Cyber Risk Indicator: ecco la formula di Yoroi per capire se la tua azienda è a rischio sul web

L'azienda italiana propone tre indici per valutare l'esposizione aziendale ad attacchi informatici

https://yoroi.company

comunicato stampa del 1 Luglio 2021

E tu, lo sai qual è il tuo **rischio cyber**? Pensi che sarebbe utile saperlo?

A Yoroi pensiamo di sì.

Per questo Yoroi ha deciso di sviluppare un indice di esposizione digitale, lo **Yoroi Cyber Exposure Index**. La sua finalità è di **misurare lo spazio digitale** utilizzabile da un possibile attaccante, contro ogni organizzazione, utilizzando tre variabili: il **numero di servizi esposti**, lo **score delle vulnerabilità** e l'**indice di data leakage**.

E la sua importanza è facile da comprendere, visto che la sicurezza informatica passa prima di tutto per la capacità di muoversi in anticipo ed evitare o limitare i danni potenzialmente distruttivi di un attacco cyber. Pericoli che non possiamo ignorare visto che la difesa dello spazio digitale gioca un ruolo centrale nella difesa del funzionamento di ogni organizzazione e, più in generale, nell'economia del nostro paese.

L'indice si basa su eventi già accaduti, come un attacco informatico di successo; sfrutta informazioni raccolte nei forum hacker del **Deep Web**; analizza i dati in vendita nei marketplace illegali del **Dark Web**.

Quest'indice di esposizione è anche la base per dare sostanza al concetto di **analisi preventiva** della **supply chain** aziendale, cioè alla necessità di valutare la potenziale "insicurezza" del proprio ecosistema di riferimento, elemento fondamentale di un **sistema di sicurezza integrato**.

Come dice **Marco Castaldo, consigliere delegato di Yoroi**, "Per ogni organizzazione, ente o azienda, oggi è cruciale avere informazioni tempestive sulla propria postura di sicurezza, prima che eventuali vulnerabilità vengano sfruttate da attaccanti. Per valutare correttamente quella postura

bisogna analizzare quell'organizzazione dall'interno, certo, ma anche all'esterno, alla ricerca delle sue "esposizioni".

E non dimentichiamoci che pure chi attacca guarda a questi dati. I sindacati criminali sono finanziati da "investitori" che puntano al massimo profitto, saranno dunque motivati ad attaccare chi "appare" più vulnerabile rispetto a chi sembra essere meno esposto.

Per migliorare le difese allora Yoroi ha sviluppato lo Yoroi Cyber Exposure Index.

Il valore finale dell'indice, comparato a quello di società simili per dimensioni, attività e servizi, permetterà inoltre di arrivare a dei veri e propri benchmark di riferimento. "Un'azienda che vedrà un numero 'alto' come indice di esposizione – continua **Castaldo** - potrà decidere se approfondire l'indice di rischio attuale con un'analisi interna. Le esposizioni tracciate dal nostro sistema di analisi ci consentiranno tra l'altro di consigliare a quella organizzazione le azioni più mirate per poter massimizzare il ritorno dall'investimento in strumenti di difesa cyber".

Ma come funziona concretamente lo Yoroi Cyber Exposure Index?

Lo **Yoroi Cyber Exposure Index** analizza l'esposizione aziendale senza alcuna azione attiva sull'organizzazione indicizzata, su tre diverse dimensioni: il **numero di servizi esposti**, le **vulnerabilità note presenti** e il **numero di data leak** legati al dominio aziendale.

Più elevato è il **numero di servizi** raggiungibili su internet, più varie sono le tecniche che un attaccante può sfruttare per ottenere un accesso non autorizzato.

Più **vulnerabilità** sono sfruttabili da un attaccante, più sarà facile compromettere un host.

Infine, più **data leak** sono presenti, più facilmente l'attaccante sarà in grado di ottenere informazioni utili per portare a termine un attacco.

Queste tre dimensioni cercano di riassumere i vari **scenari di attacco** da parte di un attaccante esterno, vediamole in dettaglio.

Numero di servizi esposti

La prima componente dello Yoroi Cyber Exposure Index è il numero di servizi esposti. Questo valore cerca di dare un'indicazione della superficie di attacco esterna, ed è calcolato dalla somma dei differenti IP, porte e protocolli associati all'azienda e accessibili dall'esterno. Per ridurre questo indice, un'azienda dovrebbe analizzare tutti gli IP e servizi esposti all'esterno e ridurre l'accesso solo a quelli strettamente necessari.

Score delle vulnerabilità

La seconda componente dell'indice è la somma della gravità delle vulnerabilità note dei servizi. Con questo indice si vuole stimare la facilità con cui un attaccante può compromettere il perimetro aziendale, sfruttando vulnerabilità da remoto.
Per questo motivo, consideriamo unicamente le vulnerabilità note che sono identificabili e sfruttabili da remoto. Per ridurre questo indice, un'azienda dovrebbe aggiornare i software vulnerabili, dando precedenza a tutti i servizi esposti in rete.

Indice di data leakage

La terza e ultima componente misura quanti leak contenenti account aziendali sono disponibili ad un attaccante. Un leak potrebbe includere solamente informazioni personali, ma anche password protette (hash), o addirittura password in chiaro.

Lo **Yoroi Cyber Security Index** prende in considerazioni questi aspetti stabilendo uno score di partenza che è fatto decadere nel tempo a partire dalla data presunta del leak.

Questo indice non si può ridurre attivamente, ma può essere solo visto come un'indicazione di quante informazioni possono essere disponibili ad un attaccante. È possibile ridurre il numero di leak futuri, ad esempio, riducendo il numero di account esterni creati, utilizzare password diverse per ogni servizio e controllare periodicamente le proprie password per verificare se siano compromesse o meno.

"Il focus del Cyber Exposure Index – dice **Marco Ramilli, CEO di Yoroi** - non è quello di giudicare l'organizzazione indicizzata ma di offrire una 'vista di esposizione' che un attaccante può utilizzare come step iniziale. È indicativo della probabilità di riuscita dell'attaccante, e si modificherà nel tempo in funzione delle azioni messe in campo per proteggersi. Ma intanto bisogna conoscerlo".

Per saperne di più, chiedi a **Yoroi**! https://yoroi.company

---

Marco Ramilli, ingegnere e dottore informatico, esperto di hacking, appassionato di intelligenza artificiale, è il fondatore di Yoroi: un service provider di cybersecurity innovativo, tra i più performanti nel settore. Il suo blog personale è nella classifica mondiale dei 50 blog più letti della cyber security.

Marco Castaldo, manager cosmopolita, è un investitore professionale in start up tecnologiche e aiuta imprese ed organizzazioni pubbliche e private a gestire i rischi cyber. Ha contribuito a creare alcune eccellenze nel campo della cybersecurity e con Yoroi ha contribuito alla nascita di Tinexta Cyber.

Che cos'è Yoroi

Yoroi è un'azienda italiana certificata di cybersecurity. Il suo nome, dal giapponese, indicava la speciale armatura, leggera e flessibile, che i Samurai indossavano per proteggersi. Come quell'armatura, a Yoroi siamo impegnati a proteggere e monitorare il cyberspazio e il nostro Threat Intelligence and Defense Center è conosciuto in tutto il mondo. In Yoroi studiamo il comportamento dei criminali informatici e progettiamo strategie e strumenti di difesa per proteggere i nostri clienti. Il nostro motto è "Defence belongs to humans". https://yoroi.company

@yoroisecurity
www.linkedin.com/company/yoroi/

Media Advisor
Arturo Di Corinto
(+39) 335 6785259

https://www.yoroi.company
https://blog.yoroi.company/
https://yomi.yoroi.company