fundacja instytut
CYBERBEZPIECZEŃSTWA

Darknet:
ciemna strona internetu

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Źródło: Flickr

W obecnych czasach, gdy ludzie coraz więcej czasu spędzają w przestrzeni wirtualnej, istnieje obszar internetu, który pozostaje ukryty przed większością użytkowników, owiany tajemnicą i potencjalnie niebezpieczny. Mowa tu o Darknecie, czyli „fragmencie" internetu głęboko skrytym pod powierzchnią globalnej sieci. Darknet wzbudza mieszane uczucia, wywołuje zarówno fascynację, jak i obawy. Ale czym dokładnie jest ten enigmatyczny „świat" i jakie zagrożenia niesie za sobą?

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

Czym jest Darknet?

Darknet, nazywany także Dark Web, to ukryta część internetu, do której dostęp jest praktycznie nieosiągalny dla przeciętnego użytkownika, co wynika ze specyficznego sposobu wejścia do niej. W przeciwieństwie do standardowych przeglądarek, takich jak Google Chrome czy Mozilla Firefox, Darknet wymaga specjalnych narzędzi, jak np. oprogramowanie TOR (The Onion Router). TOR umożliwia użytkownikom korzystanie z internetu w sposób anonimowy oraz chroni ich prywatność poprzez ukrywanie ścieżki ich połączenia. To rodzaj sieci, która kieruje ruchem internetowym przez szereg serwerów proxy na całym świecie, co utrudnia śledzenie, skąd pochodzą dane lub dokąd zmierzają. Nazwa The Onion Router (Cebulowy Router) odnosi się do sposobu działania sieci, w której dane są przesyłane przez kilka pośrednich węzłów (tzw. węzłów routingu), tworząc warstwową strukturę podobną do warstw cebuli.

Charakterystyczną cechą Darknetu są strony internetowe z końcówką „.onion" – specjalne domeny niewidoczne dla standardowych wyszukiwarek. Dzięki temu rozwiązaniu pozostają one ukryte dla większości użytkowników internetu. Darknet oferuje różnorodne treści, od legalnych i anonimowych forów dyskusyjnych po nielegalne rynki handlowe i miejsca, gdzie wymienia się poufne informacje.

Darknet to miejsce, gdzie można natrafić na przestępczość internetową, handel narkotykami, bronią oraz kradzież danych. Świadczone są tam także usługi hakerskie, w ramach których oferuje się ataki, kradzież tożsamości i dostęp do wrażliwych informacji, m.in. w celach szpiegostwa przemysłowego lub dla uzyskania kompromitujących danych. Zidentyfikowano również przypadki, w których grupy terrorystyczne wykorzystują Darknet do planowania zamachów, propagandy oraz wymiany informacji. Przykładem może być działalność grupy ISIS, która używała Darknetu do komunikacji i szerzenia swojej ideologii.

Nielegalne aktywności w Darknecie

Jak zostało wskazane, Darknet to swoista „bezpieczna przystań" dla wielu przestępców i ich nielegalnych źródeł zarobku. To miejsce, gdzie cyberprzestrzeń staje się areną dla najbardziej niebezpiecznych działań, a anonimowość niesie wymierne korzyści. Identyfikuje się wiele różnych aktywności, które są niemoralne bądź po prostu sprzeczne z prawem, a cieszą się dużą popularnością w otchłani Darknetu. My pochylimy się nad ich trzema najpopularniejszymi rodzajami.

Pierwszym z nich jest handel narkotykami – na zakazanych rynkach internetowych znaleźć można szeroki asortyment substancji odurzających, których posiadanie i dystrybucja jest w Polsce surowo zabroniona. Silk Road – popularna witryna aukcyjna w sieci TOR, mimo że upadła w 2013 r., wciąż stanowi swoisty symbol tego zjawiska i rzuca cień na całą przestrzeń Darknetu.

Drugim są praktyki związane z hackingiem i szeroko pojętą cyberprzestępczością. W Darknecie można wynająć hakerów do przeprowadzenia ataków, kradzieży tożsamości czy innych działań przestępczych, które zagrażają stabilności w sieci i bezpieczeństwu użytkowników internetu.

Trzeci rodzaj to handel bronią i kradzionymi danymi – na rynkach Darknetu oferowane są broń, dane osobowe, karty kredytowe i inne przedmioty, których obieg w przestrzeni internetowej stanowi zagrożenie dla bezpieczeństwa. Poza wspomnianymi, w odmętach Darknetu można znaleźć również oferty wynajęcia płatnego mordercy czy wyjątkowo brutalne nagrania wideo.

Pomimo niekwestionowanej szkodliwości większości treści znajdujących się w Darknecie nie wszystko, co można tam znaleźć, jest nielegalne lub szkodliwe. Funkcjonują tam również strony promujące wolność słowa, bezpieczną komunikację oraz działania na rzecz prywatności. Są to np. serwisy udostępniające informacje na temat ochrony prywatności, kryptografii oraz działalności obrońców praw człowieka w reżimach autorytarnych, gdzie internetowa wolność słowa jest skutecznie ograniczana przez służby prewencyjne.

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Legalne aspekty Darknetu

Przestrzeń Darknetu jest czymś w rodzaju inkubatora dla różnorodnych wartościowych celów, często sprzecznych z dominującymi trendami w tradycyjnej przestrzeni internetowej, co potęguje jego rolę niekonwencjonalnej strefy kreatywności i eksperymentowania w dziedzinie wolności, prywatności oraz edukacji. Eksperymenty często bywają nieudane ze względu na testowanie wielu rozwiązań – o różnym poziomie dojrzałości i zazwyczaj dopiero któraś z kolei próba kończy się sukcesem. Tak też bywa w ramach formowania się społeczności w internecie, niemniej możemy wskazać na kilka pozytywnych efektów funkcjonowania Darknetu.

Pierwsze zagadnienie zasługujące na uwagę to zapewnienie wolności słowa i prywatności. Darknet jest domem dla stron internetowych, takich jak platforma SecureDrop, które służą anonimowemu przesyłaniu informacji dziennikarzom. Poprzez zapewnienie bezpiecznej przestrzeni dla źródeł te struktury stanowią integralną część działań na rzecz obrony wolności słowa oraz zapewnienia ochrony przed potencjalnymi represjami. Platforma daje nam możliwość usłyszenia głosów ludzi, którzy za każdy przejaw nieposłuszeństwa względem władzy mogą utracić wiele – czasem nawet własne życie.

Kolejnym istotnym aspektem jest rozwój edukacyjny i osobisty. W niektórych zakątkach Darknetu istnieją fora dyskusyjne oraz strony edukacyjne, które pełnią funkcję platform do nauki i wymiany wiedzy z zakresu programowania, kryptografii czy bezpieczeństwa. Te zasoby edukacyjne wspierają rozwój umiejętności, innowacji i swobodę myśli.

Trzecim ważnym zagadnieniem są sieci społecznościowe, które funkcjonują zgodnie z założeniem, że ochrona prywatności i anonimowości to podstawa wymiany informacji w internecie. Darknet stanowi przestrzeń, w której ludzie mogą swobodnie dzielić się przemyśleniami i doświadczeniami, nie obawiając się cenzury czy śledzenia. Te społeczności stwarzają unikalne środowisko dla interakcji online, gdzie swoboda wypowiedzi współistnieje z ochroną tożsamości osobistej. Niemniej warto pamiętać, że wolność słowa może dla niektórych oznaczać przyzwolenie na szykany, rasizm czy ksenofobię.

Należy zauważyć, że Darknet nie jest jednolitą całością. Składa się z różnych warstw, z których jedna może być stosunkowo bezpieczna, a druga wręcz przeciwnie. Tak jak rozwija się technologia, tak też ewoluuje Darknet, dostosowując się do nowych wyzwań i metod ochrony prywatności. Pamiętajmy przy tym, że ochrona prywatności to często pozytywny aspekt rozwoju technologicznego, pełna anonimowość natomiast może być skrajnie niebezpieczna.

Różnorodność korzyści i zagrożeń – jak chronić się przed Darknetem

Warto zdawać sobie sprawę z różnorodności Darknetu, od pozytywnych aspektów wspierających wolność słowa i prywatność po niebezpieczeństwa związane z przestępczością. To miejsce, gdzie granica między etycznym a nieetycznym rozmywa się, dlatego użytkownicy muszą być świadomi ryzyka związanego z eksploracją tego obszaru.

W zmiennym krajobrazie Darknetu trzeba zachować zdrowy rozsądek i ostrożność. Bardzo ważne jest nie tylko zrozumienie tego, co kryje się w głębinach internetu, lecz także kształtowanie odpowiedzialnych nawyków online. Aby chronić się przed potencjalnymi zagrożeniami związanych z obecnością Darknetu, należy podjąć kilka kluczowych działań w celu zwiększenia bezpieczeństwa w przestrzeni wirtualnej.

Pierwszym i jednocześnie najistotniejszym krokiem jest poszerzenie wiedzy i świadomości na temat typowych strategii stosowanych przez cyberprzestępców oraz zrozumienie ryzyka związanego z niebezpiecznymi zachowaniami online – takimi jak włączenie się do „społeczności" Darknetu. Edukacja na temat sposobów ochrony siebie w sieci oraz świadomość na temat potencjalnych zagrożeń są kluczowe dla bezpiecznego użytkowania internetu. Rekomenduje się śledzenie publikacji i raportów fundacji oraz instytucji zajmujących się cyberbezpieczeństwem, aby pozostać na bieżąco z najnowszymi doniesieniami w dziedzinie cyberprzestępczości.

Kolejne istotne rozwiązanie to stosowanie bezpiecznych praktyk związanych z hasłami i kontami online. Należy regularnie zmieniać hasła i korzystać z unikalnych, niełatwych do odgadnięcia kombinacji znaków, co znacznie utrudnia próby nieupoważnionego dostępu do kont. Dodatkową warstwę ochrony przed atakami cyberprzestępców stanowią aktualizacja oprogramowania oraz stosowanie aktualnych wersji programów zabezpieczających.

Następnym krokiem jest ograniczenie udostępniania informacji osobistych w sieci. Należy zachować ostrożność w udostępnianiu danych osobowych, unikając publikacji wrażliwych informacji na publicznie dostępnych platformach. To znacznie ogranicza ryzyko kradzieży tożsamości i innych form cyberprzestępczości, a także całkiem realnych włamań do naszych mieszkań i domów.

Podczas przeglądania internetu należy zachować czujność i unikać klikania w podejrzane linki lub otwierania nieznanych załączników w wiadomościach e-mail. Ten prosty, ale skuteczny krok może zapobiec infekcji

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

komputera złośliwym oprogramowaniem lub kradzieży danych, które następnie – w sposób niemożliwy do namierzenia – będą sprzedawane np. na aukcjach w Darknecie.

Ważne jest również korzystanie z narzędzi bezpieczeństwa online, takich jak oprogramowanie antywirusowe, firewalle czy programy do ochrony prywatności. Należy przy tym pamiętać, aby wszelkie programy na naszych komputerach i telefonach były na bieżąco aktualizowane – niezależnie od ich przeznaczenia.

Wreszcie, korzystanie z wirtualnych sieci prywatnych (VPN) może zwiększyć prywatność i bezpieczeństwo podczas przeglądania internetu poprzez szyfrowanie połączenia i ukrywanie adresu IP. Dzięki temu zostaje zminimalizowane ryzyko ataków i naruszeń prywatności online.

Podsumowując, Darknet to miejsce, które wzbudza zarówno ciekawość, jak i obawy. Można w nim znaleźć wartościowe informacje, może jednak nieść za sobą również wiele zagrożeń. Istnienie Darknetu pokazuje, że internet może być podzielony na publicznie dostępne obszary oraz te ukryte, wymagające specjalnych narzędzi, a ponadto niezwykłej ostrożności. Warto być świadomym istnienia Darknetu, ale jednocześnie pamiętać o konieczności bezpiecznego korzystania z internetu, co wymaga odpowiedzialności i rozwagi.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

fundacja instytut
CYBERBEZPIECZEŃSTWA