|  |  |
| --- | --- |
| **RODZAJ ZABEZPIECZENIA** | **PRZYKŁADY ZABEZPIECZEŃ** |
| Fizyczne | Strefy dostępu określające obszar, w którym przetwarzane są dane wrażliwe lub krytyczne |
| Fizyczne | Zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz, wejście kodowane, czytnik biometryczny itp.) |
| Fizyczne | Zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz, drzwi ognioodporne, drzwi antywłamaniowe itp.) |
| Fizyczne | Ochrona fizyczna obiektu i/lub pomieszczeń |
| Fizyczne | Systemy alarmowe / zabezpieczenia antywłamaniowe |
| Fizyczne | Monitoring wizyjny |
| Fizyczne | Zabezpieczenia dostępu do lokalu i pomieszczeń (drzwi zamykane na klucz, drzwi ognioodporne, drzwi antywłamaniowe itp.) |
| Fizyczne | Regularne wykonywanie i testowanie kopii informacji, oprogramowania i obrazów systemów zgodnie z procedurą kopi zapasowych |
| Fizyczne | Bezpieczne wycofywanie nośników - nośniki, które nie będą dalej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami |
| Fizyczne | Bezpieczne przekazywanie nośników - nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu |
| Fizyczne | Ograniczenie dostępu do pomieszczeń i sprzętu |
| Fizyczne | Zabezpieczenie dokumentacji w pomieszczeniach (zamknięte metalowe/niemetalowe szafy, sejf, skrytki itp.) |
| Fizyczne | Ekranowanie pomieszczeń |
| Fizyczne | Nadzór nad niewykorzystywanymi zakończeniami sieci LAN |
| Fizyczne | Nadzór nad niewykorzystywanymi zakończeniami sieci LAN (odłączenie niewykorzystanych zakończeń na krosownicach) |
| Fizyczne | prowadzenie okablowania sieciowego w zamkniętych kanałach, nadzór nad krosownicami |
| Fizyczne | Stosowanie światłowodów w miejsce połączeń galwanicznych |
| Organizacyjne | Polityka stosowania zabezpieczeń kryptograficznych |
| Organizacyjne | Polityka dotycząca korzystania, ochrony i okresów ważności kluczy kryptograficznych |
| Organizacyjne | Umowy na serwis i konserwację sprzętu w celu zapewnienia jego ciągłej dostępności i integralności |
| Organizacyjne | Nadawanie i nadzór nad udzielonymi zezwoleniami dotyczącymi wynoszenia poza Izbę sprzętu, informacji i programów |
| Organizacyjne | Polityka czystego biurka i ekranu |
| Organizacyjne | Procedury eksploatacyjne |
| Organizacyjne | Procedura kopii zapasowych |
| Organizacyjne | Zasady instalowania oprogramowania przez użytkowników |
| Organizacyjne | Klauzule w umowach dotyczących wszystkich usług sieciowych, zawierające zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania |
| Organizacyjne | Polityka przesyłania informacji, procedery i zabezpieczenia w celu ochrony wymiany informacji przesyłanych z użyciem wszystkich rodzajów środków łączności |
| Organizacyjne | Polityka bezpieczeństwa informacji - zatwierdzona przez prezesa, opublikowana i zakomunikowana pracownikom i właściwym stronom zewnętrznym |
| Organizacyjne | Przegląd polityk bezpieczeństwa informacji - przeglądy cykliczne oraz, gdy wystąpią istotne zmiany, w celu zapewnienia, że nadal są właściwe, adekwatne i skuteczne |
| Organizacyjne | Polityka stosowania urządzeń mobilnych |
| Organizacyjne | Warunki zatrudnienia - umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji |
| Organizacyjne | Szkolenia wstępne dla pracowników nowozatrudnionych |
| Organizacyjne | Okresowe szkolenia dla pracowników już zatrudnionych |
| Organizacyjne | Procedury zarządzania nośnikami wymiennymi |
| Organizacyjne | Polityka kontroli dostępu - ustanowiona, udokumentowana i poddawana cyklicznym przeglądom |
| Organizacyjne | Dostęp do sieci i usług sieciowych, tylko do zasobów, do których otrzymali wyraźne upoważnienie |
| Organizacyjne | Ograniczenie dostępu do informacji zgodnie z polityką kontroli dostępu |
| Organizacyjne | Procedura bezpiecznego logowania |
| Organizacyjne | Regulamin Ochrony Danych Osobowych dla pracowników i współpracowników |
| Organizacyjne | Outsourcing |
| Organizacyjne | Polityka kluczy (kontrola kluczy zapasowych, kontrola wydawania kluczy, kontrola przechowywania kluczy) |
| Organizacyjne | Procedura audytów |
| Organizacyjne | Procedura korzystania z zasobów sieci (poczta elektroniczna, Internet, …) |
| Organizacyjne | Procedura postepowania z nośnikami i sprzętem poza Izbą |
| Organizacyjne | Procedury nadawania i odbierania uprawnień |
| Organizacyjne | Procedury postępowania na wypadek wykrycia ataków DDoS/DoS |
| Organizacyjne | Procedury postępowania w przypadku wykrycia anomalii i sposoby dokumentowania takiego postępowania |
| Organizacyjne | Procedury przeglądania uprawnień w systemach |
| Organizacyjne | Procedury reagowania na wykrycie botnet w sieci Izby |
| Organizacyjne | Procedury reagowania na wykryte incydenty / Plan ciągłości działania |
| Organizacyjne | Procedury uaktualnienia oprogramowania (instalacja łat) |
| Organizacyjne | Rozpraszanie uprawnień (zasada "czterech par oczu") |
| Organizacyjne | Stosowanie zasady wiedzy koniecznej (need to know) |
| Organizacyjne | Umowy z dostawcami usługi dostępu do Internetu zawierające klauzule przenoszące działania przeciw atakowi na dostawcę |
| Organizacyjne | Zabezpieczenie odpowiednich środków finansowych zapewniających wymianę sprzętu (zgodnie z obowiązującą w Izbie strategią rozwoju informatyzacji) |
| Organizacyjne | Zapory sieciowe skonfigurowane według zasady "wszystko jest zabronione, z wyjątkiem tego na co wyrażono zgodę" |
| Personalne | Umowy serwisowe (powierzenia, SLA, kary umowne) |
| Personalne | Bezpieczeństwo informacji w zarządzaniu projektami - bezpieczeństwo informacji należy uwzględniać w każdym projekcie (obowiązkowa współpraca z IOD) |
| Personalne | Aktualizacja zakresów odpowiedzialności i obowiązków w zakresie bezpieczeństwa informacji |
| Personalne | Zwrot aktywów - wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa Izby |
| Personalne | Sformalizowany proces rejestrowania i wyrejestrowywania użytkowników |
| Personalne | Sformalizowany proces przydzielania dostępu użytkownikom do wszystkich systemów i usług |
| Personalne | Ograniczenie i nadzorowanie przyznawania praw uprzywilejowanego dostępu |
| Personalne | Sformalizowany proces przydzielania poufnych informacji uwierzytelniającymi użytkowników |
| Personalne | Przeglądy praw dostępu użytkowników, odbywające się regularnych odstępach czasu |
| Personalne | Odbieranie praw dostępu - wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni mieć odebrane wszystkie prawa dostępu |
| Techniczne | System kontroli dostępu (karty wejścia/wyjścia, czytniki biometryczne) |
| Techniczne | Monitoring środowiskowy (czujki wilgotności, pomiary temperatury, ...) |
| Techniczne | Systemy UPS i/lub agregaty prądotwórcze |
| Techniczne | Monitorowanie zużycia - systemy monitorujące stan usług i zasobów krytycznych, serwerów, baz danych i urządzeń technicznych, dla zapewnienia właściwej wydajności systemu |
| Techniczne | System przeciwpożarowy |
| Techniczne | System zarządzania hasłami - interaktywny i zapewniający wybór haseł dobrej jakości |
| Techniczne | Ograniczenie i nadzór nad wykorzystywaniem programów narzędziowych, umożliwiających obejście zabezpieczeń systemowych |
| Techniczne | Ograniczenie / uniemożliwienie dostępu do kodów źródłowych programów |
| Techniczne | Aktualizacje systemu |
| Techniczne | Analityczny system do wykrywania zagrożeń (SIEM) |
| Techniczne | Klimatyzacja |
| Techniczne | Redundancja krytycznych zasobów (macierz dyskowa RAID3, redundancja łącz, …) |
| Techniczne | Sondy IDS / IPS do ochrony dostępności do sieci komputerowej |
| Techniczne | System wykrywania słabości i podatności (skanery podatności) |
| Techniczne | Systemy do inwentaryzacji sprzętu, zarządzania licencjami, monitoring użytkowników |
| Techniczne | Systemy firewall, NG firewall, UTM |
| Techniczne | Szyfrowanie (poczty SSL, połączeń internetowych SSl/VPN, Pendrive, dysków komputerowych przenośnych (BitLocker), plików (7zip) itp. |
| Techniczne | Testy penetracyjne |
| Techniczne | Utwardzanie systemów (hardening) - kompleksowe działania zmierzające do optymalizacji działania i poprawy stanu zabezpieczeń systemów operacyjnych serwerów oraz urządzeń końcowych pracujących w infrastrukturze informatycznej |
| Techniczne | Wirtualizacja - uruchamianie wielu systemów operacyjnych na tej samej platformie sprzętowej i systemowej |
| Techniczne | Autoryzacja dostępu do serwera DHCP |
| Techniczne | Blokowanie możliwości instalowania oprogramowania przez użytkownika |
| Techniczne | Blokowanie portów USB na stacjach roboczych |
| Techniczne | Blokowanie ruchu sieciowego z określonych adresów IP |
| Techniczne | Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych i zdemilitaryzowanych (DMZ) |
| Techniczne | Monitorowanie ruchu sieci |
| Techniczne | Nadzór nad ruchem wychodzącym |
| Techniczne | Okresowe przeglądanie logów stacji roboczej przez administratorów |
| Techniczne | Oprogramowanie klasy AV na stacjach roboczych |
| Techniczne | Oprogramowanie klasy AV na styku sieci WAN z LAN |
| Techniczne | Przejście na statyczne wersje serwisu po wykryciu ataku typu DDoS/DoS |
| Techniczne | Serwery PROXY (w tym utrzymywanie czarnej listy adresów URL oraz adresów IP) |
| Techniczne | Stosowanie strefowania |
| Techniczne | Stosowanie techniki rozpraszania danych (CDN - conten delivery network) |
| Techniczne | Systemy klasy IDS/IPS |
| Techniczne | Translacja adresów sieciowych |
| Techniczne | Weryfikacja, czy na stacji roboczej znajduje się wyłącznie dopuszczalne oprogramowanie |
| Techniczne | Wykrycie nielegalnych działań ze strony użytkowników wewnętrznych systemu |
| Techniczne | Wykrywanie i blokowanie spamu |
| Techniczne | Rozliczalność operacji |