Cybersecurity e P.A., i principali attacchi del 2022



Le Pubbliche Amministrazioni sono state fra i principali bersagli del crimine informatico nel 2022.

Enti nazionali e locali, aziende pubbliche (o partecipate da capitali pubblici) e fornitori privati di pubblici servizi affrontano già da diversi anni una trasformazione digitale dirompente, oggi ulteriormente impulsata dalle rilevanti risorse previste nel PNRR che destina alla missione *"Digitalizzazione, innovazione e sicurezza nella PA"* investimenti pari a quasi 10 miliardi di euro.

Complice anche l'improvviso e massiccio impiego dello *smart working* per diverse categorie di dipendenti pubblici, questa transizione ha determinato l'inevitabile espansione del relativo perimetro digitale: così esponendo al rischio di attacchi informatici una smisurata mole di dati sensibili, oltre a mettere a repentaglio la continuità di numerose tipologie di servizi essenziali.

I principali attacchi del 2022

Secondo i dati CLUSIT, le P.A. risultano al primo posto fra le realtà interessate da *cyber* incidenti: insieme al mondo *Finance*, nell'anno che va a concludersi esse sono state destinatarie di quasi la metà sul totale degli attacchi rilevati.

Un fronte di rischio emergente, evidenziato anche nell'*ENISA Threat Landscape 2022*, è rappresentato dalle attività di *cyberwarfare* legate alle tensioni geopolitiche internazionali.

Ne sono esempi i clamorosi attacchi ai siti del Senato e del Ministero della Difesa, di natura meramente dimostrativa –

come pure il recente DDoS rivolto alla pagina web del Parlamento Europeo – ma con significative ricadute d'immagine per le istituzioni coinvolte. Nell'ambito della medesima campagna d'attacco, in primavera simili episodi hanno interessato i Ministeri dell'Istruzione, della Transizione Ecologica e dei Beni Culturali; il Ministero dell'agricoltura è la vittima più recente, con un attacco (sempre di tipo DDoS) andato a segno i primi di dicembre.

Restando sul fronte istituzionale, è ancora da chiarire la nebulosa vicenda dei *data leak* sofferti dalla Cassa Depositi e Prestiti e dall'Agenzia delle Entrate.

Altro filone in costante aumento è relativo ai *ransomware*, che sempre più colpiscono amministrazioni locali di ogni dimensione e collocazione geografica: da Palermo a Trieste, passando per una Regione Sardegna sotto costante attacco da diversi mesi, in Italia il 75% degli enti colpiti avrebbe subito come effetto la cifratura (con conseguente indisponibilità) dei propri dati.

Negli ultimi mesi hanno, poi, fatto notizia i numerosi attacchi informatici rivolti alle Aziende Sanitarie Locali, parte del più generalizzato quadro di minacce gravante sul comparto ospedaliero; da ricordare i casi di Padova, Torino o dei vari nosocomi lombardi colpiti nel corso dell'anno, da cui sono derivati disservizi potenzialmente assai gravi per i pazienti.

Policy vigenti e obiettivi futuri

Sul piano del diritto comunitario le amministrazioni pubbliche italiane, in quanto fornitrici di servizi digitali in uno Stato membro dell'Unione, rientrano nel campo applicativo della Direttiva NIS2, del nascente *Digital Operational Resilience Act* (DORA) e ovviamente del GDPR, per quanto riguarda la protezione dei relativi dati personali.

A livello nazionale risultano centrali le prescrizioni contenute nel Perimetro di sicurezza cibernetica nazionale (legge n. 133/2019) e nel piano *"PA Digitale 2026"*, che prevede tra l'altro l'istituzione del Polo Strategico Nazionale (PSN), piattaforma *cloud* creata per ospitare *"dati e servizi critici e strategici delle pubbliche amministrazioni italiane"*.

La sorveglianza sulla *compliance* a tali normative e sulla continuità operativa dei servizi erogati spetta all'Agenzia per la Cybersicurezza Nazionale (ACN), che fra i propri poteri annovera il monitoraggio relativo alla *"operatività dei siti istituzionali – ministeri, autorità, agenzie, organi costituzionali – e delle organizzazioni che gestiscono servizi essenziali"*.

A livello operativo, sembra perciò essenziale intervenire quanto prima sulla scarsa maturità digitale delle istituzioni italiane: tenendo in conto che, a fronte di importanti vantaggi in termini di efficienza e capillarità dei servizi, la digitalizzazione della P.A. pone un'enorme sfida rispetto alla messa in sicurezza delle infrastrutture informatiche pubbliche.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/cybersecurity-e-p-a-i-principali-attacchi-del-2022/