haiku
is cyber intelligence

I rischi legati al CYBER e alle fragilità delle infrastrutture IT sono tra i principali che chiunque operi nel mondo del lavoro (…e non solo!) debba considerare e affrontare.

Uno strumento di diagnosi sulle possibili esposizioni legate all'informatizzazione digitale è imprescindibile per un broker, al fine di consigliare efficacemente il proprio Cliente nella pianificazione di un efficace, e quanto mai necessario, risk management.

haiku® è stato costruito sull'assunto imprescindibile di un supporto a tutte le parti in causa, per abbattere quello che è un evidente limite della gran parte degli attori, ossia la "non conoscenza" della materia e dei rischi. Ci sono pochi broker che conoscono concretamente la IT, ci sono pochissimi Clienti che comprendono i rischi cui sono esposti, e ancora meno consulenti informatici e sistemisti che riescono a parlare il linguaggio assicurativo, per poter trasferire l'inevitabile rischio residuo.

haiku® è una web-application ideata e costruita proprio per superare questa impasse e aiutare i broker, nella loro qualità di consulenti prioritari delle imprese e, più in generale, dei titolari di un'infrastruttura IT nella valutazione complessiva e oggettiva delle vulnerabilità presenti.

haiku® è un motore capace di raccogliere e analizzare tutte le informazioni correlate al cyber-risk perimetrale di un dominio. Un'applicazione capace di evolversi autonomamente, grazie a un algoritmo per la stima del livello complessivo di rischio che auto-apprende dalla propria esperienza, sulla base delle tecniche di intelligenza artificiale (machine learning).

haiku® - creato da un team di ethical hacker - analizza le debolezze di un'infrastruttura, valuta le potenziali vulnerabilità in diversi ambiti e restituisce uno score complessivo insieme a specifici commenti e dati.

Il report generato supporta il lavoro del broker, permettendogli di evidenziare al cliente il livello della sua esposizione e permettergli di attivare interventi correttivi e identificare al meglio i parametri necessari per sottoscrivere un'eventuale copertura CYBER.

haiku® ha scelto di esprimere e commentare i dati presenti nell'assessment con una forma espressiva che permette anche ai "non addetti ai lavori" di comprendere facilmente gli output.

L' haiku score® rappresenta la sintesi finale - definita in centesimi - dell'esposizione in nove diversi ambiti che vengono preventivamente analizzati, uno per uno:

1. CREDENTIAL LEAK

Molte "credenziali" di utenti di ogni genere sono state rubate (hackerate) e spesso rivendute nel corso degli ultimi 20 anni ed è possibile ritrovarle - complete di password in chiaro - sul darkweb e sul deepweb (le parti più nascoste e senza controlli della Rete).
Questa esposizione al rischio rappresenta una delle maggiori vulnerabilità delle infrastrutture. È infatti probabile che nonostante l'utente abbia modificato la password lo abbia fatto solo parzialmente (la maggior parte delle persone mantiene nel corso della sua vita una sorta di perniciosa coerenza nelle scelte cambiando solo alcuni caratteri o numeri). Un malintenzionato potrebbe, seguendo un pattern - una sorta di algoritmo che prova e riprova temi e combinazioni simili o collegate a quella trovata – accedere ad esempio alla VPN aziendale e/o alle mail.
Allo stesso modo l'utilizzo di e.mail aziendali per registrarsi a servizi privati (come, ad esempio, siti di streaming), sarebbe da disincentivare.

I TEST EFFETTUATI

Vengono ricercate sul deepweb e in altre fonti tutte le mail appartenenti al dominio mostrando talvolta anche la password in chiaro o crittografata.

2. CERTIFICATES Health

Il protocollo di comunicazione HTTPS serve a garantire o, quantomeno, ad aumentare la sicurezza della comunicazione tra server WEB e l'utente che lo naviga, attraverso un'operazione di cifratura asimmetrica che riduce il rischio di subire attacchi di tipo man in the middle, che si interpongono all'interno delle comunicazioni.

I TEST EFFETTUATI

haiku® controlla i certificati (SSL / TLS) che permettono il funzionamento del protocollo HTTPS per verificare che gli stessi siano aggiornati e/o installati in maniera corretta. Una criticità registrata non solo sul certificato principale ma anche su quelli intermedi potrebbe portare a una fragilità su cui un malintenzionato potrebbe intervenire modificando, impossessandosi o interrompendo la comunicazione (spesso in maniera non percepita dagli utenti dell'organizzazione).

3. DNS Health

DNS è l'acronimo di Domain Name System: si tratta di un componente fondamentale che permette di associare i nomi dei domini ai corrispettivi indirizzi IP.

I TEST EFFETTUATI

haiku® compie test diagnostici per verificare l'efficienza e/o le eventuali configurazioni errate del DNS che potrebbero portare un malintenzionato a ottenere informazioni sensibili e utili a un attacco

4. MAIL Health

I server MAIL gestiscono la posta in arrivo la posta in uscita e l'accesso alla propria casella di posta. consentendo la scambio di mail tra mittenti e destinatari. La sicurezza di tale scambio svolge un ruolo importante, inclusa la gestione di un accesso sicuro.

I TEST EFFETTUATI

Vengono operati diversi test diagnostici per verificare l'efficienza, le eventuali configurazioni errate e la sicurezza dei server dedicati alla posta. Soprattutto per le mail è necessario che la configurazione del server sia fatta secondo quando richiesto dagli standard odierni e che non esistano misconfigurazioni, che permettano a terzi di utilizzare il server per spedire mail come se provenissero dall'azienda stessa, provocando fenomeni come SPAM, PHISHING, BEC o altre tipologie di truffe legate alle e.mail fraudolente
L'evidenza di una criticità non è necessariamente un problema grave ma certamente espone di più il soggetto ai tentativi dei malintenzionati.

5. IP REPUTATION

Si tratta di un parametro molto importante al fine di verificare se l'azienda sia già esposta a rischi concreti, o addirittura – ovviamente a insaputa - ne sia vittima. In rete sono presenti centinaia di database (pubblici e nascosti) che tracciano gli indirizzi IP che siano stati o sono oggetto di eventuali tentativi di frode come lo spam e il phishing o siano fonte di infezione.
Se uno degli indirizzi IP è presente in una blacklist, il rischio che uno o più asset dell'azienda non siano al sicuro o addirittura siano sotto attacco è molto alto e aumentano i rischi connessi che ne derivano.

I TEST EFFETTUATI

Si tratta di una vera e propria interrogazione dei database precedentemente citati al fine di individuare la presenza di uno o più indirizzi IP aziendali compromessi. Queste fonti di dati sono costantemente aggiornate in modo da garantire un risultato il più accurato possibile.

6. ANALISI DELLE VULNERABILITA'

Si tratta dell'analisi probabilmente più importante della valutazione. L'intervento registra e valuta quante e quali siano state le vulnerabilità registrate (anno per anno) sugli indirizzi aziendali.
Sull'asse orizzontale sono rappresentati gli ultimi anni (ovviamente una vulnerabilità più vecchia è probabilmente meno grave in quanto potrebbe essere stata risolta con un aggiornamento), mentre sull'asse verticale è tracciato con una riga arancio il totale delle vulnerabilità registrate nell'anno (il fatto siano reiterate non è chiaramente un buon risultato), mentre la barra blu misura l'intensità del fatto, definita sulla base dello score internazionale Common Vulnerability Scoring System (CVSS) – su base 10 - che prevede un rischio basso da 0.1 a 3.9, medio da 4.0 a 6.9, alto da 7.0 a 8.9 e critico da 9.0 a 10.0. Una valutazione fino a 6.9 è da tenere in considerazione ma non costituisce di per sé stessa un segnale di allarme cosa che invece devono evidenziare punteggi superiori o uguali a 7.0.

I TEST EFFETTUATI

Si tratta di una vera e propria ricerca su tutta la rete per identificare le registrazioni delle vulnerabilità accertate sugli asset aziendali esposti verso internet. haiku® restituisce anche una specifica descrizione della vulnerabilità ed il grado di rischio associato.

7. DISTRIBUZIONE DELLE PORTE APERTE SU IP PUBBLICI

Un grafico illustra le porte di comunicazione aperte verso internet e visibili pubblicamente. Sarebbe raccomandabile che alcune di esse venissero nascoste o aperte solo a determinati indirizzi IP tramite regole IP-Check. Meglio ancora valutare la loro non pubblicazione favorendo l'uso di una VPN (rete privata virtuale) che può garantire maggior sicurezza e privacy sfruttando canali di comunicazioni cifrati.

I TEST EFFETTUATI

haiku® identifica le porte verso l'esterno, ne misura l'esposizione evidenziando quali siano a rischio nella loro attuale configurazione.

8. P2P - FILE SHARING

PER CAPIRE MEGLIO

Il Peer-to-Peer è un protocollo di condivisione file, come ad esempio Torrent, in cui è possibile caricare e scaricare documenti di ogni tipo come film, libri, foto, programmi craccati e altro ancora. Ovviamente questo fatto – se compiuto da un asset aziendale – comporta il rischio di aver introdotto all'interno dell'organizzazione virus e malware o peggio ancora ransomware.

I TEST EFFETTUATI

haiku® identifica il numero di file scaricati suddivisi per tipo, riportando anche esattamente i nomi dei file, il numero di download per ogni categoria, e il momento in cui è stata compiuta l'operazione.

9. IP PUBBLICI DISTRIBUITI PER NAZIONE

Un grafico evidenzia la collocazione "geografica" degli IP pubblici. Si tratta di un'indicazione importante perché ci sono nazioni più esposte di altre relativamente ai Malware e ai Ransomware. Non è un parametro definitivo per valutare la sicurezza di un sistema ma certamente va preso in considerazione nella valutazione della sicurezza di un'infrastruttura.

I TEST EFFETTUATI

haiku® identifica la collocazione geografica e, sulla base di un'analisi costantemente aggiornata sui rischi specifici territoriali, ne restituisce una griglia di possibili criticità. Presenta in un grafico evidenziando la percentuale di uso per ognuna di esse, evidenziandone inoltre il livello di pericolosità in base alla tipologia.

is cyber intelligence

perché la Cyber Security sia comprensibile a tutti