



Wymagania techniczne i organizacyjne dla SOC

www.smartech-it.eu

Aby zapewnić optymalne
funkcjonowanie SOC,
niezbędne jest spełnienie
krytycznych parametrów.

01.	Posiadać, utrzymywać i aktualizować system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi.	<input type="checkbox"/>
02.	Zapewnić ciągłość działania usłudze obsługi incydentu oraz wsparcie operatorowi usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej.	<input type="checkbox"/>
03.	Posiadać i udostępniać w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF).	<input type="checkbox"/>
04.	<p>Dysponować personelem posiadającym umiejętności:</p> <ul style="list-style-type: none"> a. identyfikowania zagrożeń w odniesieniu do systemów informacyjnych operatora usługi kluczowej oraz proponowania rozwiązań ograniczających ryzyko wynikające z tych zagrożeń b. analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej, c. wykrywania przełamania lub omińnięcia zabezpieczeń systemu informacyjnego operatora usługi kluczowej, d. przewodzenia analizy po włamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego operatora usługi kluczowej, 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
05.	Dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń.	<input type="checkbox"/>
06.	<p>Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo są obowiązane spełniać następujące warunki techniczne dysponować sprzętem komputerowym oraz wyspecjalizowanymi narzędziami informatycznymi umożliwiającymi:</p> <ul style="list-style-type: none"> a. rejestrowanie zgłoszeń incydentów, b. analizę kodu oprogramowania uznanego za szkodliwe, c. badanie odporności systemów informacyjnych na przełamanie lub omińnięcie zabezpieczeń, 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

- d. **zabezpieczanie informacji** potrzebnych do analizy po włamaniowej pozwalające na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej,
- e. **dysponować redundantnymi środkami łączności** umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi, oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

07

Zabezpieczenia pomieszczenia lub zespołu pomieszczeń adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej:

- a. **ściany i stropy pomieszczenia** lub zespołu pomieszczeń, w których będą świadczone usługi z zakresu cyberbezpieczeństwa, powinny mieć klasę **odporności ogniowej co najmniej EI 60**,
- b. **budynek**, w którym będą świadczone usługi z zakresu cyberbezpieczeństwa, powinien mieć **klasę odporności pożarowej nie niższą niż klasa B**,
- c. **drzwi do pomieszczenia** lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2, wyposażone w zamek spełniający co najmniej wymagania klasy 4,
- d. **konstrukcję pomieszczenia** lub zespołu pomieszczeń zapewniającą **odporność na próbę nieuprawnionego dostępu**;
- e. **system kontroli dostępu** obejmujący wszystkie wejścia i wyjścia kontrolowanego obszaru, w którym co najmniej rozpoznanie osoby uprawnionej następuje w wyniku odczytu **identyfikatora** lub odczytu **cech biometrycznych**, oraz rejestrujący zdarzenia;
- f. **system sygnalizacji napadu i włamania** spełniający co najmniej wymagania **systemu stopnia 2**, stale monitorowany przez personel bezpieczeństwa oraz wyposażony w rezerwowe źródło zasilania i obejmujący ochroną wejścia i wyjścia kontrolowanego obszaru oraz sygnalizujący co najmniej: otwarcie drzwi, okien i innych zamknięć chronionego obszaru, poruszanie się w chronionym obszarze, stan systemu, w tym generujący ostrzeżenia i alarmy;
- g. **System sygnalizacji pożarowej** obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, (obiekty wyposażone w stałe urządzenia gaśnicze i objęte całodobowym nadzorem co najmniej jednej osoby nie muszą być wyposażone w system sygnalizacji pożarowej).

08. **Monitorowanie i wykrywanie** incydentów bezpieczeństwa informacji.

09. **Reagowanie** na incydenty bezpieczeństwa.

10. **Zapobieganie** incydentom bezpieczeństwa informacji.

11. **Zarządzanie jakością zabezpieczeń** systemów, informacji i powierzonych aktywów.

12. **Aktualizowanie ryzyk** w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent.



Smartech IT Sp. z o.o., ul. Irysowa 1 (Business Point Bielany), 55-040 Bielany Wrocławskie
biuro@smartech-it.eu | +48 71 727 71 00 | www.smartech-it.eu