Fragment

NIS 2 w Polsce

Jak przygotować firmę na nowe wymogi cyberbezpieczeństwa

Rozdział IV
Techniczne i organizacyjne środki bezpieczeństwa

1. Bezpieczne utrzymanie i eksploatacja

Bezpieczne utrzymanie i eksploatacja systemów teleinformatycznych oraz infrastruktury OT stanowią fundament skutecznej ochrony zasobów organizacji. Wdrażanie środków bezpieczeństwa nie kończy się na etapie ich projektowania i implementacji – równie istotne jest zapewnienie ich ciągłej skuteczności w trakcie eksploatacji. Odpowiednie zarządzanie zmianą, konfiguracją, bezpieczeństwem sieci oraz łańcuchem dostaw pozwala na minimalizowanie ryzyka wystąpienia podatności i incydentów, które mogłyby zagrozić stabilności działania organizacji. Standardy, takie jak ISO 27001 oraz IEC 62443 wskazują na konieczność utrzymania systemów w sposób kontrolowany, z uwzględnieniem cyklicznych przeglądów, monitorowania zgodności z politykami bezpieczeństwa oraz zarządzania aktualizacjami. W rozdziale IV omówione zostaną kluczowe procesy związane z utrzymaniem systemów w sposób bezpieczny, wraz z praktycznymi wytycznymi dotyczącymi ich wdrażania i optymalizacji.

1.1. Zarządzanie zmianą

Koncepcja: zarządzanie zmianą to zestaw procesów zapewniających, że wszystkie istotne zmiany w systemach IT/OT są planowane, kontrolowane i zatwierdzane w sposób minimalizujący ryzyko dla bezpieczeństwa informacji i ciągłości działania. Norma ISO 27001 wymaga, aby zmiany wpływające na bezpieczeństwo informacji były formalnie kontrolowane i autoryzowane. Oznacza to w praktyce wprowadzenie procedury zarządzania zmianami obejmującej m.in. rejestrowanie wniosków o zmianę, analizę ryzyka i wpływu każdej zmiany, jej formalną akceptację przez uprawnione osoby oraz monitoring wdrożenia. Standardy IEC 62443 podkreślają dodatkowo znaczenie zarządzania zmianą w kontekście systemów przemysłowych – każda modyfikacja konfiguracji lub aktualizacja musi być przeprowadzona tak, by nie kompromitować bezpieczeństwa systemu. W środowiskach ICS/OT niekontrolowana zmiana może nie

tylko naruszyć bezpieczeństwo danych, ale też wpłynąć na proces technologiczny, dlatego wymagane są szczególnie rygorystyczne procedury.

Wdrożenie: kluczowym elementem jest ustanowienie sformalizowanego procesu *Request for Change* (RFC), czyli wniosku o zmianę. Każda proponowana zmiana (np. aktualizacja oprogramowania, zmiana konfiguracji sieci, wymiana urządzenia) powinna być zgłaszana poprzez RFC zawierający opis zmiany, cel, zakres, planowany termin, ocenę potencjalnego wpływu na bezpieczeństwo i działalność operacyjną oraz plan przywrócenia stanu poprzedniego (*rollback*) w razie problemów. Następnie wniosek jest analizowany pod kątem ryzyka i wpływu – zwykle przez właściciela systemu lub dedykowanego menedżera ds. zmian. Ocena obejmuje m.in. potencjalne skutki dla poufności, integralności, dostępności systemów oraz zgodności ze standardami i wymaganiami (np. czy zmiana nie naruszy istniejących polityk bezpieczeństwa lub czy dostawca zapewnia wsparcie). Dla systemów OT ocena powinna uwzględniać również wpływ na ciągłość procesu technologicznego i bezpieczeństwo fizyczne.

Po analizie ryzyk wniosek o zmianę trafia do etapu zatwierdzenia. Najlepiej, jeśli decyzję podejmuje komitet zmian (*Change Advisory Board*, CAB) złożony z przedstawicieli działu IT, OT, bezpieczeństwa i biznesu. W mniejszych organizacjach rolę tę może pełnić pojedynczy *change manager*, jednak nawet wtedy warto konsultować zmiany krytyczne z ekspertami bezpieczeństwa i właścicielami procesów. Każda zmiana powinna otrzymać status: zatwierdzona do wdrożenia, odrzucona lub wymagająca korekt/uzupełnień. Zatwierdzenie jest udokumentowane, np. podpisem cyfrowym pod wnioskiem lub zapisaniem decyzji w systemie zarządzania zmianami.

Kolejnym krokiem jest planowanie wdrożenia zmiany. Obejmuje to określenie terminu (najlepiej w oknie serwisowym, aby zminimalizować wpływ na użytkowników lub produkcję), wyznaczenie zespołu wdrożeniowego, przygotowanie listy kontrolnej działań oraz – kluczowe – przygotowanie planu przywrócenia w razie niepowodzenia. W środowisku ICS standardem jest wcześniejsze przetestowanie zmiany w warunkach testowych lub na urządzeniu zapasowym, zanim zostanie ona wprowadzona do systemu produkcyjnego. Na przykład, jeśli planowana jest aktualizacja oprogramowania sterownika PLC, najpierw wykonuje się testy na identycznym sterowniku w laboratorium. Taka ostrożność jest wymagana, ponieważ nieprzewidziany błąd po zmianie może zakłócić proces produkcyjny lub obniżyć poziom bezpieczeństwa.

Podczas samego wdrożenia należy zapewnić monitorowanie przebiegu zmiany. Po jej wprowadzeniu wykonywane są testy potwierdzające, że system działa poprawnie i że cele zmiany zostały osiągnięte (np. usunięto podatność, usprawniono wydajność) bez negatywnych skutków ubocznych. Jeśli cokolwiek pójdzie niezgodnie z planem, zespół wdrożeniowy powinien być gotowy do uruchomienia procedury wycofania zmian i przywrócenia poprzedniego stanu systemu.

Ważnym elementem jest także komunikacja – wszyscy interesariusze (administratorzy, użytkownicy, operatorzy OT, kierownictwo) powinni być poinformowani o planowanych pracach, potencjalnych przerwach w działaniu usług, a po wdrożeniu – o po-

myślnym zakończeniu lub ewentualnych problemach. Dobra komunikacja zwiększa akceptację zmian i pozwala użytkownikom przygotować się na ich skutki.

Na koniec procesu zaleca się przeprowadzenie przeglądu po wdrożeniu (*Post Implementation Review*), aby wyciągnąć wnioski: czy procedura zadziałała prawidłowo, czy ryzyka zostały właściwie ocenione, czy nie doszło do incydentów. Wnioski te pozwalają doskonalić proces. Dobrymi praktykami w zarządzaniu zmianą, wynikającymi z norm i standardów, są:

- kategoryzacja zmian – np. zmiany standardowe (rutynowe, niskiego ryzyka), zmiany istotne (wymagające pełnej procedury) oraz zmiany awaryjne. Dla każdej kategorii mogą obowiązywać nieco inne ścieżki akceptacji (np. zmiany awaryjne mogą być zatwierdzane szybciej, ale powinny potem przejść retrospektywny przegląd);
- minimalizacja ryzyka w OT – stosowanie zasad *Defense in Depth*, np. jeśli bezpośrednia zmiana w systemie ICS jest ryzykowna, rozważyć wdrożenie środków kompensujących (jak izolacja sieciowa lub wirtualne poprawki) do czasu możliwości bezpiecznego przeprowadzenia zmiany;
- dostosowanie do okoliczności – procedura powinna być proporcjonalna do skali zmiany i ryzyka. Zbyt biurokratyczny proces może zniechęcać do zgłaszania drobnych, lecz potrzebnych zmian; z kolei zbyt luźny – może przepuścić zmianę powodującą poważny incydent. Warto więc przewidzieć tryb przyspieszony dla zmian niskiego ryzyka oraz rygorystyczny nadzór nad zmianami krytycznymi;
- ścisła kontrola dostępu – tylko autoryzowany personel powinien móc inicjować i wdrażać zmiany. W systemach ICS zaleca się mechanizmy ograniczające wprowadzanie zmian konfiguracji tylko do zaufanych stacji roboczych i użytkowników (np. inżynierowie automatyk posiadający odpowiednie uprawnienia);
- audytowalność – wszystkie kroki procesu zmiany muszą być rejestrowane (kto i kiedy zatwierdził, co dokładnie zmodyfikowano). Centralny rejestr zmian pozwala na późniejsze śledzenie historii i jest wymagany podczas audytów zgodności z ISO 27001 czy kontrolami bezpieczeństwa.

Dobre zarządzanie zmianą przekłada się na stabilność i bezpieczeństwo środowiska IT/OT. Organizacja unika chaotycznych, niekontrolowanych modyfikacji, które mogłyby prowadzić do podatności lub awarii. Jednocześnie, dzięki sformalizowanemu procesowi, zmiany wspierające rozwój biznesu mogą być wdrażane szybciej i bezpieczniej, ponieważ ryzyka są zawczasu identyfikowane i adresowane.

1.2. Zarządzanie konfiguracją

Koncepcja: zarządzanie konfiguracją polega na utrzymaniu spójności i bezpieczeństwa ustawień systemów oraz możliwości śledzenia wszystkich modyfikacji konfiguracji. Innymi słowy, organizacja powinna dokładnie wiedzieć, jakie konfiguracje (ustawienia sprzętowe, programowe, sieciowe) obowiązują na poszczególnych urządzeniach i aplikacjach, i mieć pewność, że nie nastąpiły w nich nieautoryzowane lub niekontrolowane zmiany. Prawidłowo wdrożone zarządzanie konfiguracją pozwala m.in. wykryć, jeśli ktoś zmodyfikował konfigurację serwera czy sterownika przemy-