Zalecenia bezpieczeństwa dla dostawców platform IT w ochronie zdrowia – w pigułce

Przygotowaliśmy zestaw najważniejszych działań organizacyjnych i technicznych, które pomagają chronić dane medyczne i wzmacniać ciągłość działania usług cyfrowych w ochronie zdrowia.

Zalecenia służą do samooceny i ustalania priorytetów. Nie zastępują obowiązków wynikających z przepisów prawa.

CSIRT
Centrum e-Zdrowia

Jak stosować zalecenia

Na poziom ryzyka oraz potencjalne skutki incydentu bezpieczeństwa wpływają skala i koncentracja przetwarzanych danych medycznych. Zalecenia stosuj proporcjonalnie do poziomu ryzyka, skali, architektury rozwiązania i krytyczności usług (czyli ich znaczenia).

Dla kogo są przeznaczone

Zalecenia są przeznaczone dla:

- producentów oprogramowania
- dostawców platform IT
- operatorów systemów wspierających świadczenie usług zdrowotnych, w tym systemów integrujących się z platformą e-zdrowia P1 lub systemami placówek medycznych.

Obejmują ochronę danych, ludzi, aplikacji, API, infrastruktury, dostawców i podwykonawców i ciągłość działania usług.

Zarządzanie bezpieczeństwem

1. Utrzymuj system zarządzania bezpieczeństwem informacji oparty na ISO/IEC 27001.
2. Regularnie identyfikuj zagrożenia i oceniaj ryzyko.
3. Prowadź rejestr ryzyk wraz z ich właścicielami i terminami działań. Oceniaj prawdopodobieństwo i skutki.
4. Określ sposób postępowania z każdym ryzykiem. Obniżaj ryzyko rezydualne do akceptowalnego poziomu.
5. Aktualizuj ocenę ryzyka po ważnych zmianach.
6. Dokumentuj skuteczność zastosowanych zabezpieczeń.

Ochrona danych i architektura systemu

1. Inwentaryzuj systemy, bazy danych, pliki, API i przepływy danych.
2. Ograniczaj zakres oraz koncentrację gromadzonych danych do niezbędnego minimum.
3. Separuj instancje i środowiska.
4. W testach ograniczaj dane produkcyjne i stosuj anonimizację lub pseudonimizację.
5. Szyfruj transmisję danych, dane przechowywane i kopie zapasowe uznanymi metodami.
6. Przechowuj klucze kryptograficzne oddzielnie od chronionych danych.
7. Regularnie zmieniaj i unieważniaj klucze oraz poświadczenia.
8. Nie zapisuj sekretów w kodzie.
9. Określ okresy retencji danych oraz zasady ich bezpiecznego usuwania.
10. Kontroluj eksport danych i ograniczaj możliwość ich masowego pozyskania lub wyprowadzenia.

Tożsamość, dostęp i uprawnienia

1. Stosuj uwierzytelnianie wieloskładnikowe (MFA), używaj metod odpornych na phishing co najmniej dla kont uprzywilejowanych.
2. Przyznawaj użytkownikom tylko niezbędne uprawnienia i kontroluj dostęp do danych oraz funkcji systemu na podstawie ich roli lub innych określonych zasad (RBAC/ABAC) po stronie serwera.
3. Zapewnij użytkownikom indywidualne konta, stosuj PAM/JIT oraz rejestrowany dostęp serwisowy ograniczony czasowo. Ogranicz dostęp deweloperów do środowiska produkcyjnego i wyłączaj tymczasowe połączenia wykorzystywane podczas wdrożeń po zakończeniu prac.
4. Przeglądaj uprawnienia, automatycznie odbieraj zbędne dostępy i blokuj nieużywane konta.
5. Rejestruj, alarmuj i przeglądaj dostęp awaryjny (break the glass).

Bezpieczne aplikacje i integracje

1. Wdróż Secure SDLC, analizę zagrożeń, przeglądy kodu i kontrole SAST/DAST/SCA w CI/CD.
2. Zarządzaj podatnościami – krytyczne naprawiaj priorytetowo.
3. Testuj aplikacje, infrastrukturę i API, zwłaszcza po istotnych zmianach.
4. Chroń API za pomocą uwierzytelniania, autoryzacji, limitów i walidacji.
5. Stosuj odrębne tożsamości integracji, repozytorium sekretów, ewidencję i rotację poświadczeń.
6. Utrzymuj aktualny wykaz komponentów oraz bibliotek używanych w oprogramowaniu (SBOM) i korzystaj wyłącznie z takich, które są nadal wspierane przez producenta lub społeczność.

Monitorowanie i reagowanie na incydenty

1. Rejestruj informacje o logowaniu, zmianie uprawnień, nadaniu i wykorzystaniu dostępu administracyjnego, dostępie do danych oraz ich eksporcie: kto, kiedy, skąd, dokąd, co wykonał.
2. Gromadź logi w centralnym systemie i zabezpieczaj je przed nieuprawnioną modyfikacją lub usunięciem, wykorzystując odseparowany system, np. SIEM.
3. Wykrywaj anomalie w API, masowe odczyty i próby dostępu między instancjami.
4. Regularnie testuj skuteczność mechanizmów wykrywania zagrożeń (detekcji) oraz określaj charakter, skalę i skutki wykrywanych anomalii.
5. Przygotuj procedury obsługi incydentów. Określ role, zasady eskalacji i kontakty.
6. W razie incydentu blokuj zagrożone konta, unieważniaj poświadczenia, odcinaj integracje i zabezpieczaj dowody.

Kopie zapasowe i odtwarzanie usług

1. Szyfruj kopie zapasowe i odseparuj je od środowiska produkcyjnego.
2. Utrzymuj co najmniej jedną kopię zapasową, której nie można zmienić ani usunąć w przypadku przejęcia lub naruszenia środowiska produkcyjnego. Może to być np. kopia niezmienna (WORM), przechowywana offline lub w odseparowanej lokalizacji.
3. Do zarządzania kopiami zapasowymi stosuj odrębne konta i poświadczenia, niezależne od środowiska produkcyjnego.
4. Określ RTO/RPO, priorytety i scenariusze awaryjne.
5. Regularnie testuj rzeczywiste odtwarzanie usług, również w scenariuszu ataku ransomware oraz utraty kluczowego dostawcy.
6. W scenariuszach awaryjnych uwzględniaj utratę kluczy i poświadczeń.
7. Usuwaj wykryte niezgodności i ponawiaj testy.

Dostawcy i podwykonawcy

1. Oceniaj dostawców przed rozpoczęciem współpracy, a następnie okresowo w trakcie jej trwania
2. Określ w umowach i SLA odpowiedzialność za bezpieczeństwo, zasady zgłaszania incydentów i prowadzenia audytów oraz obowiązki związane z zakończeniem współpracy.
3. Prowadź rejestr dostawców i podwykonawców, świadczonych przez nich usług, nadanych uprawnień, miejsc przetwarzania danych, poziomu krytyczności oraz wyników oceny.
4. Weryfikuj podwykonawców, deklarowane zabezpieczenia i warunki przetwarzania danych w chmurze. Transfery poza Europejski Obszar Gospodarczy (EOG) oceniaj zgodnie z RODO.
5. Przygotuj plan wyjścia, bezpieczną migrację, testy eksportu i odtworzenia danych oraz ich usuwanie zgodnie z zasadami retencji.

Transparentność i rozliczalność przetwarzania danych

1. Informuj, kto przetwarza dane, w jakim celu i zakresie.
2. Utrzymuj aktualny wykaz podmiotów przetwarzających i podwykonawców.
3. Zapewnij możliwość sprawdzenia, kto i kiedy uzyskał dostęp do danych.
4. Umożliwiaj wyjaśnienie nietypowych operacji na podstawie chronionych logów.

Bezpieczeństwo systemów obsługujących wiele podmiotów

1. Zapewnij całodobowy monitoring i obsługę incydentów, odpowiednie czasy reakcji oraz zastępowalność personelu.
2. Zlecaj niezależne audyty bezpieczeństwa systemów.
3. Wymuszaj izolację w backendzie i bazach.
4. Testuj odporność na nieuprawniony dostęp do danych pomiędzy instancjami lub podmiotami.
5. Wprowadzaj ponowną autoryzację użytkownika, dodatkowe potwierdzenie i odpowiednie limity dla operacji wysokiego ryzyka.
6. Wykrywaj eksfiltrację rozłożoną w czasie.
7. Zapewnij możliwość szybkiego blokowania kont i wyłączania integracji.

Weryfikacja realizacji zaleceń

1. Każdemu zaleceniu przypisz właściciela i aktualny status realizacji.
2. Potwierdzaj realizację zaleceń dokumentacją konfiguracji, wynikami testów i audytów lub zapisami w logach.
3. Zapisuj niezgodności wraz z oceną ryzyka, działaniem naprawczym, właścicielem i terminem.
4. Prowadź rejestr wyników i weryfikuj skuteczność działań naprawczych.

CSIRT CeZ — 24/7 dla podmiotów ochrony zdrowia

Incydenty: incydent@csirt.cez.gov.pl • Formularz

Sprawy ogólne: info@csirt.cez.gov.pl

TLP / PGP (zalecane)