Backup i ransomware: zadania użytkownika

Synchronizacja mo?e powieli? tak?e usuni?cie lub zaszyfrowanie. Nie zast?puje niezale?nej kopii.

LCPD / DATPOL · aktualizacja: 24.10.2026 · materia? do dopasowania do procedur organizacji.

Gdzie pracować

Dokumenty zapisuj w zatwierdzonym miejscu obj?tym ochron?. Nie trzymaj jedynej kopii na pulpicie, prywatnym dysku lub w prywatnej chmurze. Potwierd? z IT, czy folder rzeczywi?cie jest kopiowany i jaka jest retencja.

Plan administratora

Plan okre?la w?a?ciciela, zakres, harmonogram, odseparowanie, uprawnienia i testy odtworzenia. Cz??? kopii powinna by? odporna na skasowanie z przej?tego konta produkcyjnego. „Backup zako?czony” nie dowodzi, ?e mo?na odtworzy? us?ug?.

Podejrzenie ransomware

Nie pod??czaj kopii do podejrzanego komputera i nie odtwarzaj samodzielnie. IT wybiera czysty punkt i kolejno?? uruchamiania. U?ytkownik podaje ostatni poprawny stan i priorytet dokumentów. Nie obiecuj dost?pno?ci ka?dej zmiany z ostatniej godziny bez sprawdzenia parametrów kopii.

Sprawdź w praktyce

- Znam chronione miejsce zapisu.
- Nie pod??czam kopii do podejrzanego sprz?tu.

- Odtwarzanie jest uzgodnione i testowane.

Sytuacja z pracy

Usuni?ty folder znika te? z chmury. Potrzebujesz historii wersji lub niezale?nej kopii, nie ponownej synchronizacji.

Źródła i dalsza lektura

- NCSC — ochrona przed ransomware

BHP w IT na LCPD: zasady i szybkie dzia?ania

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Jak zg?osi? incydent bez wysy?ania sekretów

Nast?pny temat: Wzór polityki hase? i dost?pów

Wersja #2
Utworzono 2026-10-24 07:56:52 UTC przez Administrator DATPOL
Zaktualizowano 2026-10-24 07:56:53 UTC przez Administrator DATPOL