01.

Zasady konta użytkowników

W każdym systemie informatycznym, zasady kont użytkowników stanowią jeden z ważniejszych elementów bezpieczeństwa ochrony danych osobowych. Aby system IT był zgodny z RODO, należy wdrożyć wymagania:

- Każdy użytkownik systemu informatycznego (systemu operacyjnego, programu, CRM, itp.) powinien mieć indywidualny login i hasło, znane tylko danemu użytkownikowi.
- Hasła każdego użytkownika powinny być cyklicznie zmieniane.
- Hasła użytkowników, powinny spełniać wymagania co do złożoności.
- Hasła użytkowników powinny być przechowywane w sposób zaszyfrowany, bez względu czy są to hasła do systemu operacyjnego, bazy danych czy innego programu.
- Usunięte loginy (identyfikatory) nie powinny być ponownie użyte.
- Użytkownicy powinni wykonywać swoją pracę bez uprawnień administracyjnych danego systemu.

02.

Zasady komputera

Zgodność z RODO w informatyce, wymusza na administratorach komputerów osobistych lub serwerów konieczność spełnienia poniższych wymagań:

- Fizyczny dostęp do komputera powinien być tylko dla osób upoważnionych.
- Komputer powinien być zabezpieczony przed jego fizycznym otwarciem np. poprzez stosowanie plomb na obudowie.
- Każdy komputer czy serwer powinien mieć zablokowaną możliwość uruchamiania systemu z innego nośnika niż wewnętrzny dysk HDD.
- Użytkownicy powinni mieć zablokowaną możliwość uruchomienia BIOS.
- Uruchamiając dany system operacyjny, każdy użytkownik powinien przeczytać komunikat informujący o przetwarzaniu danych osobowych.
- Dyski systemu operacyjnego powinny być szyfrowane np. funkcją BitLocker lub aplikacją TrueCrypt.
- Każdy komputer powinien mieć indywidualny identyfikator w postaci adresu IP lub nazwy hosta.
- Pulpit każdego komputera powinien być zablokowany przed zmianą i powinien jednoznacznie identyfikować rodzaj systemu informatycznego, jeżeli w danej organizacji występuje wiele systemów (np. odrębnych sieci typu Intranet).
- Systematyczna instalacja aktualizacji krytycznych systemów operacyjnych oraz oprogramowania sieciowego.

03.

Ochrona antywirusowa

Ochrona antywirusowa stanowi podstawę bezpieczeństwa każdego systemu operacyjnego. W tym zakresie administrator IT powinien wdrożyć następujące procedury:

- Każdy system operacyjny powinien mieć wdrożony skuteczny system antywirusowy z aktualną definicją wirusów.
- Administrator Systemu Informatycznego powinien mieć możliwość zarządzania oprogramowaniem antywirusowym z tzw. konsoli z dostępem do informacji o aktualnych definicjach wirusów, historii skanowania, kwarantannach czy zainfekowanych komputerach.
- Zainfekowany komputer powinien być automatyczne odłączany od sieci informatycznej z automatycznym powiadomieniem administratora. poprzez wiadomość email, sms lub inne.
- ASI w dowolnym momencie powinien mieć dostęp do informacji o logach w zakresie ochrony antywirusowej.

04.

Firewall / UTM / IDS / IPS

Systemy takie jak Firewall oraz Intrusion detection system / Intrusion prevention system to kluczowe elementy bezpieczeństwa sieci informatycznej. Ich wdrożenie powinno następować zawsze przy każdym projekcie infrastruktury teleinformatycznej. Administrator Systemu Informatycznego powinien wdrożyć procedury, takie jak:

- Każdy system informatyczny powinien mieć uruchomiony firewall.
- Każda sieć komputerowa powinna mieć uruchomiony firewall sprzętowy np. Cisco ASA, FortiGate, Paloalto.
- W miarę możliwość budżetowych firmy, należy wdrożyć skuteczny system IDS / IPS.
- Do niezbędnego minimum należy ograniczyć ilość otwartych portów w ruchu sieciowym.
- Do niezbędnego minimum należy ograniczyć ilość usług sieciowych (wyłączenie nieużywanych funkcjonalności na routerze, serwerze).
- Do niezbędnego minimum należy ograniczyć sposoby dostępu do routera, firewall'a, serwera.
- ASI powinien być automatycznie informowany o każdorazowej próbie ataku lub włamania do sieci.
- Żądanie echa ICMP powinno być wyłączone na interfejsach WAN.
- Systematyczna aktualizacja firmware'u urządzeń sieciowych.

05.

Kopia zapasowa / backup danych

Zapasowe kopie informacji, oprogramowania i obrazów systemów, należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych. Administrator Systemu Informatycznego powinien spełniać poniższe wymagania w zakresie kopii bezpieczeństwa:

- Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym wglądem, przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
- Tworzenie kopii zapasowych danych oraz programów i narzędzi, należy dokonywać z częstotliwością umożliwiającą skuteczne odtworzenie danych po awarii SI.
- Nośniki zawierające kopie zapasowe, należy szyfrować, gdy opuszczają one obszar przetwarzania.
- ASI wykonuje backup danych zgodnie z przyjętym harmonogramem i na podstawie wcześniej przyjętej inwentaryzacji systemów danych.
- Systemy informatyczne muszą być także zdolne do szybkiego przywrócenia dostępu do danych osobowych na skutek awarii bądź próby ich przejęcia przez osoby do tego nieuprawnione.

06.

Urządzenia mobilne

Poniższe wymagania RODO w zakresie urządzeń mobilnych dotyczą komputerów przenośnych (laptopów), pendrive’ów, telefonów lub innych zewnętrznych pamięci.

- Każdy mobilny IND (informatyczny nośnik danych) powinien być szyfrowany, kiedy opuszcza miejsce przetwarzania – miejsce firmy.
- Dostęp do IND powinien być zapewniony tylko dla właściciela, poprzez wprowadzenie np. loginu i hasła, przykładowo funkcja BitLocker.
- Administrator systemu powinien prowadzić rejestr wydanych urządzeń mobilnych.
- Każdy komputer powinien blokować możliwość podłączenia nieautoryzowanego IND np. pendrive.
- Każdy IND powinien być obowiązkowo skanowany programem antywirusowym, przed jego uruchomieniem w systemie.

07.

Urządzenia sieciowe

Urządzenia sieciowe takie jak switch’e, czy drukarki, również powinny być skonfigurowane w bezpieczny sposób, aby siec informatyczna była w zgodności z RODO. Najważniejsze ustawienia, które powinny być wdrożone to:

- Każde urządzenie sieciowe powinno mieć jednoznaczny identyfikator sieciowy np. nazwa hosta i być zabezpieczone przed nieautoryzowanym dostępem z wykorzystaniem loginu i hasła.
- Sieć powinna być tak zabezpieczona, aby nie pozwalała na komunikację nieautoryzowanych urządzeń sieciowych np. switch’y.
- VLAN administracyjny powinien być odseparowany od VLAN’u roboczego.
- VLAN sieci przewodowej powinien być odseparowany od VLAN'u sieci bezprzewodowej.
- Każdy dział firmy powinien znajdować się w osobnym VLAN'ie.
- Routing na routerach brzegowych powinien być tak skonfigurowany i zabezpieczony, aby niemożliwe było wprowadzenie fałszywych tras i przekierowanie ruchu na zainfekowane urządzenie.
- Wydruki na drukarkach sieciowych zlokalizowanych w miejscach publicznych, powinien być zabezpieczony kodem PIN (druk następuje w momencie podejścia do drukarki i wprowadzeniu PIN).
- Systematyczna aktualizacja firmware'u urządzeń sieciowych.
- Sieć dla gościa powinna posiadać odpowiednie uprawnienia np. z wykorzystaniem ACL.

08.

Strony internetowe

Wymagania RODO dla stron internetowych również występują i są to:

- Połączenie ze stroną internetową, na której występują formularze do wypełnienia np. newsletter, formularz zamówienia, logowanie się, powinno być szyfrowane z wykorzystaniem protokołu SSL.
- Zaleca się, aby certyfikat SSL na stronie internetowej był klasy OV lub EV.
- Hasła użytkowników powinny być przechowywane w sposób zaszyfrowany.
- Na stronie internetowej powinna być polityka prywatności zawierająca zasady przetwarzania danych osobowych wraz z klauzulą informacyjną.
- Jeżeli strona internetowa wykorzystuje „ciasteczka”, należy umieścić politykę cookies.
- Pod każdym formularzem kontaktowym, należy umieścić informację o zasadach przetwarzania danych osobowych.
- Strona internetowa powinna zawierać punkt kontaktowy Inspektora Ochrony Danych.
- Jeżeli posiadasz sklep internetowy należy umieścić regulamin wraz z zasadami odstąpienia od umowy oraz zasadami obowiązku zapłaty za zamówienie.

- Wyrażenie zgody na przetwarzanie danych osobowych nie może być jednocześnie zgodą na przesyłanie niezamówionej informacji, np. działania marketingowe.

09.

Ochrona fizyczna

Wymagania RODO dla ochrony fizycznej sprzętu komputerowego:

- Każde urządzenie, które przetwarza dane osobowe powinno być zabezpieczone przed nieautoryzowanym dostępem np. pomieszczenie zamykane na klucz.
- Szafy „zgodne z RODO” zamykane na klucz nie są obowiązkowe. Wystarczy zabezpieczyć dokumenty przed nieautoryzowanym dostępem.
- Powinna być wdrożona procedura, uniemożliwiająca wyniesienie komputerów i urządzeń sieciowych ze strefy bezpieczeństwa.
- Dostęp do pomieszczeń w których przetwarzane są dane osobowe, powinien być rejestrowany, np. system kontroli dostępu lub książka wydawania kluczy.
- Jeżeli w firmie wykorzystywane są kamery, należy umieścić odpowiednią informację przed wejściem do strefy nagrań.

10.

Oprogramowanie

Zgodnie z zapisami RODO systemy informatyczne, które będą wykorzystywane do przechowywania danych osobowych powinny:

- Umożliwić wycofanie zgody udzielonej na przetwarzanie danych osobowych.
- Umożliwić sprostowanie danych przez osobę, której one dotyczą;
- Dać możliwość dostępu do nich osobie, której dotyczą.
- Systemy informatyczne powinny więc dawać możliwość znakowania, edytowania lub usuwania danych osobowych. Konieczne jest także sprawdzenie, czy system działa tak, że nie będzie możliwe dłuższe przechowywanie danych osobowych niż zakładają to przepisy RODO.