NASTĘPNE DZIAŁANIA NAPRAWCZE INCYDENT Z CZUJNIKIEM CHIYU WDROŻONE PRZEZ SOLAR-OT

Wdrożenie najnowszej wersji oprogramowania i wzmocnienie platformy

Nadzór SOLAR-OT

Autor	Zatwierdzone przez
Deirdre STARSKY, kierownik projektu technicznego	Elena PIZARI, dyrektor generalna Przemysł

CEL

W dokumencie tym określono 2 działania zaradcze po incydencie w systemach kontroli dostępu wdrożonych przez SOLAR-OT:

1. Awaryjne wdrożenie aktualizacji oprogramowania sprzętowego do wszystkich systemów
2. Wzmocnienie konfiguracji platformy nadzorczej

1. AWARYJNE WDROŻENIE AKTUALIZACJI OPROGRAMOWANIA

Producent CHIYU opracował aktualizację oprogramowania układowego dla systemów kontroli dostępu „SEMAC" korygującą lukę => musi ona zostać pilnie wdrożona przez SOLAR-OT we wszystkich lokalizacjach

Oto numer wersji oprogramowania sprzętowego, które ma zostać wdrożone w SEMAC S2 (67% floty): 670VYJLN

Oto numer wersji oprogramowania sprzętowego, które ma zostać wdrożone w SEMAC S3V3 (33% floty): 628AUYSD

2. WZMOCNIENIE KONFIGURACJI PLATFORMY NADZÓR

KONFIGURACJA

Celem jest ograniczenie elementów technicznych, które można wykorzystać do przeprowadzenia ataku, poprzez zainstalowanie jedynie niezbędnych usług i sprzętu.

Wzmocnienie poziomu bezpieczeństwa wymaga zaostrzeń obejmujących:

- Ograniczenie funkcji platformy
- Opanowanie elementów sprzętowych platformy

A. Modyfikacja konfiguracji domyślnej Każdy komponent

jest konfigurowany zgodnie ze standardami, w tym:

- Konta techniczne i powiązane elementy uwierzytelniające
- Używane porty sieciowe
- Katalogi instalacyjne i robocze
- Prawa dostępu do katalogów i plików
- Konto wykorzystywane do realizacji usługi lub procesu oraz uprawnienia związane z tym kontem
- Pliki konfiguracyjne elementów bezpieczeństwa, w szczególności identyfikowalności.

B. Ograniczenie dostępnych funkcjonalności

Konserwacji podlegają wyłącznie moduły niezbędne do działania i bezpieczeństwa platformy, które podlegają odpowiedniej konfiguracji, regularnej konserwacji i nadzorowi.

W związku z tym operator analizuje techniczne funkcjonowanie platformy, aby wykluczyć usługi lub funkcjonalności zainstalowane, ale nie wykorzystywane.

Każda konfiguracja sprzętu lub oprogramowania jest inwentaryzowana w formie konfiguracji referencyjnej.

C. Inwentaryzacja połączonych elementów

Operator dokonuje pełnej inwentaryzacji technicznej elementów składających się na platformę oraz je mapuje. Inwentarz obejmuje sprzęt, który można podłączyć do platformy na stałe lub tymczasowo, fizycznie lub zdalnie (stacja robocza, serwer, urządzenie peryferyjne itp.).

W przypadku, gdy z platformą połączy się osoba trzecia, operator odnotowuje to w swoim mapowaniu i uwzględnia w analizie ryzyka.

D. Stosowanie elementów kontrolowanych

Operator bezpośrednio zarządza elementami, m.in.:

- Wdrażanie aktualizacji
- Administracja elementami
- Zdalna konfiguracja

PODZIAŁ

Platforma kieruje się logiką segmentacji, ograniczając każdy podsystem do własnych działań, aby:

- Ogranicz powierzchnię ataku
- Powstrzymać możliwy atak
- Ogranicz wpływ kompromisu
- Umożliwia dostosowanie poziomu bezpieczeństwa każdego podsystemu

Podział na przedziały dotyczy zarówno środków fizycznych, jak i logicznych.

A. Segmentacja na podsystemy

Segmentacja na podsystemy odbywa się według następujących kryteriów:

- Cechy
- Poziom ochrony danych
- Poziom ekspozycji
- Poziom bezpieczeństwa

Każde połączenie pomiędzy podsystemami musi być uzasadnione potrzebą funkcjonalną.

B. Podział fizyczny

Serwer dedykowany jest dla najbardziej krytycznych aplikacji

C. Partycjonowanie logiczne

Wszelkie dane przechowywane na serwerze są wcześniej szyfrowane. Każdy podsystem wykorzystuje swój własny mechanizm szyfrowania.

Cała komunikacja między podsystemami przechodzi przez zaszyfrowaną i uwierzytelnioną wirtualną sieć prywatną.

ZDALNY DOSTĘP

A. Dostęp publiczny

Dostęp publiczny odbywa się za pośrednictwem protokołu HTTPS, a uwierzytelnianie platformy odbywa się poprzez przedstawienie certyfikatu serwer.

Dla użytkowników platformy zaimplementowano uwierzytelnianie dwuskładnikowe.

B. Dostęp nomadyczny

Nomadyczne stacje robocze są skonfigurowane tak, aby ustanawiały uwierzytelniony i szyfrowany tunel prowadzący do platformy. Tunelu nie można dezaktywować, a dostęp do Internetu lub sieci lokalnej jest niemożliwy.
Partycja systemowa i partycja danych są w pełni zaszyfrowane

Na stacji roboczej działa uwierzytelnianie dwuskładnikowe.

FILTROWANIE SIECI

Oprócz podziału na przedziały stosowane są mechanizmy filtrujące.

A. Filtruj punkty

Połączenia między podsystemami są głównymi punktami filtrowania, w stosunku do których stosowana jest filtracja obwodowa i lokalna.

B. Reguły filtrowania

Ogólna macierz przepływu zawiera obowiązujące reguły filtrowania. Jest aktualizowana corocznie.

C. Wdrożenie

Filtrowanie zapewniają dedykowane firewalle działające na zasadzie list autoryzacyjnych.