Trasmettere il Cyber-Risk attraverso attività di controllo basate sull'Impatto Reale

Author : Massimiliano Brolli

Date : 4 dicembre 2018

Quante volte vi siete imbattuti in un controllo di sicurezza che recitava queste parole?

- Presenza di password predicibili di sistema operativo
- Account di amministrazione di default
- Mancato patching delle componenti di middleware

Ma tutto questo, per chi non si occupa di sicurezza, cosa può significare?

Come riusciamo a trasmettere, in modo efficace, la consapevolezza del rischio ai non addetti ai lavori? Ce lo siamo mai chiesto?

La Cyber Security è una materia vasta, costantemente in evoluzione dove spesso si fatica a rincorrere nuovi concetti di difficile comprensione. In questo articolo vorrei provare a raccontare come superare e migliorare l'efficacia della comunicazione nelle attività di offensive-security per consentirne una facile divulgazione del rischio, a tutti i livelli, compreso il management.

Il concetto di Api, Alveare e Miele

Prima di addentrarci su come comunicare, soffermiamo l'attenzione su una piccola metafora che spiega in maniera semplice e intuitiva un concetto chiave, il concetto di Alveare.

1. **L'Alveare:** è il sistema da violare che contiene un'infinità di possibili strade, cunicoli e percorsi da affrontare per arrivare al bene più prezioso in esso contenuto.
2. **Il Miele:** è il bene più prezioso contenuto nel sistema, ad esempio le carte di credito in applicazioni di e-commerce, i dati di traffico in sistemi telco, le transazioni in sistemi bancari, ecc...
3. **Le Api:** sono tutte le soluzioni di sicurezza e le protezioni perimetrali implementate per garantire l'inviolabilità di un sistema che occorre superare per arrivare al miele.

Una attività di controllo di sicurezza non vuol dire solo fornire “mere” vulnerabilità potenziali rilevate in campo ma verificare se risulti possibile entrare nell'alveare indisturbati dalle api che lo circondano e prelevare il bene più prezioso in esso contenuto, cioè il miele.

Pertanto, volendo svolgere attività di controllo finalizzate a rilevare gli “Impatti reali”, dobbiamo sempre tenere in considerazione quanto sopra e porci sempre una importante domanda prima di attivare la nostra Kali Linux, ovvero: quale è il miele custodito nel sistema?

Differenza tra Impatto Reale e Impatto Potenziale

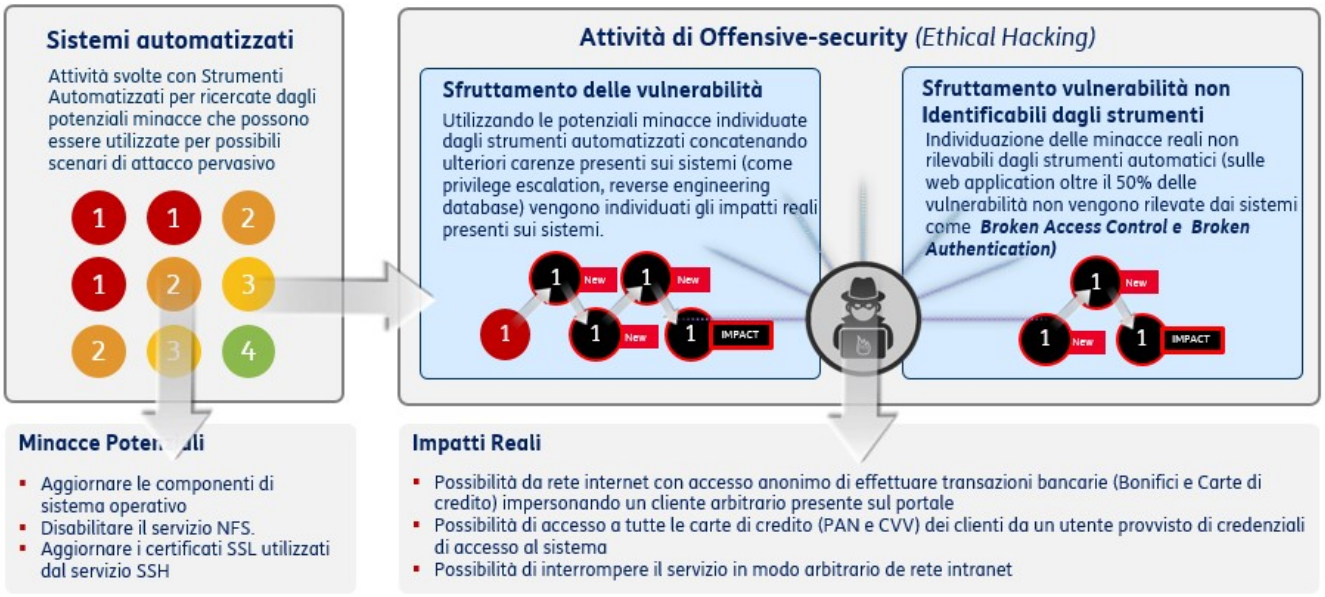
Esiste una sostanziale differenza tra una vulnerabilità di sicurezza con exploit pubblico capace di generare un “impatto reale” di compromissione della RID e una vulnerabilità di sicurezza "potenziale".

Mettere in sicurezza un sistema ha un costo e sebbene operare in logica “security by design” è sempre la scelta migliore, un sistema ben progettato dall’inizio, con il passare del tempo, tende ad essere insicuro per una serie di motivi come il mancato Patching, il fenomeno di Hardening-loss, l’obsolescenza tecnologica e tutto quello che conosciamo come Cyber-Security-Evolution.

In una logica di “coperta corta”, saper evidenziare gli “impatti reali” ai quali è esposto un sistema (e le relative vulnerabilità sfruttabili) consente di indirizzare e focalizzare al meglio l’effort disponibile evitando di agire in modo indiscriminato su tutte le minacce senza fornire una priorità di intervento.

Costruire una attività di controllo basata sull'Impatto Reale

E’ necessario quindi evolvere il modello di Assessment fino ad oggi basato nel prelevare il più alto numero di vulnerabilità potenziali presenti in campo in un modello basato sulla priorità di intervento e misurazione del rischio attraverso l'impatto reale. La realtà ci insegna che solo alcune vulnerabilità critiche potenziali presenti su un sistema possono essere sfruttate per condurre un attacco pervasivo.



Per far questo non bastano le attività automatiche (ancora oggi gli APT e i data-breach vengono preparati da persone e non da automi). Occorre svolgere attività di ethical-hacking per consentire un controllo profondo, su specifiche direttrici di rischio, mirate a "rubare" quel "miele" di cui parlavamo in precedenza.

Questo perché non esistono ancora strumenti capaci di concatenare vulnerabilità e di portarci, su un piatto d'argento, un "Impatto reale" significativo, paragonabile ad un data-breach. Pensiamo ad esempio alle Top10 Owasp e al ***Broken Access Control*** e ***Broken Authentication*** in ambito web application. Sono due esempi di falle altamente critiche, di difficile rilevazione (dalla mia esperienza di impossibile rilevazione da parte di uno scanner automatico) che possono condurre ad un data-breach senza precedenti.

Dobbiamo quindi distinguere vulnerabilità critiche, utili a generare un impatto reale, da vulnerabilità critiche (ma di minore priorità) non utili a generare un impatto significativo. Non bisogna per far comprendere quanto è critico un sistema rendere tutto indiscriminatamente “rosso”. Il “rosso” nel nostro caso sarà l’impatto reale che dovrà essere "immediatamente" rimosso dai sistemi, il resto viene dopo in termini di priorità di intervento.

L'attività di controllo cambia forma e aspetto, più orientata ad impersonare un reale "cattivo" che vuole prelevare il “miele” da un sistema per poi trarne un “reale” vantaggio.

Inoltre sarà necessario rappresentare, in un quadro più ampio di analisi, ulteriori grandezze misurate in quel preciso “time-stamp” di Assessment come ad esempio:

1. Livello di skill necessario per generare l’impatto.
2. Superfice di esposizione dell’impatto (ad es. Internet in pre-auth o in post-auth, da rete segregata, subnet, dietro firewall, mitigato da waf, ecc...)
3. Livello di compromissione del sistema attraverso la misurazione della RID; fornire un indice sulla compromissione della Riservatezza, Integrità e Disponibilità dei dati trattati per gli impatti reali analizzati.

Comunicare l'Impatto Reale

Comunicare efficacemente consente di aumentare la consapevolezza del Cyber-Risk ai non addetti ai lavori, per far capire con parole semplici - rigorosamente non tecniche - quali sono i reali rischi misurati su un sistema informatico.

L'approccio top-down aiuterà a disegnare un modello di documentazione, che, partendo dagli impatti Reali, farà addentrare l’utente negli aspetti più tecnici fino alle vulnerabilità di sicurezza rilevate. Nel documento saranno poi riportati i vettori di attacco fino ad arrivare al tecnico-specialistico di dettaglio che potrà essere utile per indirizzare le remediation da parte dei tecnici delle linee di progettazione.

Ma se vi state ancora domandando quale possa essere un reale impatto, ne riporto alcuni che credetemi, valgono più di 1000 altre parole:

- *Possibilità da rete internet, con accesso anonimo, di effettuare transazioni bancarie (utilizzando Bonifici e Carte di credito) impersonando un cliente arbitrario.*
- *Possibilità di esfiltrazione di carte di credito (compreso PAN e CVV) dei clienti, da parte di un utente provvisto di credenziali di accesso al sistema.*
- *Possibilità di interrompere il servizio da rete internet, in modo arbitrario, in assenza di autenticazione.*

D’altra parte, l’headline delle testate giornalistiche ci insegnano come trasmettere in pochi caratteri messaggi “Importanti”. Il recente Data Breach di Facebook veniva rappresentato in questo modo: “Violati 50 milioni di account Facebook, a rischio la nostra privacy” … tutto questo è diverso dall'Impatto Reale?

Conclusioni

La differenza tra “impatto reale” e “minaccia potenziale” anche se sottile, risulta sostanziale nelle attività di Controllo. Se questo concetto risulta semplice da far comprendere a persone fuori dalla Sicurezza, è paradossalmente ostico da far digerire a chi quotidianamente svolge attività tecniche specialistiche di ethical-hacking sempre focalizzato nel comunicare in modo tecnico a volte incomprensibile da chi di sicurezza conosce a malapena il significato.

Il messaggio tecnico e l’executive (ma il potere di sintesi in generale) lo sappiamo tutti, sono punti di vista poco conciliabili. Riuscire ad unirli risulta fondamentale per raggiungere un grado di rappresentazione del rischio comprensibile, a tutti i livelli.

Utilizzare messaggi semplici, fornire le priorità di intervento, far comprendere in modo inequivocabile i rischi ai quali si va in contro (magari citando anche data-breach pubblici similari e successive sanzioni amministrative sostenute dai malcapitati) consente di ottenere la giusta attenzione e quindi avviare una veloce "remediation" con conseguente ripristino della sicurezza in un sistema.

Al contrario, non fornendo un indicatore di priorità, si porta a trattare in maniera “opaca” il rischio e avviare remediation trasversali poco efficaci, magari tralasciando i punti nevralgici del sistema, solo perché, "...era finito il budget!".

L’impatto Reale risulta la sintesi finale che ci consente di arrivare a trasmettere il reale impatto presente su un sistema fornendo inoltre la giusta priorità di intervento per ogni singola attività di remediation. Questo è necessario perché quando si parla di sicurezza informatica, non sempre è possibile realizzare tutto per differenti motivazioni, non ultima quella dei costi.

Articolo a cura di **Massimiliano Brolli**