Cybersicurezza

La nuova "guerra" contro gli hacker

di Emanele Davide Ruffino e Germana Zollesi

Oggi le autostrade informatiche rappresentano quello che per secoli sono state le vie di comunicazione e non si può dimenticare quante guerre siano state combattute per detenerne il controllo. In questo contesto appare quanto mai appropriato l'intervento legislativo per la costituzione di un'Agenzia nazionale per la sicurezza informatica con il compito di predisporre una strategia di sicurezza informatica per sostenere lo sviluppo della digitalizzazione del Paese e del sistema produttivo e delle pubbliche amministrazioni in particolare. Naturalmente, siamo i primi a confidare che la sicurezza non diventi oggetto di scambio con la sovranità nazionale.

La pandemia ha indotto ad un aumento esponenziale dell'uso di strumenti informatici. E di conseguenza, aumentato gli "appetiti" degli hacker che attraverso i malware (i virus informatici) puntano a sottrarre informazioni personali o soldi. Dallo smart work (nonostante il contrasto dei burocrati refrattari ad ogni cambiamento perché compromette il loro potere), alla didattica a distanza (già sviluppato in molti stati occidentali già prima del Coronavirus) alla necessità delle famiglie di provvedere alle loro esigenze (dagli acquisti on line, alle incombenze connesse ai pagamenti per le utilities).

Come tutte le innovazioni epocali si possono rilevare problemi attuativi che vanno attentamente gestiti e monitorati: tentare di fermare il processo sarebbe semplicemente anacronistico. Ciò che risulta però assolutamente indispensabile è garantire la funzionalità del sistema a tutela dei singoli e per l'affidabilità delle comunicazioni e delle transazioni commerciali.

Un' Agenzia per la cybersicurezza nazionale

Risponde a questa esigenza il decreto-legge, messo a punto dal sottosegretario alla Presidenza del Consiglio con delega alla Sicurezza, recante "disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'agenzia per la cybersicurezza nazionale". Scopo dell'iniziativa normativa è quello di assicurare il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la una cornice di sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore.

Correttamente il decreto provvede preliminarmente a precisare il concetto di cybersicurezza, definendolo l'insieme delle attività necessarie per proteggere e assicurare la disponibilità, la confidenzialità e l'integrità di reti, sistemi informativi, servizi informatici e comunicazioni elettroniche dalle minacce informatiche, garantendone altresì la resilienza. L'importanza dell'iniziativa è sottolineata dalla costituzione di un coordinamento politico attributo direttamente al presidente del Consiglio dei Ministri (con la responsabilità generale delle politiche attuative) tramite un comitato interministeriale e disponendo di adeguate risorse (si parla di 300 esperti, nelle fase iniziale, aumentabili fino a 800: un piccolo esercito).

Usa, Giappone e Italia, i primi nel mirino

La classifica dei Paesi più attaccati è guidata da Stati Uniti (31.056.221) e Giappone (30.363.541). L'Italia è in terza posizione, seguono India (4.411.584) e Australia (4.387.315). La famiglia di malware più rilevata ad aprile in Italia a

livello aziendale, è stata quella dei cosiddetti 'Downad' che possono infettare l'intera rete di una società sfruttando sistemi operativi obsoleti e non aggiornati. Un pericolo spesso inconsapevole, ma che può provocare danni irreparabili. A rischio sono anche i consumatori colpiti dalla famiglia dei malware denominati Coinminer, che si nascondono all'interno di un sistema per sfruttare le capacità di calcolo e produrre criptovalute, come i Bitcoin, all'insaputa degli utenti.

L'Italia nel 2020, sempre secondo i ricercatori di Trend Micro, è stato il secondo paese in Europa, dopo la Germania, più colpito dai ransomware, un'altra famiglia di virus che blocca i dispositivi per chiedere un riscatto.

Gli attacchi alla sicurezza informatica aumentano, per varietà di modi e soggetti colpiti, senza precedenti: nessuno può sentirsi al sicuro. Proteggere i dati personali e aziendali diventa quindi un compito di assoluta priorità, cui lo Stato non poteva non farsene carico: una base di partenza importante, cui dovranno seguire investenti in tecnologie e miglioramento dello skill, individuale e collettivo, per creare una rete di sicurezza in modo da poter utilizzare le potenzialità dell'informatica in modo sicuro e affidabile.