Warszawa, dn. 23.08.2023 r.

Co powinna zawierać procedura wykonywania kopii zapasowych?

Procedura wykonywania kopii zapasowych (backupów) jest jednym z istotniejszych elementów budowania systemu ochrony danych osobowych, ale też zapewnienia ciągłości działania w kontekście szerszym, bo dotyczącym wszystkich istotnych dla organizacji informacji.
Kiedy taka procedura może się przydać (przy założeniu, że została wdrożona i jest stosowana)? Na pewno w przypadku awarii systemu informatycznego, ale też w sytuacji popełnienia błędu ludzkiego, ataków hakerskich albo innych zagrożeń, które mogą mieć przełożenie na integralność lub dostępność danych. W niniejszym wpisie chciałbym wskazać co powinna zawierać taka procedura.

Cel i zakres backupu

Na początek oczywiście należy określić, jakie dane osobowe (oraz inne istotne dla organizacji informacje) są kluczowe dla organizacji i powinny być objęte kopią zapasową oraz jak często backupy powinny być tworzone. Przykładowo kopia zapasowa może obejmować pliki, bazy danych, konfiguracje systemu, itp. Warto zaznaczyć, że ten etap jest bardzo ważny z punktu widzenia realizacji nadrzędnego celu jakim ma być zapewnienie ciągłości działania (ale też zgodności m.in. z RODO albo normą ISO 27001).

Metody wykonywania backupu

Skoro wiemy już co powinno być przedmiotem backupu, czas najwyższy zastanowić się jaką metodą wykonywać nasze kopie zapasowe. Dla przypomnienia wskażę, że wyróżniamy backupy pełne, różnicowe oraz przyrostowe (inkrementalne).
Backup pełny kopiuje wszystkie dane (dyski, foldery, pliki), backup różnicowy tylko zmiany od ostatniego pełnego backupu, a backup przyrostowy uwzględnia dane, które zostały zmienione lub dodane, od czasu utworzenia ostatniej, dowolnej kopii zapasowej.

Harmonogram backupów

Kolejny krok to ustalenie częstotliwości wykonywania kopii zapasowych. Można przyjąć, że kopie pełne są tworzone nieco rzadziej (np. co tydzień), a backupy różnicowe lub przyrostowe częściej (np. codziennie). Powyższe koniecznie trzeba ustalić z właścicielami biznesowymi przypisanymi do poszczególnych zasobów, które mają być zabezpieczone poprzez regularne wykonywanie kopii. Oczywiście nie bez znaczenia będzie tu też głos ze strony działu IT, który będzie odpowiedzialny za realizację tego procesu. A zatem konieczne jest tu współdziałanie zarówno IT jak i właścicieli biznesowych.

Wybór lokalizacji przechowywania

Miejsce przechowywania kopii to kolejny etap. Należy pamiętać o oczywistej oczywistości, czyli zapewnieniu, by wybrana przez nas lokalizacja zapewniała bezpieczeństwo – tak ze

strony czynników zewnętrznych np. pożar, zalanie jak i wewnętrznych np. dostęp osób nieupoważnionych.
Warto też wspomnieć, że kopie zapasowe mogą być tworzone na różnych nośnikach fizycznych np. zewnętrzne dyski twarde, taśmy magnetyczne albo – co zdarza się coraz częściej, zwłaszcza w mniejszych firmach – wykorzystywana może być do tego chmura obliczeniowa np. OneDrive od Microsoftu albo Dysk Google.

Automatyzacja backupów
Jeśli to możliwe, najlepiej zadbać o to, by kopie zapasowe wykonywane były w sposób automatyczny, przy czym automatyzm ten powinien opierać się na ustanowionym uprzednio harmonogramie. W ten sposób niwelujemy np. możliwość popełnienia jednego z najprostszych błędów ludzkich jakim może być najzwyklejsze na świecie zapomnienie o czymś co powinno zostać zrobione. Oczywiście niezbędny jest też nadzór nad tym, czy kopia została wykonana (patrz: niżej) – w tym celu administrator kopii powinien analizować logi w tym zakresie i w przypadku wykrycia błędów – poddać je analizie, ale nade wszystko zadbać o to, by kopia została wykonana.

Testowanie i weryfikacja backupów
W poprzednim punkcie mówiliśmy o nadzorze nad wykonywaniem kopii, ale to zdecydowanie za mało. Pamiętaj, by okresowo sprawdzać, czy backupy są faktycznie przydatne. Przeprowadzaj testy przywracania danych z kopii, aby upewnić się, że proces przywracania działa poprawnie. To kluczowe zadanie, bo co nam po kopii, z której nie da się odtworzyć istotnych dla organizacji danych.

Zabezpieczenie dostępu do kopii
I znów banał, ale należy o tym wspomnieć. Pamiętaj, by dostęp do backupu miały tylko wyraźnie upoważnione do tego osoby. Przecież nie chcemy, żeby jakiś przypadkowy użytkownik usunął przez przypadek (albo z premedytacją) coś co ma zapewnić organizacji ciągłość działania.

Monitorowanie procesu oraz aktualizacje procedury
Jak z każdą procedurą, tak i w przypadku omawianego procesu konieczne jest ustanowienie mechanizmu monitorowania całości. W razie jakichkolwiek problemów, takich jak nieudane backupy, powinny być generowane alerty, aby można było szybko zareagować.
Oprócz tego należy pamiętać o aktualizacji samej procedury, bo i ona powinna być poddawana regularnym przeglądom – przede wszystkim na okoliczność, czy funkcjonuje w sposób należyty, ale też każdorazowo np. w przypadku zmian w systemach informatycznych. Dbałość o to, aby procedura była zgodna z potrzebami biznesu, ma kluczowe znaczenie dla skuteczności backupów.

Michał Sztąberek – ekspert ds. ochrony danych osobowych, CEO w iSecure Sp. z o.o.