INFORAKADEMIA

Bezpieczeństwo przetwarzania danych w działach HR

Damian Gąska
Inżynier ds. bezpieczeństwa informacji, ODO24 Sp. z o.o.

Zmiany w zakresie zabezpieczania danych na gruncie RODO.

Jakie zmiany wprowadza RODO?

W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. (Motyw 83 RODO)

Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
(Artykuł 32 ust. 1 lit. b RODO)

Zakres tematyczny

- Bezpieczeństwo logowania do systemów informatycznych przetwarzających dane osobowe.
- Podstawowe zasady prawidłowego postępowania w systemach informatycznych.
- Bezpieczeństwo korzystania z poczty elektronicznej i Internetu.
- Podstawowe zasady bezpieczeństwa fizycznego.

Bezpieczeństwo logowania do systemów informatycznych przetwarzających dane osobowe

Jak stworzyć bezpieczne i łatwe do zapamiętania hasło?

- Łączenie kilka słów razem, które dodatkowo można oddzielać znakami specjalnymi np.
  moje*hasło*jest*bezpieczne
- Losowo zastępuj w wykorzystanych słowach małe litery dużymi np.
  Moje*Hasło*Jest*Bezpieczne
- Zastępuj popularne litery znakami specjalnymi np.
  Moje*H@sło*Jest*Bezpieczne
- Zastępuj popularne litery cyframi np.
  M0j3*H@sł0*J3st*B32p13czn3

Czy moje hasło może zostać złamane?

Popularne metody łamania haseł:

- metoda słownikowa,
- metoda brute force,
- keylogger.

Nie istnieją hasła w 100% bezpieczne ale ich długość, losowość i złożoność zniechęci większość przestępców!

Jak nie tworzyć haseł?

Unikaj budowania haseł:

- które mają w swojej budowie nazwę identyfikatora systemowego,
- których budowa wynika z ciągu znaków umieszczonych na klawiaturze np. **123qwerty**,
- o strukturze podobnej do haseł poprzednich np.
  moje*hasło*jest*bezpieczne082018,
  moje*hasło*jest*bezpieczne092018,
- wykorzystując znaki zmieniające się w zależności od daty lub innego przewidywalnego czynnika np.
  moje*hasło*jest*bezpieczne08,
  moje*hasło*jest*bezpieczne09,

Jak nie tworzyć haseł?

- wykorzystując w budowie imiona, nazwiska, numery telefonów, daty urodzenia lub inne proste skojarzenia.

Unikaj stosowania tych samych haseł w różnych systemach i aplikacjach!

Konfiguracja polityki kontroli dostępu

Zabezpieczenia, które warto wdrożyć w ramach podwyższenia bezpieczeństwa kontroli dostępu w systemach informatycznych:

- wymuszanie zmiany haseł tymczasowych,
- wymuszanie odpowiedniej jakości oraz częstotliwości zmiany haseł,
- zapamiętywanie określonej ilości ostatnio użytych haseł,
- konfiguracja minimalnego czasu życia hasła,

Konfiguracja polityki kontroli dostępu

- automatyczne blokowanie identyfikatora użytkownika w przypadku jego nieaktywności przez wskazany okres,
- blokowanie konta użytkownika w przypadku kilkukrotnej próby wprowadzenia błędnych poświadczeń.

Czy mogę pożyczyć swoje hasło?

Przekazanie hasła innemu pracownikowi celem udzielenia dostępu do danych np. na wypadek nieobecności.

Przekazanie hasła pracownikowi działu IT celem zrealizowania wsparcia technicznego.

Zawsze to użytkownik, właściciel konta ponosi pełną odpowiedzialność za czynności wykonywane w systemie informatycznym przy użyciu jego identyfikatora i hasła!

Czy mogę pożyczyć swoje hasło?

Pokusą dla użytkowników Internetu są serwisy, które po wprowadzeniu hasła sprawdzają czy nie zostało już ono skompromitowane. Jeśli skorzystałeś z tej usługi to Twoje hasło właśnie udostępniłeś atakującemu, który z pewnością z niego skorzysta!

Jak powinno wyglądać postępowanie w przypadku podejrzenia lub rzeczywistego ujawnienia hasła?

Czy muszę używać hasła?

Inne popularne mechanizmy uwierzytelniania:

- token,
- PIN, krótki odpowiednik hasła składający się z ciągu cyfr,
- czytnik linii papilarnych.

Czy muszę używać hasła?

Istnieją również mniej popularne metody uwierzytelniania np.:

- skan siatkówki oka,
- skan owalu twarzy,
- skan układu naczyń krwionośnych.

Niedopuszczalne jest korzystanie z urządzeń, systemów służących do przetwarzania danych organizacji bez skonfigurowania mechanizmu uwierzytelniania!

Podstawowe zasady prawidłowego postępowania w systemach informatycznych

Niebezpieczne smartfony/tablety?

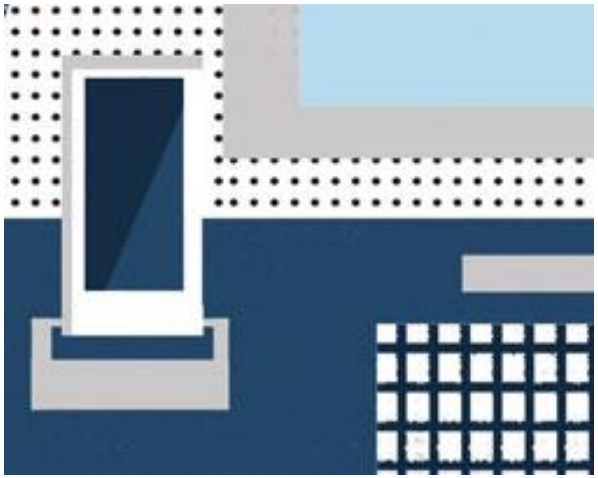
Jeżeli jesteś użytkownikiem takiego sprzętu pamiętaj o kilku podstawowych zasadach:

- zawsze stosuj blokadę urządzenia,
- zawsze stosuj szyfrowanie pamięci urządzenia oraz nośników zewnętrznych,
- nigdy nie pobieraj i nie instaluj oprogramowania bez nadzoru lub zgody działu IT,
- zawsze wyłączaj nieużywane usługi Wi-FI, GPRS, Bluetooth, NFC,
- zawsze stosuj oprogramowanie antywirusowe.

Niebezpieczne smartfony/tablety?

MDM (Mobile Device Management)

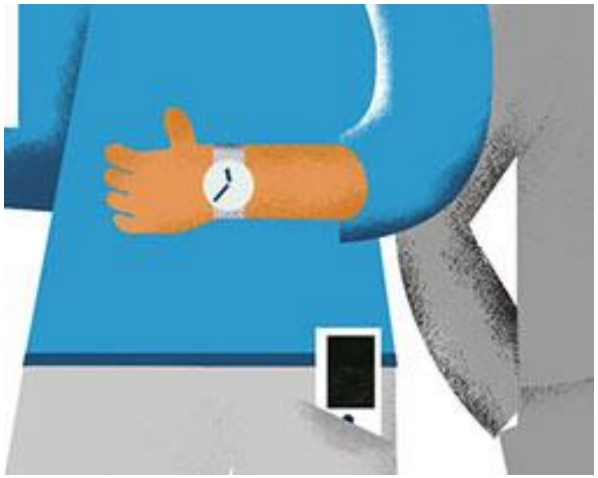
Jeżeli doszło do kradzieży, zgubienia urządzenia lub pojawiła się konieczność przekazania sprzętu do serwisu zawsze skonsultuj się w tej sprawie z działem IT.



Niebezpieczne nośniki danych?

- Prowadzenie rejestru nośników wymiennych.
- Monitorowanie informacji zapisywanych na nośnikach.
- Stosowanie technik kryptograficznych wobec nośników danych.
- Właściwy sposób utylizacji nośników.

Nigdy nie podłączaj do służbowego komputera urządzeń niewiadomego pochodzenia, w tym pendrive'ów „reklamowych" otrzymanych na konferencjach lub innych spotkaniach!



Czy mogę zainstalować dodatkowe oprogramowanie?

Tego typu zachowanie w szczególnych przypadkach może doprowadzić do:

- zainfekowania urządzenia złośliwym oprogramowaniem, które spowoduje wyciek danych lub ich zaszyfrowanie,
- nieprawidłowego działania systemu, w tym jego spowolnienia lub szkodliwego działania dla innych urządzeń korzystających z sieci Internet (tzw. DDOS),
- wysycanie, przeciążanie łącza Internetowego organizacji,
- naruszenia praw autorskich lub warunków licencyjnych.

Zasada czystego ekranu

Najprostszym i najszybszym sposobem zablokowania konta systemowego jest zastosowanie:

- kombinacji klawiszy **WIN+L**,
- kombinacji klawiszy **CTRL+ALT+DEL** oraz wybranie z wyświetlonego **MENU** przycisku **ZABLOKUJ**,
- wygaszacz ekranu.

Pamiętaj, że pozostawienie niezablokowanego komputera może ponieść za sobą takie same skutki jak wyciek Twojego hasła!

Pamiętaj, żeby zadbać o odpowiednie ustawienie ekranu komputera!

Zasada czystego pulpitu

Gdzie bezpiecznie przechowywać dokumenty w formie elektronicznej?

Zasada czystej drukarki

Jak w praktyce mam stosować zasadę czystej drukarki?

Przesyłanie skanów dokumentów lub danych organizacji w innej formie na zewnętrzne zasoby, w tym prywatne usługi poczty elektronicznej, portale społecznościowe, chmury obliczeniowe lub inne serwisy umożliwiające przechowywanie lub wymianę informacji jest SUROWO ZABRONIONE!

Zasady napraw urządzeń teleinformatycznych

- Naprawa realizowana przez lokalnego informatyka.
- Naprawa sprzętu realizowana przez informatyka zewnętrznej firmy w siedzibie organizacji.
- Naprawa sprzętu realizowana przez informatyka zewnętrznej firmy poza siedzibą organizacji.

Po odebraniu urządzenia z serwisu zewnętrznego po przeprowadzeniu konserwacji przed jego ponownym uruchomieniem w firmowej sieci należy skontrolować, czy sprzęt nie został zmanipulowany oraz nie realizuje szkodliwych funkcji.

Bezpieczeństwo korzystania z poczty elektronicznej i Internetu

Jak bezpiecznie korzystać z Internetu?

Jedną z podstawowych zasad bezpiecznego korzystania z Internetu jest każdorazowa weryfikacja obecności protokołu szyfrującego na przeglądanej stronie Internetowej.

Jak bezpiecznie korzystać z Internetu?

Dodatkowym, równie ważnym elementem jest dokładne zweryfikowanie adresu www.

Przyjrzyj się poniższym domenom internetowym!

https://allegro.pl	https://alleğro.pl
https://rnbak.pl	https://mbank.pl
https://pIay.pl	https://play.pl

Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

Jak bezpiecznie korzystać z poczty elektronicznej?

- Podczas wysyłania wiadomości poza organizację załączniki należy szyfrować lub zabezpieczać hasłem.
- Pamiętaj o stosowaniu kopii ukrytej, szczególnie w sytuacji kiedy realizujesz „masową” wysyłkę wiadomości.
- Nie należy otwierać załączników i linków od nieznanych adresatów.

Niezależnie od sytuacji o wszystkich przypadkach podejrzanych wiadomości informuj dział IT.

Podstawowe zasady bezpieczeństwa fizycznego

Polityka czystego biurka

Jak w praktyce mam stosować politykę czystego biurka?

Odpowiedni sposób przechowywania dokumentów to nie jedyna rzecz, o których powinieneś pamiętać. Równie ważne jest odpowiednie niszczenie takich danych. Do tego celu wykorzystuj tylko i wyłącznie niszczarki dokumentów lub specjalne pojemniki utylizacyjne, które zapewniła organizacja.

Czy dodatkowo powinienem zabezpieczyć pomieszczenie, w którym przetwarzam dane osobowe?

Bezpieczne archiwum dokumentów?

- Ilość osób posiadających uprawnienia dostępu do pomieszczenia.
- Sposób dostępu do pomieszczenia.
- Budowa pomieszczenia.
- System przeciwpożarowy.
- Sposób przechowywania dokumentów w archiwum.
- Sprzątanie.

Pamiętaj, że współpraca z podmiotem zewnętrznym, który świadczy usługę archiwizacji dokumentów lub też jej utylizacji wymaga zawarcia odpowiedniej umowy zawierającej zapisy dot. powierzenia przetwarzania danych osobowych oraz zachowania ich w poufności.

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

INFORAKADEMIA

Zapraszamy do zadawania pytań

WEBINARIUM DOSTĘPNE TAKŻE W

INFORLEX

INFORAKADEMIA

Bezpieczeństwo przetwarzania danych w działach HR

Damian Gąska
Inżynier ds. bezpieczeństwa informacji, ODO24 Sp. z o.o.