Zdarzenia i reakcja

Instrukcje i sytuacje z codziennej pracy.

- Klikn??em link lub poda?em has?o: pierwsze kroki
- Jak zg?osi? incydent bez wysy?ania sekretów
- Backup i ransomware: zadania u?ytkownika

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

Jak zgłosić incydent bez wysyłania sekretów

Dobre zg?oszenie zawiera fakty, nie has?a i kody jednorazowe.

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

Co podać

Czas i stref? czasow?, numer sprz?tu, us?ug?, objaw, wykonane czynno?ci i kontakt zwrotny. Wska?, czy wpisano dane, otwarto plik, zaakceptowano MFA, wykonano przelew lub udost?pniono dokument. Oddziel obserwacje od przypuszcze?.

Dowody

Korzystaj z ustalonego kana?u. Zrzut ekranu nie powinien ujawnia? hase?, kodów lub przypadkowych danych osób. Nie wklejaj aktywnych tokenów i linków odzyskiwania na publiczny czat. EML/MSG przeka? zespo?owi bez uruchamiania za??czników.

Gdzie jeszcze zgłosić

Podejrzany SMS: oryginalna tre?? na 8080. Strona lub e-mail: incydent.cert.pl. Odpowiedzialna osoba ustala dodatkowe obowi?zki wobec w?a?ciwych instytucji. Nie przyjmujemy jednego terminu prawnego dla wszystkich podmiotów i zdarze?. Przy zagro?eniu pieni?dzy równolegle kontaktuj si? z bankiem.

Sprawdź w praktyce

- Znam wewn?trzny kontakt i zast?pstwo.

- Nie przesy?am sekretów.
- Zachowuj? numer zg?oszenia.

Sytuacja z pracy

Wzór: „24.10, 10:15, LAP-042, poczta. Otworzy?em link i poda?em has?o. Nie poda?em kodu i nie uruchamia?em pliku. Prosz? o pilny kontakt”.

Źródła i dalsza lektura

- CERT Polska — zg?aszanie incydentów

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Klikn??em link lub poda?em has?o: pierwsze kroki

Nast?pny temat: Backup i ransomware: zadania u?ytkownika

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