SECURITY OPERATIONS CENTER: COME SCEGLIERE IL GIUSTO SERVIZIO SOC

di Giuseppe Mazzoli
Amministratore Unico di 3CiME Technology

Il Security Operations Center è un servizio di cyber security ormai offerto da diverse realtà. Ma quali sono le caratteristiche indispensabili di un SOC aziendale?

Ci sono SOC e SOC. Per avere una visione chiara su quale scegliere, non possiamo prescindere dal ricapitolare che cos'è il servizio di **Security Operations Center (SOC)**. Questa volta per spiegarlo partiamo dal punto di arrivo: la security as a service, ossia la sicurezza venduta come servizio.
La sicurezza è un processo talmente complicato che neanche le grandi organizzazioni riescono più a governare internamente e, come è evidente parlando del PAM, gli attacchi informatici sono ormai mirati, ovvero volti a colpire una determinata organizzazione. I pirati che riescono ad entrare non attaccano subito, ma studiano le reti, i punti di debolezza e, un determinato giorno vicino al fine settimana, lanciano l'evento distruttivo.
E quindi chiara per tutti la ormai evidente necessità di avere un **controllo preventivo e automatizzato che funzioni 24 ore su 24, 7 giorni su 7 per 365 giorni l'anno** – perché la notte tutti vorremmo dormire e perché, in molte organizzazioni, neanche i tecnici dell'IT saprebbero cosa fare in caso di attacco.
Ecco, quindi, che entra in gioco il SOC, il Security Operation Center, che prevede una squadra di lavoro composta da:

- Prodotti dotati di tecnologie con intelligenza artificiale;
- Persone capaci di intervenire per difenderci.

Questa è la sicurezza come servizio completo e nella pletora di offerte che si trovano in giro – alcune, dobbiamo ammetterlo, un po' stravaganti – tutte includono almeno questi due punti. Quindi, per capire bene la differenza e concentrare la nostra scelta bisogna porre l'attenzione sul **livello di SOC security che viene erogato e sui servizi aggiuntivi.**

Cyber Security e SOC: livelli di servizio e considerazioni

Per individuare il Security Operation Center di interesse, partiamo dai livelli di servizio di Cyber Security erogabili:

- **Allarme**: il cliente finale viene semplicemente avvisato che è sotto attacco;
- **Allarme + blocco dell'attacco**: questo servizio dipende dall'accesso del SOC alle risorse aziendali e da come lavora. Ad esempio, se viene attaccato il firewall e il SOC non ha le password dello stesso, bisogna mettere in isolamento il firewall, o, se non si può, dire a tutto il resto della rete di "non parlargli più". Comprendiamo quindi che, in questo caso, la situazione va ben gestita e conosciuta a priori;
- **Allarme + blocco dell'attacco + remediation**: questo è il livello più completo, dove il Security Operation Center si preoccupa, sia in via preventiva che consuntiva, di tamponare le falle, correggere le configurazioni laddove possibile e fin dove i tecnici del SOC hanno accesso.

Ma possiamo declinare la remediation in un ulteriore dettaglio:

- **Remediation correttiva**: in questa azione i tecnici del SOC "buttano fuori i cattivi" dalla nostra rete, fanno sostanzialmente **pulizia** delle sporcizie che sono entrate e che minacciano i nostri dati;
- **Remediation preventiva**: gli operatori del SOC attivano ex-ante tutti quei miglioramenti e cambi di configurazione che **riducono ai minimi termini i rischi di intrusione ed attacco**, sia lato client e che lato server, e, se ne hanno accesso, anche lato firewall.

Cosa deve difendere un servizio SOC

Possiamo individuare essenzialmente 5 punti, uno dei quali articolato. In sostanza il monitoraggio e la difesa devono riguardare (non è un ordine di importanza, ma solo logico):

1. Il network
2. Le mail
3. I server
4. Gli endpoint
5. I dati e le applicazioni:
    - On-premise
    - In cloud 365
    - In cloud SAAS

Questo è sicuramente il Cyber Security Operation Center definitivo e, considerato questo, vien da sé il perché la nostra azienda abbia scelto di **investire nei rapporti con un SOC esistente**: con la massima trasparenza e rettitudine, abbiamo pensato che per erogare un servizio di qualità ci vogliono centinaia di persone, che se si licenziano sono, almeno in Italia, di difficile sostituzione. E non è solo questo il punto d'interesse.

Se ti trovi nella scelta di valutare un SOC, le prime considerazione da fare sono:

- **Valutare la squadra di persone**. Nel nostro caso oggi ne contiamo più di 680 (che non sono tutte ovviamente a nostro libro paga);
- Valutare la **copertura oraria del livello di servizio**;
- Valutare la **copertura mondiale di un SOC**: ad esempio il nostro SOC ha 4 sedi, secondo il concetto di "*follow the sun*" che si distribuiscono fra Australia, Europa, Usa est ed USA ovest; questo permette che una minaccia rilevata in Australia sia immediatamente disponibile a tutto il gruppo di lavoro, e quindi agli operatori di tutto il mondo. Se viceversa un SOC è basato esclusivamente in Italia, per accorgersene bisogna aspettare che la minaccia arrivi…in Europa;
- Considerare l'inclusione a **forfait delle remediation** nel prezzo proposto che, a nostro avviso, aiuta davvero le organizzazioni ad andare verso la security as a service dalla quale siamo partiti. E poi quale remediation? Solo correttiva o anche correttiva + preventiva?
- Considerare come plus la presenza di una "**garanzia**" **contro il data breach**, ossia la possibilità di avere un rimborso economico in caso di attacco andato a buon fine. Questo è un parametro del livello di servizio offerto ed è un punto di qualità da tenere in assoluta considerazione.