Cybersecurity Supply Chain: cosa non va e che cosa si può fare

Author : Marcello Fausti

Date : 10 Gennaio 2019

Molto sinteticamente, se ci riferiamo ad un modello generico che può essere considerato valido per una grande organizzazione, le attività e di conseguenza le competenze che rientrano nella catena di fornitura cyber sono:

- Attività specialistiche per la gestione del SOC (Security Operation Center), per la Threath Intelligence, per le verifiche tecniche, per la forensic analysis e per il l'Internal Lab;
- Attività specialistiche per la progettazione, realizzazione e mantenimento in esercizio delle contromisure di sicurezza;
- Attività specialistiche per la definizione delle policy di sicurezza, per l'analisi del rischio, per la definizione dei requisiti di sicurezza per infrastrutture, applicazioni, dati e device e per il monitoraggio dell'applicazione di policy, requisiti e contromisure.

Ovviamente, i modelli di fornitura possono variare in modo significativo: si va da soluzioni in-house con ricorso all'acquisizione di servizi professionali esterni a volume (FTE/FFP)[1] o di servizi a canone, fino al full-outsourcing o perfino all'offshoring.

Struttura dell'industria cyber

Ora, le attività ed i modelli di fornitura precedentemente citati sono "animati" da tre tipologie di soggetti:

1. I vendor;
2. I system integrator;
3. Le società di sicurezza specializzate.

Vediamo brevemente quali sono le rispettive caratteristiche ed i ruoli che giocano nella catena di fornitura cyber.

Vendor

Si tratta per lo più di aziende statunitensi e israeliane, con poche eccezioni. Di norma hanno strutture europee molto snelle con capacità di supporto tecnico bassa o pressoché nulla e che comunque dipende dalla storia del fornitore e dalla dimensione del suo mercato di riferimento. Queste aziende sono disposte a sconti esagerati (anche del 90%) pur di mantenere fissa e non trattabile la manutenzione annua che oscilla, in genere, intorno al 20% del prezzo di acquisto e costituisce – per il vendor - un significativo battente di fatturato ripetitivo destinato a coprire costi di R&D, sviluppo prodotti e supporto ai clienti. Per inciso, contabilmente le manutenzioni sono classificate come costi (opex), a differenza dell'acquisto dei prodotti che è classificato tra gli investimenti (capex); ovviamente, per un puro criterio contabile si tende a favorire gli investimenti rispetto ai costi e questo ha un impatto non irrilevante sulle negoziazioni pluriennali e sui rinnovi delle manutenzioni. In queste condizioni, l'acquisto di un prodotto software o di una piattaforma hardware è quasi sempre un salto nel buio che può produrre risultati soddisfacenti solo se il cliente ha notevoli capacità di governo "tecnico" del processo o se si rivolge ad un system integrator certificato (e quindi con competenze sul prodotto). In ogni caso, non è una passeggiata di salute e bisogna essere pronti ad esercitare un'azione di controllo molto stringente. A complicare ulteriormente il quadro, spesso, accanto al vendor si posizionano due tipi di intermediari che intervengono rispettivamente nella fase iniziale e nella fase conclusiva della vendita.

Si tratta di:

- Agenzie commerciali e/o procacciatori d'affari che agiscono nell'ambito di un contratto di mandato per conto dei vendor (spesso di nicchia o start-up) che non hanno una struttura di vendita diretta in Italia o in Europa;
- Canale distributivo, ovvero, azienda specializzata nel cosiddetto "box moving" sia esso effettivamente relativo all'acquisto di apparati hardware o alla semplice movimentazione di licenze software.

Come si può immaginare, è un contesto piuttosto complesso, una specie di circo che – spesso – non ti consente di capire come stanno effettivamente le cose.

System Integrator

Sono società che nascono nel mondo dello sviluppo software "generalista" e si sono successivamente spostate sul mercato adiacente della cybersecurity che, negli ultimi anni, ha conseguito tassi di crescita più elevati della media degli altri settori. Le competenze specifiche sono – generalmente – basse, tranne che nel caso in cui il system integrator scelga di "sposare" uno o più prodotti di un vendor; in questo caso, gli accordi con il vendor li obbligano a sviluppare competenze specifiche in quantità regolate contrattualmente e certificate dal vendor medesimo. Tranne che per il caso appena descritto, il focus dei system integrator è sul prezzo per FTE o FFP che deve essere commisurato alle richieste delle gare nel mercato della pubblica amministrazione e delle grandi aziende. Come è comprensibile, i grandi system integrator ottengono questo risultato creando una rete di aziende subfornitrici, un bacino da cui

pescare risorse a basso costo, a cui corrispondono competenze scarse e trattamenti retributivi commisurati ai minimi di mercato. A parte le considerazioni etiche sullo sfruttamento del lavoro giovanile e non (che però riguarda anche le aziende committenti che accettano quelle subforniture); il fatto è che le tariffe basse si pagano con competenze di basso livello, scarsa o nulla capacità propositiva e livelli di turnover esageratamente elevati, spinti anche dalla endemica carenza di skill su temi tecnologici e digitali in genere e sulla cybersecurity in particolare. Il side effect di tutto ciò è la creazione di una nicchia di mercato del lavoro distorta dal potere di attrazione della PA e delle grandi imprese e dalla carenza di risorse con skill adeguate.

Società specializzate

Sono poche e con competenze di punta o addirittura di eccellenza. Si concentrano su poche fasi della catena di fornitura, per lo più quelle a più alto valore aggiunto, ad esempio, la costruzione e/o la gestione dei SOC (Security Operations Center,) la forensic analysis, la strategia, la progettazione di alto livello, e così via. Non hanno capacità di scalare su volumi medio-alti per limiti culturali facenti capo alla cosiddetta cultura hacker e per conseguente scarsa (o scarsissima) capacità finanziaria e, soprattutto, organizzativa. Non potrebbero mai reggere i tempi di pagamento imposti dalla PA e dalle grandi aziende e per questo sono quasi sempre ingaggiate dai system integrator per coprire fasi della fornitura che non sono in grado di realizzare. Ovviamente (e nessuno deve stupirsi) il system integrator gestisce queste subforniture pregiate muovendo le leve che ha, che sono PXQ: Prezzo x Quantità. Il prezzo, ovviamente, non può cambiare perché è fissato contrattualmente e la quantità, quindi, è l'unica leva disponibile.

I clienti

Gli effetti di questa situazione su chi acquista servizi professionali specialistici sono i seguenti:

- Risorse con scarse competenze, spesso neo, demotivate e posizionate a livello retributivo ai minimi di mercato;
- Conseguente necessità di un periodo di formazione in affiancamento per rendere queste persone idonee a supportare i processi operativi dell'azienda cliente;
- Elevato turnover delle risorse esterne che – appena consolidato un livello di operatività soddisfacente – prendono il volo verso incarichi che consentono di raggiungere stipendi più alti valorizzando il periodo di formazione effettuato.

Quindi, le grandi aziende, quelle che acquistano grandi volumi di FTE di esterni, pagano la scelta di ricorrere a gare fortemente basate sul prezzo (e come potrebbero fare altrimenti) con il fatto che stanno pian piano diventando dei grandi centri di formazione on-the-job per risorse che, prima o poi, si re-immetteranno nel mercato del lavoro, alimentando un circolo tutt'altro che virtuoso: scarse competenze-prezzo basso-training on the job- turnover elevato e così via.

Fin qui lo scenario. Ora che cosa si può fare per correggere questo sistema?

Intanto il problema principale è la scarsità di risorse con skill adeguati. Se ci fosse una disponibilità adeguata di risorse con skill, probabilmente, il mercato si autoregolerebbe riducendo il turnover a livelli accettabili.

Poi, dall'analisi delle aziende fornitrici, emerge un panorama eccessivamente frammentato. Il mercato sembra maturo per l'avvio di una forma di aggregazione di realtà complementari in modo da risolvere due problemi: la massa critica e di conseguenza la capacità finanziaria; la maggiore copertura della catena di fornitura cyber. Una buona soluzione potrebbe essere quella di creare strutture societarie a rete focalizzate sulla catena di fornitura cyber per come sopra descritta. Una società specializzata sulle attività più strettamente tecniche afferenti al mondo cyber; una società focalizzata sul risk management a livello micro ma anche sull'ERM[2] e sul sistema di controllo interno e una società dedicata ai servizi di progettazione, sviluppo ed esercizio delle infrastrutture di sicurezza e delle contromisure in genere. Un'eventuale aggiunta interessante potrebbe riguardare un'Academy sui temi Cyber con lo scopo di fornire servizi ai clienti, ma anche di formare gli interni in un ciclo di continous education. Una riduzione della frammentazione consentirebbe, inoltre, di ottenere un maggiore fattore di scala nella gestione di infrastrutture e funzionalità di sicurezza (MSS[3]) consentendo, cosi, a questo mercato di decollare anche in Italia.

Che cosa succede, invece, per le piccole e medie imprese che – di certo – non possono permettersi né budget milionari, né grandi strutture interne capaci di controllare le dinamiche appena raccontate?

La prospettiva delle PMI è strettamente connessa alla sfida della digitalizzazione dei processi che – per loro in particolare - è basata sull'adozione di servizi in cloud ed in particolare sull'utilizzo di SaaS. Tutte le PMI, sia quelle più innovative che quelle più tradizionali hanno bisogno di proteggere i loro dati, quelli dei loro clienti e, soprattutto devono proteggere la proprietà intellettuale sulla base della quale affrontano i mercati domestici e l'export sui mercati internazionali. Inoltre, esse svolgono spesso un ruolo importantissimo nella catena di fornitura delle grandi aziende rispetto alle quali – se non indirizzano correttamente i fondamentali di sicurezza – rischiano di diventare una criticità molto rilevante.

Anche, è ovvio, le PMI beneficerebbero del consolidamento del settore in strutture organizzative a rete aventi la dimensione industriale necessaria a supportarle nel loro viaggio per la trasformazione digitale e verso il cloud.

Note

[1] FTE = Full Time Equivalent; FFP = Free Function Point

[2] ERM = Enterprise Risk Management

[3] MSS = Managed Security Services

Articolo a cura di **Marcello Fausti**