**W Światowy Dzień Backupu pomyśl o systemie kopii zapasowych w firmie**

* **31 marca przypada Światowy Dzień Backupu – to okazja, aby zastanowić się nad bezpieczeństwem danych firmowych.**
* **83% firm zbadanych przez IBM doświadczyło więcej niż jednego wycieku danych w ciągu 2022 roku, a średnia strat finansowych wyniosła niemal 5 mln dolarów.**
* **Jednym ze sposobów na minimalizację skutków ryzyka utraty danych jest wdrożenie efektywnego systemu tworzenia kopii zapasowych.**

Światowy Dzień Backupu funkcjonuje w kalendarzu branży IT od 2011 roku. Ma on przypominać wszystkim użytkownikom technologii o tym, że warto regularnie wykonywać kopię zapasową plików. Do ich utraty może dojść m.in. w wyniku awarii sprzętu, pożaru, zalania, kradzieży urządzenia czy przypadkowego usunięcia plików przez pracownika.

*– Przyczyny utarty danych mogą być bardzo różne. Jednak ważniejsze od przyczyn są skutki, a te mogą być naprawdę poważne. Utrata danych oznacza paraliż działania firmy. Może to być np. zatrzymanie produkcji, czy świadczenia usług, co prowadzi do strat finansowych. Utrata danych osobowych z kolei naraża firmę na kary finansowe i tworzy ryzyko cyberataków na osoby, których dane trafiły w ręce cyberprzestępców. Straty wywołane wyciekiem danych mogą poważnie zagrozić płynności finansowej firmy, a w skrajnym przypadku nawet do jej bankructwa –* mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

Ryzyko utraty danych z różnych przyczyn jest duże. Według raportu IBM „Cost of Data Breach Full Report 2022”, w ciągu ubiegłego roku 83% badanych firm doświadczyło więcej niż jednego incydentu związanego z wyciekiem danych. Spowodowana tym średnia kwota strat finansowych wyniosła 4,35 mln dolarów. To niemal 3% więcej niż rok wcześniej, kiedy średnia wyniosła nieco ponad 4,2 mln dolarów. Jak więc minimalizować takie ryzyko?

– *Tutaj odpowiedzią znów może być tworzenie kopii zapasowych. We wspomnianym raporcie autorzy wskazują, że ponad połowa badanych firm nie stosuje w swoich systemach architektury Zero Trust, ale w tym przypadku chodzi jedynie o zabezpieczanie dróg dostępu do danych, a nie ich przechowywanie. Backup umożliwia „cofnięcie się w czasie” z danymi do wybranej sesji z przeszłości. A to właśnie zapewnia regularne tworzenie kopii zapasowych. Dzięki nim da się odtworzyć dany proces i w miarę szybko przywrócić pracę na jej właściwe tory, co pozwala zminimalizować ewentualne straty finansowe. Warto więc wdrożyć takie rozwiązanie w swojej firmie, korzystając ze wsparcia zewnętrznych specjalistów* – wyjaśnia Patrycja Tatara ze Sprint S.A.

**Backup to nie archiwizacja**

Te pojęcia bywają mylone, więc warto wyjaśnić na czym polega różnica. Backup to dublowanie plików w aktualnej wersji lub jednym, określonym momencie, który pozwala na powrót do nich w razie jakiegokolwiek incydentu. Zazwyczaj przeprowadza się kilka backupów w regularnych odstępach czasowych, np. dziennych, tygodniowych albo jeszcze dłuższych. Dane skopiowane podczas sesji backupowych są usuwane z repozytorium po określonym czasie, gdy użytkownik uznaje, że nie będą one już potrzebne, bo np. zostaną zastąpione nowszymi kopiami. Z kolei archiwizacja to proces przeniesienia danych na inny i zazwyczaj wolniejszy nośnik. Tę czynność wykonuje się z myślą o długotrwałym przechowywaniu plików, tak jak robi się to z klasycznymi, papierowymi dokumentami. Archiwizuje się dane, które rzadko są przetwarzane, a mogą niepotrzebnie zajmować przestrzeń istotną w środowisku produkcyjnym.

Źródło: Sprint S.A.