Kliknąłem link lub podałem hasło: pierwsze kroki

Zg?o? zdarzenie od razu, nawet bez pewno?ci. Nie trzeba udowodni? ataku, aby poprosi? o pomoc.

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

Otwarta strona

Przerwij dalsze dzia?ania. Nie wpisuj danych ani nie pobieraj kolejnych plików. Zapisz adres i czas, zawiadom IT. Samo otwarcie linku nie dowodzi infekcji: wa?ne jest, co pobrano, uruchomiono i jakie uprawnienia przyznano.

Ujawnione dane

Z zaufanego urz?dzenia otwórz znany adres us?ugi. Zmie? ujawnione has?o i has?a kont, gdzie u?yto tego samego sekretu. IT powinno odwo?a? sesje, tokeny, nieznane metody MFA i zgody aplikacji oraz sprawdzi? przekazywanie poczty. Zamkni?cie karty nie uniewa?nia dost?pu atakuj?cego.

Uruchomiony plik lub szyfrowanie

Na komputerze pracownika od??cz Wi-Fi i Ethernet, zg?o? z innego urz?dzenia. Nie kasuj plików, nie uruchamiaj „czy?cicieli” i nie wy??czaj komputera bez uzgodnienia, chyba ?e wymaga tego bezpiecze?stwo fizyczne. Izolacj ? urz?dze? steruj?cych i systemów krytycznych uzgadnia si? z odpowiedzialnym personelem, by nie zagrozi? procesowi.

Sprawdź w praktyce

- Zg?osi?em znanym kana?em.
- Ujawni?em wszystkie wykonane czynno?ci.
- Nie zacieram ?ladów i nie testuj? linku ponownie.

Sytuacja z pracy

Po wpisaniu has?a strona znika. Powiedz IT tak?e, czy poda?e? MFA i czy uruchomi?e? plik — to zmienia zakres reakcji.

Źródła i dalsza lektura

- CERT Polska — zg?aszanie incydentów
- 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: AI, t?umacze i konwertery PDF

Nast?pny temat: Jak zg?osi? incydent bez wysy?ania sekretów

Wersja #2
Utworzono 2026-10-24 07:56:51 UTC przez Administrator DATPOL
Zaktualizowano 2026-10-24 07:56:53 UTC przez Administrator DATPOL