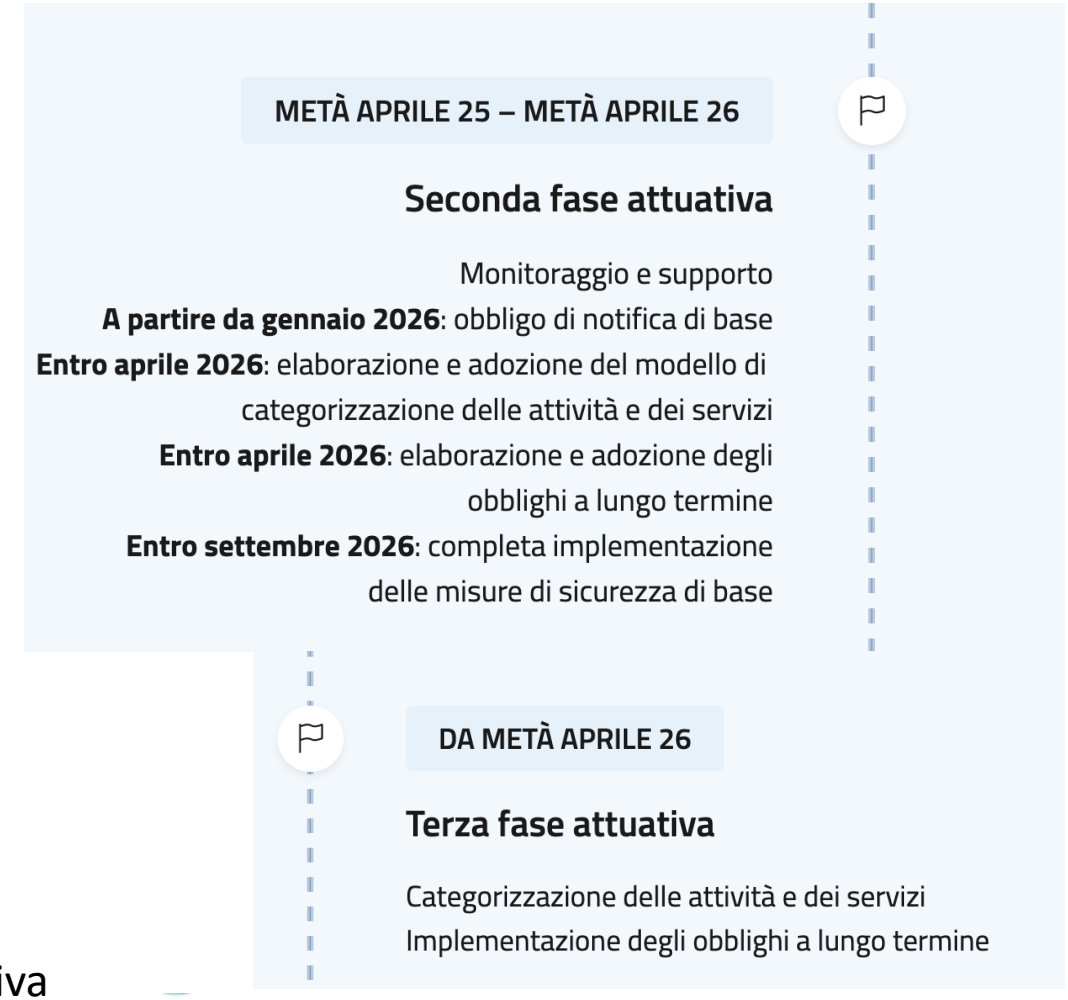
La Direttiva NIS2 – Scadenze

1. La registrazione e l'aggiornamento delle informazioni (articolo 7); **(28 FEB e 31* MAG di ogni anno)**
2. responsabilizzazione degli organi di amministrazione e direttivi (articolo 23); **(30 SET 26)**
3. gli obblighi in materia di misure di sicurezza informatica (articolo 24); **(30 SET 26)**
4. gli obblighi in materia di notifica di incidente (articolo 25); **(Obbligo dal 1/1/26)**
5. **Nomina del referente CSIRT (entro il 31/12/2025)**

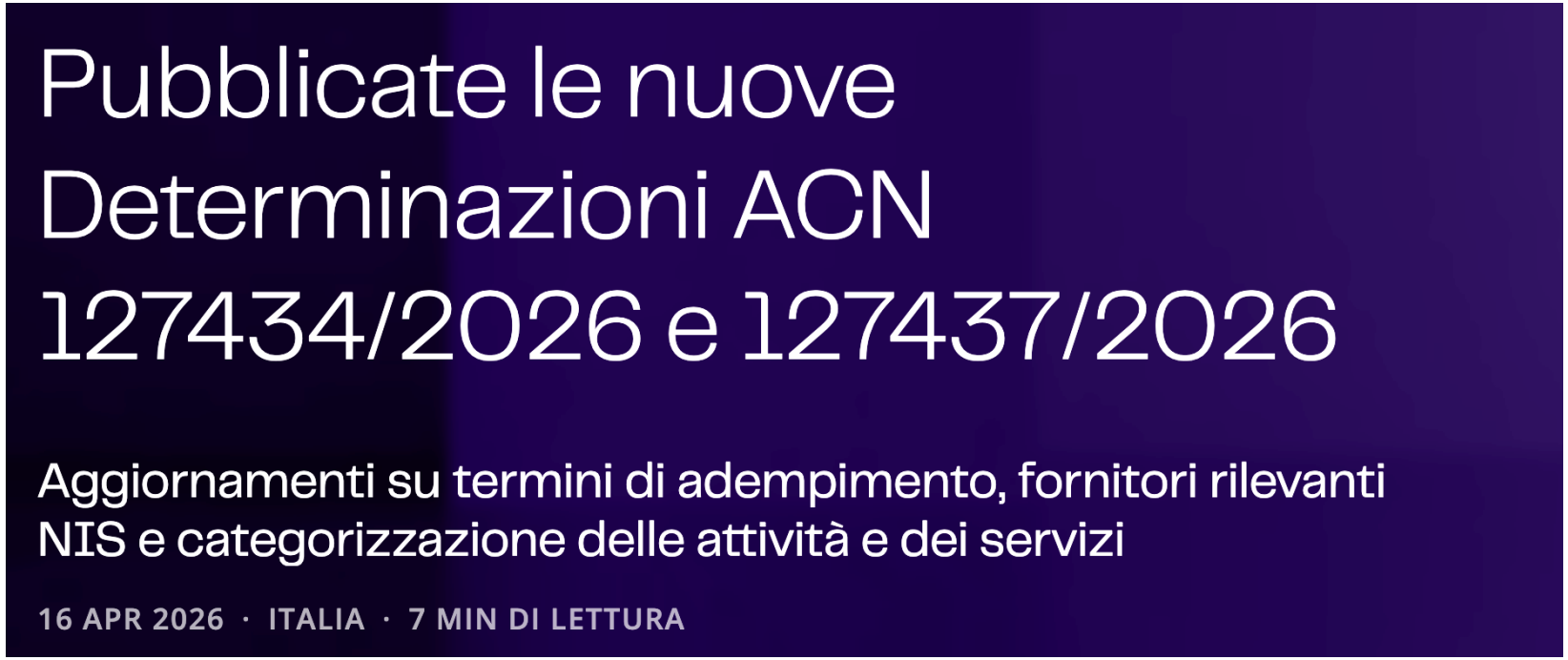
Prorogato al 31 luglio per l'anno 2025

Modello di categorizzazione delle attività e dei servizi

Nell'impianto regolatorio è di fondamentale importanza anche il principio di proporzionalità, realizzato tramite l'attività di categorizzazione delle attività e dei servizi dei soggetti NIS (**articolo 30**). L'attività, che dovrà essere condotta a partire dal 2026 (**articolo 42**), consentirà ai soggetti NIS di distinguere, all'interno della loro organizzazione e con il supporto di ACN, i diversi livelli di esposizione al rischio dei propri sistemi informativi e di rete. A tali sistemi si applicheranno, coerentemente con la loro esposizione al rischio, maggiori obblighi finalizzati a innalzarne progressivamente i livelli di sicurezza informatica.



FONTE :https://www.acn.gov.it/portale/nis/la-normativa



Aggiornamento delle informazioni compreso elenco dei fornitori rilevanti (scadenza 31 maggio)

Comunicazione della categorizzazione delle attività (scadenza 30 giugno)

Categorizzazione delle attivita

Capo V
Elencazione e categorizzazione delle attività e dei servizi

Art. 20
(Processo per l'elencazione e la categorizzazione delle attività e dei servizi)

1. Dal 1° maggio al 30 giugno di ogni anno, i soggetti NIS comunicano e aggiornano, tramite il "Servizio NIS/Categorizzazione", elenco categorizzato delle attività e dei servizi.
2. Per tutti i soggetti NIS, gli utenti compilano l'elenco delle attività e dei servizi del soggetto, attribuendovi le categorie di rilevanza stabilite dal modello adottato con la determinazione di cui all'articolo 40, comma 5, lettera i), del decreto NIS, secondo le modalità e i criteri di cui alla medesima determinazione.
3. Gli utenti designati quali punti di contatto confermano, ai sensi del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, le informazioni fornite e le trasmettono telematicamente tramite il "Servizio NIS/Categorizzazione" all'Autorità nazionale competente NIS. Copia di tali informazioni, per ricevuta, è inviata al domicilio digitale del soggetto.
4. Decorsi i termini di cui al comma 1, l'elenco categorizzato delle attività e dei servizi si intende definitivamente acquisita e non ulteriormente modificabile.
5. Gli elenchi categorizzati delle attività e dei servizi sottomessi oltre i termini di cui al comma 1 sono considerati tardive e ne è preclusa l'ulteriore modifica, salvo che il ritardo sia determinato da documentate criticità tecnico-operative non imputabili al soggetto.
6. Le entità finanziarie di cui al Regolamento (UE) 2022/2554 che rientrano nell'ambito di applicazione del decreto NIS sono esentate dall'attuazione di quanto previsto dal presente articolo. È fatta salva l'adesione a tali previsioni su base volontaria.

OBBLIGO DI COMUNICAZIONE
dal 1 maggio al 30 giugno

CYBER Think Tank ASSINTEL

Confcom

Assintel Associazione Italia Imprese Digitali

CSI your digital partner

Macro-area

Ogni macro-area rappresenta un **contenitore** di attività e servizi ed è caratterizzata da denominazione, descrizione, elenco di esempi (*per 2 macro-aree, gli esempi forniti sono specifici sulla base della tipologia di soggetto*) e categoria di rilevanza pre-assegnata.

Ogni soggetto **inserisce** proprie attività e propri servizi che rientrano nella macro area, eventualmente **modificando** la categoria di rilevanza anche a livello di singola attività o servizio. Se non dovesse avere alcuna attività o servizio, **rimuove** la macro-area.

MACRO AREE

Ricerca, sviluppo e progettazione	Insieme delle attività e dei servizi finalizzati alla ricerca, sviluppo e progettazione, ivi inclusi lo studio di nuove tecnologie e materiali, la prototipazione e sperimentazione di nuovi prodotti, le partnership e collaborazioni scientifiche, la definizione ed elaborazione di progetti, la gestione della proprietà intellettuale e dei brevetti nonché il controllo di conformità dei servizi dell'organizzazione anche in relazione ai fornitori
Gestione finanziaria	Insieme delle attività e dei servizi finalizzati alla gestione finanziaria, ivi inclusi la pianificazione finanziaria, la gestione dei flussi di cassa, la fatturazione e i pagamenti, la contabilità, il bilancio e l'amministrazione della tesoreria.
Gestione dei Clienti	Insieme delle attività e dei servizi finalizzati alla gestione dei clienti, ivi inclusi l'onboarding, la gestione dell'anagrafica e del CRM, l'help desk e il supporto tecnico di primo livello, la gestione delle richieste commerciali e di servizio, il monitoraggio della soddisfazione.
Gestione delle risorse umane	Insieme delle attività e dei servizi finalizzati alla gestione delle risorse umane, ivi inclusi la selezione e il reclutamento, la gestione amministrativa e la retribuzione, la valutazione delle performance, la formazione e lo sviluppo delle competenze.
Logistica	Insieme delle attività e dei servizi finalizzati alla logistica, ivi inclusi la pianificazione e la gestione dei flussi logistici, la gestione dello stoccaggio e del magazzino, la preparazione degli ordini (picking e packing), la gestione delle spedizioni, la distribuzione e la consegna, anche in relazione al supporto del funzionamento generale dell'organizzazione.
Comunicazione e marketing	Insieme delle attività e dei servizi finalizzati alla comunicazione e al marketing, ivi inclusi la gestione dei canali di comunicazione digitali e social, le relazioni esterne e l'ufficio stampa, la gestione dell'identità e del brand, la produzione di contenuti, la gestione degli eventi e delle campagne promozionali.
Gestione amministrativa	Insieme delle attività e dei servizi finalizzati alla gestione amministrativa ivi inclusi la gestione e l'amministrazione degli immobili, la gestione dei contratti, la gestione amministrativa dei fornitori e delle forniture, la gestione fiscale e tributaria, la gestione delle pratiche amministrative e autorizzative.
Altri servizi e attività	Insieme delle attività e dei servizi che non rientrano nelle altre macro-aree

Scenari\Categorie	Impatto minimo	Impatto basso	Impatto medio	Impatto alto
Economico	Costi minimi, interamente as-sorbibili nelle spese operative correnti senza generare alcuno scostamento rispetto al budget previsto.	Oneri finanziari imprevisti (costi extra) che risultano comunque gestibili attingendo a riserve, senza rischi per il business.	Perdite economiche rilevanti che erodono l'utile annuale o riducono la capacità di investimento, pur non compro-mettendo la solvibilità immediata.	Passività insostenibili o costi di ripristino tali da minacciare la solvibilità finanziaria e la continuità aziendale stessa (rischio insolvenza).
Operativo	Disservizi impercettibili o rallentamenti su processi non critici, senza intaccare l'erogazione delle attività o dei servizi NIS.	Fermo parziale, risolto entro i tempi previsti dai livelli di servizio senza generare effetti a cascata e preservando l'integrità dei dati.	Interruzione del servizio che supera le tempistiche previste dai livelli di servizio, impattando una vasta utenza e settori interdipendenti.	Blocco totale, rischi per la sicurezza fisica o effetti a cascata su altri settori interdipendenti con ricadute anche a livello sistemico.
Reputazionale	Danno d'immagine trascurabile, confinato all'interno dell'organizzazione senza alcuna risonanza mediatica esterna.	Visibilità negativa limitata al settore o agli addetti ai lavori, generando una crisi passeggera gestibile con gli strumenti ordinari.	Perdita di fiducia da parte di stakeholder rilevanti e una copertura sui media generalisti che richiede campagne correttive per limitare il danno.	Visibilità negativa di portata sistemica che causa un danno strutturale e duratura perdita di fiducia degli stakeholder.

IMPATTI su MACRO AREE

Monitoraggio e controllo	Impatto alto
Produzione di beni e servizi	Impatto medio
Ricerca, sviluppo e progettazione	Impatto medio
Gestione finanziaria	Impatto basso
Gestione dei clienti	Impatto basso
Gestione delle risorse umane	Impatto basso
Logistica	Impatto minimo
Comunicazione e marketing	Impatto minimo
Gestione amministrativa	Impatto minimo
Altri servizi e attività	Impatto minimo

ESEMPI ACN DI CATEGORIZZAZIONE ATTIVITA

Comunicazione e marketing	Attivita strategiche	Definire la strategia di branding e stabilire le linee guida di comunicazione dell'organizzazione. • Analizzare il mercato e i competitor, definendo il posizionamento strategico, la segmentazione e il target di riferimento. • Sviluppare la strategia di offerta e il piano di go-to-market, gestendo il portfolio e l'intero ciclo di vita del prodotto.
	Attivita di coordinamento	Coordinare l'ufficio stampa e l'organizzazione degli eventi, gestendo le situazioni di crisi, il media monitorizza la sentiment analysis. • Assicurare la governance dei canali digitali, supervisionando le approvazioni legali e di conformità e monitorando i relativi KPI. • Gestire e coordinare i canali di distribuzione commerciale. • Pianificare ed eseguire le campagne di comunicazione integrata.

CYBER Think Tank ASSINTEL

Confcom

Assintel
Associazione Italiana
Imprese Digitali

CSI
your digital partner

!!! ATTENZIONE !!!

GLI ESEMPI RIPORTATI NEI TEMPLATE DI ACN NON SONO PRESCRITTIVI NE ESAUSTIVI, SONO UNICAMENTE DEGLI ESEMPI DI CATEGORIZZAZIONE DELLE ATTIVITA PER INDICARE FORMALISMO E GRANULARITA' CON CUI ACN SI ASPETTA IL RISCONTRO

CYBER Think Tank ASSINTEL

Confcom

Assintel
Associazione Italiana
Imprese Digitali

CSI
your digital partner

ESEMPI ACN DI CATEGORIZZAZIONE ATTIVITA

Gestione delle risorse umane	Assunzione	• Curare il processo di reclutamento, selezione e inserimento in azienda, gestendo la relativa contrattualistica.
	Sviluppo HR	• Implementare il sistema di valutazione delle performance e definire i piani formativi individuali e collettivi.
	Amministrazione	• Amministrare la rilevazione presenze e le retribuzioni, gestendo le relazioni sindacali, il clima interno e garantendo la salute, la sicurezza e la compliance lavoristica.

Nella analisi della macro area potrei eventualmente aggiungere/sostituire

- Gestire e aggiornare l'anagrafica del personale nei sistemi informativi HR, monitorando dati contrattuali, qualifiche, scadenze, ferie, permessi e posizioni organizzative.
- Analizzare i dati del personale attraverso report e dashboard HR per supportare decisioni su fabbisogni, turnover, assenteismo, competenze e pianificazione delle risorse.

CYBER Think Tank ASSINTEL

Confcom

Assintel
Associazione Italiana
Imprese Digitali

CSI
your digital partner

ESEMPI ACN SPECIFICI PER CATEGORIA SOGGETTO NIS

Produzione di beni e servizi	**Servizi Digitali**	• Eseguire la registrazione: Inoltrare la richiesta di assegnazione di un nuovo dominio al Registry competente (es. Registro .ito .com) per conto del cliente. • Gestire il ciclo di vita del dominio: Processare i rinnovi, i trasferimenti (tramite codice AuthInfo) e le modifiche ai contatti amministrativi/tecnici. • Fornire servizi DNS di base: Configurare i record NS (Name Server) iniziali per rendere il dominio risolvibile in rete
	Gestione Cloud Provider	• Provisionare risorse (IaaS): Allocare dinamicamente CPU, RAM e Storage virtuali su richiesta del cliente tramite hypervisor. • Erogare piattaforme (PaaS): Mettere a disposizione ambienti di runtime gestiti (es. Kubernetes,Database) pronti per il deploy di applicazioni. • Orchestrare i servizi: Gestire l'automazione che crea, scala e distrugge le istanze in base alle regoledefinite dall'utente. • Erogare potenza elettrica: Fornire energia stabilizzata e continua (tramite UPS e generatori) ai rack ospitati. • Gestire il raffreddamento: Produrre aria o liquido refrigerato per mantenere la temperatura operativa dei server (HVAC). • Fornire spazio fisico (Colocation): Mettere a disposizione cabinet sicuri e interconnessi per l'alloggiamento degli apparati dei clienti. • Erogare servizi strumentali: Fornire all'ente controllante i servizi operativi delegati (es. gestionepaghe, servizi IT, gestione protocollo).
	Gestione servizi DNS	• Gestire servizi pubblici locali: Operare infrastrutture e servizi per la cittadinanza su mandato dellaPA (es. gestione parcheggi, illuminazione pubblica, riscossione tributi). • Gestire piattaforme Smart City: Monitorare e operare i sensori e i sistemi IoT urbani (es. varchi ZTL, rilevamento ambientale) per il controllo del territorio

CYBER Think Tank ASSINTEL

Confcom

Assintel Associazione Italiana Imprese Digitali

CSI your digital partner

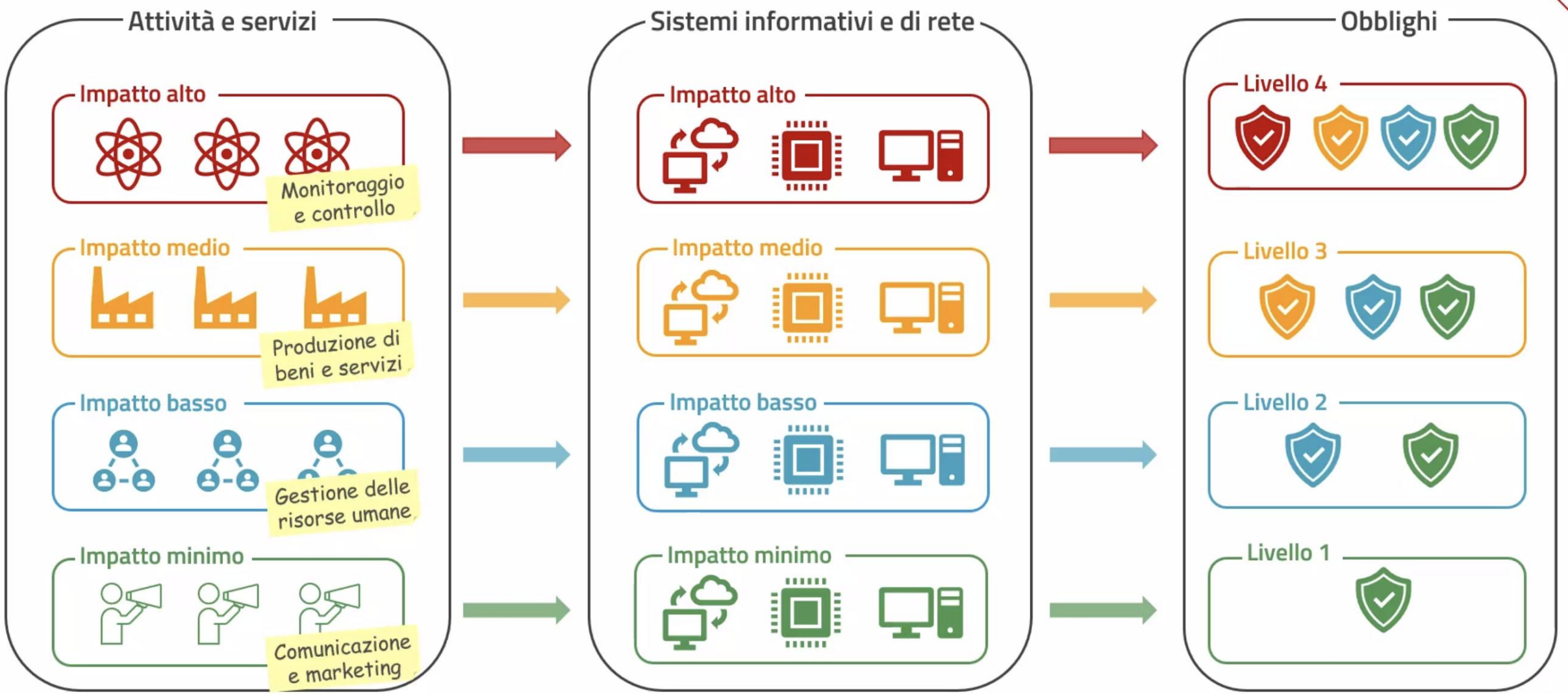
Monitoraggio e controllo	**Servizi Digitali**	Monitorare i servizi al cittadino (Smart City): Supervisionare le piattaforme digitali gestite per conto dell'Ente (es. pagamento tributi, anagrafe, ZTL) garantendo uptime e sicurezza dei dati. • Controllare le infrastrutture urbane: Se applicabile, monitorare i sistemi di illuminazione pubblica intelligente, i semafori o i parcheggi automatizzati gestiti dalla società partecipata. • Verificare la compliance amministrativa: Monitorare i flussi informativi verso la PA controllante per garantire la trasparenza e la correttezza dei dati di bilancio e di servizio. • Proteggere i dati dei contribuenti: Sorvegliare gli accessi ai database che contengono dati sensibili dei cittadini gestiti in outsourcing per conto del Comune/Regione. • Supervisionare gli Hypervisor: Monitorare lo stato del layer di virtualizzazione che separa le risorse dei vari tenant (clienti) per garantire isolamento e performance. • Monitorare le API di gestione: Controllare la disponibilità delle interfacce programmatiche che permettono ai clienti di creare o distruggere risorse cloud. • Gestire la capacità (Capacity Planning): Analizzare i trend di utilizzo di CPU, RAM e Storage per allocare risorse dinamicamente senza interrompere i servizi. • Controllare i parametri ambientali: Monitorare h24 temperatura e umidità nelle sale server (isole calde/fredde) per prevenire guasti hardware. • Supervisionare l'alimentazione elettrica: Verificare lo stato degli UPS, dei generatori ausiliari e delle PDU (Power Distribution Units) per garantire la continuità assoluta (Tier IV). • Monitorare le transazioni EPP: Sorvegliare in tempo reale lo stato e i tempi di risposta delle connessioni verso i Registri (Registry) per rilevare fallimenti nelle procedure di registrazione o rinnovo. • Tracciare le modifiche critiche: Controllare i log delle attività per evidenziare variazioni anomale ai record DNS autoritativi o ai dati di contatto (WHOIS) che potrebbero indicare tentativi di Domain Hijacking
	Gestione Cloud Provider	
	Gestione servizi DNS	

Misure di sicurezza e modello di implementazione

Proporzionalità delle misure

- ✓ I sistemi informativi e di rete ereditano la categoria di rilevanza del servizio o dell'attività che abilitano (ossia che supportano, svolgono o erogano).
- ✓ Qualora i sistemi informativi e di rete abilitino servizi o attività con categorie di rilevanza differenti, ereditano la categoria rilevanza con impatto maggiore.
- ✓ Gli obblighi a lungo termine definiranno 4 *set* di misure di sicurezza definite su 4 livelli di mitigazione del rischio crescente (L1, L2, L3, L4) e differenziate tra soggetti essenziali e importanti:
  - per i **soggetti privati**, ognuna delle 4 categoria di rilevanza corrisponde a un set di misure di sicurezza;
  - per i **soggetti pubblici**, i sistemi informativi e di rete oggetto del regolamento cloud classificati come ordinari, critici, strategici implementano le misure di sicurezza L2, L3 e L4, i restanti sistemi informativi e di rete (infrastruttura informatica client) implementano le misure di sicurezza di livello L1.

Proporzionalità degli obblighi

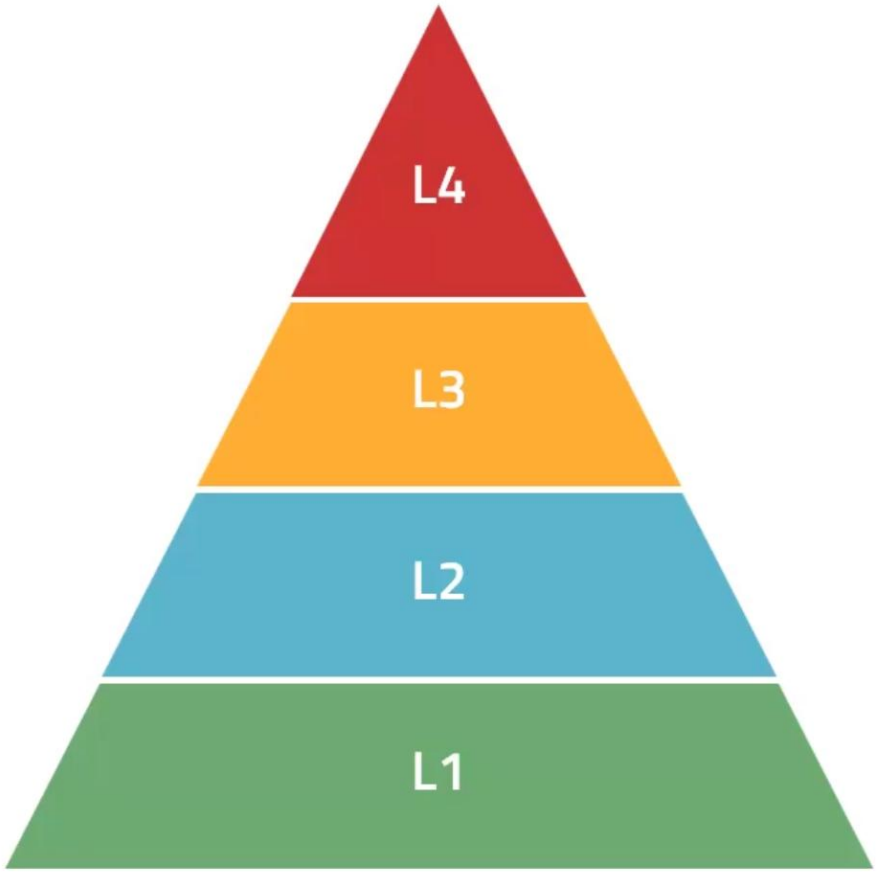


Categoria di rilevanza e misure di sicurezza (3/5)

Sistemi informativi e di rete soggetti privati

- Impatto alto
- Impatto medio
- Impatto basso
- Impatto minimo

Misure di sicurezza a lungo termine



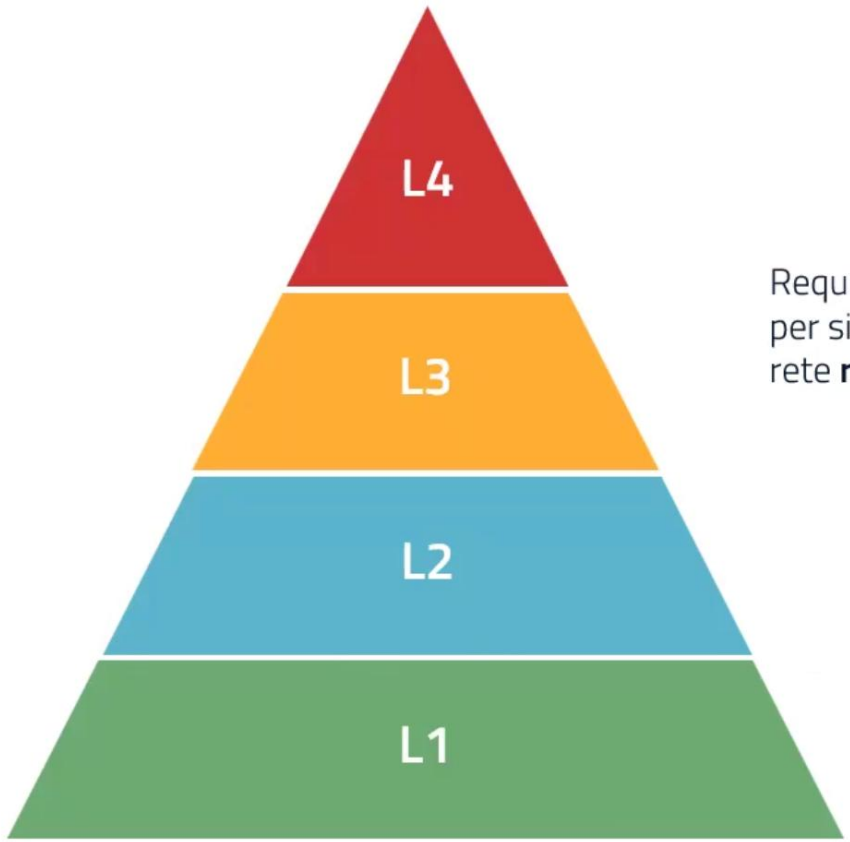
Sistemi informativi e di rete soggetti pubblici

- Cloud strategico
- Cloud critico
- Cloud ordinario
- No Cloud

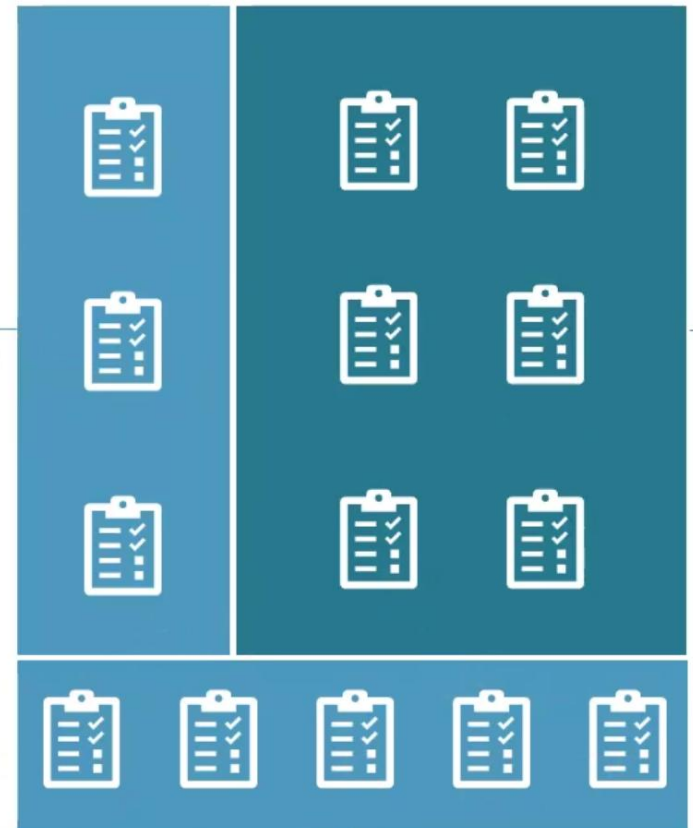
Categoria di rilevanza e misure di sicurezza (4/5)

Proposta su 4 livelli

Misure di sicurezza a lungo termine



Requisiti **specifiche di base** per sistemi informativi e di rete **rilevanti**.



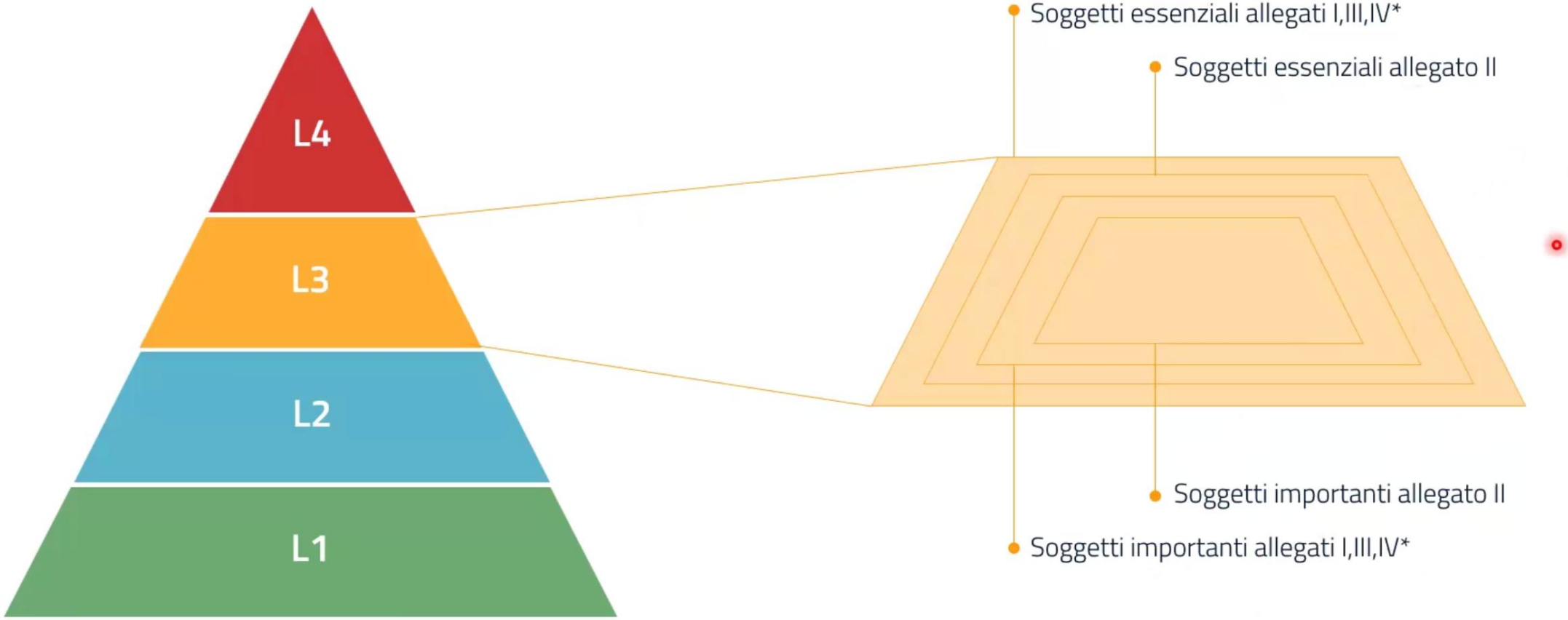
Requisiti **aggiuntivi**

Requisiti **specifiche di base** per sistemi informativi e di rete **non rilevanti**.

Categoria di rilevanza e misure di sicurezza (5/5)

roposta su 4 livelli

Misure di sicurezza a lungo termine



Cosa devono fare gli Organi di Amministrazione e Direttivi

In sintesi:

Gli organi di amministrazione e gli organi direttivi NON devono occuparsi direttamente dell'implementazione delle misure di sicurezza, ma **devono**:

- **Supervisionare i processi** di gestione della sicurezza informatica
- Definire la **propensione al rischio dell'Ente**
- Garantire lo svolgimento di adeguate **attività di formazione**
- **Approvare i piano di attuaizne della normativa all'interno dell'Ente**

Cybersecurity: Vulnerabilità, tecniche di attacco, il fattore umano

Cos’è la Cybersecurity

La sicurezza **NON E’** un prodotto o un servizio

La sicurezza **E’** l’insieme di:

- Processi
- Regole - Procedure
- Servizi specializzati
- Risorse
- Organizzazione
- Cultura
- Strumenti
- Controlli

I principi fondamentali

RISERVATEZZA

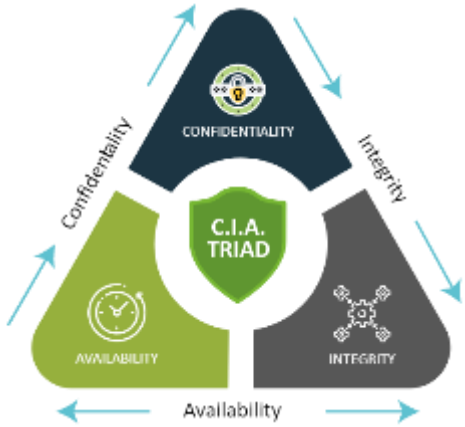
- Avere la certezza che una determinata informazione possa essere conosciuta solo da chi ha il diritto di farlo

INTEGRITA'

- Avere la certezza che una determinata informazione possa essere modificata solo da chi ha diritto di farlo e solo attraverso modalità note e verificabili

DISPONIBILITA'

- Avere la certezza che una determinata informazione possa essere prontamente reperita ed utilizzata tutte le volte che si ha necessità di farlo



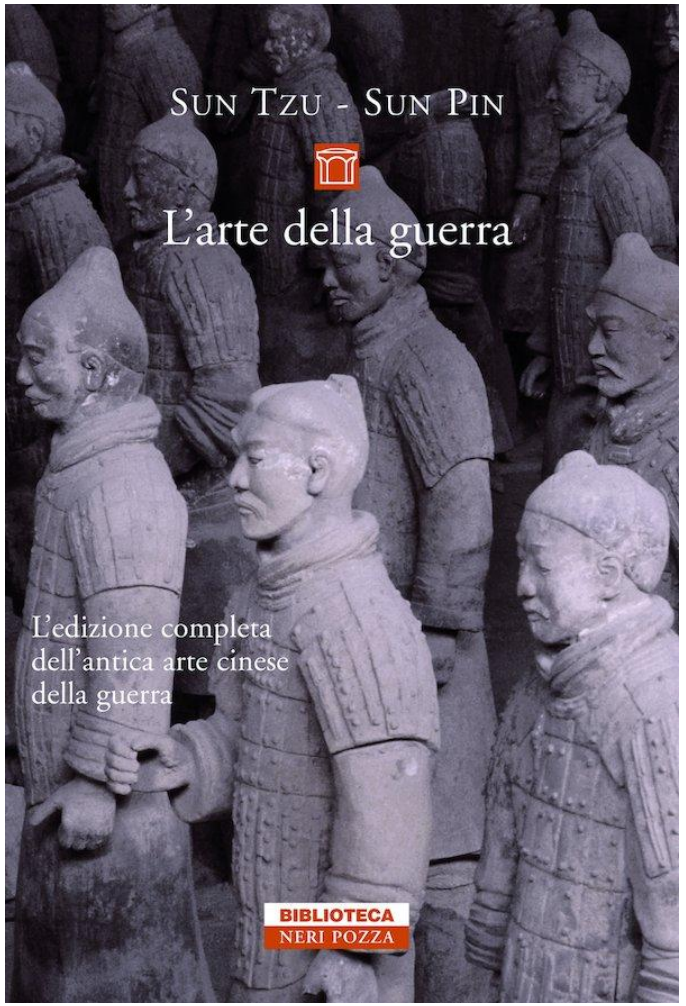
Conosci il nemico

«Se conosci il nemico e conosci te stesso, non devi temere il risultato di cento battaglie.

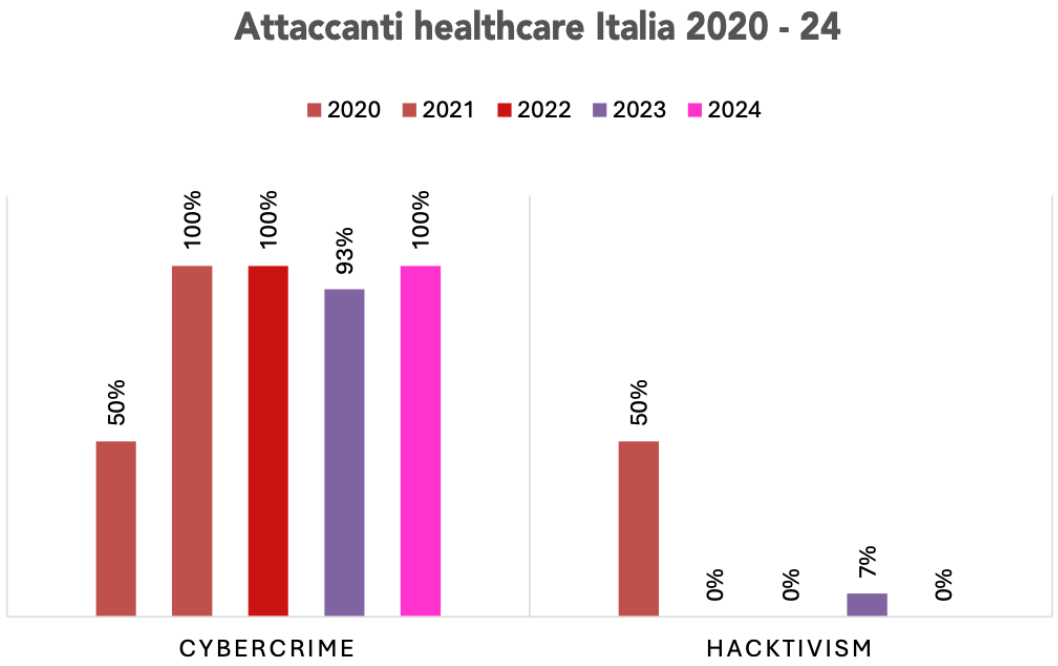
Se conosci te stesso ma non il nemico, per ogni vittoria ottenuta subirai anche una sconfitta.

Se non conosci né il nemico né te stesso, soccomberai in ogni battagia»

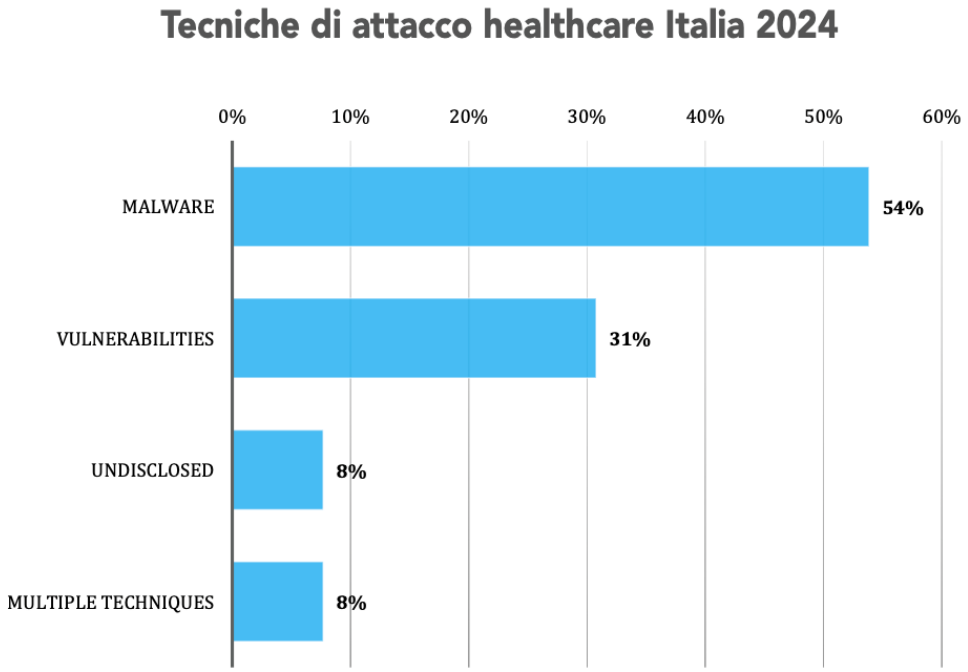
Sun Tzu - "L'arte della guerra" VI secolo a.C.



Conosci il nemico



© Hackmanac Global Cyber Attacks Report 2025



© Hackmanac Global Cyber Attacks Report 2025

Conosci il nemico

Le principali cause individuate da ACN:

1. **gestione decentralizzata dei sistemi IT**, con reparti che adottano soluzioni differenti senza una politica di sicurezza comune;

2. **obsolescenza delle tecnologie**, con dispositivi medicali non aggiornabili che rimangono vulnerabili;

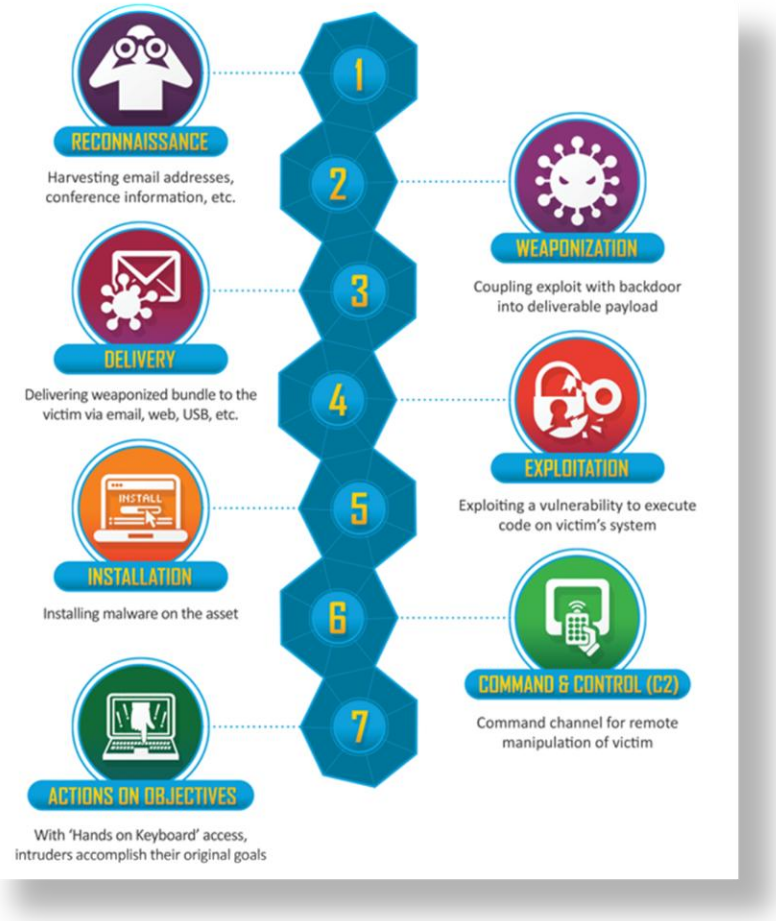
3. **carenza di personale specializzato**, con la sicurezza informatica spesso affidata a personale IT non dedicato.

Conosci il nemico: la kill chain

La Cyber Kill Chain descrive i passaggi seguiti dagli hacker per effettuare un attacco informatico:

1. **Ricognizione:** Identificazione del bersaglio attraverso la raccolta di informazioni.
2. **Armamento:** Creazione di un malware specifico per il bersaglio.
3. **Consegna:** Trasmissione del malware al bersaglio, ad esempio tramite email.
4. **Sfruttamento:** Il malware sfrutta una vulnerabilità per entrare nel sistema.
5. **Installazione:** Il malware si installa consentendo l'accesso futuro.
6. **Comando e Controllo:** L'hacker comanda il malware da remoto.
7. **Azioni sugli Obiettivi:** L'hacker esegue azioni dannose, come furto di dati.

Ogni fase rappresenta un'opportunità per intercettare e bloccare l'attacco.



RANSOMWARE: Estorsione Digitale

Il **ransomware** è un tipo di malware che limita o impedisce agli utenti di accedere ai loro sistemi o file, richiedendo il **pagamento di un riscatto** per il ripristino dell'accesso.

Gli utenti colpiti vedono di solito un messaggio che spiega come pagare il riscatto per **sbloccare i propri file o sistema.**

Il pagamento è spesso richiesto in **criptovalute**, come Bitcoin, per mantenere l'anonimato degli aggressori

RANSOMWARE: Estorsione Digitale + livelli

Estorsione Singola

In un attacco ransomware classico, i dati della vittima vengono crittografati e l'accesso viene negato fino al **pagamento di un riscatto.**

Non ci sono ulteriori minacce o azioni da parte degli aggressori.

Analisi delle Vulnerabilità

Obiettivi

Gli obiettivi principali del "vulnerability assessment" sono:

1. **Identificare** le vulnerabilità esistenti nei sistemi informatici.
2. **Quantificare** la gravità e il potenziale impatto di queste vulnerabilità.
3. **Prioritizzare** l'ordine di risoluzione basato sul rischio che ciascuna vulnerabilità rappresenta.

Analisi delle Vulnerabilità

Utilità

Il "vulnerability assessment" è fondamentale per mantenere la **sicurezza dei sistemi informatici**. I suoi benefici includono:

- **Prevenzione di Attacchi**: Identificare e correggere le vulnerabilità prima che gli aggressori possano sfruttarle.
- **Conformità Normativa**: Assicurare che i sistemi siano conformi agli standard di sicurezza richiesti da leggi e regolamenti.
- **Gestione del Rischio**: Aiutare le organizzazioni a comprendere e gestire meglio i rischi associati alle vulnerabilità dei loro sistemi.
- **Miglioramento Continuo**: Fornire un percorso chiaro per il miglioramento continuo delle pratiche di sicurezza.

SOCIAL ENGINEERING

Il Social Engineering è una tecnica di **manipolazione psicologica** utilizzata per indurre le persone a **compiere azioni** o a **rivelare informazioni** confidenziali.

È spesso impiegato in attacchi informatici non perché sfrutta vulnerabilità nei software, ma piuttosto **vulnerabilità umane**.

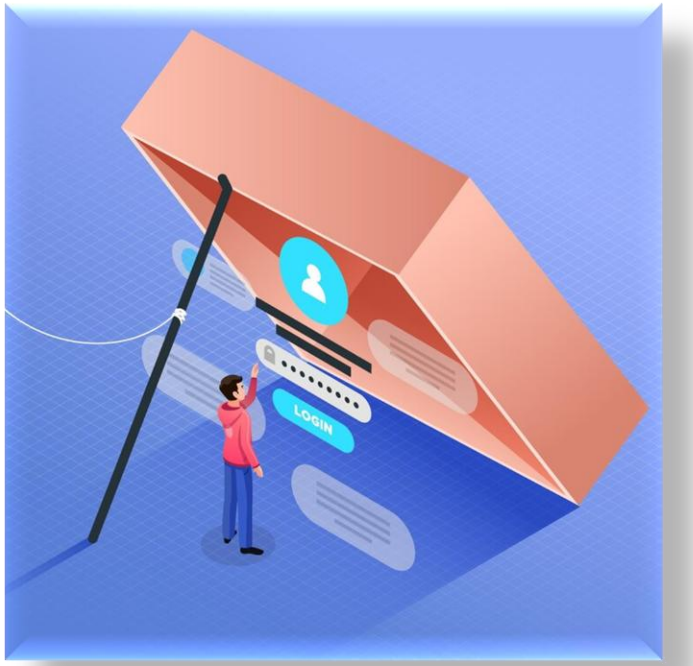
SOCIAL ENGINEERING

Esempi comuni

- **Phishing**: Email o messaggi che sembrano provenire da fonti affidabili, come banche o enti governativi, ma che in realtà sono **trappole per ottenere dati sensibili** (password, numeri di carta di credito, ecc.).

- **Pretexting**: L'attaccante **crea una storia credibile (un pretesto) per ottenere informazioni riservate**. Questo potrebbe includere, ad esempio, fingere di essere un collega o un responsabile che necessita di accesso urgente a determinati dati.

- **Baiting**: Simile al **phishing, ma con l'aggiunta di un "esca**", come l'offerta di software gratuito su un supporto infetto, che una volta utilizzato può compromettere il sistema



75% of ransomware attacks start with email phishing

Fonte: https://www.proofpoint.com/it/blog/email-and-cloud-threats/tips-developing-your-ransomware-defense-strategy

SOCIAL ENGINEERING

Come ci proteggiamo?

- **Formazione e sensibilizzazione**: Educare il personale sulla natura e sui metodi del Social Engineering è fondamentale. **Riconoscere le tattiche usate** può aiutare a prevenire gli attacchi.

- **Verifica**: Insegnare ai colleghi a **verificare l'identità** di chi richiede informazioni sensibili, soprattutto se la richiesta arriva tramite canali non ufficiali.

- **Politiche di sicurezza**: Avere chiare **politiche di sicurezza** che includano **procedure** per la gestione delle richieste di informazioni sensibili può ridurre il rischio di cadere vittima di questi attacchi.

Riferire gli incidenti…

Non segnalo un incidente di sicurezza perché…

…sentirsi VULNERABILI ha un effetto paralizzante sull'essere umano.

Risposta agli incidenti

L'"Incident Response" (risposta agli incidenti) è un approccio organizzato per affrontare e gestire le **conseguenze di un attacco informatico o di una violazione della sicurezza**, con l'obiettivo di **limitare il danno** e **ridurre il tempo di recupero e i costi**.

Risposta agli incidenti

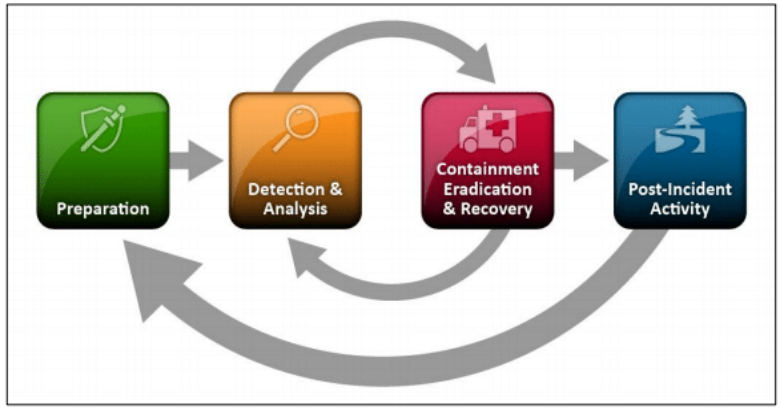
Pensiamo a un incendio in un edificio: l'obiettivo principale è non **solo spegnere l'incendio** il più rapidamente possibile, ma anche **evacuare in sicurezza le persone, limitare i danni e investigare sulle cause per prevenire futuri incendi**.

In modo simile, l'Incident Response si occupa di "spegnere" gli attacchi informatici, proteggere i dati e le risorse, e apprendere dall'incidente per rafforzare le difese.

Risposta agli incidenti – processo di incident response

- **preparazione**: sviluppo di un **piano di risposta** agli incidenti, formazione del team di risposta e preparazione delle risorse necessarie
- **identificazione:** rilevamento di un **potenziale incidente** di sicurezza attraverso sistemi di monitoraggio, allarmi o segnalazioni
- **contenimento**: adozione di misure immediate **per limitare l'estensione del danno** che può includere l'isolamento della rete o dei dispositivi colpiti.
- **eradicazione**: rimozione della causa dell'incidente, che può implicare la disinfestazione da malware o la chiusura di vulnerabilità sfruttate
- **recupero**: ripristino dei sistemi e dei servizi alla loro operatività normale, assicurandosi che non siano più vulnerabili agli stessi attacchi
- **post-incident review**: analisi dell'incidente per trarre insegnamenti, migliorare i processi di risposta e rafforzare le misure di sicurezza

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Risposta agli incidenti: perché è importante?

limitazione del danno

ridurre l'impatto finanziario e di reputazione derivante da violazioni o attacchi informatici

ripristino rapido

assicurare il ritorno alla normalità operativa in breve tempo e minimizzare l'interruzione delle attività

conformità legale

molte normative richiedono piani di risposta agli incidenti e notifiche in caso di violazioni dei dati

miglioramento continuo

ogni incidente offre l'opportunità di rafforzare le difese contro future minacce

Esempi pratici di attacchi o truffe

Cybersecurity – Più del 90% degli incidenti di sicurezza deriva dall'errore umano*

Tempo di lettura: 7 minuti

Capterra Da 18 anni aiutiamo le aziende a scegliere i migliori software

Cerca un software...

Sicurezza informatica aziendale: i dirigenti sono presi di mira dai cybercriminali

Data di pubblicazione: 24/10/2024

*Scritto da **Giorgia Pisano**.*

Secondo un nuovo studio di Capterra, i dirigenti aziendali sono sempre più il bersaglio di attacchi informatici. Le aziende devono assicurarsi che i dipendenti, e soprattutto i dirigenti, siano formati e pronti a evitare e rispondere alle minacce informatiche che potrebbero ricevere

Gli attacchi informatici alle aziende italiane sono sempre più diffusi e i dirigenti, probabilmente a causa della quantità di dati a cui hanno solitamente accesso, stanno diventando un bersaglio comune. Il 58% degli intervistati nel nostro studio Executive Cybersecurity 2024*, afferma che almeno uno dei propri dirigenti è stato preso di mira da una minaccia alla sicurezza informatica negli ultimi 18 mesi.

FONTE: https://www.capterra.it/blog/7533/sicurezza-informatica-aziendale-minacce

I Dati in Lombardia

I dati 2024 dell'attività della Polizia postale in Lombardia: 9,6 milioni persi in frodi informatiche

Netta contrazione anche delle frodi informatiche -21%, con 564 casi rispetto ai 713 del 2023 ma gli importi persi sono aumentati del 30%, passando da 7,4 milioni di euro a 9,6 milioni. Tra le tipologie in crescita spiccano (+62%) le cosiddette "CEO fraud", ovvero frodi in cui il truffatore, spacciandosi per l'Amministratore Delegato o comunque un alto dirigente di un'azienda, si mette in contatto con un dipendente e lo convince a effettuare bonifici verso conti correnti esteri riferibili all'organizzazione criminale.

https://www.youtube.com/watch?v=sflGB--jxws

Frodi sui pagamenti: i dati allarmanti del rapporto 2025 di Banca d'Italia

4 mar 2025 | 6 min di lettura | Pubblicato da Cristina B.

Nel 2024 i **valori delle truffe sui bonifici** ammontavano a 50 mln mentre sulle frodi con le carte di pagamento toccavano quota 33 mln di euro, una crescita del 67%, nel primo caso, e del 4%, nel secondo caso, su base annua. In crescita anche quelle con moneta elettronica, pari a 13,1 mln di euro (+35%). L'interessante fotografia sulle frodi dei mezzi di pagamento la scatta **Banca di Italia nel Rapporto sulle operazioni fraudolente di pagamento 2025**. La numerosità delle frodi vede primeggiare le **carte e la moneta elettronica** nelle operazioni tra persone fisiche. Un'argine lo pone il meccanismo di **doppia identificazione**. **Facile.it** leader nel confronto tra **prestiti personali**, approfondisce l'argomento.

FONTE: https://www.facile.it/prestiti/parola-all-esperto/frodi-sui-pagamenti-2025-i-dati-della-banca-d-italia.html

L'ANALISI TECNICA

Phishing contro le PA per rubare credenziali degli account Outlook: i dettagli e come difendersi

È stata segnalata una campagna di phishing mirata alle pubbliche amministrazioni italiane che, sfruttando e-mail fraudolente che promettono aggiustamenti salariali o accessi a buste paga elettroniche, consente agli attaccanti di rubare le credenziali di accesso agli account di posta elettronica MS Outlook. I dettagli

Pubblicato il 29 mar 2024

Salvatore Lombardo
Funzionario informatico, Esperto ICT, Socio Clusit e autore

L'ANALISI TECNICA

Phishing via PEC, la truffa delle finte fatture elettroniche: i consigli per difendersi

I criminal hacker portano avanti campagne di phishing via PEC per colpire le caselle di posta elettronica certificata di molte pubbliche amministrazioni, aziende private e iscritti a diversi ordini professionali. Ecco i dettagli tecnici e i consigli per difendersi

Pubblicato il 15 apr 2025

Paolo Tarsitano

20 maggio 2025

Tutto Lavoro 24 .IT
Quando il lavoro fa notizia

Politica | Economia & Lavoro | Lavoro & Diritti | Cronaca Sindacale | Giurisprudenza | Scuola & Formazione | Salute & Benessere

Lavoro & Diritti

di **Sergio Manzon** 20 Maggio 2025

Stipendi NoiPA Spariti per Furto d'Identità: Cresce il Numero delle Vittime e l'Allarme Nazionale

Un'ondata di attacchi informatici mirati sta colpendo il sistema **NoiPa**, il portale utilizzato dal Ministero dell'Economia e delle Finanze per l'erogazione degli stipendi ai dipendenti pubblici e la gestione di numerose altre voci fiscali. L'allarme è stato lanciato dopo la scoperta di numerosi casi di furto di identità digitale tramite SPID (Sistema Pubblico di Identità Digitale), che hanno permesso ai cybercriminali di modificare i dati di pagamento e deviare su conti correnti fraudolenti stipendi statali, pensioni, assegni unici e rimborsi Irpef.

L'AGENZIA

Chi siamo

Uffici e Pec

Azioni collettive

Carta dei servizi e sistema di ascolto

Amministrazione trasparente

Prevenzione della corruzione e trasparenza

L'Agenzia comunica

- Cosa c'è di nuovo
- Eventi e convegni
- Consultazioni pubbliche

Avviso del 18 febbraio 2025 - Nuova ondata di false comunicazioni relative a rimborsi fiscali

Sono riprese a circolare false comunicazioni a nome dell'Agenzia delle Entrate relative a rimborsi fiscali, inviate con il fine di attirare l'attenzione della vittima, invogliandola a compilare un modulo web per ottenere un fantomatico rimborso. Si tratta di una campagna malevola analoga a quelle delle quali avevamo dato notizia sia nella segnalazione dell'11 luglio 2024 che nella segnalazione del 9 Aprile 2024.

Le e-mail afferenti a questa nuova ondata si caratterizzano per:

- Mittente indirizzo estraneo all'Agenzia delle Entrate
- Oggetto "Avviso di Rimborso - ITXXXXXXXXXX" dove XXXXXXXXXX è variabile e casuale
- Riferimento nel corpo del messaggio ad un fantomatico rimborso fiscale a favore della vittima
- Presenza di un link "Modulo di rimborso" che rimanda ad un modulo pubblicato su un portale contraffatto sotto il controllo dell'hacker
- Firma "Agenzia delle Entrate – Direzione Provinciale"
- Senso d'urgenza generale

Riportiamo di seguito un esempio di e-mail malevola appartenente a questa campagna.

Spid rubato, rimborsi 730 a rischio: la truffa del "doppio Spid". Come funziona,... PENSIONI Segui

Hai 2 notifiche

Spid rubato, rimborsi 730 a rischio: la truffa del "doppio Spid". Come funziona, come come difendersi e cosa fare subito

mercoledì 9 aprile 2025, 16:30 - Ultimo agg. 10 aprile, 07:37

1 di 7

1 Minuto di Lettura

FONTE: https://www.ilmessaggero.it/schede/spid_rubato_truffa_rimborsi_730_doppio_spid_come_difendersi_cosa_fare_subito-8768946.html#

alanews.it

Cronaca Politica Economia Esteri Sport Spettacoli Salute Tecnolo

Attenzione ai caricatori USB pubblici negli aeroporti: mettono a rischio i dati

di **Alessandro Bolzani** — 12 Giugno 2025

Il pericolo nascosto del “port jacking”

La Transportation Security Administration (TSA) ha recentemente emesso un avvertimento chiaro: i caricatori USB pubblici possono essere vulnerabili agli attacchi informatici. Questo tipo di minaccia, noto come “port jacking”, consiste nella possibilità che hacker installino malware all’interno delle porte di ricarica, con l’obiettivo di accedere ai dati personali degli utenti

Collegando il proprio telefono a una porta USB manomessa, il dispositivo può interpretare quella connessione come una tastiera virtuale, oppure può essere indotto a scaricare un’app dannosa. In entrambi i casi, il controllo del dispositivo può essere compromesso. Per questo motivo gli esperti sconsigliano vivamente l’utilizzo delle porte USB pubbliche.

DIGITALCAMPUS
guidiamo l'innovazione

CSI
your digital partner

Grazie

pierpaolo.gruero@csi.it