Dominika Cybulska

Biały wywiad (OSINT) jako narzędzie w cyberprzestępczości i cyberbezpieczeństwie

Rozwój technologii informacyjno-komunikacyjnych oraz postępująca cyfryzacja życia społecznego sprawiły, że informacje stały się jednym z najcenniejszych zasobów współczesnego świata. Każdego dnia użytkownicy Internetu publikują ogromne ilości danych dotyczących swojego życia prywatnego i zawodowego, często nie zdając sobie sprawy z konsekwencji wynikających z ich powszechnej dostępności. Dane te pochodzą nie tylko z mediów społecznościowych, lecz także z rejestrów publicznych, stron internetowych przedsiębiorstw, dokumentów udostępnianych online czy baz danych tworzonych przez instytucje państwowe i organizacje komercyjne. Powszechna dostępność informacji stworzyła nowe możliwości zarówno dla specjalistów zajmujących się cyberbezpieczeństwem, jak i dla cyberprzestępców. Jednym z najważniejszych narzędzi wykorzystywanych do pozyskiwania oraz analizy informacji z ogólnodostępnych źródeł jest Open Source Intelligence (OSINT), określany w języku polskim mianem białego wywiadu.

Znaczenie OSINT systematycznie wzrasta wraz z rozwojem Internetu oraz zwiększającą się ilością danych pozostawianych przez użytkowników w przestrzeni cyfrowej. Informacje, które pojedynczo wydają się nieistotne, po odpowiednim zestawieniu mogą stworzyć szczegółowy obraz osoby, przedsiębiorstwa lub instytucji. Z tego względu biały wywiad stanowi obecnie jedno z podstawowych narzędzi wykorzystywanych zarówno podczas analiz bezpieczeństwa, jak i przygotowywania cyberataków. Celem niniejszego artykułu jest przedstawienie istoty OSINT oraz omówienie jego znaczenia w kontekście współczesnej cyberprzestępczości i cyberbezpieczeństwa.

Istota białego wywiadu

Pojęcie Open Source Intelligence odnosi się do procesu systematycznego pozyskiwania, selekcjonowania, weryfikowania oraz analizowania informacji pochodzących z publicznie dostępnych źródeł. W odróżnieniu od działań polegających na nieuprawnionym dostępie do systemów teleinformatycznych, OSINT opiera się wyłącznie na legalnie dostępnych danych, których pozyskanie nie wymaga przełamywania zabezpieczeń ani stosowania metod charakterystycznych dla cyberprzestępczości. O wartości białego wywiadu nie decyduje jednak samo odnalezienie informacji, lecz umiejętność ich odpowiedniego zestawienia i interpretacji. W praktyce nawet pozornie niepowiązane dane mogą po przeprowadzeniu analizy ujawnić

informacje o strukturze organizacyjnej przedsiębiorstwa, wykorzystywanych technologiach, relacjach biznesowych czy codziennych aktywnościach określonych osób.

Źródła wykorzystywane podczas analiz OSINT są niezwykle zróżnicowane. Obejmują one między innymi media społecznościowe, strony internetowe przedsiębiorstw, publiczne rejestry państwowe, wyszukiwarki internetowe, fora dyskusyjne, dokumenty zawierające metadane, informacje o domenach internetowych, publicznie dostępne bazy wycieków danych oraz repozytoria kodu źródłowego. Rozwój technologii cyfrowych sprawił, że liczba dostępnych źródeł stale rośnie, co z jednej strony zwiększa możliwości analityczne, z drugiej natomiast znacząco utrudnia selekcję informacji oraz ocenę ich wiarygodności.

OSINT jako narzędzie cyberprzestępczości

We współczesnej cyberprzestępczości etap rozpoznania celu odgrywa kluczową rolę w przygotowaniu skutecznego ataku. Zanim cyberprzestępcy podejmą próbę przełamania zabezpieczeń technicznych, dążą do zgromadzenia możliwie największej ilości informacji dotyczących potencjalnej ofiary. W tym celu wykorzystują właśnie techniki OSINT, które pozwalają na poznanie struktury organizacyjnej przedsiębiorstwa, danych kontaktowych pracowników, wykorzystywanego oprogramowania, partnerów biznesowych czy informacji ujawnionych podczas wcześniejszych incydentów bezpieczeństwa.

Pozyskane informacje są następnie wykorzystywane do przygotowania ataków socjotechnicznych, których skuteczność zależy przede wszystkim od wiarygodności przekazu. Szczególnym zagrożeniem są ataki typu spear phishing, polegające na wysyłaniu starannie przygotowanych wiadomości elektronicznych do konkretnych osób. Przestępca, dysponując wiedzą na temat stanowiska pracownika, realizowanych projektów czy relacji służbowych, jest w stanie stworzyć wiadomość niemal nieodróżnialną od autentycznej korespondencji. W rezultacie ofiara znacznie częściej otwiera złośliwy załącznik lub korzysta z przesłanego odnośnika, co prowadzi do przejęcia danych uwierzytelniających lub zainfekowania systemu informatycznego.

Warto zauważyć, że skuteczność tego rodzaju działań wynika przede wszystkim z wykorzystania informacji dobrowolnie udostępnionych przez użytkowników. Publikowanie zdjęć z miejsca pracy, informacji o pełnionych funkcjach czy danych kontaktowych może wydawać się niegroźne, jednak w połączeniu z innymi publicznie dostępnymi informacjami tworzy wartościowy materiał analityczny dla osób planujących cyberatak.

Przykład wykorzystania OSINT w ataku typu spear phishing

Jednym z najbardziej charakterystycznych przykładów wykorzystania metod OSINT w cyberprzestępczości są ataki typu spear phishing, których skuteczność opiera się na wcześniejszym rozpoznaniu ofiary. Cyberprzestępcy często rozpoczynają działania od analizy publicznie dostępnych informacji zamieszczonych w serwisach społecznościowych oraz na stronach internetowych przedsiębiorstw. Na podstawie takich danych możliwe jest ustalenie struktury organizacyjnej firmy, zakresu obowiązków poszczególnych pracowników, wykorzystywanych technologii, a także relacji służbowych pomiędzy zatrudnionymi osobami. Przykładowo, pracownik działu finansowego publikuje w serwisie LinkedIn informację o rozpoczęciu pracy w nowej organizacji oraz uczestnictwie w projekcie związanym z wdrożeniem nowego systemu finansowo-księgowego. Równocześnie na stronie internetowej przedsiębiorstwa pojawia się komunikat dotyczący współpracy z nowym dostawcą usług informatycznych. Dla osoby postronnej informacje te mogą wydawać się nieistotne, jednak po ich zestawieniu tworzą spójny obraz działalności organizacji.

Cyberprzestępca, wykorzystując zgromadzone dane, przygotowuje wiadomość elektroniczną podszywającą się pod przedstawiciela firmy wdrażającej nowe oprogramowanie. W treści wiadomości odwołuje się do rzeczywiście realizowanego projektu oraz używa nazwisk pracowników odpowiedzialnych za jego koordynację. Wiadomość zawiera odnośnik prowadzący do fałszywej strony logowania lub złośliwy załącznik. Ze względu na zgodność treści z aktualną sytuacją przedsiębiorstwa prawdopodobieństwo, że odbiorca uzna wiadomość za autentyczną, znacząco wzrasta.

Przedstawiony przykład pokazuje, że skuteczność ataku nie wynika z przełamania zabezpieczeń technicznych, lecz z umiejętnego wykorzystania informacji dobrowolnie udostępnionych przez użytkowników. Właśnie dlatego ograniczenie ilości publicznie dostępnych danych oraz prowadzenie regularnych analiz OSINT stanowią istotny element strategii cyberbezpieczeństwa współczesnych organizacji.

Znaczenie OSINT w cyberbezpieczeństwie

Paradoksalnie te same metody wykorzystywane przez cyberprzestępców stanowią jedno z podstawowych narzędzi specjalistów odpowiedzialnych za bezpieczeństwo informacji. Organizacje coraz częściej prowadzą regularne analizy OSINT w celu identyfikacji własnych podatności wynikających z nadmiernego ujawniania informacji w Internecie. Pozwala to na wykrywanie wycieków danych, monitorowanie pojawiania się firmowych adresów poczty elektronicznej w publicznych bazach, identyfikowanie fałszywych stron internetowych

podszywających się pod przedsiębiorstwo oraz ocenę poziomu ekspozycji organizacji na potencjalne zagrożenia.

Biały wywiad znajduje również zastosowanie podczas testów penetracyjnych oraz analiz Threat Intelligence, których celem jest identyfikacja nowych zagrożeń i monitorowanie aktywności grup cyberprzestępczych. Coraz częściej informacje pozyskane metodami OSINT integrowane są z nowoczesnymi systemami monitorowania bezpieczeństwa, umożliwiając szybsze wykrywanie incydentów oraz skuteczniejsze reagowanie na pojawiające się zagrożenia. Można zatem stwierdzić, że skuteczna ochrona organizacji wymaga obecnie spojrzenia
na bezpieczeństwo z perspektywy potencjalnego napastnika i przewidywania sposobów wykorzystania publicznie dostępnych informacji.

Znaczenie białego wywiadu w obszarze cyberbezpieczeństwa systematycznie wzrasta wraz z rozwojem społeczeństwa informacyjnego. Powszechna dostępność danych sprawia, że informacje publikowane w Internecie stają się cennym zasobem wykorzystywanym zarówno do ochrony systemów teleinformatycznych, jak i do przygotowywania cyberataków. OSINT jest przykładem narzędzia, którego wartość zależy przede wszystkim od celu jego wykorzystania. Dla specjalistów ds. cyberbezpieczeństwa stanowi skuteczną metodę identyfikowania zagrożeń, monitorowania wycieków danych oraz wzmacniania odporności organizacji na ataki. Dla cyberprzestępców jest natomiast źródłem informacji umożliwiającym prowadzenie skutecznych działań socjotechnicznych i zwiększanie efektywności prowadzonych kampanii.

Współczesne bezpieczeństwo informacji nie może ograniczać się wyłącznie do stosowania zaawansowanych zabezpieczeń technicznych. Równie istotne staje się świadome zarządzanie informacjami udostępnianymi w przestrzeni cyfrowej oraz budowanie świadomości użytkowników dotyczącej konsekwencji pozostawiania cyfrowych śladów. W świecie, w którym informacje są jednym z najcenniejszych zasobów, umiejętność prowadzenia analiz OSINT staje się nieodzownym elementem skutecznej ochrony przed zagrożeniami cyberprzestrzeni.