AbruzzoWeb
Tutte le notizie d'Abruzzo a portata di click

“HACKER MINACCIA PER NOSTRA VITA QUOTIDIANA” URBANI, “ALLARMI BOMBA, IMPORTANTE VERIFICARLI”

16 Novembre 2026



L’AQUILA – “Più digitalizziamo e automatizziamo le nostre attività, più aumentano le dipendenze tecnologiche e, di conseguenza, le possibili vulnerabilità. La sicurezza informatica non è più una questione riservata agli addetti ai lavori: riguarda tutti, la nostra vita quotidiana, ed è ormai anche il fronte delle guerre ibride, sempre più esposto a rischi”.

Non vuole creare allarmismo, ma invita a un bagno di realtà Riccardo Urbani, 67 anni, tra i maggiori esperti a livello nazionale di innovazione tecnologica e cybersicurezza. Con un passato in IBM, al fianco del guru dell’informatica Ernesto Hofmann, Urbani è stato chiamato già nel 2019 dal presidente della Regione Abruzzo, Marco Marsilio, di FdI, come superconsulente per affiancarlo nei principali progetti di trasformazione digitale, in particolare in ambito sanitario, con l’obiettivo di abbattere le liste d’attesa e migliorare l’efficienza del sistema.

Non a caso, è stato in prima linea anche in occasione dell’attacco informatico subito dalla Asl Avezzano-Sulmona-L’Aquila nella notte tra il 2 e il 3 maggio 2023, quando criminali informatici russi condussero un’incursione ransomware, esfiltrando circa 500 gigabyte di dati sensibili e paralizzando per settimane il Cup e diversi reparti, prima del graduale ripristino di tutti i sistemi digitali.

In un’intervista rilasciata a luglio ad Abruzzoweb, Urbani aveva lanciato un monito che oggi appare profetico: “C’è poco da stare tranquilli: assieme ai droni di ultima generazione, un’arma sempre più minacciosa è quella degli attacchi informatici, con cui compromettere pesantemente le funzionalità del Paese nemico. Dobbiamo dunque prepararci agli scenari peggiori”.

E ora uno scenario, se non il peggiore, senz’altro molto preoccupante si sta concretizzando. Nelle ultime settimane, il gruppo NoName057 ha diffuso sul dark web informazioni e richieste di dati personali riguardanti esponenti istituzionali e investigatori italiani. Tra i nomi citati figura quello di Antonio Tajani, ministro degli Esteri. Successivamente, sono state violate alcune caselle di posta elettronica di deputati a Montecitorio. A questi episodi si aggiungono l’attacco che ha alterato da remoto i parametri dei sistemi frigoriferi, provocando surriscaldamento e deterioramento degli alimenti, in Francia e anche in Italia, e la sottrazione di dati da un server della società impegnata nella realizzazione del tunnel ferroviario del

Brennero.

Infine, forse in un quadro di minacce più ampio e potenzialmente connesso, si registrano gli allarmi bomba su diversi voli europei, con aerei costretti a cambiare rotta o a effettuare atterraggi precauzionali. Mercoledì scorso, inoltre, circa 6.300 scuole italiane, di cui 36 in Abruzzo, hanno ricevuto un'e-mail contenente minacce di attentati con ordigni esplosivi.

Le ipotesi sono molteplici: attori informatici organizzati, campagne di intimidazione transnazionali e possibili operazioni di guerra ibrida. Tra i primi sospettati c'è la Russia dell'autocrate Vladimir Putin, impantanata nella guerra di invasione dell'Ucraina e potenzialmente interessata ad alimentare il panico. Ma c'è anche chi sospetta un coinvolgimento dell'Iran.

Sugli allarmi bomba, Urbani è netto: "Effettivamente c'è qualcosa che non ha funzionato. Le segnalazioni devono naturalmente essere prese sul serio, ma devono essere accompagnate da verifiche tempestive e da un'attività di intelligence capace di valutarne l'attendibilità e individuarne la provenienza. Non si può bloccare mezzo Paese per un allarme che è palesemente falso". Affermazioni rese prima che una circolare firmata dal ministro Matteo Piantedosi, spedita a prefetti e questori, ha invitato a ritenere inaffidabili le comunicazioni come quelle dei giorni scorsi. Spiegando invece che "occorre evitare che il ricorso sistematico a comunicazioni minatorie, anche manifestamente generiche, possa tradursi in uno strumento capace di provocare la paralisi di scuole, uffici, infrastrutture e servizi essenziali", e che "si è ritenuto necessario promuovere un approccio fondato sulla valutazione dell'attendibilità delle minacce e sull'adozione di misure proporzionate alle effettive condizioni di rischio".

Per quanto riguarda gli attacchi informatici, l'esperto avverte: "I settori maggiormente esposti sono quelli dai quali dipende la continuità della vita quotidiana: sanità, trasporti, banche, transazioni finanziarie ed energia. Pensiamo a cosa potrebbe accadere se venissero compromessi i sistemi informatici che supportano la gestione del traffico ferroviario. Oppure se un attacco provocasse l'indisponibilità di alcuni servizi aeroportuali".

Da qui il forte appello al governo nazionale: "Una parte delle risorse destinate alla sicurezza nazionale dovrebbe essere investita anche nel potenziamento delle strutture dell'Agenzia per la Cybersicurezza Nazionale, del CSIRT Italia e delle capacità di intelligence. Non basta avere strutture che intervengono quando un incidente si è già verificato. Occorre anche un'organizzazione capace di analizzare preventivamente le minacce, monitorare le attività sospette e comprendere la reale attendibilità delle segnalazioni".

Riccardo Urbani: la sicurezza informatica è un nuovo fronte di una guerra ibrida? Cosa c'è dietro gli attacchi hacker sempre più frequenti ed inquietanti?

Dobbiamo partire da una considerazione: la continuità della nostra vita quotidiana dipende ormai da sistemi tecnologici e informatici. Pensiamo agli ospedali, ai trasporti, alle banche, alle reti energetiche e ai servizi essenziali. Tre anni fa si cominciava a parlare di questi rischi, ma gli strumenti disponibili allora non sono quelli di oggi. Ormai tutto ciò che è connesso a Internet può diventare un potenziale obiettivo. La sicurezza informatica non è più una questione riservata agli addetti ai lavori: riguarda tutti. Un attacco può interrompere un servizio, ritardare una cura, mettere in difficoltà un'intera organizzazione o compromettere il funzionamento di un'infrastruttura.

C'è dunque un paradosso: la digitalizzazione, l'intelligenza artificiale e l'automazione hanno semplificato enormemente la nostra vita, ma allo stesso tempo hanno aumentato la vulnerabilità del sistema Paese?

Esattamente. Più digitalizziamo e automatizziamo le nostre attività, più aumentano le dipendenze tecnologiche e, di conseguenza, le possibili vulnerabilità. La sicurezza deve riguardare tutte le apparecchiature connesse, ma anche gli accessi delle persone che le gestiscono. Chi amministra questi impianti deve monitorare costantemente i sistemi, controllare gli accessi e verificare che non ci siano anomalie. Non possiamo più permetterci una gestione superficiale della sicurezza.

Gli allarmi bomba nelle scuole e ancor prima sui voli aerei sono connessi?

Non necessariamente. Bisogna distinguere tra un attacco informatico vero e proprio e l'invio di messaggi intimidatori. Un'email minatoria può essere inviata da chiunque e non significa automaticamente che sia stato violato il sistema informatico della scuola. Quello che mi preoccupa è il rischio che messaggi non ancora verificati possano provocare il blocco di interi servizi e creare panico nella popolazione. Il terrore è spesso l'obiettivo principale di questi soggetti: mettere sotto pressione un Paese, creare disorientamento e compromettere la fiducia nelle istituzioni.

Ma è normale che una stessa, delirante mail a firma di un tal "Mikhail Antropov, leader del Vilayat di Misoginistan", che dice di voler ,mettere in atto un genocidio degli italiani, può paralizzare per ora buina parte del sistema scolastico italiano?

Effettivamente c'è stato qualcosa che non ha funzionato: le segnalazioni devono naturalmente essere prese sul serio, ma devono essere accompagnate da verifiche tempestive e da un'attività di intelligence capace di valutarne l'attendibilità e individuarne la provenienza. Non si può bloccare mezzo Paese per un allarme che è palesemente falso, Quando si verificò l'attacco alla sanità dell'Aquila, organizzai due gruppi di lavoro: uno dedicato al recupero dei sistemi e uno all'attività di intelligence, che monitorava quotidianamente anche il dark web per verificare la fondatezza delle informazioni e identificare eventuali minacce. È un'attività che ritengo fondamentale. Oggi tutti parlano di cybersecurity, ma noi abbiamo affrontato concretamente queste situazioni, lavorando in prima linea durante l'attacco alla sanità aquilana. Conosciamo le difficoltà operative e le dinamiche che si sviluppano quando un'organizzazione viene colpita.

Chi può avere interesse a creare questa situazione di caos? Si parla spesso della Russia, di gruppi hacker e di organizzazioni criminali che operano sul dark web.

Nel dark web c'è praticamente di tutto: organizzazioni criminali, gruppi di attivisti informatici, mitomani e soggetti che operano con finalità terroristiche o di destabilizzazione. La Russia e Putin hanno responsabilità importanti nel quadro delle attività informatiche ostili che conosciamo. Tuttavia, dalle informazioni che mi sono arrivate nelle ultime ore, emergono elementi che suggeriscono come non tutti gli attacchi e non tutte le situazioni siano necessariamente riconducibili alla Russia. Potrebbero esserci interessi internazionali differenti. In un Paese particolarmente esposto sul piano mediatico e vicino a importanti appuntamenti elettorali, una strategia di intimidazione può assumere un peso ancora maggiore.

E se fossero autonomi, schegge impazzite?

Non tutti i gruppi hacker hanno le stesse finalità. Alcune organizzazioni possono avere rapporti o interessi convergenti con apparati statali e svolgere attività informatiche funzionali a strategie geopolitiche. Allo stesso tempo, alcuni gruppi criminali utilizzano gli attacchi ransomware per ottenere riscatti e autofinanziarsi. Nel caso dell'attacco alla sanità dell'Aquila, la mia valutazione è che l'obiettivo fosse prevalentemente economico: ottenere un riscatto, non necessariamente perseguire una strategia politica diretta del governo russo. Questa è una mia interpretazione, basata sull'esperienza maturata sul campo.

Possiamo però parlare, comunque, di un attacco all'Occidente e all'Europa?

È un'ipotesi che merita attenzione, ma bisogna essere prudenti. Non possiamo attribuire automaticamente ogni episodio a un'unica regia internazionale. Dobbiamo distinguere le responsabilità accertate dalle ipotesi investigative e dalle valutazioni di chi opera nel settore.

L'intelligenza artificiale, che sta conoscendo uno sviluppo straordinario, può diventare uno strumento potentissimo nelle mani di soggetti malintenzionati?

Certamente può essere utilizzata anche per finalità criminali, ma dobbiamo ricordare che dietro queste attività c'è sempre una persona. L'intelligenza artificiale è uno strumento: il problema è l'utilizzo che ne viene fatto. Pensiamo, per esempio, alle autorizzazioni di pagamento. Diventa sempre più difficile fidarsi soltanto di una voce o di un messaggio apparentemente convincente. Per autorizzare un pagamento o consentire un accesso delicato serve una verifica attraverso un canale indipendente. Oggi le tecnologie permettono di contraffare non soltanto i messaggi scritti, ma anche le voci e le immagini. Questo espone le persone al rischio di truffe e impersonificazioni sempre più sofisticate.

L'intelligenza artificiale, però, può essere anche un importante strumento di difesa, non soltanto di attacco?

Assolutamente. L'intelligenza artificiale può aiutare a individuare anomalie, analizzare enormi quantità di dati e riconoscere comportamenti sospetti. Può quindi diventare uno strumento molto potente per chi deve difendere le infrastrutture. Si apre una competizione tra chi utilizza queste tecnologie per attaccare e chi le utilizza per proteggere i sistemi. Ma torno a quello che dicevo prima: l'intelligenza artificiale non agisce nel vuoto. C'è sempre una responsabilità umana nell'utilizzo di questi strumenti.

Veniamo alla sanità abruzzese, che conosci molto bene e nella quale hai vissuto direttamente l'esperienza di un attacco hacker. Oggi possiamo considerare sicuri i sistemi sanitari della regione?

Noi in Abruzzo abbiamo vissuto direttamente questa esperienza e proprio per questo abbiamo compiuto passi importanti sul fronte della protezione informatica, probabilmente più di altre realtà che non hanno attraversato una situazione analoga. Il processo, tuttavia, non è ancora terminato. Restano da affrontare questioni importanti, soprattutto per quanto riguarda gli apparati elettromedicali e i software applicativi. È necessario prestare grande attenzione ai programmi obsoleti e ai dispositivi che non possono essere aggiornati con facilità. Anche recentemente il direttore generale dell'Agenzia per la Cybersicurezza Nazionale ha richiamato l'attenzione sul problema dei software non aggiornati. È un tema che avevamo già

evidenziato nella nostra precedente intervista, circa sei mesi fa. Una volta completati questi interventi, potremo raggiungere un livello di protezione molto elevato. Naturalmente, la sicurezza informatica non è mai un processo che si conclude definitivamente: richiede aggiornamento e monitoraggio continui.

Che cosa dovrebbe fare il Governo nazionale per rafforzare la sicurezza informatica del Paese? Servono maggiori investimenti?

Sicuramente. Una parte delle risorse destinate alla sicurezza nazionale dovrebbe essere investita anche nel potenziamento delle strutture dell'Agenzia per la Cybersicurezza Nazionale, del CSIRT Italia e delle capacità di intelligence. Non basta avere strutture che intervengono quando un incidente si è già verificato. Occorre anche un'organizzazione capace di analizzare preventivamente le minacce, monitorare le attività sospette e comprendere la reale attendibilità delle segnalazioni. Bisogna inoltre investire nelle infrastrutture tecnologiche, nella protezione delle reti e nella separazione dei sistemi. La segmentazione è fondamentale: se viene compromessa una parte di un'infrastruttura, il problema non deve propagarsi automaticamente a tutto il sistema.

Facciamo le ipotesi peggiori. Un Paese ostile, dotato di gruppi hacker particolarmente preparati, quali danni potrebbe provocare?

I settori maggiormente esposti sono quelli dai quali dipende la continuità della vita quotidiana: sanità, trasporti, banche, transazioni finanziarie ed energia. Pensiamo a cosa potrebbe accadere se venissero compromessi i sistemi informatici che supportano la gestione del traffico ferroviario. Oppure se un attacco provocasse l'indisponibilità di alcuni servizi aeroportuali. Un'interruzione dei servizi può avere conseguenze molto serie. Lo stesso vale per gli ospedali, dove il malfunzionamento dei sistemi informatici può rallentare attività diagnostiche, amministrative e assistenziali. Non dobbiamo necessariamente immaginare scenari cinematografici: anche il semplice blocco di un servizio essenziale può produrre conseguenze importanti.

L'episodio dei frigoriferi dei supermercati ha colpito particolarmente l'opinione pubblica. Come è stato possibile intervenire su apparecchiature di questo tipo?

Non è così sorprendente come potrebbe sembrare. Oggi molti impianti di refrigerazione sono collegati a sistemi di controllo remoto. I fornitori possono monitorare a distanza le temperature, verificare eventuali anomalie e intervenire in caso di malfunzionamento. Non è necessario che un tecnico sia fisicamente presente nell'impianto. È un sistema simile, per certi aspetti, a quello utilizzato in Formula 1, dove dal box vengono monitorati costantemente i parametri delle vetture. La stessa logica viene applicata ormai a numerosi impianti industriali e commerciali. Il problema nasce quando questi collegamenti non sono adeguatamente protetti. Ogni dispositivo connesso e ogni accesso remoto possono rappresentare un potenziale punto di vulnerabilità.

Anche la distribuzione dell'energia elettrica potrebbe essere coinvolta in uno scenario del genere?

Certo, e le reti energetiche sono infrastrutture estremamente strategiche e devono essere protette con particolare attenzione. Un'interruzione dei servizi energetici avrebbe ripercussioni su moltissime altre attività: ospedali, trasporti, comunicazioni e imprese. È proprio questa interdipendenza a rendere necessario un approccio complessivo alla sicurezza.

Tornando all'organizzazione della risposta nazionale, ritieni che l'ACN debba dotarsi di ulteriori gruppi specializzati?

Ritengo importante rafforzare anche le capacità di intelligence e di analisi preventiva. Il CSIRT Italia, il Computer Security Incident Response Team nazionale, svolge un ruolo fondamentale nella gestione e nella risposta agli incidenti informatici. Ma accanto alla risposta tecnica occorre una capacità di intelligence che permetta di analizzare le minacce, verificare le segnalazioni e comprendere chi possa esserci dietro determinate attività. Non possiamo limitarci a intervenire quando il danno è già avvenuto. Dobbiamo essere in grado di anticipare i rischi.

© 2026 Abruzzo Web Enfasi srl - Quotidiano digitale registrato presso il Tribunale dell'Aquila con decreto n°501 del 2 settembre 2003
Iscrizione al ROC n. 26362 - P.IVA 01812420667
Direttore responsabile Berardo Santilli