VerbanoNews

Le news del Lago Maggiore

Italia hackerata: le accuse di Gratteri e il piano europeo per difendersi

Michele Mancino · Sunday, November 24th, 2024

Le rivelazioni di Gratteri. Lilli Gruber ha ospitato questa settimana Nicola Gratteri, procuratore capo di Napoli, per discutere di legalità e giustizia in Italia. Uno dei temi forti toccati è stato quello della sicurezza informatica. Il controverso e roboante Gratteri non ha usato mezzi termini aprendo a una serie di rivelazioni, tanto illuminanti, quanto inquietanti. “Io non ho mai utilizzato la tecnologia del Ministero della Giustizia. Sul mio telefonino non c’è nessuna app. Il sistema informatico italiano è come gli acquedotti: il 45% delle informazioni preziose si perde. Abbiamo avuto il dominio del ministero della giustizia per mesi nelle mani di un hacker. Nel dark web c’erano 30 milioni di numeri di telefono e gli indirizzi di una di una società di telefonia italiana”. Il procuratore ha indicato le vie di soluzione: “Bisogna rifare il cablaggio, comprare tutti i computer nuovi. Ci vogliono soldi ma ci vogliono competenze.”. Infine, ha rivelato il livello di preparazione dell’Italia rispetto ai partner europei con un aneddoto. “Era il giorno in cui c’era il G7 in Puglia. Noi dovevamo fare una riunione con i francesi e gli olandesi. I francesi hanno detto: Non vogliamo gli italiani perché non portano nessun aiuto. All’estero usano tecnologia militare. Oggi loro ci chiamano e ci dicono: abbiamo 20.000 file audio vostri. Loro sono in grado di bucare le vostre reti”.
In realtà, non è che all’estero siano davvero così immuni. Ricordiamo questo caso tedesco come uno dei tanti: ***https://www.varesenews.it/2024/03/scandalo-della-sicurezza-come-i-vertici-militari-tedeschi-si-sono-fatti-hackerare-dallintelligence-russa/1863342/***

Il lavoro dell’ACN. In Italia abbiamo certamente un gap da colmare, ma lo si può fare con il lavoro concreto e non con le provocazioni ad effetto. In effetti, l’Agenzia per la Cybersicurezza Nazionale (ACN), l’ente governativo istituito per proteggere gli interessi nazionali nel settore della cybersicurezza, è una creatura molto recente. L’ACN è stata istituita dal governo Draghi nel 2021 per unificare le attività di protezione contro le minacce informatiche. Questa riforma ha assegnato al Presidente del Consiglio il coordinamento delle politiche di cybersicurezza e ha creato il Comitato interministeriale per la cybersicurezza (CIC) per consulenza e vigilanza. Le forze di polizia mantengono il compito delle cyber-investigation, mentre le operazioni di cyber-intelligence sono gestite dalle agenzie di intelligence. Il primo Direttore generale dell’ACN è stato Roberto Baldoni. Dal marzo 2023, il prefetto Bruno Frattasi ricopre questo ruolo. Dal 2023, l’ACN ha assunto nuove responsabilità, come la qualificazione degli operatori di servizi cloud per la Pubblica Amministrazione, in precedenza gestita dall’Agenzia per l’Italia digitale. A metà novembre l’Agenzia ha fatto un significativo passo avanti, pubblicando le nuove e prime Linee guida per il rafforzamento della resilienza delle amministrazioni pubbliche. Questo documento rappresenta uno strumento cruciale per migliorare la sicurezza digitale di istituzioni locali, regionali e centrali. Ma

cosa significa tutto questo per i cittadini? E come queste linee guida possono avere un impatto concreto nella vita quotidiana? Negli ultimi anni, attacchi cibernetici a sistemi pubblici sono diventati sempre più frequenti e pericolosi. Immaginate di trovarvi all'ospedale e scoprire che un cyber-attacco ha bloccato i sistemi informatici, impedendo al personale sanitario di accedere ai dati clinici. Oppure pensate a General un'interruzione improvvisa nel trasporto pubblico causata da un malware che paralizza le operazioni. Sono situazioni che evidenziano quanto la nostra vita sia interconnessa con i sistemi digitali. Le linee guida dell'ACN mirano proprio a evitare scenari come questi, imponendo alle amministrazioni di adottare una serie di misure preventive per proteggere dati, infrastrutture e servizi essenziali.

Sanità. Le aziende sanitarie locali dovranno mappare i loro sistemi informatici e assicurarsi che solo dispositivi e software autorizzati abbiano accesso ai dati sensibili dei pazienti. Questo significa che, in caso di attacco, i danni saranno limitati e i dati personali saranno al sicuro.

Trasporti. Immaginate un sistema che monitori in tempo reale i flussi di comunicazione tra i diversi componenti digitali dei mezzi pubblici, come biglietterie elettroniche o sistemi di guida automatica. Le linee guida richiedono la verifica costante di questi flussi, evitando interruzioni del servizio causate da intrusioni esterne.

Organizzazione. Ogni ente pubblico deve nominare un referente per la cybersicurezza. Questo significa che, in caso di attacco o di vulnerabilità, ci sarà sempre una persona preparata a gestire l'emergenza e a coordinare le azioni necessarie per il ripristino dei servizi. Supponiamo che un comune utilizzi un software per la gestione delle bollette che presenta una vulnerabilità nota. Grazie alle linee guida, il comune sarà obbligato a intervenire entro 15 giorni dall'identificazione del problema, aggiornando il sistema o implementando misure di sicurezza temporanee.

La cooperazione internazionale. Sul tema della cooperazione internazionale ci sono novità incoraggianti. Questa settimana, il Direttore Frattasi, ha incontrato il Prefetto Stéphane Bouillon, Segretario Generale della Difesa e della Sicurezza Nazionale francese. Durante l'incontro, si è discusso di cybersicurezza, resilienza e cooperazione internazionale, con particolare attenzione alla protezione delle infrastrutture critiche e alla gestione delle minacce cibernetiche. L'incontro ha rafforzato la collaborazione tra Italia e Francia, già consolidata durante le recenti Olimpiadi in Francia, e si è focalizzato sulla preparazione dei Giochi Olimpici di Milano-Cortina 2026. Tra i temi trattati: formazione digitale, gestione delle crisi cibernetiche, cooperazione G7 sulla cybersicurezza e collaborazione tra ACN e ANSSI. Questo dialogo rappresenta un passo verso una rete di cybersicurezza europea più forte e integrata. I recenti casi di cronaca hanno mostrato che il problema non è solo legato agli hacker ma agli insider stessi.

Quindi i livelli di allerta e prevenzione devono essere a 360°. La cybersicurezza non è un tema distante o tecnico, ma una questione che riguarda la qualità della nostra vita quotidiana.

"L'invincibilità sta nella difesa. La vulnerabilità sta nell'attacco. Se ti difendi sei più forte. Se attacchi sei più debole", Sun Tsu.

This entry was posted on Sunday, November 24th, 2024 at 9:52 am and is filed under Lombardia
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.