Bitdefender

Krajobraz naruszeń w Wielkiej Brytanii w 2022 r. Co zrobić w razie wycieku danych?

09.03.2023

Obecnie, gdy nasze dane osobowe mogą służyć jako waluta nowego cyfrowego świata, naruszenia bezpieczeństwa i cyberkradzieże stały się sposobem na życie wielu cyberprzestępców. Jeśli cenisz swoją prywatność w sieci, zachęcamy do zapoznania się z krajobrazem naruszeń w Wielkiej Brytanii w 2022 roku. Praca zawiera przekrój najgłośniejszych cyberataków ukazujący aktualne zagrożenia, które każdy z nas może napotkać podczas korzystania z sieci.

Zatrważające dane

Zgodnie z najnowszy raportem przygotowanym na zlecenie rządu Wielkiej Brytanii aż 39% firm i 26% organizacji charytatywnych z wysp brytyjskich zgłosiło jakieś naruszenie lub atak hakerski.

Ponadto 49% firm, które zgłosiły cyberprzestępstwo lub jego próbę, twierdzi, że ataki zdarzają się co najmniej raz w miesiącu. Co więcej, 27% z nich konstatuje, że odnotowuje próby włamań średnio raz w tygodniu.

Niestety aż 21% firm, które zgłosiły że stały się celem cyberataku, ostatecznie poniosło szkodę finansową na skutek działań hakerów.

Wyniki powyższego raportu nie oddają skali problemu, z jakim borykają się firmy i instytucje na całym świecie, ponieważ podczas badania uwzględniono tylko zgłoszone przypadki cyberincydentów. Wiele prób ataków nie zostało udokumentowanych, a często nie udało się ich nawet zidentyfikować.

Krótki przegląd najgłośniejszych naruszeń, które miały wpływ na miliony Brytyjczyków w 2022 roku

Oto trzy najgłośniejsze naruszenia, na skutek których wyciekły miliony danych osobowych Brytyjczyków:

- Prawie 300 restauracji typu fast food, w tym oddziały KFC i Pizza Hut, zostało zmuszonych do zamknięcia lokali po ataku ransomware na firmę Yum! Brands. Korporacja potwierdziła, że atak wpłynął na część jej infrastruktury IT oraz że hakerzy wykradli dane z jej serwerów.

- 10 milionów klientów brytyjskiego detalisty JD Sports (a także siostrzanych firm Millets, Blacks, Size?, Scotts i Millets Sports) zostało dotkniętych naruszeniem bezpieczeństwa. Hakerzy przejęli ich nazwy kont, adresy, adresy e-mail, numery telefonów, szczegóły zamówień i ostatnie cztery cyfry kart płatniczych.

- Niedawno brytyjski dealer samochodowy Arnold Clark poinformował klientów, że hakerzy mogli ukraść ich dane paszportowe, dane praw jazdy, a także numery ubezpieczenia społecznego i kont bankowych po cyberincydencie z grudnia 2022 roku.

Co zrobić w razie wycieku danych?

Niestety w wielu przypadkach nie mamy wpływu na to, że nasze dane mogą wyciec do sieci. Aby zapobiec temu niebezpieczeństwu, musielibyśmy praktycznie w ogóle nie korzystać z Internetu. Zakładając nowe konta na wirtualnych platformach i prowadząc profile w mediach społecznościowych, warto mieć świadomość, że w każdej chwili nasze dane mogą zostać skradzione, a my sami możemy stać się celami kampanii phishigowych. Dlatego zastanówmy się, zanim umieścimy w sieci zbyt wiele informacji na swój temat.

Jeśli dojdzie do naruszenia naszych danych osobowych, niezwłocznie musimy przejąć kontrolę nad naszą cyfrową prywatnością i zacząć działać, zanim będzie za późno. Dlatego zespół Bitdefender przygotował krótki poradnik, co zrobić w razie wycieku danych.

- Zmień hasło do ujawnionego konta. Jeśli nie używasz menedżera haseł, rozważ jego zakup. W ten sposób możesz mieć pewność, że Twoje konta internetowe są zabezpieczone najsilniejszymi możliwymi hasłami bez konieczności zapamiętywania lub zapisywania ich. Skonfiguruj również uwierzytelnianie dwuskładnikowe na swoich kontach.

- Jeśli uważasz, że Twoje dane finansowe zostały skradzione lub zauważysz podejrzaną aktywność na swoich rachunkach bankowych, natychmiast powiadom swój bank lub dostawcę karty kredytowej.

- Jeśli Twoje konta w mediach społecznościowych zostały zhakowane, skontaktuj się z administratorem portalu oraz ze swoimi kontaktami, aby ostrzec je przed wiadomościami, które atakujący mogli wysłać, podszywając się pod Ciebie.

- Uważaj na wszelkie dziwne e-maile lub telefony, które otrzymujesz po incydencie. Mogą to być próby wyłudzenia danych osobowych lub dodatkowych informacji na Twój temat.

„W przypadku wycieku naszych danych powinniśmy być szczególnie wyczuleni na wszelkiego rodzaju nietypowe wiadomości z linkami, ponieważ mogą to być próby phishingowe. W takich sytuacjach najlepiej nie klikać w niechciane linki. Przede wszystkim zaś należy korzystać ze skutecznego antywirusa wyposażonego w moduł antyphsihingowy" – radzi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/co-zrobic-w-razie-wycieku-danych/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 09.03.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza

najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.