ROSNĄ KOSZTY NARUSZEŃ DANYCH. PONAD 4 MLN DOLARÓW STRAT NA JEDNĄ FIRMĘ

Pandemia stała się przyczyną rekordowo wysokich kosztów naruszeń danych na świecie – wynika z raportu IBM Security. Średni koszt jednego przypadku wyniósł wśród badanych firm 4,24 miliona dolarów. Jest to najwyższy wynik w 17-letniej historii raportu. Najczęściej naruszenia danych dotyczyły poufnych informacji o klientach.

IBM Security przedstawiła wyniki globalnego badania, z którego wynika, że w okresie maj 2020 – marzec 2021 średni koszt jednego przypadku naruszenia danych wyniósł wśród badanych firm 4,24 mln dol. To najwyższy rezultat odnotowany w 17-letniej historii raportu.

Badanie przeprowadzono w oparciu o analizę danych dotyczących rzeczywistych przypadków naruszeń, które wystąpiły w ponad 500 organizacjach. Wynika z niego, że poszczególne incydenty stały się bardziej kosztowne, a ich skutki trudniejsze do naprawienia w związku z drastycznymi zmianami sposobu prowadzenia działalności w trakcie pandemii. Koszty wzrosły o 10 proc. w porównaniu z poprzednim rokiem.

Naruszenia w skali mega

Według danych IBM, średni koszt naruszenia w skali mega (obejmującego od 50 do 65 mln rekordów) wyniósł 401 mln dol. Jest to o ponad 100 razy więcej niż koszt większości naruszeń przeanalizowanych w ramach badania (obejmujących od 1 do 100 tys. rekordów).

W podziale na branże najbardziej kosztowne były przypadki naruszenia danych, do których dochodziło **w ochronie zdrowia** (9,23 mln dol. na firmę). Kolejne miejsca zajęły **sektor finansowy** (5,72 mln) oraz **farmaceutyczny** (5,04 mln). Choć ogólne koszty naruszeń ponoszone w branży handlowej, medialnej, hotelarskiej i w sektorze publicznym były niższe, to znacząco wzrosły w porównaniu z rokiem poprzednim.

W podziale na kraje i regiony, koszty naruszenia danych były najwyższe w USA (9,05 mln dol. na incydent), na Bliskim Wschodzie (6,93 mln) oraz w Kanadzie (5,4 mln).

Winna pandemia, medycyna w czołówce

IBM przypomina, że w 2020 roku firmy zostały zmuszone do szybkiego dostosowania swoich metod pracy do nowych warunków. Wiele z nich zachęcało personel do pracy zdalnej. Podczas pandemii 60 proc. organizacji zwiększyło także stopień wykorzystania usług opartych na chmurze.

Z najnowszych danych wynika, że szybkim zmianom informatycznym nie towarzyszyły jednak równie skuteczne modyfikacje stosowanych przez firmy zabezpieczeń, co obniżyło ich zdolność do właściwego reagowania na przypadki naruszeń danych.

Raport pozwolił na zidentyfikowanie wśród uczestniczących w badaniu firm następujących trendów:

Wpływ pracy zdalnej

Szybkie przejście na wykonywanie pracy z domu podczas pandemii mogło doprowadzić do wzrostu kosztów przypadków naruszenia danych. **Były one średnio o 1 mln dol. wyższe w tych przypadkach, w których jako jedną z ich przyczyn wskazywano pracę zdalną** (w porównaniu do kosztów incydentów, w których praca zdalna nie była kluczowym czynnikiem). Koszty dla obu tych grup wynosiły odpowiednio 4,96 oraz 3,89 mln dol.

Gwałtowny wzrost kosztów naruszeń danych medycznych

W branżach, które zmagały się w trakcie pandemii z największymi zmianami operacyjnymi (ochrona zdrowia, handel, hotelarstwo, produkcja/dystrybucja dóbr konsumenckich) również odnotowano znaczny wzrost kosztów naruszenia danych w stosunku do roku poprzedniego.

Najbardziej kosztowne były przypadki naruszenia danych medycznych wynoszące 9,23 mln dol. na incydent, czyli o 2 mln więcej niż w roku poprzednim.

Utrata kontroli nad danymi uwierzytelniającymi prowadzi do ujawnienia informacji

Najczęstszą przyczyną naruszeń zidentyfikowanych podczas badania była kradzież danych uwierzytelniających użytkowników systemów. Naruszenia dotyczyły najczęściej danych osobowych klientów, takich jak imię i nazwisko, adres e-mail i hasło.

Aż 44 proc. przypadków naruszeń było związanych z tego rodzaju danymi. Połączenie obydwu powyższych czynników często prowadziło do efektu domina - zdobycie nazwy użytkownika/hasła pozwalało atakującym na pozyskanie informacji umożliwiających bezprawne wykorzystanie zdobytych danych w przyszłości.

Nowoczesne rozwiązania jako czynnik obniżający koszty

Według raportu wdrożenie sztucznej inteligencji, zaawansowana analityka bezpieczeństwa oraz szyfrowanie to trzy czynniki, które w największym stopniu przyczyniały się do obniżenia kosztów naruszeń. Pozwalały one firmom zaoszczędzić od 1,25 do 1,49 mln dol. w porównaniu z tymi organizacjami, które nie stosowały tego rodzaju rozwiązań na szeroką skalę.

Firmy, które wdrożyły rozwiązania z zakresu chmury hybrydowej, ponosiły niższe koszty incydentów związanych z naruszeniem danych przechowywanych w chmurze (3,61 mln), niż te polegające głównie na chmurze publicznej (4,80 mln) lub na chmurze prywatnej (4,55 mln).

Praca zdalna i chmura to krytyczne obszary

W swoim opracowaniu IBM zaznacza, że podczas pandemii społeczeństwo w większym stopniu polegało na interakcjach cyfrowych, a firmy przechodziły na pracę zdalną i na usługi w chmurze, dostosowując swój model działania do wymagań świata online.

Z raportu wynika, że powyższe czynniki miały znaczący wpływ na sposób reakcji na przypadki naruszenia danych. Niemal 20 proc. firm objętych badaniem wskazało, że praca zdalna przyczyniała się do częstszego naruszania danych, zaś naruszenia tego rodzaju kosztowały 4,96 mln dol. (niemal o 15 proc. więcej niż średnia).

Biorące udział w badaniu organizacje, w których doszło do naruszenia podczas projektów związanych

z przenoszeniem danych do chmury, również zmagały się z kosztami, które były wyższe o 18,8 proc. od średniej. Wykazano również, że podmioty, które były bardziej zaawansowane we wdrażaniu nowoczesnych strategii opartych na chmurze (etap „dojrzały") były w stanie skuteczniej wykrywać incydenty i na nie reagować. Robiły to średnio o 77 dni szybciej niż firmy, które były na początkowym etapie wdrażania tego rodzaju rozwiązań.

Ponadto firmy, które wdrożyły rozwiązania z zakresu chmury hybrydowej, ponosiły niższe koszty incydentów związanych z naruszeniem danych przechowywanych w chmurze (3,61 mln dol.) niż te polegające głównie na chmurze publicznej (4,8 mln) lub na chmurze prywatnej (4,55 mln).

Kradzione dane klientów

Raport pozwolił również dostrzec, że rosnącym problemem - z jakim firmy zmagają się w ramach naruszeń danych - jest ujawnianie informacji dotyczących konsumentów, w tym danych uwierzytelniających, które mogą następnie służyć do przypuszczania kolejnych ataków.

82 proc. badanych przyznało się, że **stosuje te same hasła dla wielu kont.** Ujawnienie tego rodzaju danych uwierzytelniających stanowi najczęstszą przyczynę, a zarazem skutek przypadków naruszenia danych, dodatkowo zwiększając poziom ryzyka ponoszonego przez firmy.

Niemal połowa (44 proc.) analizowanych przypadków naruszeń była związana z ujawnieniem danych osobowych klientów, takich jak imię i nazwisko, adres e-mail, hasło czy nawet dane medyczne - był to najbardziej popularny rodzaj naruszeń zidentyfikowany w raporcie.

Ujawnienie danych umożliwiających identyfikacje klientów jest najbardziej kosztowne. Utrata danych umożliwiających identyfikację klientów była najbardziej kosztowna w porównaniu z innymi rodzajami danych (180 dol. na utracony lub skradziony rekord, w porównaniu ze średnią dla jednego rekordu wynoszącą 161 dol.).

Z kolei ujawnienie danych uwierzytelniających użytkownika było najczęstszą metodą pozwalającą atakującym na dostanie się do systemów - odpowiadało za 20 proc. przeanalizowanych przypadków naruszeń.

Według raportu naruszenia spowodowane ujawnieniem danych uwierzytelniających były wykrywane najpóźniej - proces ten zajmował średnio 250 dni (w porównaniu do średniej wynoszącej 212 dni).

Raport dotyczący kosztów naruszeń danych z roku 2021, opracowany przez IBM Security oraz Instytut Ponemon opiera się na analizie rzeczywistych przypadków naruszeń obejmujących do 100 tys. rekordów, które miały miejsce w ponad 500 organizacjach od maja 2020 do marca 2021 roku. Uwzględnia on setki różnych czynników związanych z naruszeniami danych: od strategii prawnych i regulacyjnych, poprzez działania techniczne, aż do utraty reputacji marki, klientów i spadku wydajności pracowników.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.

Czytaj też: IBM i Apple krytykują firmy technologiczne za niewłaściwe użycie danych