Previsioni ed Analisi sullo stato della Cyber Security, intervista a Pierluigi Paganini

Date : 1 febbraio 2018

Intervista a **Pierluigi Paganini**, *CTO presso CSE CybSec SPA e Membro dell'ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group*

Le tecniche, tattiche e procedure (TTP) degli attori malevoli appaiono sempre più complesse: pensiamo a gruppi come APT Lazarus, responsabile di attacchi condotti a livello globale contro giganti della tecnologia (come Samsung) e *cryptocurrencies* (bitcoin). Esistono strumenti di prevenzione contro tali minacce?

Più che il numero preoccupa ormai il livello di complessità degli attacchi, in particolare per quanto concerne attori persistenti noti come APT (advanced persistent threat), che dispongono di notevoli risorse economiche e umane.

Tra i fenomeni fonte di maggiore preoccupazione vi è, senza dubbio, il modello di crime-as-a-service, fenomeno in espansione che vede gruppi altamente specializzati offrire i propri prodotti e servizi ad organizzazioni criminali e talvolta ad attori nation-state. Parliamo di servizi, prodotti ed infrastrutture complete per gestire ed organizzare persino attacchi su larga scala in grado di arrecare danno ad organizzazioni di qualunque dimensione.

Anche la varietà dei moventi è un tema di difficile analisi con notevoli sovrapposizioni - si può spaziare dai reati economici al terrorismo. L'analisi dei fenomeni impone un radicale cambio di approccio nel campo del contrasto e della prevenzione delle minacce. Metodologie di attacco più complesse richiedono un'attenzione più elevata, e da questo punto di vista il fattore umano è imprescindibile, così come l'*information sharing* tra attori della sicurezza. C'è da dire che sul piano della consapevolezza e dell'attenzione, anche mediatica, qualcosa sta cambiando (il GDPR è un segnale positivo, anche se molti opportunisti lo stanno usando come una sorta di "spauracchio" per vendere i propri prodotti per la sicurezza) ma la strada è ancora lunga.

Guardiamo all'enorme espansione dell'IoT: senza porci il problema della sicurezza, siamo destinati a soccombere. La *security* non deve essere percepita come una spesa inutile ma come un investimento fondamentale per garantire l'appetibilità e, spesso, la stessa

sopravvivenza del proprio business: ritengo che sia fondamentale diffondere *awareness* su questo concetto.

Nelle sue previsioni per il 2017 in tema di cyber security, lei paventava "un significativo aumento del numero di infezioni causate da malware sempre più sofisticati"; un panorama nel quale "ransomware e mobile malware la faranno da padroni" e dove sarebbero aumentati gli "attacchi contro i sistemi di controllo industriale (ICS)". Ritiene che questi scenari si siano verificati? Quali prospettive ipotizza, invece, per il 2018?

Il modello estorsivo implementato tramite ransomware si è effettivamente imposto come predominante nel mercato del cybercrime; accennando a sistemi ICS ricordo come proprio in queste ore si stia discutendo del malware *Triton* - disegnato appositamente per attaccare sistemi industriali - che avrebbe compromesso diverse infrastrutture critiche in Arabia Saudita, con ricadute economiche inimmaginabili.

Nel campo della tecnologia *mobile*, oggi grossi rischi sono veicolati dalle applicazioni: in questo gioca un ruolo importante la scarsa consapevolezza della minaccia, la totalità degli utenti ritiene che un'applicazione trovata su uno store ufficiale come Google Play sia sicura e la scaricano senza controllarne feedback e numero di download effettuati. Prevedo che questa tendenza proseguirà nel 2018, sfruttando il paradigma imperante dei dispositivi mobili.

Minacce significative vengono, poi, anche dall'IoT: dobbiamo prepararci a malware in grado di attaccare centinaia di migliaia di macchine connesse - come è già successo con la botnet Mirai, che ha attaccato i sistemi DNS utilizzati dalle principali aziende statunitensi oscurando per diverse ore siti del calibro di Amazon e PayPal sulle reti Usa.

Sembra prevedibile che l'interesse degli Stati per la sicurezza informatica - non più soltanto in termini di reazione agli attacchi ma anche di *offensive defence* - comporterà a breve significativi cambiamenti nell'approccio legislativo alle tematiche cyber. Pensa che il cosiddetto *state sponsored hacking* rappresenterà un fenomeno evolutivo nella cyber security o che rischierà, al contrario, di inasprire i conflitti e le disparità già esistenti tra diverse zone del mondo?

Il *Nation-state hacking* e la corsa agli "armamenti cibernetici" sono già realtà da oltre un decennio; urgono regole vincolanti per prevenire scenari in cui davvero nessuno sarebbe al sicuro. A livello legislativo, in Europa già la Direttiva NIS mirava ad incentivare la comunicazione tra attori. Più specificamente la dichiarazione di Lucca (*adottata l'11 aprile 2017 a conclusione del G7 degli Esteri, ndr*) alla cui stesura ho preso parte come membro del Gruppo Cyber G7 del Ministero degli Esteri, cerca proprio di definire le norme di comportamento degli stati nel cyberspazio: è stata accettata dagli Stati membri del G7 in modalità non obbligatoria, a dimostrazione di un approccio più consapevole ma ancora non abbastanza forte rispetto alla proporzione dei rischi in gioco. Considerato che il *cyberwarfare* si muove su un piano parallelo e meno visibile, preparando o coadiuvando le modalità belliche più tradizionali, in assenza di regole d'ingaggio condivise tra gli Stati rischia senz'altro di trasformarsi in un'arma devastante su più fronti: basti pensare alla vulnerabilità delle infrastrutture critiche o all'uso del *machine learning* nella propaganda politica sul web.

Il fatto che la sicurezza informatica sia ormai entrata ufficialmente nelle agende dei massimi summit internazionali, incluso il G7, per lei potrebbe definirsi "too little, too late" o segna, invece, un reale cambio di passo nella cooperazione tra potenze mondiali in materia di cyberdefense? Quali ritiene gli Stati più virtuosi da una prospettiva cyber?

Non è troppo tardi, anche se siamo piuttosto indietro. Come anticipavo, Wannacry ha "dato la sveglia" in questo senso, quindi la consapevolezza dei pericoli è aumentata; ora esistono soprattutto esigenze di coordinamento e comunicazione, per evitare la dispersione di risorse che si determina quando ciascuno lavora per conto suo. Al G7 si è fatto un ottimo lavoro ma resta da vedere se seguiranno azioni concrete, strategie continuative e condivise, che è quello di cui c'è realmente bisogno.

Analogamente alle aziende, gli Stati devono comprendere che la sicurezza informatica non è un costo ma un'opportunità - anche per attrarre investimenti e competere sul piano dell'innovazione - e mettere in campo risorse proporzionate. Molti Paesi già lo fanno: posso citare Israele e diversi Stati del Sud Est asiatico, specialmente la Corea del Sud ma anche la Malesia e il Vietnam, che da situazioni di povertà si stanno trasformando in eccellenze tecnologiche investendo in settori paradossalmente trascurati dai Paesi più "avanzati" nell'economia tradizionale. In Europa spicca l'Irlanda, che sta dimostrando una grande capacità attrattiva di capitali esteri determinata sicuramente dall'effetto Brexit, ma anche da massicci investimenti aziedali in termini di innovazione e sicurezza.

Tornando ai bilanci di fine anno, gli ultimi mesi sono stati segnati da attacchi su larghissima scala capaci di determinare effetti a livello globale, come nei casi di *WannaCry* e *NotPetya* o del caso, di cui lei stesso ha scritto di recente, degli archivi dell'intelligence USA finiti in chiaro sui cloud server di Amazon. Potremmo anche richiamare, restando nei nostri confini nazionali, gli attacchi rivolti a Unicredit e Confindustria. Cosa possiamo imparare da queste esperienze?

Innanzitutto ad aggiornare i sistemi (includendo il *patch-management* tra le priorità assolute) per non offrire il fianco a questo tipo di attacco. Poi l'*information sharing*, come dicevamo: la comunicazione tra attori e la condivisione di strumenti è assolutamente fondamentale.

A questo proposito WannaCry ha dimostrato i pericoli e la pervasività di un attacco su larga scala - le multinazionali coinvolte hanno dichiarato danni, in media, per 2-300 milioni di euro - ma ricordiamo che ha fatto leva sulle falle di aggiornamento di codici microsoft; se avesse usato, ad esempio, codici Zeroday l'impatto avrebbe potuto essere infinitamente più devastante: se vogliamo prevenire un'eventualità del genere, le parole chiave restano consapevolezza e condivisione.

A cura della Redazione