IL CONVEGNO CORCOM-FPA

Cybersecurity, ecco la strategia italiana

Al convegno Fpa-Corcom riflettori puntati sulla strategia-Paese e sulle novità di mercato. Parola d'ordine: cooperazione. Pubblico e privato devono allearsi per spingere l'execution e garantire uno "scudo" forte ai sistemi informatici

di Patrizia Licata

Consapevolezza dei rischi, atteggiamento proattivo che valorizzi la prevenzione accanto alla soluzione, execution efficace e veloce delle strategie e collaborazione tra tutti i player pubblici e privati: potremmo sintetizzare così i messaggi chiave emersi dal **Cyber Security 360 Summit,** l'evento che si è svolto oggi a Roma, alla Camera dei deputati, promosso da **Digital360** e in particolare dalla nostra testata**, Corcom,** e da **Fpa** (organizzatori di **Forumpa**), col supporto di **Accenture, Almaviva, BT, Business-e, Check Point, Cisco.**

"La superficie di attacco oggi è molto aumentata: la **cyber-sicurezza** ha un impatto pervasivo, perché i prodotti e i servizi digitali sono ovunque. Occorre mettere i campo in primo luogo tramite un'adeguata conoscenza dei rischi e disponibilità di competenze", ha osservato **Gabriele Faggioli**, Presidente del **Clusit** e Associate Partner di **Partners4Innovation**, aprendo i lavori con i dati aggiornati del rapporto **Clusit**. **Faggioli** ha sottolineato la necessità di chiudere il gap tra percezione del rischio e rischio effettivo: ci sono tanti strati della popolazione (soprattutto i **Millennials**) non attenti ai **cyber** rischi. I dati di febbraio 2016 del **Clusit** portano in evidenza l'aumento di attacchi su infrastrutture critiche e **cloud**: "Non è un no al **cloud**, anzi", ha chiarito Faggioli; "ma occorre porre attenzione a distribuire e gestire il rischio". Il report **Clusit** evidenzia ancora l'aumento di attacchi (andati a buon fine o no) ai settori health e finance e, ovviamente, al mondo governativo e militare, bersaglio preferito degli hacker. Un dato però è incoraggiante: nel primo semestre 2016 l'Europa segna per la prima volta un rallentamento del tasso di attacchi.

L'Italia è chiamata ora ad accelerare sulla sua strategia nazionale per la **cyber security** dalla direttiva europea **NIS (Network and Information Security)** approvata a luglio per la sicurezza delle reti e dell'informazione, che definisce un primo insieme univoco di norme in materia di **cyber security** a livello europeo. Su questo punto **Faggioli** è chiaro: "Bene la normativa Ue ma ribadisco che è fondamentale l'approccio culturale; norme e sanzioni non sono l'elemento primario - anzi, direi che abbiamo troppe norme sui dati personali e troppo poche su altri settori della **cyber-sicurezza**: la normativa è un po' squilibrata verso la difesa della **privacy**".

Il quadro normativo ha costituito il centro della prima tavola rotonda, moderata da Alessandro Longo, Direttore Responsabile, Forumpa.it; **Vincenza Bruno Bossio**, Membro dell'Intergruppo parlamentare Innovazione, Camera dei Deputati, ha ribadito che "non è solo la norma a generare l'attenzione sulla **cyber-sicurezza** - anzi, l'Italia ha cominciato già da qualche anno a occuparsi del tema ma l'attenzione è rimasta finora bassa e anche in Europa si è arrivati relativamente tardi alle direttive sulla **cyber security**". Oggi, con il **NIS** le norme si mettono al passo "e cercano di superare la frammentarietà e di incentivare la collaborazione pubblico-privato". Certo, Italia e Europa si trovano a dover rincorrere, e intanto i rischi sono aumentati; per questo la strategia digitale del governo cerca di correre velocemente, per affrontare temi come **Industria 4.0**, **Spid** e identità digitale, digital by default per la PA. "In Italia è importante anche che ci sia un solo **Cert** nazionale: questa è la prima condizione per dare coerenza al network italiano ed europeo della **cyber-sicurezza** e al mercato unico digitale europeo e per dare forza a nostri rapporti globali", ha concluso la **Bruno Bossio**.

Sulla direttiva **NIS, Roberto Di Legami**, Capo della **Polizia Postale**, intervenuto all'interno della Tavola rotonda dedicata a "I principali Protagonisti dell'architettura nazionale per la sicurezza informatica" (moderata da Carlo Mochi Sismondi, Presidente, **FPA**), ha tenuto a precisare che "l'Italia

non è impreparata e non è all'anno zero: il paese si è già dotato di un'architettura. Il legislatore italiano è stato pioniere nell'occuparsi della tutela delle infrastrutture critiche, sia fisiche che elettroniche, e affidarla alla **Polizia di Stato**". Il **NIS** ora è importante perché in Italia porta all'istituzione dell'autorità nazionale per la **cyber security** che fa da raccordo per l'intero sistema, anche se andrà definito meglio come i vari elementi si metteranno in relazione tra loro. "Il **Cert** nazionale può essere ottimizzato con nuove risorse umane e tecnologiche e il nucleo per la **sicurezza cyber** potrebbe fare da sintesi tra i vari interlocutori e le varie funzioni, ottimizzando la capacità operativa", ha detto **Di Legami** dando il pieno avallo a un potenziamento delle attività di prevenzione e un sì convinto al mandatory reporting che "fa emergere il sommerso e serve a migliorare l'attività di prevenzione".

Uno degli temi chiave che entrano nella macro categoria della **cyber security** è quello della fiducia degli utenti nel mondo digitale, il cosiddetto **trust**. Lo ha sottolineato **Paolo Dal Cin**, Managing Director, Security Lead per Italia, Europa Centrale e Grecia, **Accenture,** nel suo intervento: il **NIS** aiuterà anche a questo riguardo perché per ora, secondo dati Ue, solo il 22% dei consumatori digitali online si fida a comprare online. Le **cyber** minacce sono un grave ostacolo allo sviluppo di una prospera economia digitale; uno studio del **World Economic Forum** afferma che il **cyber** risk è tra i massimi cinque rischi enterprise al mondo e l'impatto stimato è di 3.000 miliardi di dollari nel 2020. Anche **Accenture** ha di recente condotto una ricerca internazionale sulla **cyber security**: il paradosso è che il 70% delle aziende si dice consapevole e 3 top manager su 4 si ritengono pronti a rispondere agli attacchi, ma la realtà è che un attacco ogni tre alle aziende va a buon fine: "L'economia digitale oggi non è sicura, l'ecosistema deve essere più efficiente, molte aziende non si accorgono degli attacchi se non dopo mesi, si pensa più alla compliance che alla sicurezza, e non si fa abbastanza per accrescere la consapevolezza e creare competenze". La ricetta di **Dal Cin** per l'Italia? "Fare sistema: le aziende con gli enti pubblici", ma non solo: "lavorare su una federazione di **Cert** nazionali, anche di settore, come per banche o Tlc, e fare innovazione e investire in **cyber** difesa, track intelligence, capability di **security**, analytics, ecc.

Dopo le Tavole rotonde su "Le risposte concrete del mercato" moderate da Mila Fiordalisi, Caporedattore, **CorCom**, la conclusione dei lavori è stata affidata a **Roberto Baldoni**, Direttore del **Centro di Ricerca di Cyber Intelligence e Information Security**, Sapienza Università di Roma**:** "Il **NIS** ci dà una chiave di lettura, e sicuramente gli organismi internazionali, dall'Ue alla Nato sono acceleratori per il nostro modello di sviluppo su **cyber sicurezza**, ma dobbiamo anche fare i compiti a casa e avere il nostro progetto e la nostra vision", ha detto **Baldoni**. "Il mondo economico una volta era separato dal **cyber** space, e l'IT e il business in azienda non si parlavano: oggi non può più essere così". Sono le rivoluzioni **cloud**, **mobile** e, più di recente, **IoT**, **Industria 4.0**, **Blockchain**, robotica, a imporci un veloce cambio di marcia: "Nel futuro possiamo prevedere che l'Italia diventi una piattaforma digitale integrata nell'Ue dove l'investitore troverà una serie di servizi per fare business in modo sicuro: tutte le nazioni avanzate investono in questa direzione perché **cyber security** means business, ovvero proteggere la sicurezza delle infrastrutture vuol dire proteggere la prosperità economica". Aderire al **NIS** e ai suoi vincoli, dunque, è fondamentale, "ma non possiamo accontentarci, dobbiamo fare di più: l'ICT è un abilitatore ma non l'unico settore coinvolto, occorre mettere in piedi un vero ecosistema **cyber** per proteggere infrastrutture e paese; PA, industria e accademia devono contribuire a una risposta non più isolata ma coordinata", ha affermato **Baldoni**, ricordando che per l'Italia sarà fondamentale non disperdere le risorse economiche e sviluppare la capacità di trattenere anche le risorse umane: "Senza human capabilities ci si porta il nemico dentro casa: non è un caso che Uk o Francia facciano grossi investimenti quinquennali e non si fermeranno qui, perché la **cyber-sicurezza** richiede una strategia continuativa. Il mondo si dividerà presto tra chi fa le tecnologie e chi le usa soltanto: cerchiamo di fare in modo che l'Italia rientri nel primo gruppo, puntando con forza su ricerca e sviluppo e **start up**".

Al **Cyber Security 360 Summit** di oggi sono intervenuti anche: **Antonio Samaritani**, Direttore, Agenzia Digitale per l'Italia **(vedi articolo separato); Rocco Panetta**, Equity Partner NCTM Law Firm and Legal Advisor Italian Government on Internet; **Andrea Rigoni** - Partner di Intellium – Deloitte; **Andrea Servida**, Head of Unit "eGovernment and Trust", DG CONNECT, European Commission; **Ruggiero Di Biase**, Direttore del IV Reparto Coordinamento dei Programmi di Armamento - Segretariato generale della Difesa/Direzione nazionale degli armamenti; **Rita Forsi**, Direttore Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, Ministero dello Sviluppo Economico; **Gianfranco Incarnato**, Vice Direttore Generale e Vicario del DG/Direttore Centrale per la sicurezza, il disarmo e la non proliferazione, Ministero degli Affari Esteri e della Cooperazione Internazionale; **Francesco Paolo Schiavo**, Capo della Direzione dei sistemi informativi e dell'innovazione del MEF; **Mario Terranova**, Dirigente Responsabile Area "Sistemi, tecnologie e sicurezza informatica", Agenzia Digitale per l'Italia; **Romolo Buonfiglio**, Responsabile Cyber Security Practice, Almaviva; **Andrea Costa**, Responsabile Business, Marketing Infrastructure Solutions, TIM; **Simone Posti**, Security Account Manager - Center–South Italy, Cisco Systems; **Rosario Sorrentino**, Head of BT Security Business Italy; **David Gubiani**, Security Engineering Manager Italy, Check Point Software Technologies; **Loredana Mancini**, Chief Operating Officer, Business-e; **Gastone Nencini**, Country Manager, Trend Micro Italia; **Rodolfo Rotondo**, Business Solutions Strategist, VMware.