4. Sicurezza e contromisure

Durante una sessione OSINT, l'anonimato e la sicurezza sono aspetti fondamentali da considerare. La protezione della propria identità è essenziale per evitare di esporre dati personali o di compromettere l'indagine.

La profilazione è un rischio concreto, poiché esistono numerosi strumenti per raccogliere informazioni su un utente o un sistema. Siti come Panopticlick possono dimostrare quanto sia facile identificare un utente attraverso caratteristiche uniche del browser, dei plugin installati o della configurazione del sistema. Anche il traffico generato durante un'attività OSINT, se abbondante o anomalo, può attirare l'attenzione, risultando sospetto o soggetto ad analisi. Inoltre, bisogna fare attenzione a non rivelare inavvertitamente dati personali, come attraverso post o messaggi non valutati con attenzione.

Per evitare di lasciare trapelare la propria identità, è necessario prestare attenzione a dettagli apparentemente banali. Collegarsi da una rete WiFi pubblica senza adeguata protezione, inviare email senza crittografia o dimenticare di attivare una VPN sono errori comuni ma potenzialmente gravi. In ambienti ostili, l'analisi del traffico, la perdita o il sequestro dell'hardware possono compromettere seriamente l'anonimato. Anche il malware e la persistenza dello storico delle ricerche effettuate rappresentano rischi da non sottovalutare.

Proteggere la propria identità richiede due livelli di sicurezza: quello fisico, legato all'indirizzo IP, e quello logico, che riguarda i dati personali reali. Qualsiasi elemento utilizzato durante un'attività OSINT, come indirizzi email, foto, sistema operativo, lingua, timezone, browser e add-on, può rivelare dettagli sull'identità dell'utente. Anche i cookie e i contatti sui social network possono contribuire a identificare un soggetto.

L'uso di strumenti per mascherare l'indirizzo IP, come VPN, proxy o TOR, è indispensabile per nascondere la posizione e mantenere l'anonimato. Tuttavia, è importante non commettere errori come acquistare una VPN con la propria carta di credito personale, che potrebbe rivelare informazioni identificative. Questo aspetto diventa ancora più cruciale se si utilizza un fake profile, poiché ogni traccia può comprometterne la credibilità e l'efficacia. L'attenzione ai dettagli e l'uso di strumenti adeguati sono quindi imprescindibili per garantire una sessione OSINT sicura e anonima.

Virtual Machines

L'uso di macchine virtuali dedicate rappresenta una misura importante per garantire un livello aggiuntivo di sicurezza durante le attività OSINT. Le macchine virtuali consentono di creare un ambiente isolato dal sistema principale, riducendo i rischi associati all'esposizione di dati personali o di configurazioni del proprio dispositivo.

Separare le attività di ricerca da quelle di analisi è fondamentale. La ricerca può avvenire su una macchina virtuale configurata appositamente, mentre l'analisi dei dati raccolti può essere effettuata in un ambiente separato, garantendo una maggiore sicurezza e protezione. Tra i software di virtualizzazione gratuiti disponibili ci sono VMware Player e VirtualBox, che offrono strumenti robusti per configurare e gestire ambienti virtualizzati.

Oltre alle macchine virtuali, ci sono altre soluzioni per migliorare la sicurezza e l'anonimato. L'utilizzo di web proxy gratuiti, come hidemyass o soluzioni analoghe, permette di nascondere il proprio indirizzo IP e di accedere a risorse online senza rivelare la propria posizione. È utile mantenere una lista aggiornata di proxy provenienti da diversi paesi per garantire flessibilità e ridondanza.

L'adozione di un sistema operativo GNU/Linux live, come Tails, offre un'opzione eccellente per proteggere la privacy. Tails è progettato per non lasciare tracce sul dispositivo utilizzato e per garantire la crittografia delle comunicazioni. Inoltre, una VPN affidabile è essenziale per nascondere l'indirizzo IP e garantire un canale di comunicazione sicuro. È importante scegliere un provider serio che offra una politica rigorosa di no-log.

Il browser TOR, basato su The Onion Router, rappresenta un'altra soluzione efficace per garantire l'anonimato online. TOR instrada il traffico attraverso una rete di nodi volontari, rendendo difficile il tracciamento dell'attività e della posizione dell'utente.

Combinare queste misure, come l'uso di macchine virtuali, web proxy, sistemi operativi live, VPN e TOR, contribuisce a creare un ambiente sicuro e protetto per le attività di investigazione online, riducendo al minimo i rischi di esposizione e mantenendo l'anonimato.

Proteggere la propria azienda

Proteggere la propria azienda richiede un approccio strutturato che integri formazione, policy, strumenti di prevenzione e un'analisi continua delle informazioni condivise. La formazione di dipendenti e dirigenti è essenziale per garantire un utilizzo consapevole e sicuro di strumenti come computer, dispositivi mobili, email e social network. Questo passaggio deve essere affiancato dalla definizione e dall'applicazione di policy aziendali e best practice, che includano linee guida chiare su cosa condividere e come farlo in modo sicuro.

Un ulteriore elemento chiave è la verifica periodica del grado di consapevolezza degli utenti. Attraverso simulazioni, test o audit interni, è possibile identificare lacune nella conoscenza e intervenire con ulteriore formazione. Gli strumenti di prevenzione giocano un ruolo fondamentale, permettendo di bloccare l'accesso a siti o servizi pericolosi e di analizzare e filtrare i contenuti in entrata e in uscita.

Un altro aspetto importante è l'analisi delle informazioni rilasciate dall'organizzazione. È necessario verificare quali dati sono stati resi pubblici, valutando e sanitizzando i documenti pubblicati o da pubblicare per evitare di divulgare informazioni sensibili. Questo processo

deve essere esteso anche alle informazioni disponibili pubblicamente su altre fonti riguardanti l'organizzazione, i suoi membri o le sue attività.

Un approccio proattivo che combina formazione, policy, strumenti tecnologici e analisi delle informazioni è essenziale per proteggere la propria azienda da rischi legati a fughe di dati, attacchi informatici o uso improprio delle informazioni.

Strumenti utili

Per rimanere anonimi e sotto il radar durante le attività online, ci sono servizi utili per la creazione di account temporanei o anonimi, come email usa e getta o numeri di telefono virtuali. Questi includono:

- **BugMeNot**: fornisce accessi condivisi a siti web.
- **GuerrillaMail**, **Mailinator**, **10MinuteMail**, e **GetAirMail**: offrono email temporanee per registrazioni anonime.
- **Receive-SMS-Online** e **Pinger**: permettono di ricevere SMS online senza rivelare il proprio numero di telefono.

L'uso combinato di questi strumenti può migliorare l'efficacia delle indagini OSINT, garantendo al contempo anonimato e sicurezza.