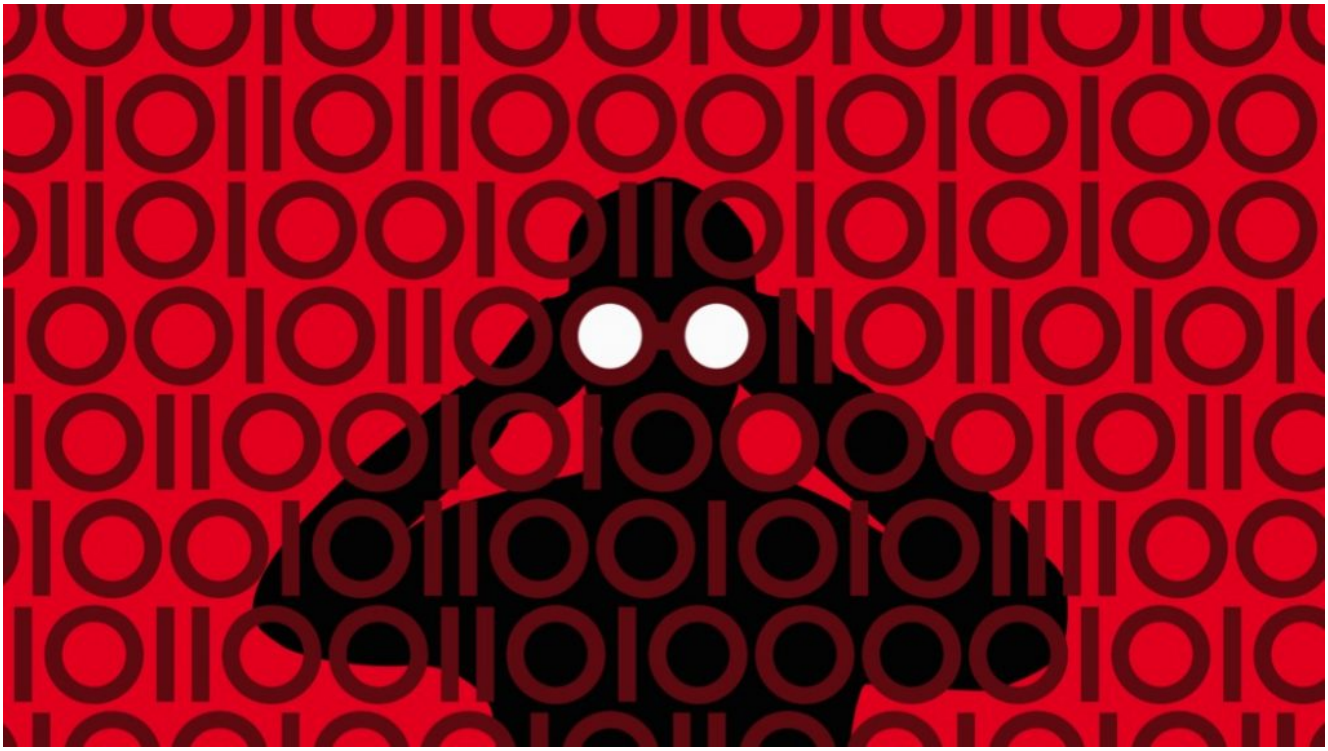
Parte il cantiere per costruire il perimetro nazionale di cybersecurity



Duecento persone al lavoro. Primo compito: scegliere asset e infrastrutture che hanno la priorità in caso di attacco hacker

Confidenzialità e integrità. Sono questi i due criteri con cui il governo sceglierà quali **aziende e infrastrutture** devono stare all'interno del **perimetro nazionale di sicurezza cibernetica**. Ossia gli asset da proteggere per primi dai rischi di attacchi informatici. A spiegare l'evoluzione della strategia cyber italiana è Roberto Baldoni, vicedirettore generale del Dipartimento delle informazioni per la sicurezza (Dis). A Itasec, la più grande conferenza italiana dedicata alla cybersecurity (che si è chiusa ad Ancona il 7 febbraio), il numero due dei servizi segreti con delega proprio alla galassia digitale traccia i prossimi passi dei piani nazionali.

"*Il perimetro nazionale oggi è un grande cantiere*", spiega

l'accademico oggi ai piani alti di piazza Dante. Il primo lavoro è esaminare asset e funzioni dello stato, valutare l'impatto che potrebbero avere se fossero vittime di un attacco e **stabilire le priorità**: chi ha la precedenza a entrare nel perimetro. "*Applicheremo un criterio di gradualità* – spiega Baldoni -. *Si parte con un* ***numero ragionevole di asset e soggetti ict***". Già nove gruppi sono al lavoro per fare questa scrematura: intorno ai tavoli sono riuniti duecento tra tecnici e giuristi di 20 amministrazioni.

A differenza della direttiva europea Nis, sempre sulla cybersecurity, che ha come principio base per **stabilire gli asset da proteggere il blocco del servizio** (e ha già portato in Italia a censire 465 operatori dei servizi essenziali), il perimetro sarà più restrittivo. Non si ragionerà solo in termini di danni che un attacco hacker può provocare se mette ko un servizio fondamentale per la vita quotidiana, come l'energia elettrica. Ma anche di quelli causati dalla violazione della confidenzialità e dell'integrità di un asset. Che sono condizioni sufficienti per finire nel perimetro. È il caso, per esempio, di infrastrutture legate allo **spazio o delle industrie high-tech**.

In parallelo, per Baldoni occorre sviluppare una **rete di laboratori di certificazione**. Non solo a supporto del ministero dello Sviluppo economico, per effettuare nei tempi gli scrutini tecnologici che il rafforzato golden power impone su tecnologie come il 5G. Ma anche, secondo il cyberzar, per arruolare esperti da spedire a Bruxelles a lavorare a **standard produttivi per l'high tech adatti alle aziende italiane**. Per Baldoni "*ora occorre ragionare su un'autonomia nazionale strategica digitale: è chiaro che ci sono tante tecnologie, ma dobbiamo capire quelle fondamentali per il nostro Paese e portarle avanti*".

Il 2020 sarà l'anno della costruzione dei cyberteam nei ministeri, dalla Difesa agli Interni. Ma tra le sfide Paolo Prinetto, professore del Politecnico di Torino e presidente

del Laboratorio nazionale di cybersecurity, espressione del Consorzio interuniversitario nazionale per l’informatica (Cini), elenca la costruzione di **centri di cybersecurity regionali**, sull’esempio di quello toscano, per il sostegno alle amministrazioni locali. E la **costituzione di cyber range**, “poligoni di tiro” per le esercitazioni. Oltre alla scommessa di portare in Italia il centro europeo di ricerca e competenza sulla cybersecurity, previsto dalla direttiva Nis.