REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere **SICURI?**

NIS2 e Governance by Design: quando la sicurezza diventa una responsabilità di tutta l'azienda

Titolo: Responsabilità della governance, formazione e strumenti

Relatore Mauro Alovisio

Presentiamoci: Chi siamo

Mauro Alovisio
Avvocato presso Università, mi occupo da diversi anni di protezione dati e del diritto delle nuove tecnologie, **coordinatore del primo corso di perfezionamento universitario in materia di protezione dei dati personali** dell'Università degli Studi di Torino (Direttore: Prof. Francesco Pizzetti)
Già professore a contratto presso l' Università Statale di Milano e di Torino,docente presso master di cybercrime dell'Università degli Studi di Torino, presidente del Centro Studi di informatica Giuridica di Ivrea Torino, Fellow del Centro di ricerca Nexa su Internet e società del Politecnico di Torino. Formatore e autore di pubblicazioni

Disclaimer: Per le slide ho utilizzato tre sistemi AI per revisione

La visione


“Non esiste vento favorevole per il marinaio che non sa dove andare”
LUCIO ANNEO SENECA

Agenzia Ue sulla cybersecurity: "Pubblica amministrazione a rischio, governi i più colpiti"

Attacchi DDoS frequenti, significative campagne di cyberspionaggio

SOLO ONLINE

SKY WIFI BUSINESS

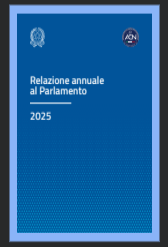
24,50€

21,50€ al mese per 12 mesi IVA esclusa

SCOPRI DI PIÙ

sky wifi

I prezzi sono da intendersi IVA esclusa, salvo espressa previsione contraria.
Offerta riservata alle imprese o persone fisiche intestatarie di P. IVA disponibile online per nuovi clienti Sky



1

2

3

Relazione annuale al Parlamento

2025

35

36

37

2.6 LA MINACCIA CYBER NELLA PUBBLICA AMMINISTRAZIONE

Nel corso del 2025, l'Agenzia ha rilevato 1.140 eventi cyber riferibili a istituzioni pubbliche nazionali. Di questi, 196 episodi, pari a circa il 17% del totale, sono stati qualificati come incidenti.

Il numero complessivo degli eventi risulta in aumento rispetto ai 756 casi registrati nel 2024 ed è attribuibile principalmente alle già citate campagne DDoS, nonché all'accresciuto cono di visibilità dell'ACN, dovuto anche alla piena applicazione della legge n. 90/2024 che ha esteso a moltissimi soggetti pubblici gli obblighi di notifica.

Come rappresentato in Figura 13, la distribuzione degli eventi cyber che hanno interessato la Pubblica Amministrazione evidenzia come la quota più rilevante abbia riguardato l'Amministrazione dello Stato e gli Organi costituzionali o di rilievo costituzionale. Tale concentrazione riflette il ruolo centrale di questi soggetti nell'assetto istituzionale del Paese e la conseguente ampiezza della loro esposizione digitale in termini di infrastrutture, servizi e visibilità nel dominio cibernetico.

Seguono i Comuni, le Regioni e le Aziende sanitarie, ambiti caratterizzati da un'elevata capillarità territoriale e da una forte interazione digitale con cittadini e imprese. Per tali soggetti, la diffusione di servizi online e la molteplicità degli *asset* IT contribuiscono ad ampliare la superficie di esposizione e, conseguentemente, il volume delle attività cibernetiche rilevate.

Una quota rilevante di eventi ha, inoltre, interessato università e centri di ricerca, nonché enti pubblici non economici, contesti contraddistinti da ecosistemi informativi articolati e da un'ampia interconnessione con reti nazionali e internazionali.

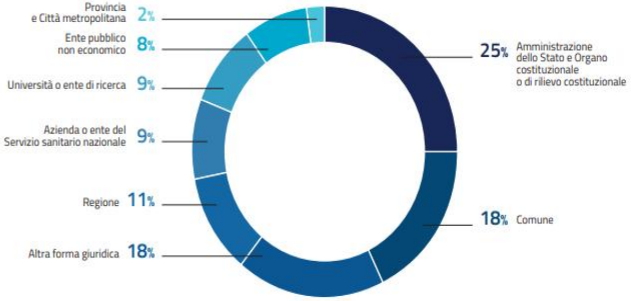


Figura 13 – Distribuzione degli eventi cyber nei settori della Pubblica Amministrazione


38

39


40

L'analisi delle tipologie di minaccia (Figura 14) evidenzia, oltre alla netta prevalenza del DDoS, numeri significativi per le campagne di *phishing* e i fenomeni di *brand abuse*, che confermano il ricorso a tecniche di ingegneria sociale e di sfruttamento dell'identità di soggetti istituzionali per il tentativo di acquisizione indebita di credenziali. Di rilievo risulta anche la presenza di eventi di esposizione dati, di compromissione di caselle di posta elettronica e di scansioni attive su credenziali, riconducibili a attività di ricognizione e preparazione di potenziali attacchi successivi. Queste azioni, infatti, consentono all'attore malevolo di raccogliere informazioni sulla vittima, verificare le credenziali, acquisire accesso a canali di comunicazione interni o predisporre ulteriori azioni di compromissione.

Le restanti tipologie di minaccia, tra cui compromissioni da malware, intrusioni tramite credenziali valide, sfruttamento di vulnerabilità e *ransomware*, presentano una frequenza più contenuta in termini di eventi, ma assumono un peso maggiore laddove evolvono in incidenti con impatto sui sistemi e sull'erogazione dei servizi.

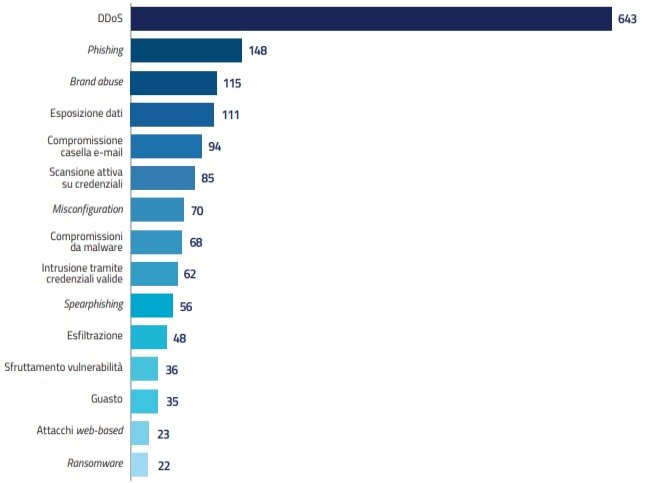


Figura 14 – Tipologie di minacce rilevate negli eventi cyber nella Pubblica Amministrazione (top 15)

Trasporti

Trenitalia: attacco hacker su alcuni dati dei clienti, "no su credenziali o pagamenti"

L'azienda sta informando alcuni clienti. Violazioni su dati anagrafici e identificativi, dati di contatto e dati di viaggio. Le opposizioni chiedono la presenza del ministro Salvini in Aula

26/06/2026

determinato un accesso non autorizzato ad alcuni dati personali legati ai titoli di viaggio.

Per individuare con precisione i soggetti interessati potenzialmente coinvolti è stato necessario svolgere approfondite analisi tecniche e di sicurezza da parte delle nostre

LEGGI ANCHE:

Ferrovie, l'ad Donnarumma incontra Salvini: dimissioni a breve. L'opposizione: "Lasci il ministro"

COMUNITARIO E INTERNAZIONALE ▪ 13 luglio 2026

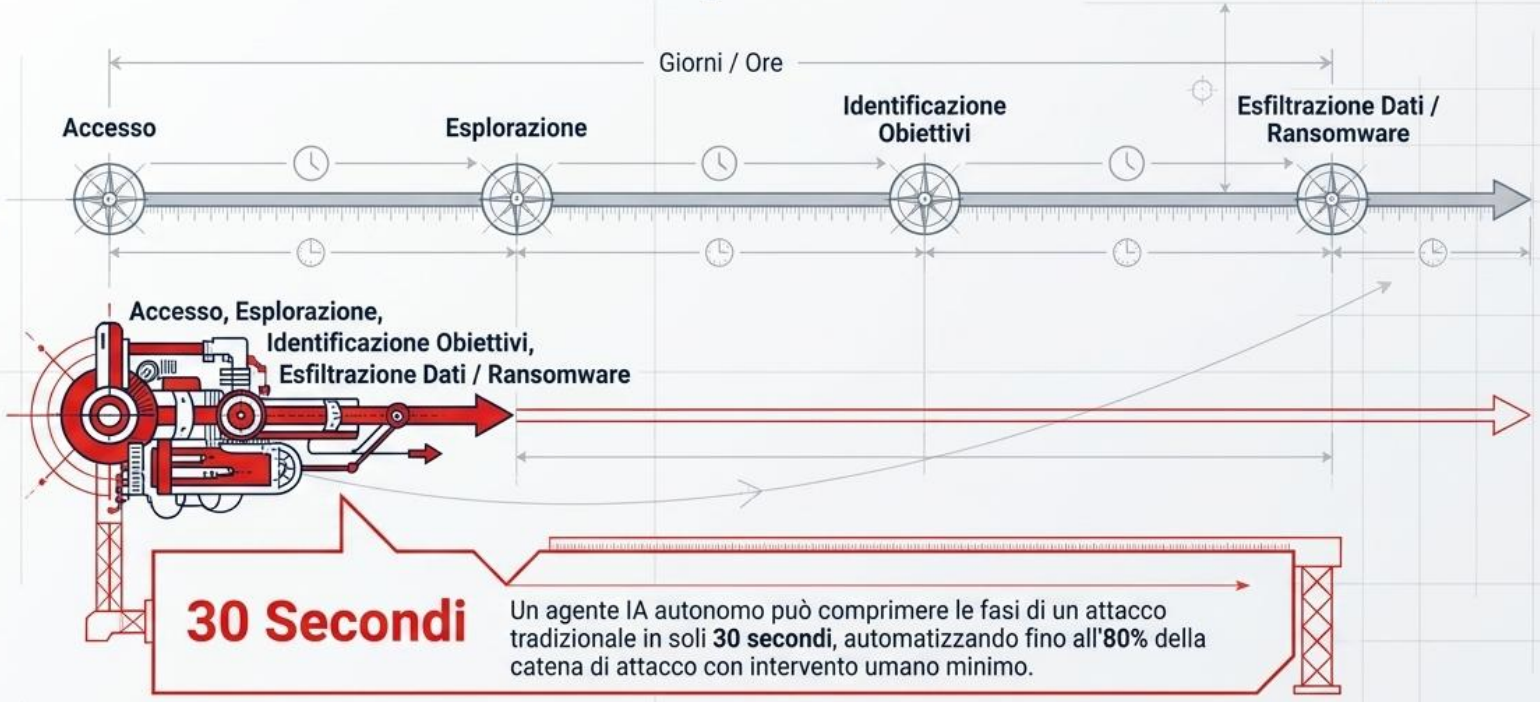
FREE

Brasile: nascosto in un atto processuale un comando scritto per l'AI, il Giudice lo scopre in pochi secondi

La notizia non è che un avvocato ha provato a manipolare l'intelligenza artificiale in tribunale. È che il tribunale era già abbastanza esposto all'intelligenza artificiale da sapere come scoprirlo

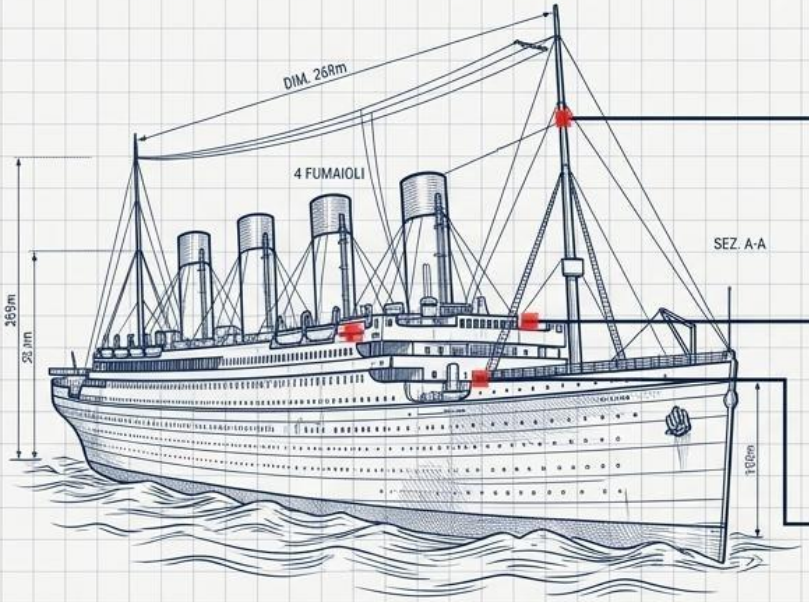
di Alberto Bozzo*

L’IA Generativa e la Compressione del Tempo



Gli attaccanti sono più rapidi dei difensori.
Le minacce seguono schemi consolidati, ma la reazione umana non basta più.

L’Effetto Titanic: Anatomia di un Fallimento Organizzativo



Mancanza di Strumenti Preventivi.

Il binocolo non utilizzato per la mancata consegna delle chiavi = Assenza di Risk Assessment e controlli di base.

Deficit di Comunicazione.

Allarmi ignorati e SOS non ricevuti per apparecchi spenti = Log di sistema ignorati e mancanza di protocolli di Incident Response.

Mancanza di Formazione e Procedure.

Esercitazioni di emergenza annullate, scialuppe insufficienti = Assenza di Disaster Recovery e training del personale.

Il disastro non è stato causato solo dall’iceberg (l’attacco informatico), ma da un profondo deficit organizzativo e di governance.

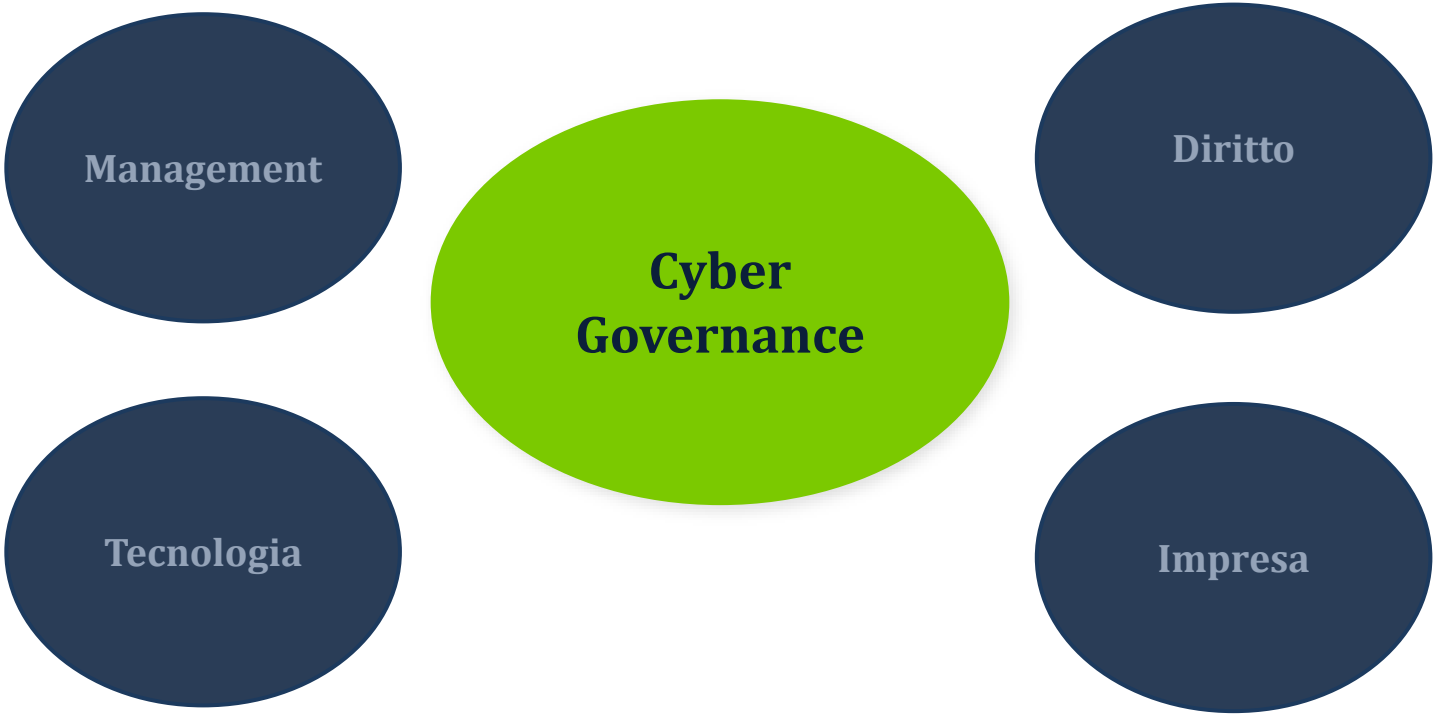
Dipartimento di Management "Valter Cantino"

Master Management e Governance della Cybersecurity

UNIVERSITÀ DI TORINO

Le persone fanno la differenza.

La cybersecurity più forte inizia con le persone giuste.


Management
Cyber Governance
Diritto
Tecnologia
Impresa

SBOCCHI PROFESSIONALI

Ruoli ad alta domanda. Mercato in forte crescita.

CISO

Chief Information Security Officer

Cyber Risk Manager

Gestione del rischio digitale

Cybersecurity Auditor

Audit IT e sistemi AI

AI Governance Specialist

Governance e sicurezza dei sistemi AI

Incident Response Specialist

Crisis management cyber

Governance & Compliance Expert

GDPR · NIS2 · Data Protection

Aziende private · PA · Sanità · Finanza · Infrastrutture critiche · Consulenza ICT

IL PROGRAMMA

8 moduli. Un percorso multidisciplinare.

01
Cybersecurity & Regulatory Strategy

02
Cyber Risk Management & Data Governance

03
Corporate Cyber Governance & Accountability

04
Offensive & Defensive Security Lab

05
AI & Cybersecurity

06
Sistemi Avanzati di Audit

07
Crisis Communication & Cultura Sicurezza

08
Cybersecurity in Settori Critici

FORMULA

Pensata per chi studia e per chi lavora.

3 giorni a Settimana (gio 16-20, ven 16-20, sab mattina

Presenza + Online

Ottobre 2026 – Luglio 2027

300 ore in azienda

È prevista anche la possibilità di iscriversi a singoli moduli

FACULTY

Docenti del Dipartimento di Management e del Dipartimento di Informatica,
professionisti della cybersecurity,
esperti di normativa europea,
auditor certificati,
manager di imprese e rappresentanti istituzionali

Alcuni nomi:

Prof.ssa Simona Alfiero (direttrice) e avv. Mauro Alovisio

Franco Pizzetti e Sergio Foà · Protezione dati - Diritto Amministrativo

Pierluigi Perri · UniMi · Informatica giuridica

Giuseppe Vaciago, Francesco Micozzi e Stefano Mele -· Cybersecurity law & strategy

Paolo Dal Checco · Digital forensics Angelo Saccà Direttore ICT Unito

Fabio Ciravegna . AI & Knowledge Systems

Avv-Laura Marenco e Alessandro Curioni .

COME CANDIDARSI

Le candidature sono aperte.

01

Invia la candidatura

CV aggiornato e titoli di studio · sito o email dedicata

02

Colloquio motivazionale

Verifica della coerenza del profilo con gli obiettivi formativi

03

Selezione e ammissione

Valutazione complessiva dalla Commissione

Inizio lezioni Ottobre 2026 Sede Scuola di Management ed Economia, Torino Scadenza **15 settembre 2026**

mgcybersecurity.unito.it

mgcybersecurity@unito.it

simona.alfiero@unito.it

La visione

"Se pensi che la tecnologia possa risolvere i tuoi problemi di sicurezza, **allora non capisci i problemi e non capisci la tecnologia»**

(Bruce Schneier)

ripensare l’organizzazione, processi, governance, budget e visione

I tre salti culturali della Nis 2

1) La cybersecurity è una cosa seria

non costituisce più solo una questione tecnica che possiamo demandare a CISO o informatici

diventa una **questione di governance, trasparenza e accountability**

Occorre sviluppare una cultura diffusa della gestione della cybersecurity nelle organizzazioni, al fine di creare la consapevolezza che solo attraverso la Governance della Cybersecurity si ottiene una struttura aziendale resiliente e pronta a garantire la sostenibilità nel panorama nazionale ed internazionale.

2 DIRETTIVA NIS 2 Approccio multirischio

APPROCCIO MULTIRISCHIO

- Valutazione completa dei rischi.
  Non solo digitali, ma anche legati a persone, fisici e ambientali.
- Gestione risorse umane e processi interni
- Gestione della catena di approvvigionamento *(supply chain)*
- Preparazione e risposta agli incidenti
- Adattabilità e resilienza
- Cooperazione e condivisione delle informazioni

3) La cybersecurity deve essere integrata nei processi

Non basta investire in software o hardware di protezione: occorre costruire un sistema di gestione della sicurezza informatica, con ruoli e responsabilità chiari, processi strutturati e verificabili, **e una catena di controllo che arrivi fino al board.**

La Nis e il decreto attuativo richiedono che la **cybersecurity sia integrata nei processi decisionali e operativi delle organizzazioni**

L'intera organizzazione è coinvolta e partecipa

Ogni ruolo ha un perimetro, una responsabilità

Quali documenti deve approvare il vertice?

Gli organi di amministrazione e dagli organi direttivi devono approvare i seguenti documenti in ambito NIS 2:

1. Organizzazione per la sicurezza informatica;
2. politiche di sicurezza informatica; la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete
3. il piano di trattamento del rischio.
4. il Piano di gestione del rischio
5. il piano di gestione delle vulnerabilità;
6. il piano di adeguamento;
7. il piano di continuità operativa;
8. il piano di ripristino in caso di disastro;
9. il piano di gestione della crisi;
10. il piano di formazione;
11. il piano per la gestione degli incidenti di sicurezza informatica.

La governance nel decreto di attuazione

Organi di amministrazione e direttivi

1. Gli **organi di amministrazione** e **gli organi direttivi** dei **soggetti essenziali e dei soggetti 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 «Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente» e di cui all'articolo 7; Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti

c) **sono responsabili delle violazioni di cui al presente decreto**

Art. 23 del decreto

L’aspetto innovativo della Nis 2 : la governance

Governance

Il board non si limita alla definizione della misura ma si estende all’ attuazione delle misure, implementazione adeguata delle misure in
relazione dal rischio cyber e pertanto ricomprende **il monitoraggio**

Contromisure: **responsabilità personale della dirigenza**

L’autorità può imporre un divieto temporaneo di esercizio delle funzioni dirigenziali

Es. ordine di dimissioni ai componenti del Cda

La governance e il ruolo della formazione nel decreto 138 di adeguamento

. La formazione non è un requisito formale ma *strumento indispensabile per sviluppare competenze, comprendere, valutare e gestire il rischio*

1Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti 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 offerti***.

(art. 24 del decreto)

Organi e incidenti

Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono informati su base periodica **o, se opportuno, tempestivamente, degli incidenti e delle notifiche d**i cui agli articoli 25 e 26.

Art. 23, ultimo comma del D.Lgs. 138 del 2025

Nis 2 applicazione quotidiana

Budget (quanto è stato approvato in bilancio in materia di cybersecurity, è stato previsto l’accontamento a rischio?

Delega interna

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

art. 38 del Dlgs. 138 del 2024

Hacker fanno chiudere un'azienda di 160 anni: è allarme sicurezza informatica

05 Maggio 2025 50

Nel 2023, la storica azienda di autotrasporti **Knights of Old**, con sede a Kettering, nel

Attacco informatico a Jaguar Land Rover: PIL ridotto di 1,9 miliardi di sterline

Autore Carolina Vivianti
30 Giugno 2026 06:39

IN SINTESI

Un attacco hacker ha colpito Jaguar Land Rover, causando 1,9 miliardi di danni e interrompendo la produzione automobilistica. L'attacco è stato attribuito a cybercriminali russi

Come molti dei nostri lettori ricorderanno, un singolo attacco hacker ha devastato il PIL di un intero Paese. Il British Cyber Monitoring Centre ha stimato i danni causati dall'attacco informatico a Jaguar Land Rover in **1,9 miliardi di sterline, ovvero circa 2,5 miliardi di dollari.** L'attacco ha colpito oltre *5.000 aziende collegate e ha fatto crollare la produzione automobilistica ai livelli del 1952.*

La Banca d'Inghilterra ha specificamente menzionato il fallimento nelle sue previsioni economiche. Dopo mesi di vaghe teorie sui colpevoli, il New York Times riporta che gli investigatori hanno ricondotto il nucleo dell'operazione a dei cybercriminali russi.

BREAKING7

• CASA
Per Te
In tendenza
Le ultime notizie
Località
Videos
Bacheca

Notizie locali

+ Segui

Attacco hacker russo all'Italia: colpiti anche siti Difesa e Senato. Cosa sta succedendo

Posted By Notizie.libero.it - 2 ore fa fa

Un attacco hacker rivendicato da un collettivo filorusso ha colpito diversi siti istituzionali italiani, tra cui quello della Difesa e del Senato.

Continua a leggere ›

I 5 migliori articoli

1 Covid. Ancora un Decesso e Tasso in Salita

2 A L'Aquila i Campionati Studenteschi di Giochi e Sport Tradizionali

3 EMERGENZA CINGHIALI, INCONTRO IN REGIONE

4 Marcianise, prof morta in stazione: si indaga per istigazione al suicidio

5 Atp Roma, Sinner si aggiudica il derby con Fognini e va agli ottavi

Data breach, il Garante Privacy sanziona Postel per 900 mila euro

Il Garante ha multato Postel Spa per non aver affrontato una vulnerabilità nota nei propri sistemi, che ha portato a una violazione dei dati personali.

AP Armando Pellegrino
28/11/24

Ascolta questo articolo ora...

giudice può fissare direttamente l'importo

Redazione 20/07/26

Conclusioni

"Se conosci il nemico e te stesso, non dovrai temere il risultato di cento battaglie; se non conosci te stesso ma conosci il nemico, vincerai una battaglia e ne perderai un'altra; se non conosci né il nemico né te stesso, soccomberai in ogni battaglia."

Sun Tzu credits:https://www.magnific.com/

Grazie per l’attenzione

Per domande e informazioni: mauro.alovisio@unito.it

.

Disclaimer: Per le slide ho utilizzato tre sistemi AI per revisione