Comunicato stampa

ALLARME BOMBA NELLE SCUOLE, CNI: «SERVE MAGGIORE PREVENZIONE SULLA CYBERSICUREZZA. UNA SEMPLICE MAIL HA SCATENATO IL PANICO»

Il Consiglio Nazionale degli Ingegneri interviene dopo le minacce inviate a migliaia di istituti scolastici italiani. Perrini: «La sicurezza digitale è anche capacità di prevenire e gestire le emergenze». Cappiello: «Fondamentale valorizzare le competenze degli ingegneri dell'informazione». Annunziata: «Non serve necessariamente violare un sistema per provocare conseguenze rilevanti. Occorrono formazione, strumenti di verifica e procedure condivise».

Una semplice e-mail può essere sufficiente a generare un'emergenza su scala nazionale, provocando evacuazioni, interruzioni delle attività scolastiche e un diffuso stato di allarme tra studenti, famiglie e personale degli istituti. È quanto dimostra l'episodio di mercoledì 11 novembre, quando comunicazioni anonime contenenti minacce di attentati sono state recapitate a oltre 6.000 scuole italiane, determinando l'intervento delle Forze dell'Ordine e l'attivazione di misure precauzionali in numerosi istituti. L'accaduto richiama l'attenzione su una dimensione della cybersicurezza che non riguarda esclusivamente la protezione dei sistemi dalle intrusioni, ma anche la capacità delle organizzazioni di riconoscere, valutare e gestire minacce veicolate attraverso gli strumenti digitali.

«Quanto accaduto nelle scuole italiane dimostra che la sicurezza digitale ha conseguenze molto concrete sulla vita delle persone - afferma **Angelo Domenico Perrini, Presidente del Consiglio Nazionale degli Ingegneri -**. Una comunicazione elettronica è stata sufficiente a generare preoccupazione in migliaia di famiglie, interrompere attività didattiche e mobilitare uomini e mezzi per le necessarie verifiche. La sicurezza informatica non può essere considerata soltanto una questione tecnologica: riguarda la capacità delle nostre istituzioni di prevenire i rischi, affrontare le situazioni critiche e garantire la continuità dei servizi. Come sistema ordinistico siamo pronti a mettere le nostre competenze al servizio di questo obiettivo».

SCUOLE PIÙ PREPARATE, NON SOLTANTO SISTEMI PIÙ PROTETTI

Per il CNI, l'episodio deve rappresentare un'occasione per rafforzare la preparazione delle istituzioni scolastiche di fronte alle minacce digitali. Accanto agli strumenti tecnologici di protezione, è necessario investire nella formazione dei dirigenti e del personale, nella capacità di riconoscere comunicazioni sospette e nell'adozione di procedure condivise che

consentano una tempestiva interlocuzione con le autorità. L'obiettivo non è sottovalutare le minacce o scoraggiare l'adozione delle misure di sicurezza necessarie, ma garantire che le decisioni siano assunte sulla base di informazioni attendibili, valutazioni appropriate e indicazioni delle Forze dell'Ordine. Un ruolo importante può essere svolto dagli ingegneri dell'informazione, le cui competenze permettono di affrontare in maniera integrata gli aspetti tecnologici, organizzativi e procedurali della sicurezza.

«La vicenda delle scuole dimostra quanto sia importante riconoscere il valore delle competenze professionali nella gestione dei sistemi digitali - sottolinea **Carla Cappiello, Vicepresidente Vicario del CNI con delega al settore dell'Informazione -**. La proposta avanzata dal Consiglio Nazionale nell'ambito della riforma degli ordinamenti professionali va proprio nella direzione di definire meglio le competenze e le responsabilità degli ingegneri dell'informazione. La crescente dipendenza dai sistemi digitali rende indispensabile una maggiore attenzione alla qualità della progettazione, alla gestione dei rischi e alla qualificazione di chi è chiamato a garantire la sicurezza e l'affidabilità dei servizi. Anche il mondo della scuola deve poter contare su competenze tecniche adeguate, perché la prevenzione non può essere lasciata all'improvvisazione».

UNA MINACCIA INFORMATICA PUÒ PRODURRE EFFETTI ANCHE SENZA UN'INTRUSIONE

Secondo le informazioni finora disponibili, l'episodio si configura come una campagna di comunicazioni minatorie su larga scala. Non risultano, allo stato, evidenze pubbliche di una compromissione dei sistemi informatici degli istituti scolastici destinatari delle e-mail. Si tratta di una distinzione fondamentale: **non è necessario violare l'infrastruttura informatica di un'organizzazione per provocare conseguenze significative sul suo funzionamento**. L'invio massivo di messaggi può infatti raggiungere contemporaneamente migliaia di destinatari, generare disorientamento e innescare una sequenza di verifiche e interventi. La disponibilità pubblica degli indirizzi istituzionali può agevolare campagne di questo tipo, senza che ciò comporti necessariamente accessi non autorizzati alle reti delle organizzazioni coinvolte.

Un ulteriore elemento di attenzione riguarda l'identità digitale del mittente. Un indirizzo apparentemente riconducibile a un dominio reale non costituisce, di per sé, una garanzia sull'effettiva provenienza del messaggio. Per accertare le modalità utilizzate nel caso specifico sono necessarie verifiche tecniche e investigative.

«L'episodio evidenzia un aspetto spesso sottovalutato della cybersicurezza: l'impatto di una minaccia non dipende necessariamente dalla complessità dello strumento utilizzato - spiega **Gennaro Annunziata, Coordinatore del C3i, Comitato Italiano Ingegneria dell'Informazione del CNI -**. Anche una campagna di e-mail può produrre effetti rilevanti quando colpisce contemporaneamente migliaia di organizzazioni. Per questo è indispensabile un approccio che integri la protezione della posta elettronica, il monitoraggio delle minacce, la formazione del personale e procedure chiare per la gestione delle segnalazioni. La sicurezza non consiste soltanto nell'impedire un'intrusione, ma anche nel saper riconoscere tempestivamente una

minaccia, valutarne la credibilità e limitarne le conseguenze, sempre in coordinamento con le autorità competenti».

L'IMPEGNO DEL C3I PER LA CULTURA DELLA CYBERSICUREZZA

Il tema della sicurezza informatica è da tempo al centro dell'attività del **C3i**, all'interno del quale opera un gruppo di lavoro specificamente dedicato alla cybersicurezza, impegnato nell'approfondimento delle problematiche tecniche e professionali legate alla protezione dei sistemi e delle infrastrutture digitali.

L'episodio delle e-mail minatorie dimostra quanto sia necessario affiancare alla sicurezza tecnologica una maggiore consapevolezza dei rischi e una preparazione organizzativa adeguata.

«Il gruppo di lavoro sulla cybersicurezza del C3i è particolarmente attivo nell'approfondimento di queste problematiche - aggiunge **Annunziata -** La vicenda delle scuole ci ricorda che la sicurezza deve essere affrontata come un problema di sistema. Non basta disporre di strumenti di protezione: occorre sapere come utilizzarli, come interpretare le segnalazioni e come reagire in modo coordinato. Il nostro impegno è contribuire alla diffusione di questa cultura della prevenzione, mettendo le competenze degli ingegneri dell'informazione a disposizione del sistema ordinistico e favorendo il confronto con le istituzioni».

Il CNI ritiene che la **rete degli Ordini territoriali** possa rappresentare una risorsa importante per promuovere iniziative di sensibilizzazione e formazione sui temi della sicurezza digitale, anche attraverso il dialogo con le istituzioni scolastiche e le amministrazioni competenti.

«La risposta a episodi come quello dell'11 novembre non può esaurirsi nella gestione dell'emergenza - conclude **Perrini -**. Occorre investire nella prevenzione, nella formazione e nella capacità delle organizzazioni di affrontare i rischi digitali. La scuola è un luogo particolarmente importante da cui partire, perché proteggere le sue attività significa tutelare studenti, famiglie e personale. Gli ingegneri sono pronti a fare la propria parte, mettendo a disposizione competenze e cultura della sicurezza nell'interesse dell'intera collettività».

Roma 12 novembre 2026

Antonio Felici

Capo Ufficio Stampa

Consiglio Nazionale degli Ingegneri

Via XX Settembre 5 - 00187 Roma

tel 06.69.76.701

cell 347-8761540

www.cni.it