DIFENDERSI CON UN APPROCCIO INTEGRATO

di BENIAMINO MUSTO

NELLA MAGGIOR PARTE DEI CASI GLI ATTACCHI CYBER POTREBBERO ESSERE EVITATI SE LA PERSONA DAVANTI AL COMPUTER FOSSE CONSAPEVOLE DEI RISCHI, O SE CONOSCESSE LE PROCEDURE DA ADOTTARE, AD ESEMPIO, QUANDO ARRIVA UNA EMAIL SOSPETTA. DALL'ALTRO LATO BISOGNA CONTINUARE A SVILUPPARE TECNOLOGIE PER PROTEGGERE I SISTEMI DA UN PUNTO DI VISTA CIBERNETICO, COME SPIEGA PIERLUIGI BARBERINI, ANALISTA RESPONSABILE DEL DESK DIFESA & SICUREZZA DEL CESI

Se non fosse una parola così abusata, probabilmente anche per i cyber attacchi si potrebbe parlare di emergenza. L'ultimo rapporto **Clusit** ci dice che nel 2021 sono stati registrati globalmente 2.049 cyber attacchi gravi, cioè con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica. Il dato è in un aumento di quasi il 10% rispetto all'anno precedente, per una media mensile di 171 attacchi, il valore più elevato mai registrato.

Secondo **Pierluigi Barberini**, analista responsabile del desk *Difesa & Sicurezza* del **CeSi**, "sono aumentati nel complesso il numero degli attacchi cibernetici perché parallelamente è aumentata la superficie di attacco disponibile", anche per via del massiccio ricorso al lavoro da remoto durante la pandemia. I pericoli maggiori arrivano dai malware, e in particolare dai ransomware, che restano gli strumenti preferiti dei cyber criminali per generare profitti. Difficile fare un identikit di chi si cela dietro questi episodi. "Le categorie di attori malevoli – dice Barberini – sono molteplici. Nella maggior parte dei casi ci troviamo di fronte a personaggi che rubano online allo stesso modo con cui dei rapinatori rubano nel mondo reale. Poi vi sono, in percentuale più limitata, una serie di attacchi portati avanti da hacker che potremmo definire *etici*, cioè non mossi da finalità di lucro. Infine, c'è una percentuale di attacchi riconducibili ad attività statali, i cosiddetti attacchi *state-sponsored*, portati avanti da reparti cibernetici, o direttamente dai servizi di sicurezza di uno Stato".

DAL CYBER CRIME ALLA CYBER WARFARE

Uno degli elementi caratterizzanti della guerra cibernetica (o per dirla all'inglese, *cyber warfare*) riguarda il fatto che se uno Stato ne vuole colpire un altro, l'utilizzo del canale cibernetico ne garantisce l'anonimato. "Oggi – conferma Barberini – con le tecnologie a disposizione a livello militare, possiamo riuscire a sapere quando e da dove un missile viene lanciato. Ma nell'ambito cyber, invece, è davvero difficile attribuire con certezza la paternità di un attacco". Nella stragrande maggioranza dei casi gli Stati adottano questo

QUANTO GIOCA L'ELEMENTO UMANO

Il problema degli attacchi cyber non è percepito nella misura in cui dovrebbe. Soprattutto, l'esplosione dello smart working non ha ancora portato a un adeguato livello di consapevolezza. Pierluigi Barberini, analista responsabile del desk Difesa & Sicurezza del CeSi, sottolinea che con lo smart working "non è solo l'azienda responsabile della propria difesa, ma lo anche è il singolo individuo che deve essere in prima linea e consapevole dei rischi cibernetici. Essendo ormai tutti i sistemi completamente integrati tra loro, non è più il singolo reparto IT di un'azienda che si deve occupare in maniera chiusa della sicurezza, ma ci deve essere una partecipazione attiva da parte di tutti i dipendenti".
Ci sono casi sofisticati in cui i cyber criminali entrano nei sistemi per studiare le prassi e la cultura aziendale. "Una prima modalità attraverso cui ci si infiltra è quella di restare silenti, osservando e non portando avanti l'attacco immediatamente. E dopo aver compreso quale potrebbe essere un punto debole, si va a scegliere un target ben definito che si ritiene essere penetrabile".

tipo di attacco perché possono colpire un competitor evitando di venire accusati direttamente dell'azione. Ecco perché da alcuni anni il dominio cibernetico (e quello spaziale) è stato riconosciuto dalla Nato al pari dei domini tradizionali (terrestre, aereo e marittimo) in cui possono verificarsi scenari di guerra. "Questo è indicativo dell'importanza della considerazione che sta assumendo da anni la dimensione cibernetica anche a livello militare".
Diventa a questo punto inevitabile fare un accenno alla guerra in corso tra Russia e Ucraina. "Gli ucraini – ricorda l'esperto del CeSi – sono stati attaccati molte volte dal punto di vista cibernetico dai russi nel corso degli ultimi anni. Ad esempio ci sono stati diversi attacchi alla rete elettrica nazionale, tutti attribuibili ai russi, anche se non esistono prove evidenti proprio per i motivi cui si accennava in precedenza. Ad ogni modo,


© Vit_Mar – iStock

proprio perché è stata già vittima in passato di questo tipo di aggressione, Kiev si è preparata per tempo e ha provato a rafforzare le proprie difese cyber, anche grazie al supporto dell'Ue e degli Usa".

I RISCHI PRINCIPALI IN ITALIA

Per quanto riguarda nello specifico il nostro Paese, il rischio principale resta il ransomware. "La frequenza di questo tipo di attacchi è aumentata molto negli ultimi anni perché risponde alla logica di avere un lucro immediato. E il metodo per effettuare questo tipo di attacco nella maggior parte dei casi avviene tramite email di phishing". Per quanto riguarda il mondo produttivo, secondo Barberini le Pmi italiane, per dimensione, per scarsità di mezzi economici, ma anche per un approccio culturale superficiale, investono poco in cyber security rispetto alle aziende di altri competitor europei. Per provare a invertire la tendenza si potrebbe agire in due modi che vanno combinati tra loro. Uno, spiega, riguarda fattore umano: "bisogna ricordarsi che nella maggior parte dei casi gli attacchi potrebbero essere evitati se la persona davanti al computer fosse al corrente e fosse consapevole dei rischi, o se conoscesse le procedure da adottare in determinati casi, ad esempio quando arriva una email sospetta. Dall'altro lato bisogna continuare a sviluppare tecnologie per proteggere i sistemi da un punto di vista cibernetico. In definitiva, serve un approccio integrato, cioè unire l'aspetto tecnologico a quello umano, operando in parallelo su entrambi gli aspetti".