

Czym jest darknet i jak trafiają tam nasze dane?

Darknet to ukryta część Internetu. Można się tam dostać jedynie za pomocą specjalnych przeglądarek, takich jak Tor. Choć ma legalne zastosowania, często jest wykorzystywany do działalności przestępczej, m.in. do handlu skradzionymi danymi. W przeciwieństwie do „zwykłego” Internetu, strony w darknecie nie są indeksowane przez standardowe wyszukiwarki, co sprawia, że działalność w nim jest trudniejsza do wykrycia i monitorowania.



Wyciek danych to sytuacja, w której nasze poufne informacje - np. loginy, hasła, numery kart kredytowych, dane osobowe, dane wrażliwe - trafiają do niepowołanych osób. Może to być wynikiem ataku hakerskiego, złośliwego oprogramowania lub niewłaściwego przechowywania danych. W darknecie takie dane mogą być sprzedawane na forach lub aukcjach, gdzie kupują je przestępcy z różnych części świata.

Jak cyberprzestępcy wykorzystują wykradzione dane?

Jeśli Twoje dane trafią do darknetu, mogą zostać wykorzystane w różny sposób:

- **Wyłudzenie kredytu lub pożyczki** - skradzione dane osobowe mogą posłużyć do zaciągnięcia zobowiązań finansowych na Twoje nazwisko, co może skutkować długotrwałymi problemami prawnymi i finansowymi.
- **Kradzież tożsamości** - podszywając się pod Ciebie, przestępcy mogą np. założyć konto w banku, które posłuży do działań przestępczych, wynająć mieszkanie na Twoje nazwisko lub wyłudzić pieniądze od Twoich bliskich.
- **Phishing** - oszuści mogą wykorzystać Twoje dane np. numer telefonu lub adres e-mail, by podszyć się pod pracownika banku. W ten sposób mogą próbować wyłudzić od Ciebie dodatkowe informacje, takie jak dane logowania czy numery kart kredytowych. Stąd już tylko jeden krok, aby ukraść Twoje oszczędności.
- **Szantaż** - oszuści mogą grozić upublicznieniem Twoich prywatnych danych lub zdjęć.
- **Przejęcie konta i oszustwa finansowe** - wykradzione dane logowania do banków, sklepów internetowych czy portali społecznościowych mogą posłużyć oszustom do dokonywania transakcji lub zakupów na Twoje dane, bez Twojej wiedzy.
- **Sprzedż danych** - skradzione informacje mogą trafić do kolejnych przestępców, którzy wykorzystają je do różnych nielegalnych działań.

Jak zabezpieczyć się przed wyciekiem danych?

Najczęstszą przyczyną wycieków danych jest brak odpowiednich zabezpieczeń i wiedzy, jak dbać o bezpieczeństwo naszych danych. Aby chronić się przed zagrożeniami:

- Używaj silnych haseł i nigdy nie stosuj tych samych haseł na różnych stronach.
- Korzystaj z menedżera haseł, czyli aplikacji umożliwiającej generowanie i przechowywanie skomplikowanych haseł - np. KeePass, 1Password, Bitwarden.
- Włącz uwierzytelnianie dwuetapowe (2FA) wszędzie tam, gdzie to możliwe.
- Zainstaluj oprogramowanie antywirusowe, antymalware i antyspyware - np. Bitdefender, Kaspersky, Malwarebytes.
- Regularnie aktualizuj system operacyjny i aplikacje, aby unikać luk w zabezpieczeniach.
- Uważaj na podejrzan e-maile i linki - nie klikaj w wiadomości od nieznanym nadawców.
- Szyfruj ważne pliki i korzystaj z bezpiecznych dysków chmurowych.
- Korzystaj z VPN, szczególnie podczas łączenia się z publicznymi sieciami Wi-Fi.
- Włącz w swoim banku powiadomienia e-mail, SMS, push, dzięki czemu dowiesz się np. o logowaniach do systemu oraz transakcjach bankowych.

- Aktywuj Alerty BIK - dzięki nim otrzymasz powiadomienia o każdej próbie zaciągnięcia kredytu na Twoje dane. Wraz z Alertami BIK będziesz otrzymywać ostrzeżenia o sposobach działania cyberprzestępców i o wyciekach danych. Pomoże Ci to uniknąć oszustów lub zareagować właściwie, jeśli padniesz ich ofiarą.

Co zrobić, jeśli na Twoim komputerze pojawi się niechciane oprogramowanie?

Jeśli podejrzewasz, że Twój komputer został zainfekowany:

- Odłącz go od Internetu, aby ograniczyć rozprzestrzenianie się zagrożenia.
- Przeskanuj system za pomocą programu antywirusowego i antymalware, np. Windows Defender, Malwarebytes.
- Usuń pliki i programy, których nie instalowałeś.
- Zresetuj hasła do ważnych kont, aby zapobiec przejęciu dostępu. Zrób to na urządzeniu, co do którego masz pewność, że nie ma na nim wirusów.
- Przywróć system do wcześniejszego stanu lub przeinstaluj system operacyjny, jeśli infekcja jest poważna np. pojawiają się nieznane programy i ikony, zauważasz zmiany w ustawieniach systemowych lub przeglądarki internetowej bez Twojej zgody.
- Skontaktuj się z profesjonalnym serwisem, jeśli nie masz pewności, czy samodzielnie potrafisz sprawdzić i wyczyścić komputer w sytuacji podejrzenia infekcji.

Co zrobić, gdy Twoje dane trafiły do darknetu?

Jeśli dowiesz się, że Twoje dane są w darknetcie:

- Jeśli masz Alerty BIK z monitorowaniem darknetu, informacje o tym, które z Twoich danych wyciekły, otrzymasz w alercie.
- Zmień hasła do wszystkich kont powiązanych z danymi, które wyciekły. Zrób to na urządzeniu, co do którego masz pewność, że nie ma nim wirusów.
- Natychmiast zmień hasło do bankowości internetowej i monitoruj swoje konto bankowe pod kątem podejrzanych operacji.
- Regularnie sprawdzaj swoją historię kredytową w BIK, aby upewnić się, że nikt nie wyłudził na Ciebie kredytu. Warto mieć Alerty BIK, żeby otrzymywać informacje o wnioskach kredytowych złożonych na Twoje dane.
- W Raporcie BIK możesz sprawdzić, czy przed aktywacją Alertów BIK nie doszło do wyłudzenia kredytu na Twoje dane (Alerty BIK nie działają wstecz).
- Jeśli zauważysz nieznane transakcje na swoim koncie bankowym lub dowiesz się o zobowiązaniu finansowym, którego nie brałeś, koniecznie skontaktuj się z bankiem oraz zgłoś się na Policję.
- Zgłoś sprawę na Policji także wtedy, gdy podejrzewasz, że ktoś wykorzystał lub próbuje wykorzystać Twoje dane w celach przestępczych.

Ochrona przed cyberatakami to ciągły proces. Oszuści nigdy nie próżnują i przełamują coraz to nowsze zabezpieczenia. Dlatego musimy być przezorni i korzystajmy z narzędzi, które nas wspierają np. Alertów BIK z monitorowaniem darknetu, programów antywirusowych i menedżerów haseł. Dbajmy o swoje bezpieczeństwo w Internecie i bądźmy czujni wobec potencjalnych zagrożeń.

Biuro Informacji Kredytowej oraz BIG InfoMonitor są inicjatorami Programu edukacyjnego Nowoczesne Zarządzanie Biznesem i partnerami w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym”.

Więcej: www.nzb.pl / www.facebook.com/NowoczesneZarządzanieBiznesem