

LA CYBERSECURITY NON È PIÙ SOLO UN PROBLEMA IT

È una questione di sicurezza nazionale...
e aziendale

Le tensioni tra Stati si combattono sempre più nel dominio digitale; gli attacchi ibridi che combinano disinformazione, sabotaggio infrastrutturale e intrusioni nei sistemi critici sono realtà documentate

Dalla compromissione alla destabilizzazione

L'obiettivo non è il denaro: è l'effetto

Interrompere servizi essenziali, generare incertezza e il confine tra cyber e fisico è saltato: droni, ordigni e ransomware convivono nella stessa campagna:

SICUREZZA

Retelit Bucata da Qilin: 300GB, 2 Mesi di Silenzio [2026]

Get the Latest News

Home Threat Intelligence Vulnerabilities Cyber Attacks Webinars Expert insights Awards

Attacco hacker a infrastrutture Pa, indaga l'Antiterrorismo di Roma
Attacco hacker a TeamSystem, esposti migliaia di IBAN: chi riguarda?

the U.K.

espionage / Threat Intelligence

Italia attaccata dagli hacker cinesi, ecco come sono entrati (e sono rimasti settimane)

Sistemi Informativi, controllata IBM che gestisce ministeri, INPS, INAIL e sanità digitale, è stata violata per due settimane. ACN al lavoro, dati esposti ancora ignoti.



Germania · settembre 2026

Il gruppo ransomware Rhysida ha rivendicato l'esfiltrazione di circa 5,7 terabyte di dati dalla rete amministrativa del Lander di Berlino a ridosso delle elezioni



Lipsia-Halle · agosto 2026

Drone esplosivo tra i cargo militari. Il 1° settembre Berlino attribuisce l'attacco alla Russia.



Europa · settembre 2026 - Collins Aerospace

Un ransomware su un solo fornitore ferma i check-in a Heathrow, Bruxelles e Berlino.

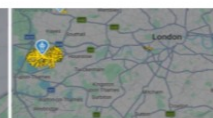
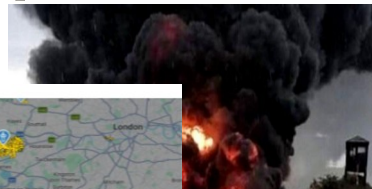
Guerra ibrida



Ordigni contro la centrale elettrica: Germania in massima allerta per i sabotaggi di Mosca. Pista russa anche per Lipsia

HOME » Germania sotto tiro: doppio attacco alla rete elettrica in 24 ore

Germania sotto tiro: doppio attacco alla rete elettrica in 24 ore



Caos voli nel Regno Unito, decolli bloccati in almeno 10 aeroporti: «guasto tecnico nel controllo del traffico». Tutto fermo anche a Heathrow e Gatwick

La banca come infrastruttura della fiducia

Per una banca l'impatto non è tecnico: continuità dei pagamenti, integrità delle scritture e fiducia del mercato diventano sicurezza nazionale.



Caos voli nel Regno Unito, un errore in un documento militare avrebbe mandato in tilt il sistema



Che cosa è cambiato nel 2026

Marzo 2026: i data center diventano bersaglio

Droni sui data center AWS nel Golfo: pagamenti digitali e app bancarie fermi per ~50 milioni di persone.

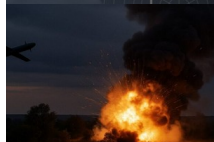


Settembre 2026: il cloud che non si ripristina

Danni di guerra: AWS non riesce a ripristinare l'accesso al cloud in Bahrain e in una zona degli Emirati, con impatti sulle infrastrutture critiche



La guerra invisibile. Quando i data center diventano obiettivi militari



INFRASTRUTTURE CRITICHE

Iran, attacchi ai datacenter: così la guerra cambia la cyber security

Il confine tra sicurezza aziendale e dell'ecosistema

Il perimetro difendibile è una **finzione contabile**.

LA FILIERA



L'attaccante entra dal punto di maggior vulnerabilità e risale la catena.

La catena del rischio non si ferma al grande fornitore



La forte **interdipendenza** tra fornitori tecnologici crea un effetto moltiplicatore: colpendo un **singolo fornitore**, un **attore statale** può raggiungere numerose imprese e trasformare un **incidente** in una **minaccia sistemica**.

LinkedIn

The Hacker Who Almost Stole the Internet: The Inside Story of the XZ Backdoor

CYBERSECURITYITALIA

Toyota: un attacco ransomware costringe a fermare la produzione

Westpole e l'attacco informatico che sta paralizzando pubblica amministrazione. Cosa sta succedendo

Volkswagen Subsidiary Cariad Exposes Data of 800,000 Electric Vehicles

Avis Confirms Data Breach Affecting Nearly 300,000 Customers

TECH CNBC MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING

Hackers steal \$1.5 billion from exchange Bybit in biggest-ever crypto heist

PUBLISHED FRI, FEB 21 2025-5:21 PM EST | UPDATED SAT, FEB 22 2025-11:32 AM EST

Portare il rischio al tavolo che decide

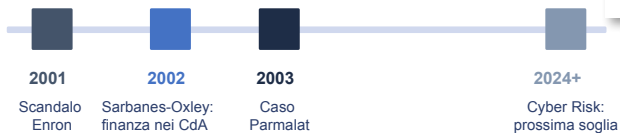
Al tavolo del Board non si porta un allarme: si portano scenari, opzioni e conseguenze.
Ma per decidere tra le opzioni serve competenza: essere informati è solo il primo passo



Il precedente è noto

Dopo gli scandali contabili, la **competenza finanziaria** è diventata una **presenza stabile** nei CdA.

Oggi il **rischio tecnologico** sta seguendo lo **stesso percorso**.



ECONOMIA E FINANZA

Crac Parmalat: la storia dello scandalo finanziario che ha cambiato l'Italia

Italyfinanza · 12 Mesi Ago · 0 · 8 Mins

ATTUALITÀ

Worldcom: lo scandalo finanziario che scosse il mondo delle telecomunicazioni

Lo scandalo WorldCom, che scosse il mondo della telecomunicazione nei primi anni duemila. Una grandissima frode finanziaria e qui cerchiamo di ricostruire come è andata.

La truffa che sconvolse Wall Street (e non la cambiò per niente): i 20 anni del crac della Enron

Il 2 dicembre 2001 dichiarava bancarotta una delle più grandi compagnie energetiche del mondo: la storia di un crac da 65 miliardi di dollari



«Chi di noi sa?»

La **competenza Cyber interna al CdA** non è più un'opzione.

STEP 1 Awareness

Il Board conosce il rischio cyber

STEP 2 Informazione

Il Board comprende le implicazioni

STEP 3 Competenze

Il Board valuta e decide autonomamente