Praktyczny wymiar ochrony danych

Kwestie wizerunku i bezpieczeństwa

W TYM WYDANIU:

Włodzimierz Dola

Wizerunek osoby fizycznej – praktyczne aspekty korzystania z wizerunku na gruncie RODO i prawa autorskiego

Wizerunek definiowany jest w słowniku języka polskiego jako: (1) czyjaś podobizna na rysunku, obrazie, zdjęciu, itp. (2) sposób w jaki dana osoba lub rzecz jest postrzegana lub przedstawiana. W zakresie tego artykułu zajmiemy się praktycznymi aspektami wykorzystywania wizerunku w pierwszym rozumieniu definicji ze słownika języka polskiego, a mianowicie wizerunku rozumianego jako wyglądu zewnętrznego i innych cech indywidualizujących osobę fizyczną — takich jak twarz, sylwetka, sposób zachowania czy inne charakterystyczne elementy.

Stan prawny

Przepisy prawa nie zawierają legalnej definicji pojęcia wizerunku, jednakże jest kilka aktów prawnych, które chronią wizerunek osoby fizycznej. Do takowych możemy zaliczyć m.in. przepisy Kodeksu Cywilnego, RODO, czy Ustawy o prawie autorskim i prawach pokrewnych. Zgodnie z art. 23 Ustawy z dnia 23 kwietnia 1964 Kodeks Cywilny (dalej: Kodeks cywilny) wizerunek jest zaliczany do dóbr osobistych człowieka i pozostaje pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Z kolei zgodnie z art. 4 pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej; RODO) dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Z cytowanej definicji danych osobowych, a przede wszystkim z utrwalonego stanowiska doktryny i orzecznictwa w tym zakresie wiemy, że wizerunek stanowi dane osobowe, bowiem wizerunek pozwala rozpoznać osobę fizyczną i ją zindywidualizować. Art. 81 Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (dalej: Prawo autorskie), stanowi, że rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. Ustęp 2 cytowanego przepisu stanowi, z kolei, że zezwolenia nie wymaga rozpowszechnianie wizerunku: (1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności

politycznych, społecznych, zawodowych; (2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza. Wizerunek osoby fizycznej jest więc chroniony na podstawie co najmniej 3 aktów prawnych: jako dobro osobiste – na podstawie kodeksu cywilnego, jako dane osobowe na podstawie RODO oraz na podstawie Prawa autorskiego.

Uwagi ogólne

Przedsiębiorca prowadząc działalność gospodarczą może mieć do czynienia m.in. z następującymi kategoriami osób, których wizerunek może być przez niego przetwarzany: kandydaci, pracownicy (szeroko rozumiani również jako zatrudnieni np. na podstawie umów cywilnoprawnych), klienci, kontrahenci, osoby, które zarejestruje monitoring wizyjny, osoby uczestniczące w aktywnościach organizowanych przez przedsiębiorcę (np. eventach, akcjach marketingowych, sesjach zdjęciowych, etc.).

Warto, aby w każdej firmie funkcjonowały zasady wykorzystywania wizerunku, najlepiej w formie wewnętrznej regulacji lub w innej formie informacyjnej – np. informacji wewnętrznych czy dobrych praktyk. W zakresie zgodności z RODO w niniejszej publikacji skupię się przede wszystkim na kwestiach legitymowania się podstawą prawną i treści obowiązków informacyjnych, natomiast w zakresie Prawa autorskiego nad formami pozyskania zgody z art. 81 Prawa Autorskiego.

RODO

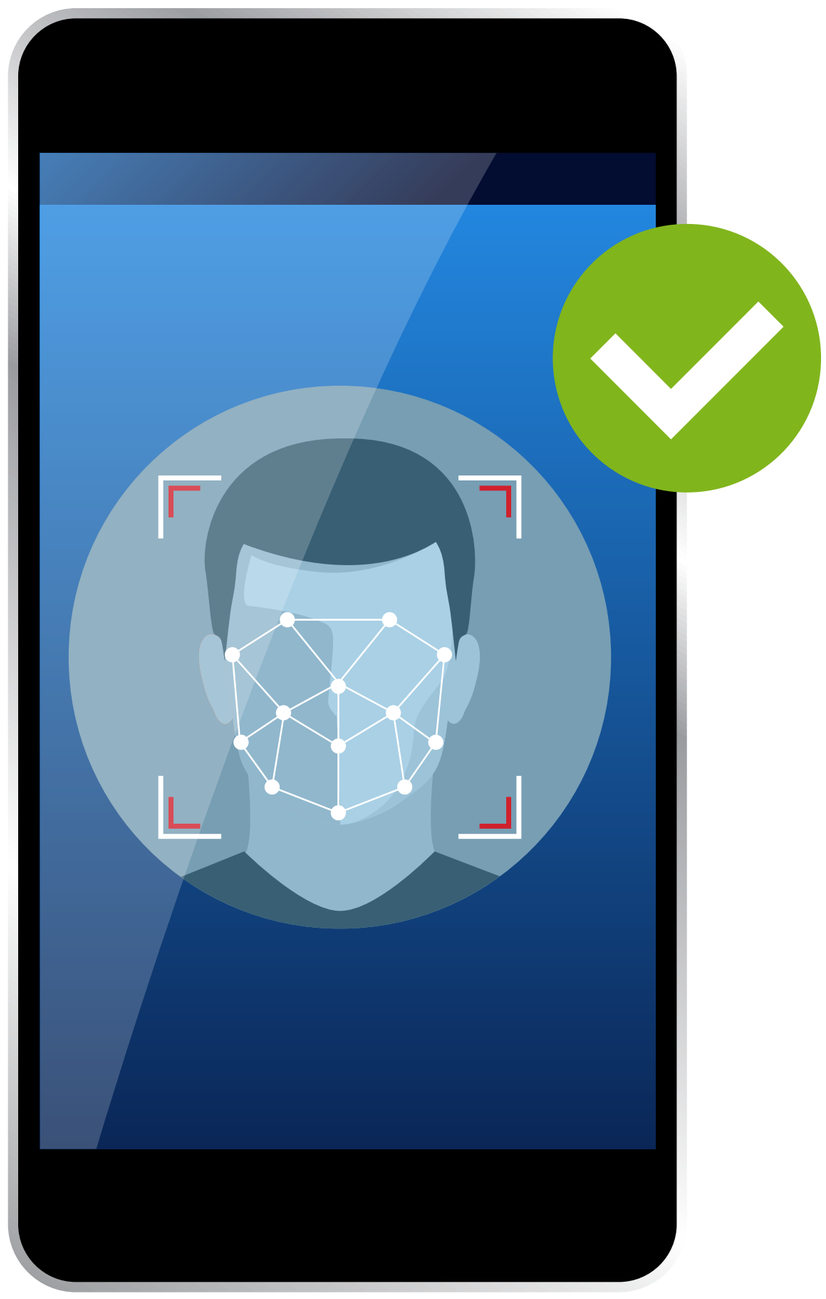
Podstawami prawnymi pozwalającymi na przetwarzanie danych osobowych w postaci wizerunku mogą być: art. 6 ust. 1 lit. a RODO (zgoda), art. 6 ust. 1 lit. b RODO (umowa), art. 6 ust. 1 lit. f RODO (prawnie usprawiedliwiony interes administratora danych). Wybór podstawy zależy od stanu faktycznego oraz możliwości jakie dają nam przepisy prawa. W zakresie kandydatów do pracy z wizerunkiem osoby fizycznej zetkniemy się najprawdopodobniej na etapie rekrutacji, bowiem to kandydaci często zamieszczają zdjęcie w CV. Sami jako potencjalny pracodawca nie mamy prawa na podstawie kodeksu pracy lub innych przepisów żądać tego typu informacji, jednakże kandydat sam je może przekazać, a my je przetwarzamy. W takiej sytuacji podstawą przetwarzania danych osobowych w postaci wizerunku będą albo zgoda (np. na prowadzenie przyszłych procesów rekrutacyjnych) albo prawnie usprawiedliwiony interes (w związku z bieżącą rekrutacją). W okresie zatrudnienia wizerunek pracownika może być przetwarzany przez pracodawcę w wielu sytuacjach w tym m.in.: w celach związanych z dostępem do biura lub zakładu – na identyfikatorach (kartach dostępu), na monitoringu wizyjnym, w relacjach wewnętrznych z wydarzeń firmowych (np. w artykule w intranecie), w relacjach wewnętrznych z targów lub konferencji, w których dany pracownik reprezentuje firmę, itp.

W wielu przypadkach podstawą przetwarzania danych osobowych może być prawnie usprawiedliwiony interes administratora danych. W związku z przetwarzaniem danych osobowych w oparciu o prawnie usprawiedliwiony interes administratora danych w zakresie obowiązków dotyczących ochrony danych osobowych należy pamiętać o tym, że musimy być w stanie wykazać, że: przetwarzanie danych osobowych we wskazanym celu jest **niezbędne, konieczne i proporcjonalne** do tego celu; interesy lub podstawowe prawa i wolności osób, których dane dotyczą nie mają charakteru nadrzędnego nad interesami administratora lub strony trzeciej. Aby powyższe wykazać, przed rozpoczęciem przetwarzania jesteśmy zobowiązani do przeprowadzenia testu równowagi prawnie usprawiedliwionego interesu dla każdego z celów przetwarzania.

Są jednak sytuacje, w których pracodawca będzie zobowiązany do skorzystania ze zgody jako podstawy przetwarzania. Zgodnie z art. 4 pkt. 11) RODO pojęcie zgody osoby, której dane dotyczą oznacza **dobrowolne, konkretne, świadome i jednoznaczne** okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. W tym miejscu chciałbym zwrócić szczególną uwagę na atrybuty zgody, czyli jej dobrowolność, konkretność, świadomość i jednoznaczność. Dobrowolność należy rozumieć jako brak przymusu i możliwość odmowy wyrażenia zgody – jest to szczególne istotne w relacjach pracodawca – pracownik, gdzie istnieje brak równowagi między stronami.

Konkretność oznacza, iż zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach, natomiast jeżeli przetwarzanie służy różnym celom, potrzebna jest osobna zgoda na wszystkie te cele. Świadomość z kolei zakłada, że osoba jest poinformowana i powinna zdawać sobie sprawę z konsekwencji swojego działania. Jednoznaczność oznacza natomiast, że przyzwolenie na przetwarzanie danych nie może budzić wątpliwości co do zamiaru osoby, która takie działanie podejmuje.

Właściwa konstrukcja zgody pracownika ma więc kluczowe znaczenie dla legitymowania się nią jako właściwą podstawą przetwarzania. Do sytuacji, gdzie zgoda może być podstawą przetwarzania należy zaliczyć – np. wykorzystywanie wizerunku pracownika w związku z publikacjami zewnętrznymi (np. na portalach lub w prasie, gdzie zamieszczany jest wizerunek pracownika i jego wypowiedź) czy na stronie internetowej pracodawcy (relacja z wydarzenia firmowego, zaangażowania firmy w targi konferencje, etc.), na folderach reklamowych firmy, itp.



Ostatnia ze wskazanych podstaw przetwarzania wizerunku czyli Umowa może mieć miejsce przykładowo w sytuacji, gdy druga strona dostaje wynagrodzenie za użyczenie swojego wizerunku – np. firma tworzy foldery reklamowe lub materiały video, które następnie będą rozpowszechniane w celach marketingowych. Taka umowa może być zawarta zarówno z pracownikiem, jak i z osobą trzecią – np. modelem/aktorem.

Ważnym obowiązkiem w zakresie ochrony danych osobowych jest spełnienie tzw. obowiązku informacyjnego uregulowanego w art. 13 lub 14 RODO. Przepisy te, w zależności od sposobu pozyskania danych osobowych, tj. w zależności od tego czy administrator pozyskał dane bezpośrednio od osób, których dane dotyczą, czy pośrednio, oprócz legitymowania się podstawą prawną przetwarzania danych osobowych obowiązany jest do przekazania osobie, której wizerunek jest przetwarzany informacji wymienionych w ww. przepisach. Stosownie do art. 13 lub 14 RODO osoba, której wizerunek jest przetwarzany powinna zostać poinformowana m.in. o tym kto jest administratorem danych, jak można się z administratorem i Inspektorem Ochrony Danych (jeśli jest powołany) skontaktować, jakie są cele i podstawy przetwarzania danych osobowych, informacji o sposobie pozyskania danych osobowych, informacji o przysługujących prawach, informacja o odbiorcach danych, a także o ewentualnym transferze danych do państw trzecich i zautomatyzowanym podejmowaniu decyzji. RODO nie precyzuje, w jakiej formie Administrator danych powinien przekazywać osobie, której dotyczą dane, informacje dotyczące o przetwarzaniu jej danych. Należy jednak pamiętać o zasadzie rozliczalności — tzn. Administrator powinien spełnić obowiązek w taki sposób, żeby być w stanie wykazać i potwierdzić, że dopełnił ciążącego na nim obowiązku informacyjnego. W zakresie wizerunku jako danych osobowych najważniejszym praktycznym elementem obowiązku informacyjnego jest prawidłowe opisanie celów i podstaw przetwarzania danych osobowych, aby dla osoby, której dane dotyczą było jasne, co się dzieje w tym aspekcie z jej danymi osobowymi.

Prawo autorskie

Jak zostało wyżej wspomniane, wizerunek jest chroniony na mocy Prawa autorskiego i co do zasady jego rozpowszechnianie wymaga zgody. Ustawa przewiduje wyjątki, a mianowicie – pierwszy związany z wykorzystywaniem wizerunku osoby powszechnie znanej w związku z wykonywaniem przez nią różnych funkcji. Wśród wymienionych funkcji są wymienione m.in. funkcje zawodowe. W związku z powyższym w mojej opinii, wykorzystywanie wizerunku osób wypowiadających się publicznie w imieniu przedsiębiorcy, nie wymaga zgody na rozpowszechnianie wizerunku regulowanej prawem autorskim, dotyczyć to będzie w szczególności osób reprezentujących firmę, czy rzecznika prasowego. Jednakże musi istnieć związek pomiędzy rozpowszechnianiem wizerunku, a pełnioną funkcja. Nie można bez zgody rozpowszechniać wizerunku takich osób z życia prywatnego, np. urlopu. Drugim wyjątkiem jest sytuacja, kiedy wizerunek stanowi szczegół większej całości. Taka sytuacja może mieć miejsce gdy wizerunek danej osoby znajduje się na zdjęciach z wydarzeń publicznych – np. zgromadzeń lub otwartych eventów. Stosowanie do wyroku Sądu Apelacyjnego w Warszawie z dnia 10 lutego 2005 r. (sygn. akt I ACa 509/04) gdy wizerunek stanowi jedynie szczegół, element „akcydentalny lub akcesoryjny" przedstawionej całości zgromadzenia, rozpowszechnianie wizerunku nie będzie wymagało zezwolenia. W takiej sytuacji wizerunek osoby stanowi rzeczywiście jedynie przypadkowy element, a usunięcie jej wizerunku w żaden istotny sposób nie wpływa i nie zmienia charakteru wydarzenia ani też sposobu przedstawienia jego problematyki. Trzecim wyjątkiem jest sytuacja gdy za osoba udostępniająca wizerunek otrzymała wynagrodzenie za pozowanie.

Warto w tym miejscu zwrócić uwagę na kwestie tego, kiedy dochodzi do rozpowszechniania, a ma to miejsce w sytuacji gdy rozpowszechnianie zakłada udostępnianie wizerunku do nieokreślonej grupy osób. W związku z powyższym rozpowszechnianie wizerunku nie będzie obejmowała sytuacja, gdy dochodzi do publikacji wizerunków w wewnętrznym

systemie firmowym (np. zamieszczenie zdjęć z wyjazdu integracyjnego w intranecie). Sytuacja wyglądałaby inaczej, gdyby zdjęcia z wyjazdu integracyjnego miały być umieszczone na ogólnodostępnej stronie internetowej lub w mediach społecznościowych.

W zakresie przepisów Prawa autorskiego odnieść należy się również do zgody w rozumieniu tych przepisów. Prawo autorskie nie wskazuje formy udzielenia zgody i nie odsyła w tym zakresie do definicji zgody z RODO. Przedsiębiorca powinien przygotować taki wzór zgody, który nie będzie budzić wątpliwości. Zgoda na wykorzystanie wizerunku powinna zostać skonkretyzowana co do pól eksploatacji wizerunku. Osoba przedstawiona powinna wiedzieć o miejscu, czasie i częstotliwości udostępniania podobizny. Oznacza to, że w treści zgody powinniśmy określić szczegółowo w jakich miejscach planujemy rozpowszechnianie wizerunku na przykład: strona www, firmowe media społecznościowe, materiały reklamowe dla klientów. W przeciwieństwie do zgody jako podstawy danych osobowych do przetwarzania wynikającej z RODO, zgoda na rozpowszechnianie wizerunku może być elementem umowy pomiędzy stronami.

Podsumowanie

Wizerunek osoby fizycznej jest chroniony prawnie przez kilka aktów prawnych. Gdy chcemy korzystać z czyjegoś wizerunku należy spełnić wymagania zarówno RODO, jak i Prawa autorskiego, jednocześnie pamiętając, że wizerunek stanowi dobra osobiste, których naruszenie może się wiązać z potencjalną odpowiedzialności. Zajmując się aspektami związanymi z wykorzystywaniem czyjegoś wizerunku należy pamiętać o licznych obowiązkach wynikających z przepisów prawa. Jako najważniejsze należy wymienić: legitymowanie się podstawą przetwarzania danych osobowych, spełnienie obowiązku informacyjnego, zapewnienie realizacji praw osób fizycznych, legitymowanie się zgodą na rozpowszechnianiem wizerunku lub korzystanie z jednego z wyjątków niewymagających takiej zgody.

Patrycja Żarska Cynk

Cykl Czy Twój system ochrony danych ma solidne fundamenty?

Polityka haseł - elementarz higieny cyfrowej

Ochrona aktywności online stała się aktualnie kwestią najwyższej wagi w cyfrowym świecie. Według jednego z licznych raportów [1], w 2024 roku firmy coraz częściej korzystają z zaawansowanych metod uwierzytelniania:

1. uwierzytelnianie wieloskładnikowe (MFA) - aż 83% organizacji wymaga stosowania MFA do dostępu do zasobów firmowych
2. logowanie biometryczne - 66% firm wykorzystuje biometrię (np. odciski palców, rozpoznawanie twarzy) jako jeden z czynników uwierzytelniania
3. logowanie bezhasłowe - coraz więcej organizacji przechodzi na metody uwierzytelniania bez użycia haseł, takie jak klucze dostępu czy linki jednorazowe
4. adaptacyjne uwierzytelnianie - systemy analizujące kontekst logowania i dostosowujące poziom zabezpieczeń do ocenionego ryzyka
5. Single Sign-On (SSO) - rozwiązania umożliwiające dostęp do wielu systemów za pomocą jednego logowania.

Mimo to, tradycyjne logowanie za pomocą hasła wciąż jest stosowane w 83% organizacji dla niektórych zasobów.

Hasła są często pierwszą linią obrony przed nieautoryzowanym dostępem; im silniejsze hasło, tym bardziej chronione będą wrażliwe dane. Ochrona hasłem to rodzaj kontroli dostępu, który pomaga chronić wrażliwe i ważne dane przed cyberatakami, kradzieżą tożsamości, naruszeniami danych osobowych i nie tylko. Zapewniając, że tylko właściwa osoba z odpowiednimi poświadczeniami może uzyskać dostęp do tych informacji, można znacznie zmniejszyć ryzyko cyberataku lub naruszenia danych. Silne zasady dotyczące haseł mogą również pomóc w spełnieniu zgodności z przepisami prawa - patrz kontekst RODO czy NIS2.

Niniejszy artykuł podkreśla znaczenie odpowiedniego zarządzania hasłami, w tym ich szyfrowania, stosowania odpowiedniej długości i złożoności haseł, oraz wdrażania skutecznych

1 2024 Multi-Factor Authentication (MFA) Statistics & Trends to Know
https://jumpcloud.com/blog/multi-factor-authentication-statistics

środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych.

Dlaczego właściwe zarządzanie hasłami jest w interesie każdego podmiotu, także z perspektywy obowiązków wynikających z RODO?

Skutki nieodpowiedniego zarządzania hasłami, braku polityki i edukacji personelu w tym obszarze mogą być katastrofalne dla firmy:

- zwiększone ryzyko włamania - słabe hasła są łatwe do złamania, a brak MFA [2] ułatwia nieautoryzowany dostęp
- utrata danych - w wyniku włamania może dojść do wycieku poufnych informacji firmowych
- straty finansowe - zarówno bezpośrednie (np. kradzież środków) jak i pośrednie (koszty naprawy szkód)
- zakłócenia w działalności - ataki mogą prowadzić do przestojów w pracy i utraty produktywności
- utrata reputacji - incydenty bezpieczeństwa mogą negatywnie wpłynąć na wizerunek firmy
- naruszenie prywatności - wyciek danych osobowych pracowników lub klientów może prowadzić do poważnych konsekwencji prawnych i roszczeń cywilnych
7. sankcje prawne - nieprzestrzeganie wymogów bezpieczeństwa może skutkować karami finansowymi - kara pieniężna, która może dotknąć organizację przy stwierdzeniu naruszeń RODO - do 20 mln EUR lub 4% rocznego obrotu.

Dla zobrazowania problemu przytaczamy decyzje Prezesa Urzędu Ochrony Danych Osobowych. Dotyczą innego obszaru obowiązków, ale każda związana jest ze skutecznym przełamaniem zabezpieczeń systemu informatycznego:

Decyzja wobec drobnego przedsiębiorcy prowadzącego działalność jednoosobową [3]**:**

Dotyczyła naruszenia ochrony danych osobowych polegającego na niezgłoszeniu Prezesowi Urzędu Ochrony Danych Osobowych naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia oraz niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą. W wyniku przełamania zabezpieczeń systemu doszło do przestępstwa kradzieży dokumentów z pulpitu laptopa - dokumenty przechowywane na pulpicie zawierały dane klientów, tj.: Imię, nazwisko, niekiedy adresy zamieszkania, adresy e-mail, nr telefonów a także sporadycznie nr PESEL. Nałożono karę pieniężną **11 790 PLN**.

2 Uwierzytelnianie wieloskładnikowe (ang. Multi-Factor Authentication – MFA)

3 Decyzje Prezesa UODO
https://uodo.gov.pl/decyzje/DKN.5131.43.2022

Decyzja wobec American Heart of Poland SA [4]**:**

Organ stwierdził naruszenie polegające na niewdrożeniu:

1. Odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą, na podstawie przeprowadzonej analizy ryzyka uwzględniającej stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych,

2. Odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia skutkującym, naruszeniem zasady integralności i poufności oraz zasady rozliczalności,

Zdarzenie polegało na przełamaniu zabezpieczeń systemu informatycznego Spółki w wyniku czego nieuprawnione osoby uzyskały dostęp do danych pacjentów i pracowników spółki. Zdarzenie objęło szeroki zakres danych, tj.: nazwisko, imię, imiona rodziców, nazwisko rodowe matki, datę urodzenia, dane dotyczące zarobków lub posiadanego majątku, dane dotyczące zdrowia, numer rachunku bankowego, adres zamieszkania lub pobytu, numer PESEL, nazwę użytkownika lub hasło, serię i numer dowodu osobistego, numer telefonu oraz adres e-mail. O wycieku danych spółka dowiedziała się od hakerów, którzy zażądali 3 mln dolarów okupu za nieujawnienie przechwyconych danych.

— Spółka nie wdrożyła wszystkich niezbędnych środków służących ochronie przetwarzanych przez nią danych, a ponadto nie była w stanie ustalić przyczyny wycieku. Wśród licznych zarzutów padły też te, iż Spółka niewłaściwie chroniła się przed atakami „phishingowymi", polegającymi na podszywaniu się osoby atakującej system pod inny podmiot (osobę). Według ustaleń Prezesa UODO, z dużym prawdopodobieństwem właśnie w taki sposób hakerzy dostali się do systemu informatycznego. Spółka założyła, że poziom bezpieczeństwa przetwarzanych przez nią danych jest właściwy, tylko na podstawie przeprowadzonego w niej wewnętrznego audytu, którego celem było przedłużenie ważności certyfikatu ISO/IEC 27001:2013, działała w błędnym przeświadczeniu, że ww. ryzyka są na poziomie jedynie małym lub, co najwyżej, średnim. Nałożono karę pieniężną **1 440 549,00 PLN**.

4 Decyzje Prezesa UODO
https://www.uodo.gov.pl/decyzje/DKN.5112.35.2021

Decyzja wobec anonimowej Spółki Akcyjnej [5]**:**

Organ stwierdził naruszenie polegające na doborze nieskutecznych zabezpieczeń systemu informatycznego oraz braku odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych objętych naruszeniem, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia.

Zdarzenie polegało na przełamaniu zabezpieczeń systemu informatycznego Spółki wykorzystywanego przez nią do przetwarzania danych osobowych, a następnie zaszyfrowaniu przetwarzanych w nim danych. W konsekwencji Spółka została pozbawiona dostępu do ww. systemu oraz znajdujących się w nim danych osobowych. Spółka określiła skalę powstałego naruszenia, która wykazała, że zaszyfrowane bazy danych obejmowały około 80 000 rekordów danych pracowników, klientów oraz pacjentów w zakresie imienia i nazwiska, imion rodziców, daty urodzenia, numeru rachunku bankowego, adresu zamieszkania, numeru PESEL, adresu e-mail, serii i numeru dowodu osobistego, numeru telefonu oraz danych dotyczące zdrowia. **Zastosowano upomnienie wobec spółki.**

Ta ostatnia decyzja jest efektem dalszego postępowania Spółki, która przeprowadziła ocenę środków technicznych w zakresie infrastruktury IT, m.in. **zwiększyła restrykcje na stacjach roboczych oraz w zakresie polityki haseł** oraz rozszerzono politykę tworzenia kopii zapasowych - zastosowano też inne środki bezpieczeństwa dążąc do minimalizacji ryzyka wystąpienia podobnego zdarzenia w przyszłości.

Na podstawie dostępnych informacji, można wyróżnić kilka najczęstszych naruszeń bezpieczeństwa haseł w firmach technologicznych [6]:

Przechowywanie haseł w formie niezaszyfrowanej

Jednym z najpoważniejszych naruszeń jest przechowywanie haseł użytkowników w formie zwykłego tekstu, bez odpowiedniego szyfrowania. Przykładem jest przypadek Meta (Facebook), gdzie setki milionów haseł użytkowników były przechowywane w niezaszyfrowanej formie na wewnętrznych serwerach firmy. Za to naruszenie Meta została ukarana grzywną w wysokości 91 milionów euro przez irlandzką Komisję Ochrony Danych [7].

Używanie słabych haseł

Pracownicy często używają prostych, łatwych do odgadnięcia haseł, takich jak "123456", "password" czy "qwerty". To znacząco zwiększa ryzyko nieautoryzowanego dostępu do systemów.

Wielokrotne używanie tych samych haseł

Pracownicy często używają tego samego hasła do wielu różnych kont i systemów. W przypadku naruszenia jednego konta, wszystkie pozostałe stają się zagrożone.

5 Decyzje Prezesa UODO
https://uodo.gov.pl/decyzje/DKN.5130.2815.2020

6 Przewodnik dotyczący polityki haseł w firmie
https://www.politykabezpieczenstwa.pl/pl/a/przewodnik-dotyczacy-polityki-hasel-w-firmie

7 Ireland Data Protection Commission fines Meta €91M over improper password storage
https://www.jurist.org/news/2024/09/ireland-data-protection-commission-fines-meta-e91m-over-breach/

Udostępnianie haseł

Dzielenie się hasłami między pracownikami, nawet w obrębie zespołu, zwiększa ryzyko nieautoryzowanego dostępu.

Brak regularnej zmiany haseł

Chociaż nie zawsze jest konieczna regularna zmiana haseł, wiele firm nie wymaga od pracowników aktualizacji haseł nawet w przypadku podejrzenia naruszenia bezpieczeństwa.

Zapisywanie haseł w niezabezpieczonych miejscach

Pracownicy często zapisują hasła na kartkach przyklejonych do monitorów lub w niezaszyfrowanych plikach na komputerach.

Niewystarczające zabezpieczenia techniczne

Firmy czasem nie wdrażają odpowiednich środków technicznych do ochrony haseł, takich jak szyfrowanie, haszowanie czy solenie (techniki kryptograficzne).

Brak powiadomień o naruszeniach

Niektóre firmy nie informują odpowiednich organów o naruszeniach bezpieczeństwa danych, co jest naruszeniem przepisów RODO.

Niewystarczające szkolenia z zakresu bezpieczeństwa

Wiele firm nie zapewnia pracownikom odpowiednich szkoleń na temat tworzenia i zarządzania bezpiecznymi hasłami.

Brak wdrożenia uwierzytelniania wieloskładnikowego

Wiele firm nie wymaga lub nie zachęca do korzystania z uwierzytelniania dwuskładnikowego lub wieloskładnikowego, co znacznie zwiększyłoby bezpieczeństwo kont.

Aby przeciwdziałać tym naruszeniom, organizacje powinny wdrażać kompleksowe polityki bezpieczeństwa haseł, zapewniać regularne szkolenia dla pracowników, stosować zaawansowane metody szyfrowania i zachęcać do korzystania z menedżerów haseł oraz uwierzytelniania wieloskładnikowego.

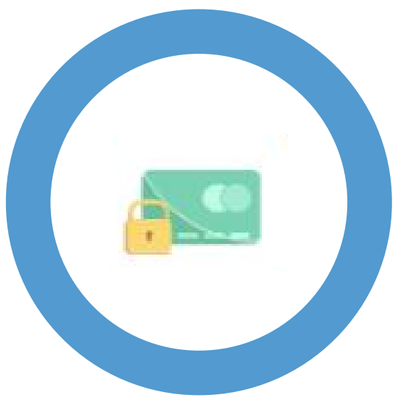
Oto kiedy twoje hasło zostałoby złamane, gdyby...

Dzisiaj

...miało 8 znaków lub mniej

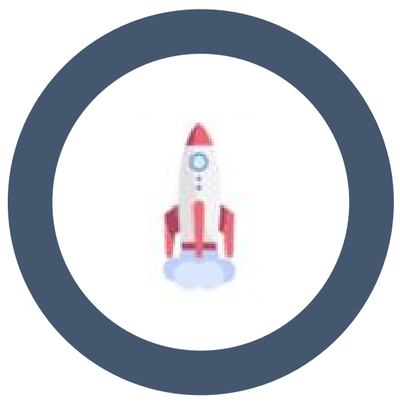
w przeciągu 14 dni

...składało się z 12 małych liter



w przeciągu 5 lat

...składało się z 12 znaków z 1 wielką literą



w przeciągu 63 000 lat

...składało się z 12 znaków z 1 wielką literą, 1 cyfrą i znakiem specjalnym

źródło: https://www.linkedin.com/pulse/corporate-password-policy-critical-internal-safeguard-rwose

Bezpieczne logowanie – czyli jakie?

Prawidłowe zarządzanie hasłami ma kluczowe znaczenie dla ochrony naszej tożsamości cyfrowej i wrażliwych danych czy to w sferze osobistej czy w działalności. Kilka organizacji przygotowało zalecenia dotyczące tworzenia i zarządzania hasłami do logowania.

NIST (National Institute of Standards and Technology)

NIST to amerykańska agencja rządowa zajmująca się standardami i technologią. Ich zalecenia zawarte w publikacji SP 800-63B obejmują [8]:

- minimalną długość hasła 8 znaków (dla haseł generowanych przez użytkownika)
- maksymalną długość hasła 64 znaki
- sprawdzanie haseł względem list znanych, słabych haseł
- rezygnację z wymuszania okresowej zmiany haseł

NIST zaleca również stosowanie uwierzytelniania wieloskładnikowego.

NCSC (National Cyber Security Centre)

NCSC to brytyjska organizacja zajmująca się cyberbezpieczeństwem. Ich zalecenia są zbieżne z NIST i obejmują [9]:

- skupienie się na długości hasła zamiast jego złożoności
- rezygnację z wymuszania okresowej zmiany haseł
- unikanie przewidywalnych wzorców w hasłach

CISA (Cybersecurity and Infrastructure Security Agency)

CISA to amerykańska agencja rządowa zajmująca się cyberbezpieczeństwem. Ich zalecenia obejmują [10] :

- stosowanie długich (minimum 16 znaków), losowych i unikalnych haseł
- korzystanie z menedżerów haseł
- stosowanie uwierzytelniania wieloskładnikowego
- zmianę domyślnych poświadczeń na wszystkich urządzeniach i oprogramowaniu

CERT Polska

CERT Polska to zespół reagowania na incydenty bezpieczeństwa komputerowego, działający w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej). Ich zalecenia obejmują [11]:

- minimalną długość hasła 12 znaków
- brak wymuszania okresowej zmiany haseł
- blokadę tworzenia haseł znajdujących się na liście słabych/często używanych haseł
- brak dodatkowych kryteriów złożoności (np. znaków specjalnych, cyfr)
- limit znaków w haśle nie mniejszy niż 64 znaki

8 NIST Password Guidelines 2024 - AuditBoard
https://www.auditboard.com/blog/nist-password-guidelines/

9 Password Policy Best Practices 2025 For Strong Security
https://www.metacompliance.com/blog/cyber-security-awareness/password-policy-best-practices

10 Require Strong Passwords - CISA
https://www.cisa.gov/secure-our-world/require-strong-passwords

11 Kompleksowo o hasłach - CERT Polska
https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

Zmieniasz hasło co miesiąc? Nie powinieneś!
https://www.nask.pl/pl/aktualnosci/4388,Zmieniasz-haslo-co-miesiac-Nie-powinienes-CSIRT-NASK-przypomina-aktualne-zalecen.html

CERT Polska kładzie nacisk na długość i oryginalność hasła zamiast jego skomplikowania, zalecenie też nie blokowanie funkcji “wklej” na polu hasła.

CNIL

CNIL (Commission nationale de l'informatique et des libertés) - francuski organ regulacyjny zajmujący się ochroną danych osobowych również wydał zalecenia dotyczące haseł [12]:

- CNIL zaleca systematyczną zmianę hasła w przypadku jego kompromitacji
- użytkownik nigdy nie powinien otrzymywać hasła w formie czystego tekstu, szczególnie przez e-mail
- administrator powinien narzucać wymóg zmiany hasła z odpowiednią częstotliwością zależną od złożoności hasła, przetwarzanych danych i ryzyka.

W projekcie nowych zaleceń z 2021 roku, CNIL proponuje:

- definiowanie reguł w oparciu o stopień nieprzewidywalności hasła (entropia) zamiast minimalnej długości
- rezygnację z obowiązku okresowej zmiany haseł dla zwykłych kont użytkowników
- wprowadzenie listy złożonych, ale znanych haseł do unikania
- doprecyzowanie zasad tworzenia i odnawiania haseł.

CNIL podkreśla, że około 60% zgłoszeń naruszeń danych w 2021 roku było związanych z włamaniami, a większości z nich można było uniknąć, stosując najlepsze praktyki dotyczące haseł.

Podsumowanie zaleceń - zasady tworzenia bezpiecznych haseł

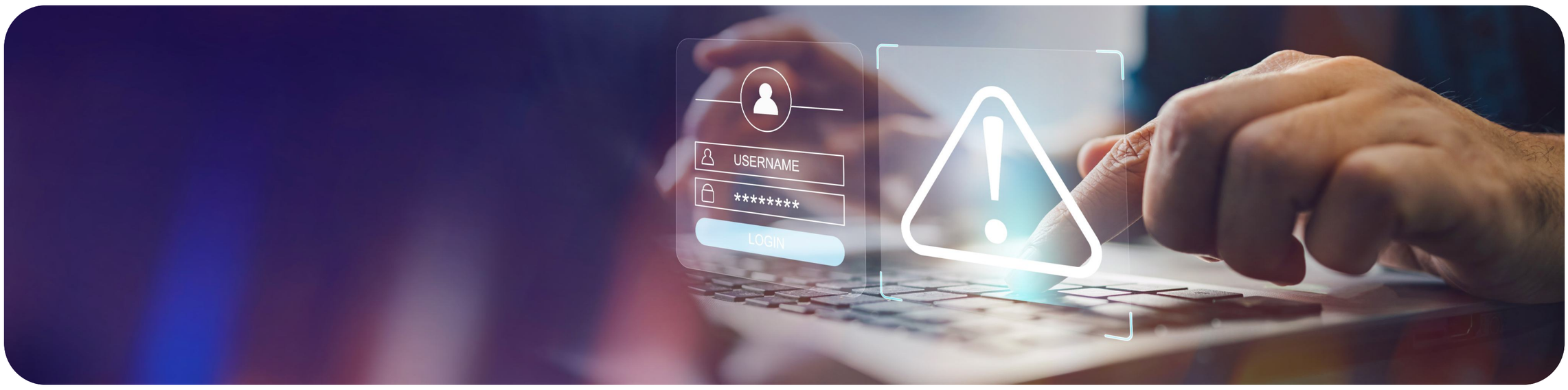
Podsumowałam zalecenia opisane krótko powyżej dotyczące bezpieczeństwa haseł. Poniżej następujące kluczowe elementy zaleceń, które warto wykorzystać konstruując politykę haseł w organizacji.

Podstawowe zasady tworzenia bezpiecznych haseł

- Długość - hasło powinno mieć co najmniej 12 znaków
- Złożoność - używaj kombinacji małych i wielkich liter, cyfr oraz znaków specjalnych
- Unikalność - każde konto powinno mieć inne hasło
- Unikaj oczywistości - nie używaj dat urodzenia, imion czy popularnych słów.

Polityka zmiany haseł

- Rezygnacja z wymuszania okresowej zmiany haseł
- Zmiana hasła wymagana tylko w przypadku podejrzenia lub potwierdzenia jego kompromitacji.



12 [PDF] Recommandation about passwords - CNIL
https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation_passwords_en.pdf

Blokowanie słabych haseł

- Zakaz używania haseł znajdujących się na listach popularnych lub skompromitowanych haseł
- Blokowanie haseł zawierających przewidywalne elementy (np. nazwa firmy).

Korzystanie z menedżerów haseł, które:

- Generują silne, unikalne hasła
- Przechowują hasła w zaszyfrowanej formie
- Automatycznie wypełniają formularze logowania
- Synchronizują hasła między urządzeniami.

Dodatkowe zabezpieczenia

- Zalecane stosowanie uwierzytelniania wieloskładnikowego (MFA). To dodatkowa warstwa zabezpieczeń, która wymaga podania drugiego czynnika (np. kodu z aplikacji lub SMS) oprócz hasła. Włączenie 2FA znacząco zwiększa bezpieczeństwo konta
- Implementacja mechanizmów blokady konta po nieudanych próbach logowania
- Stosowanie opóźnień między kolejnymi próbami logowania (throttling).

Praktyczne wskazówki

- Zachęcanie do używania długich fraz zamiast skomplikowanych haseł
- Umożliwienie wklejania haseł w polach logowania
- Wyświetlanie wskaźnika siły hasła podczas jego tworzenia.

Specjalne przypadki

- Bardziej rygorystyczne zasady dla kont administracyjnych i zdalnego dostępu
- Dostosowanie polityki haseł do konkretnych scenariuszy użycia (np. różne wymagania dla haseł używanych z dodatkowym czynnikiem uwierzytelniającym).

Podsumowując, widoczna jest tendencja do odchodzenia od tradycyjnych, restrykcyjnych polityk haseł na rzecz bardziej elastycznych rozwiązań, które kładą nacisk na długość hasła, unikanie przewidywalnych wzorców i stosowanie dodatkowych zabezpieczeń, takich jak uwierzytelnianie wieloskładnikowe.

Jak wdrożyć skuteczną politykę zarządzania hasłami?

Skuteczna polityka haseł powinna być spersonalizowana na infrastruktury i charakteru danej organizacji.

Pierwszą częścią polityki ochrony haseł powinno być ich wzmocnienie.

Uaktualnij do silniejszych, złożonych haseł: Zastąp stare, słabe hasła nowymi, solidnymi. Używaj kombinacji wielkich i małych liter, cyfr i symboli. Hasła powinny składać się z co najmniej 19 znaków, aby utrudnić atakującym ich złamanie za pomocą ataków siłowych. Unikaj popularnych słów lub fraz, które są łatwe do odgadnięcia.

Unikaj danych osobowych: Unikaj używania łatwych do odgadnięcia informacji, takich jak data urodzin, pseudonim lub adres. Choć dane te są łatwe do zapamiętania, hakerzy często wykorzystują je do łamania haseł.

Frazy zamiast haseł: Rozważ używanie haseł zamiast tradycyjnych haseł. Są to dłuższe kombinacje słów, które są łatwiejsze do zapamiętania i trudniejsze do złamania.

Porzuć ponownie używane hasła: Oprzyj się pokusie ponownego używania haseł na wielu kontach, zwłaszcza osobistych i służbowych. Każde konto powinno mieć własne hasło; jeśli ponownie użyjesz hasła, a cyberprzestępca je odgadnie, będzie mógł uzyskać dostęp do wszystkich kont. Nie używaj też ponownie hasła z tylko jednym zmienionym znakiem (hasło1 vs. hasło2).

Regularnie zmieniaj hasła: Zmieniaj hasła co najmniej co 90 dni, aby zminimalizować ryzyko nieautoryzowanego dostępu. Regularne zmiany utrudniają hakerom złamanie danych uwierzytelniających. Należy jednak unikać zbyt częstych zmian, ponieważ mogą one skłaniać użytkowników do wybierania słabszych haseł lub uciekania się do możliwych do odgadnięcia wzorców. Powinieneś także zmienić hasła, jeśli podejrzewasz jakikolwiek rodzaj naruszenia.

Korzystaj z menedżerów haseł: Przeciętna osoba ma ponad 100 kont online z hasłami, więc zapamiętanie ich wszystkich może być trudne. Nie powinieneś przechowywać haseł na swoich urządzeniach w postaci czystego tekstu lub w jakiejkolwiek odwracalnej formie i nigdy nie powinieneś ich zapisywać. Zamiast tego skorzystaj z narzędzi do zarządzania hasłami, aby bezpiecznie przechowywać i generować złożone hasła. Oferują one wygodę, zapewniając jednocześnie silną higienę haseł.

Druga część polityki ochrony haseł powinna koncentrować się na ulepszeniu środków bezpieczeństwa.

Wdrożenie uwierzytelniania wieloskładnikowego (MFA): W miarę możliwości włącz MFA, aby dodać dodatkową warstwę zabezpieczeń. Ten środek bezpieczeństwa wymaga od użytkowników podania dwóch lub więcej form identyfikacji przed uzyskaniem dostępu do konta. Zazwyczaj wiąże się to z kombinacją czegoś, co wiesz, czegoś, co masz lub czegoś, czym jesteś. Znacznie zmniejsza to prawdopodobieństwo nieautoryzowanego dostępu, nawet jeśli hasła zostaną naruszone.

Oto ile czasu zajmie złamanie twojego hasła jeżeli...

źródło: https://www.linkedin.com/pulse/corporate-password-policy-critical-internal-safeguard-rwose

Wyloguj się po każdej sesji: Zawsze wylogowuj się z programów i kont po zakończeniu korzystania z nich, zwłaszcza na urządzeniach współdzielonych lub publicznych. Zapobiega to nieautoryzowanemu dostępowi do kont.

Regularne audyty i monitorowanie: Wdrażaj procedury regularnego audytu kont użytkowników pod kątem słabych haseł, podejrzanej aktywności i prób nieautoryzowanego dostępu. Monitoruj próby logowania i wymuszaj blokady kont po wielu nieudanych próbach logowania, aby udaremnić ataki typu brute-force.

Edukuj użytkowników: Biorąc pod uwagę, że błąd ludzki przyczynia się do 95% wszystkich naruszeń, edukowanie użytkowników na temat znaczenia silnych haseł, ryzyka związanego z udostępnianiem haseł i taktyk stosowanych przez cyberprzestępców może pomóc zmniejszyć ryzyko naruszenia danych. Istotne jest umożliwienie użytkownikom szybkiego rozpoznawania i zgłaszania podejrzanych działań. Skuteczny program szkoleń na pewno powinien opierać się na jego regularności, praktycznych warsztatach tworzenia i zarządzania hasłami, symulacji ataków (w szczególności phishingowych), stosowaniu elementów rywalizacji i nagradzania za bezpieczne zachowania, demonstrowania konsekwencji najlepiej na przykładach innych organizacji.

Edukacja cyfrowa o osobistym charakterze: Warto odwołać się również do osobistej motywacji i wspomnianej codziennej higieny cyfrowej, która uwzględnia stosowanie bezpieczeństwa haseł również w życiu prywatnym. Stosowanie zasad bezpiecznego logowania i cyfrowej higieny przynosi pracownikom korzyści również w życiu prywatnym:

Ochrona finansów osobistych
- Bezpieczna bankowość elektroniczna
- Ochrona przed kradzieżą tożsamości
- Zabezpieczenie kart płatniczych

Prywatność w sieci
- Ochrona kont społecznościowych
- Bezpieczeństwo komunikacji
- Ochrona danych osobowych

Zabezpieczenie urządzeń domowych
- Smart home
- Urządzenia IoT
- Prywatne sieci Wi-Fi

Podsumowanie

Właściwe zarządzanie hasłami to nie koszt, a inwestycja w bezpieczeństwo firmy. Według najnowszych badań, firmy które wdrożyły kompleksową politykę zarządzania hasłami, odnotowują o 70% mniej incydentów bezpieczeństwa i oszczędzają średnio 23% kosztów związanych z cyberbezpieczeństwem.

Pamiętaj:
bezpieczeństwo Twojej firmy jest tak silne, jak najsłabsze hasło używane przez Twoich pracowników. Nie czekaj na incydent - zacznij działać już dziś.

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI

LexDigital

lexdigital.pl LinkedIn