Cybersecurity, I-Com: "*Diciotto mesi per ottenere una certificazione di sicurezza. E' necessario accorciare i tempi e ricercare un approccio europeo comune*"

Per i fornitori di apparecchiature di rete ci vogliono tra i 12 e i 18 mesi per ottenere una certificazione di sicurezza: tempi lunghissimi, con il concreto rischio di esporre le applicazioni innovative delle nuove tecnologie ICT a un estenuante imbuto procedurale a causa di procedure di verifica molto articolate basate sui cosiddetti **Common Criteria**, i cui risultati sono valutati in termini di **Evaluation Assurance Level** (EAL). In pratica, 7 livelli di sicurezza, ciascuno dei quali corrisponde a un pacchetto di requisiti (Security Functional Requirements e Security Assurance Requirements). Fatta eccezione per i livelli EAL1 e EAL2 che possono richiedere anche "solo" poche settimane, **i livelli dal terzo in poi possono coprire un orizzonte temporale di vari mesi**, il che espone il prodotto/sistema al **rischio di essere divenuto obsoleto nel momento del rilascio della certificazione**. I livelli di sicurezza richiesti per le reti sono relativi almeno al livello EAL 4, le cui verifiche comportano procedure complesse che possono terminare addirittura dopo un anno e mezzo. In questi casi, la quantità di documentazione richiesta cresce progressivamente con il livello di valutazione, aumentandone anche i **costi**, che sono a carico del fornitore. Il tema è stato approfondito nel Policy Brief dal titolo "*ICT a prova di sicurezza. Evoluzione dei requisiti e impatto sulle aziende*" realizzato dall'Istituto per la Competitività (I-Com) – il think tank guidato dall'economista **Stefano da Empoli** – nell'ambito delle attività dell'Osservatorio sulla sicurezza del 5G condotte nel corso del 2021.

Secondo gli analisti dell'istituto, gli strumenti disponibili per procedere con una valutazione di sicurezza di questo tipo, per quanto efficaci, non risultano scevri da gravi limiti, soprattutto in termini di tempi, costi e procedure. Dal punto di vista tecnico, sistemi di valutazione della sicurezza per prodotti e sistemi ICT affidabili e condivisi, come i **Common Criteria**, sono strutturati per rispettare criteri qualitativi tali da garantire alla documentazione prodotta un elevato livello di fiducia, efficacia e correttezza.

Il Policy Brief, inoltre, evidenzia come un'altra debolezza dello schema consista nella **rigidità** del sistema per il **mantenimento della certificazione**: se ne prevede la perdita non appena ci si discosta dalla configurazione verificata, e non viene contemplata la possibilità di installare nuove patch senza una nuova certificazione.

Una maggiore agilità e rapidità – suggerisce la ricerca – sembrerebbe poter essere garantita dal **Nesas**, lo standard sviluppato da 3GPP e GSMA che semplifica notevolmente i Common Criteria con procedure e tempi di valutazione brevi, a basso costo, che consentirebbero un time-to-market dei prodotti da testare di circa **3-6 mesi**. Attualmente le certificazioni sono volontarie ma le autorità nazionali potranno definire eventuali obbligatorietà, che andrebbero a incidere sugli equilibri di mercato perché, se per i prodotti ancora da realizzare è possibile progettare il design in modo da rispettare gli standard, la richiesta della certificazione per prodotti e sistemi già attivi potrebbe comportare oneri estremamente elevati per alcuni fornitori.

Le istituzioni europee e le agenzie comunitarie, come l'ENISA, sono consapevoli **dell'importanza di promuovere iniziative comuni per sviluppare un ecosistema sicuro**, uniforme ed efficiente, come mostrano il Cybersecurity Act, le Raccomandazioni sulla standardizzazione e il Cybersecurity Certification Market Study della stessa agenzia. Rispetto alla necessità di **trovare un equilibrio tra una certificazione in grado di mitigare le possibili minacce, e che tenga conto allo stesso tempo di esigenze relative a costi, tempi e prestazioni** da raggiungere, il paper sottolinea l'opportunità di tenere in considerazione fattori relativi alle dinamiche di mercato e anche agli aspetti socioeconomici. In questo contesto, l'Italia si sta dimostrando consapevole dell'importanza di collaborare a livello internazionale. L'estensione dell'ambito di applicazione della disciplina sul golden power, la pubblicazione della legge sul perimetro di sicurezza nazionale cibernetica e dei relativi decreti attuativi (tutt'ora in corso), così come la legge per l'istituzione dell'Agenzia per la cybersicurezza nazionale costituiscono un'articolata attività legislativa che, sebbene assolutamente pregevole nelle finalità perseguite, sembra tuttavia richiedere un'azione maggiormente decisa in termini di semplificazione e bilanciamento dei vari fattori in gioco, tenendo insieme le ragioni della sicurezza con quelle dell'innovazione e dello sviluppo.