Stai al passo: informati e agisci tempestivamente contro le vulnerabilità.

Nell'attuale scenario digitale in continua evoluzione, le aziende di tutte le dimensioni si trovano costantemente sotto la minaccia di violazioni della sicurezza informatica. Secondo l'Agenzia per la Sicurezza delle Infrastrutture Informatiche (CISA), il 50% delle vulnerabilità note (KEV) vengono sfruttate entro due giorni dalla loro identificazione e il 75% viene sfruttato in meno di un mese. È imperativo avere in atto un programma di gestione delle vulnerabilità per agire rapidamente e intervenire prima che attività maligne entrino e si diffondano in tutta la rete di un'organizzazione.

Chubb Dynamic Vulnerability Detection

Grazie al nostro Programma di Gestione delle Vulnerabilità, il nostro Team di Cyber Intelligence monitora, scansiona e identifica regolarmente le vulnerabilità e le nuove minacce critiche per contribuire a proteggere i nostri assicurati. Gli assicurati che si registrano per ricevere gli avvisi sono informati tramite:

Programma di sensibilizzazione sulle vulnerabilità - una notifica proattiva agli assicurati Cyber se nel loro ambiente vengono individuate vulnerabilità critiche note che hanno un'alta probabilità di essere sfruttate.

- Una comunicazione iniziale via email, che fornisce dettagli sull'esposizione e le azioni necessarie per la risoluzione.
- Successive comunicazioni via email o telefono.

Avvisi Urgenti - sono inviati agli assicurati Cyber quando vengono scoperte nuove vulnerabilità con un'alta probabilità di essere sfruttate e che potrebbero impattare il loro ambiente.

- Una comunicazione via email, con informazioni sulla nuova minaccia, di solito viene inviata entro 24 ore dalla sua scoperta.

Ulteriori Soluzioni di Gestione delle Vulnerabilità Informatiche

Oltre al nostro Programma di Gestione delle Vulnerabilità, tutti gli assicurati della polizza Chubb Cyber possono registrarsi per i seguenti servizi Cyber gratuiti:

- **Monitoraggio Esterno delle Vulnerabilità** - In collaborazione con BitSight, gli assicurati possono monitorare il rischio informatico come misurazione quotidiana delle loro prestazioni di sicurezza tramite una piattaforma che utilizza metriche chiave per evidenziare punti di forza e potenziali debolezze, fornendo una visibilità sulla sicurezza della loro organizzazione.

I titolari di polizze Cyber possono inoltre usufruire delle seguenti soluzioni a costi preferenziali:

- **Difesa preventiva dal ransomware Falcon** - Consente di accedere a un software antivirus di nuova generazione di CrowdStrike. La protezione della rete informatica è garantita dal rilevamento e dal blocco 24/7 di molte minacce o tattiche ransomware che potrebbero essere utilizzate dai nemici. La soluzione CrowdStrike offre funzionalità che vanno oltre il rilevamento di malware o i programmi antivirus tradizionali. Servizio fornito da CrowdStrike.
- **Analisi sensibilizzazione phishing** - Permette di testare i dipendenti per vedere come rispondono ad attacchi di phishing simulati, basati sulle più recenti minacce attive, e successivamente di utilizzare i risultati per adattare il programma di sicurezza informatica o di sensibilizzazione indirizzato agli utenti del cliente. Servizio disponibile in 36 lingue. Fornito da Cofense.

Per registrarti al programma di sensibilizzazione sulle vulnerabilità e per ottenere più informazioni sui Servizi Cyber di Chubb visita il nostro sito: https://www.chubb.com/it-it/servizi-cyber-italia.html

Programma di sensibilizzazione sulle vulnerabilità a cura di Chubb

Domande frequenti sugli avvisi di allerta Red Flags

FAQ generiche

Qual è la finalità del programma di sensibilizzazione sulle vulnerabilità di Chubb?

- Il programma è destinato a comunicare alle organizzazioni un'eventuale esposizione a vulnerabilità ad alto rischio e ad altri gravi errori di configurazione (porte aperte, presenza di malware, ecc.). Chubb ha adottato questo approccio per allertare e assistere i propri assicurati nell'individuazione e nella correzione dei problemi connessi a Internet che il nostro team di Cyber Intelligence ha classificato come esposizioni ad alto rischio. Ciascuna delle vulnerabilità da noi individuate può e sarà identificata come tale anche dagli autori delle minacce. Infatti le vulnerabilità ricercate dalle scansioni effettuate da Chubb hanno un'alta probabilità di essere sfruttate all'esterno.

Perché Chubb mi segnala le vulnerabilità del mio ambiente operativo?

- Questa è una componente importante dello stretto rapporto esistente tra Chubb e gli assicurati. Da oltre cento anni, forniamo servizi di risk engineering ai nostri assicurati in tutto il mondo, consentendo agli stessi assicurati di gestire meglio il rischio e a Chubb di essere migliore in ambito sottoscrittivo. Lo stesso vale per la cybersicurezza. Nel momento in cui individuiamo vulnerabilità che causano perdite e/o sono presenti negli elenchi di Cyber Intelligence ad alto rischio, visibili negli ambienti dei nostri assicurati, la riduzione dell'esposizione a tali vulnerabilità diventa una priorità.

Questi avvisi influiscono sulla copertura?

- No. Tuttavia, la riluttanza ad agire per porre rimedio a queste vulnerabilità prioritarie potrebbe avere un impatto sulla sottoscrizione della polizza in futuro. Ad esempio, se verifichiamo costantemente la presenza di queste vulnerabilità e non registriamo alcuna risposta o azione da parte di un contraente, potremmo considerare di non rinnovare la copertura.

Si tratta di un test di penetrazione?

- Questo non è un test di penetrazione. Non sono previste scansioni attive né tentativi di infiltrarsi nel tuo ambiente. Questo processo utilizza piattaforme di scansione passiva esterne che operano attraverso una combinazione di intelligenza open-source (OSINT) e scansione passiva. La scansione passiva è una metodologia non intrusiva e sicura per individuare gli asset esposti a Internet e le potenziali vulnerabilità o configurazioni errate ad essi associate.

FAQ sugli avvisi di allerta Red Flag

Perché ricevo questi avvisi?

- Ricevi questi avvisi perché sei iscritto al Programma di sensibilizzazione sulle vulnerabilità di Chubb, disponibile per i nostri assicurati come servizio aggiuntivo alla Polizza Cyber. Esso fa riferimento a una vulnerabilità nota sfruttata (KEV) o a qualsiasi altro grave problema di sicurezza informatica rilevato tramite strumenti di scansione esterni non intrusivi come BitSight e Security Scorecard. L'avviso include informazioni che i team IT degli assicurati potranno utilizzare per identificare e correggere l'asset esposto.

Che cosa succede se non capisco questi avvisi?

- Il team di Cyber Intelligence di Chubb sarà lieto di chiarire questa procedura e i dettagli dell'avviso con qualsiasi interlocutore della tua organizzazione. Potrai anche inoltrare l'avviso al tuo specialista interno per la sicurezza informatica o a un MSP terzo che supervisiona l'ambiente della tua azienda, per qualsiasi chiarimento e/o approfondimento.

Non so di cosa si tratti o cosa fare al riguardo. Potete aiutarmi?

- Sì, è possibile ricevere una chiamata di supporto generale dal team di consulenza sui rischi Cyber di Chubb inoltrando una richiesta all'indirizzo Cyber@chubb.com
- Si prega di aggiungere un commento in cui si precisa di avere ricevuto un avviso di vulnerabilità e di volerne discutere.

Questo non è il mio indirizzo IP. Devo fare qualcosa?

- Si prega di inoltrare l'avviso all'indirizzo Cyber@Chubb.com indicando gli indirizzi IP specifici attribuiti erroneamente e aggiorneremo i nostri registri, segnalando che si riferiscono a un asset non assicurato. Se di interesse, il team di consulenza sui rischi Cyber di Chubb può fornire le istruzioni al tuo team IT per inviare una richiesta relativa ai risultati ottenuti tramite Bitsight o Security Scorecard, in modo da prevenire futuri avvisi automatici relativi a IP attribuiti erroneamente.

Questo non è il mio dominio.

- Ti preghiamo di inviare un'e-mail all'indirizzo Cyber@Chubb.com con la conferma del dominio corretto e Chubb si assicurerà che la tua polizza sia aggiornata con tale dominio. Aggiorneremo quindi i nostri dati per segnalare che la vulnerabilità riguarda un asset non assicurato e chiuderemo il relativo caso.

Tutti i servizi cyber sono suscettibili di modifiche. Eventuali modifiche all'offerta di servizi verranno riportate sul modulo web locale dei servizi cibernetici. I titolari delle polizze sono responsabili della revisione delle specifiche condizioni di ciascun fornitore di servizi cyber per garantire l'ammissibilità e restare aggiornati su eventuali modifiche che potrebbero verificarsi.

SERVIZI CYBER A PREZZO SCONTATO OFFERTI DA FORNITORI TERZI:
Monitoraggio delle vulnerabilità esterne. Gestore di password sicura

I servizi cyber sopra descritti sono offerti da fornitori terzi senza alcun costo aggiuntivo per i titolari di polizze Chubb per il periodo iniziale indicato, a condizione che il titolare di polizza sia un nuovo abbonato/cliente dei servizi cibernetici offerti dal fornitore terzo scelto e che il titolare di polizza soddisfi le specifiche condizioni di ammissibilità. Dopo la scadenza del periodo iniziale indicato, i titolari di polizze potrebbero avere l'opzione di continuare i servizi cyber a un costo scontato al momento del rinnovo. Si tenga presente che lo sconto può variare tra specifici prodotti e servizi. Gli sconti su prodotti e servizi offerti da fornitori di servizi cyber sono disponibili solo per i titolari di polizze Chubb con polizze in vigore e sono soggetti alle leggi assicurative applicabili. I prodotti e servizi forniti dai fornitori terzi saranno disciplinati dai termini contrattuali che il titolare di polizza stipulerà con il fornitore terzo. Chubb non sarà coinvolta nella decisione del titolare di polizza di acquistare servizi e non ha responsabilità per i prodotti o servizi forniti da qualsiasi fornitore terzo.

Il presente documento è reso noto unicamente a fini informativi e non costituisce alcun tipo di consulenza o raccomandazione per individui o aziende relative ad alcun prodotto o servizio. Per maggiori dettagli sui termini e le caratteristiche del prodotto si prega pertanto di fare riferimento alle condizioni generali di assicurazione.

Chubb European Group SE, Sede legale: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francia - Capitale sociale €896.176.662 i.v.- Rappresentanza generale per l'Italia: Via Fabio Filzi n. 29 - 20124 Milano - Tel. 02 27095.1 - Fax 02 27095.333 – P.I. e C.F. 04124720964 – R.E.A. n. 1728396 – Abilitata ad operare in Italia in regime di stabilimento con numero di iscrizione all'albo IVASS I.00156. L'attività in Italia è regolamentata dall'IVASS, con regimi normativi che potrebbero discostarsi da quelli francesi. Autorizzata con numero di registrazione 450 327 374 RCS Nanterre dall'Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 RCS e soggetta alle norme del Codice delle Assicurazioni francese. info.italy@chubb.com - italy@pec.chubb.com - www.chubb.com/it

Trattiamo i dati personali da Lei forniti o raccolti tramite soggetti da noi autorizzati, come per esempio gli intermediari assicurativi, per le finalità connesse alla sottoscrizione e gestione delle polizze nonché per la valutazione di eventuali richieste di indennizzo derivanti dal verificarsi di un sinistro. L' Informativa completa sul trattamento dei dati personali è disponibile sul nostro sito internet www.chubb.com/it-it/footer/privacy-statement.html