Ufficio Stampa della Provincia autonoma di Trento
Piazza Dante 15, 38122 Trento
Tel. 0461 494614 - Fax 0461 494615
uff.stampa@provincia.tn.it

COMUNICATO n. 3081 del 20/10/2025

Il dato arriva dalla prima giornata dell’evento dedicato alla sicurezza informatica, organizzato da Trentino Digitale , Acn e Cerchio Ict

Cybercrime, le pubbliche amministrazioni locali sono sotto attacco

Le pubbliche amministrazioni locali sono tra i settori più interessati dagli attacchi informatici. Il numero di vittime per attacco è aumentato nel corso del primo semestre del 2025 del 542% rispetto allo stesso periodo dello scorso anno. I settori che hanno subito un incremento maggiore di vittime per evento sono le società di servizi (Acqua, + 480%), le università e gli istituti di ricerca (+315%), le società private (+278%) e la Sanità (+273%). I dati nazionali sono emersi oggi in occasione dell’evento "Cybersecurity nella PA: strategie e azioni" che si è tenuto negli spazi del palazzo della Provincia autonoma. All’emergenza del crimine informatico, il Trentino risponde con azioni concrete, ribadite dal vicepresidente della Provincia autonoma di Trento, Achille Spinelli: “La sicurezza informatica non è più un argomento per pochi esperti, ma una priorità assoluta per la pubblica amministrazione, per le imprese e per ogni cittadino. Viviamo in un'era in cui la digitalizzazione permea ogni aspetto della nostra vita, offrendo opportunità straordinarie ma esponendoci anche a rischi sempre più complessi e sofisticati. Il Trentino, grazie anche alla in-house Trentino Digitale, investe da tempo sulla sicurezza, non solo in tecnologia ma anche in risorse umane e sinergie con le più importanti realtà nazionali ed europee”. A conferma dell'impegno della Provincia autonoma di Trento nella tutela dei dati e dei servizi arriva la notizia dell’istituzione dello Csirt della Provincia autonoma di Trento (Computer Security Incident Response Team), gruppo specializzato nella prevenzione, rilevamento, analisi e risposta agli incidenti di sicurezza informatica, con l’obiettivo di supportare gli enti locali nel mitigare i rischi, coordinare le attività in caso di attacchi e condividere informazioni con altre istituzioni e partner, sia a livello nazionale che internazionale.

La conferenza "Cybersecurity nella PA: strategie e azioni" è organizzata dalle quattro società in-house - Trentino Digitale, Informatica Alto Adige, Lepida (Emilia Romagna) e Pasubio Tecnologia (Schio/Veneto), riunite nell'accordo di rete "Cerchio ICT" - in collaborazione con l'Agenzia per la Cybersicurezza Nazionale (ACN) e vede la partecipazione delle amministrazioni regionali e provinciali, della Polizia postale e del Csirt Italia di Acn. Mercoledì è in programma, presso le sale della cantina Rotaliana di Mezzolombardo, la seconda giornata con la simulazione di un attacco informatico, alla quale parteciperanno i responsabili degli enti locali di Trentino ed Alto Adige.

La minaccia cyber e l'impegno di Trentino Digitale
Come evidenziato nel corso dell'evento da Kussai Shahin, direttore generale di Trentino Digitale, i numeri degli attacchi cyber subiti dalla pubblica amministrazione sono in costante crescita. Nel primo semestre del 2025 si è registrato un significativo aumento delle vittime di eventi cyber rispetto al 2024, confermando la gravità della minaccia e la necessità di strategie e azioni coordinate. Con circa 18.000 postazioni di lavoro e 2.200 server gestiti, Trentino Digitale si trova in prima linea nella difesa del sistema pubblico, monitorando

in maniera continuativa oltre 4.000 fonti per la gestione delle informazioni, grazie al Security operation center (Soc) attivo 24 ore su 24 e 7 giorni su 7.

Il richiamo alla collaborazione
Nel corso del suo intervento, Maria Vittoria Mottes, assessore del Consiglio delle autonomie locali con delega alla Digitalizzazione e sindaco di Fai della Paganella, ha sottolineato "l'urgenza di rafforzare la collaborazione tra gli enti territoriali e Trentino Digitale per contrastare efficacemente il cybercrime".

La richiesta di supporto a Trentino Digitale evidenzia il ruolo cruciale della società in-house come punto di riferimento per la sicurezza informatica del territorio, così come ribadito dal presidente Paolo Girardi: "L''evento odierno è importante per condividere lo stato dell'arte, le azioni in corso e le novità normative a cura dell'Agenzia della Cybersicurezza Nazionale (ACN), che ringraziamo per la fattiva collaborazione, sin dalla sua nascita, con Trentino Digitale, e per tracciare un percorso che va rafforzato, tutti insieme, a favore del Sistema Trentino. La cybersicurezza - ha proseguito il presidente Girardi - è questione culturale e richiede l'impegno e il contributo di tutti, anche come singoli, ciascuno per la sua parte. Pertanto informazione e formazione continue sono indispensabili per accompagnare azioni e tecniche di monitoraggio, protezione e gestione degli incidenti. In questo, Trentino Digitale gioca un ruolo centrale a favore del sistema pubblico e tutto il sistema del territorio Trentino".

Sulla capacità di fare sistema si è speso Antonino Di Napoli, responsabile del Centro operativo per la sicurezza cibernetica del Trentino-Alto Adige della Polizia di Stato: "Il passaggio al digitale - ha esordito Di Napoli - è stato repentino e non abbiamo avuto il tempo per assimilare comportamenti adeguati. Giornate come queste sono fondamentali per fare rete e diffondere una nuova cultura a tutela della sicurezza della struttura informatica. Il nostro ruolo è basato sulla prevenzione, grazie anche al protocollo d'intesa sottoscritto con Trentino Digitale, in modo tale da agire durante l'attacco cyber, analizzare la macchina e cercare di capire la falla. L'azione più importante è però condividere le informazioni e le migliori pratiche, investire sulla prevenzione e la crescita del capitale umano".

Il ruolo dell'Agenzia per la cybersicurezza nazionale. La giornata odierna, moderata dal direttore generale di Trentino Digitale, Kussai Shahin, ha visto un'intensa sessione dedicata ai rappresentanti dell'Agenzia per la cybersicurezza nazionale, che ha preso il via con i saluti istituzionali dell'Ammiraglio Gianluca Galasso, Capo del Servizio operazioni e gestione delle crisi cyber, il quale ha evidenziato come le iniziative del PNRR, le indicazioni della normativa NIS2, la collaborazione tra lo CSIRT Italia e i territori rappresentano tutte opportunità per alzare lo standard di protezione del Paese e rendere più rapida ed efficace la risposta agli incidenti informatici in un'ottica di sistema.

Agostino Sperandeo, Capo Divisione strategia e politiche di cybersicurezza nazionale, e **Luigi Addorisio De Feo**, del Servizio programmi industriali, tecnologici e di ricerca di ACN, hanno presentato le azioni a supporto del potenziamento della postura di cybersicurezza della pubblica amministrazione, con particolare riguardo agli interventi di attuazione della Strategia nazionale di cybersicurezza 2022-2026. Le leve economiche includono l'investimento 1.5 del PNRR e i fondi dedicati all'attuazione della Strategia nazionale, che con l'esaurirsi dei finanziamenti europei saranno il principale strumento a disposizione della PA in ambito cybersicurezza. Rispetto ad essi, ACN svolge un ruolo di coordinamento e monitoraggio.

Nicolò Rivetti Di Val Cervo, Capo divisione Nis e discipline unionali di Acn, ha approfondito la Direttiva NIS2 e le sue implicazioni per pubblica amministrazione e imprese. La direttiva, in sintesi, introduce nuovi settori e soggetti per la cybersicurezza e classifica le pubbliche amministrazioni come essenziali o importanti. Gli obblighi di sicurezza sono proporzionati e graduali nel tempo, così come sono previste misure di sicurezza di base e a lungo termine, mentre la notifica degli incidenti significativi è obbligatoria per tutti i soggetti.

Il Trentino e la strategia per la Cybersicurezza
Il ruolo della Provincia autonoma di Trento è fondamentale per garantire la sicurezza dell'ecosistema digitale e dei servizi che abilitano il rapporto tra la pubblica amministrazione, cittadini ed imprese. Daniela Ceccato, dirigente servizio ICT e trasformazione digitale della Provincia, ha presentato la strategia cybersecurity provinciale: "La crescente diffusione delle tecnologie, l'espansione dei servizi digitali e l'aumento degli attacchi informatici verso enti pubblici e infrastrutture locali rendono la cybersicurezza un fattore abilitante fondamentale. In Trentino, la strategia si basa su un approccio articolato che combina

allineamento normativo, potenziamento tecnologico e infrastrutturale, sviluppo di capacità interne (formazione del personale) e creazione di una struttura di risposta agli incidenti. Un elemento chiave - ha annunciato Ceccato - è la creazione del CSIRT (Computer Security Incident Response Team) della Provincia autonoma di Trento, finanziato dal Pnrr, con l'obiettivo di migliorare le capacità di prevenzione e gestione degli incidenti informatici sul territorio".

E proprio sul ruolo e i servizi di cybersicurezza del Csirt della Provincia autonoma di Trento è intervenuto Francesco Telch, responsabile Area cyber security di Trentino Digitale. "Il team garantisce un servizio strategico per la sicurezza del territorio, focalizzato su prevenzione e risposta. Trentino Digitale lo eroga grazie al suo ruolo strategico di gestore della rete provinciale, garantendo monitoraggio h24 e protezione trasversale. Il modello operativo si articola in cinque aree di servizio: gestione degli eventi di sicurezza informatica, conoscenza dello stato di sicurezza attuale, trasferimento di conoscenze, gestione delle vulnerabilità e gestione degli incidenti di sicurezza informatica".

L'obiettivo principale dell'ecosistema cybersicurezza in Trentino, come ribadito dal dg Kussai Shahin, è in definitiva quello di rafforzare la resilienza del sistema pubblico provinciale, supportandolo nella gestione del panorama cyber e collegandolo alla rete di difesa nazionale.

La seconda giornata di mercoledì prossimo
L'evento offrirà anche un'occasione unica per partecipare attivamente a una simulazione di attacco informatico nella giornata del 22 ottobre a Mezzolombardo, a partire dalle ore 9.30. Il programma prevede la mattina la presentazione dei servizi di Csirt Italia e nel pomeriggio, l'esercitazione "table top" condotta, sempre insieme a Csirt Italia, per testare tempi di reazione, coordinamento e resilienza dei team ICT pubblici e dei responsabili degli enti locali presenti.

L'iniziativa "Cybersecurity nella PA: strategie e azioni" si configura come un laboratorio di cooperazione interistituzionale, dove la condivisione delle competenze, la solidarietà operativa e la costruzione di una rete di protezione digitale sono al centro di un percorso volto a rendere la pubblica amministrazione più consapevole, preparata e resiliente di fronte alle sfide della cybersicurezza.

Per maggiori informazioni e per il programma completo, si prega di visitare il sito cerchioict.it/cybersecurity-2025.

Coperture e interviste video:
https://drive.google.com/drive/folders/1zDc-AWdsllsd2aopInlnV-HYXuq18ZqB?usp=sharing

(pff)