inlockly

Przyczyny i skutki potencjalnego wycieku danych w Twojej firmie.

Jak zabezpieczyć firmę przed stratami finansowymi spowodowanymi wyciekiem haseł dostępowych, kart płatniczych i innych poufnych danych w wyniku cyberataku?

www.inlockly.com

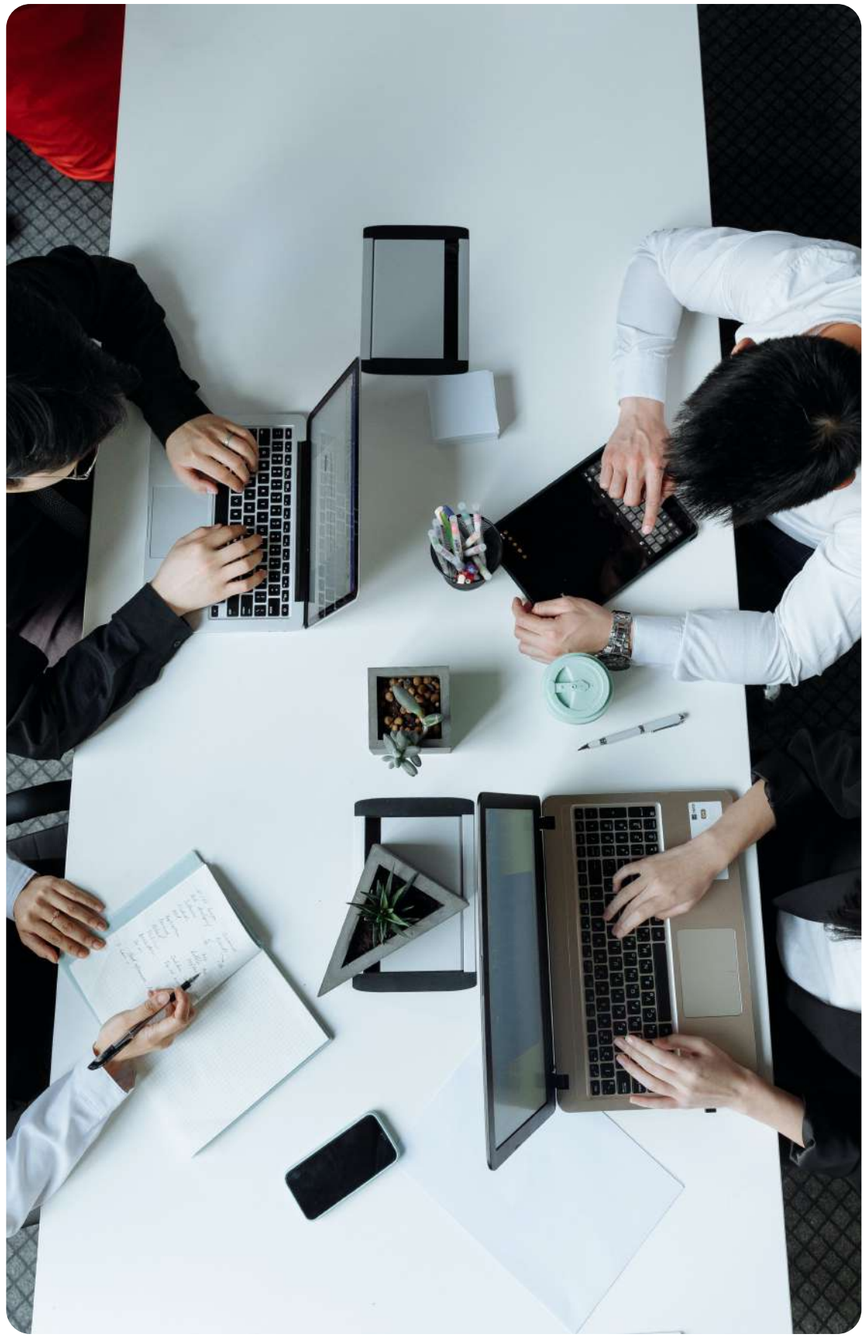


Wstęp

Szanowni Państwo,
Dziś poruszymy kwestię, która staje się coraz bardziej kluczowa dla funkcjonowania każdej firmy - mianowicie, **bezpieczeństwa danych**. Ochrona informacji ma kluczowe znaczenie dla sukcesu i integralności przedsiębiorstwa. W ramach dzisiejszej prezentacji skoncentrujemy się na zagadnieniu potencjalnych przyczyn oraz konsekwencji wycieku danych w wielu firmach.

Na początku wykonajmy krótką wizualizację. Wyobraźmy sobie następujący scenariusz: w naszej firmie doszło do wycieku danych. Jakie mogą być potencjalne skutki tego incydentu? Utrata poufnych informacji, takich jak hasła, dane kart płatniczych czy innych wrażliwych danych, może stanowić poważne zagrożenie dla stabilności finansowej przedsiębiorstwa. To nie tylko kwestia utraty danych, ale również wpływu na zaufanie klientów i partnerów biznesowych.

Poniższy materiał ma na celu głębsze zrozumienie czynników prowadzących do wycieku danych w kontekście biznesowym oraz analizę potencjalnych konsekwencji. Przedstawimy również narzędzie, które można wdrożyć w celu zminimalizowania ryzyka i zwiększenia ochrony przedsiębiorstwa.



Z wyrazami szacunku,
zespół inlockly.com

inlockly

Przyczyny i skutki potencjalnego wycieku danych w Twojej firmie.

Jakie firmy są narażone na cyberataki?

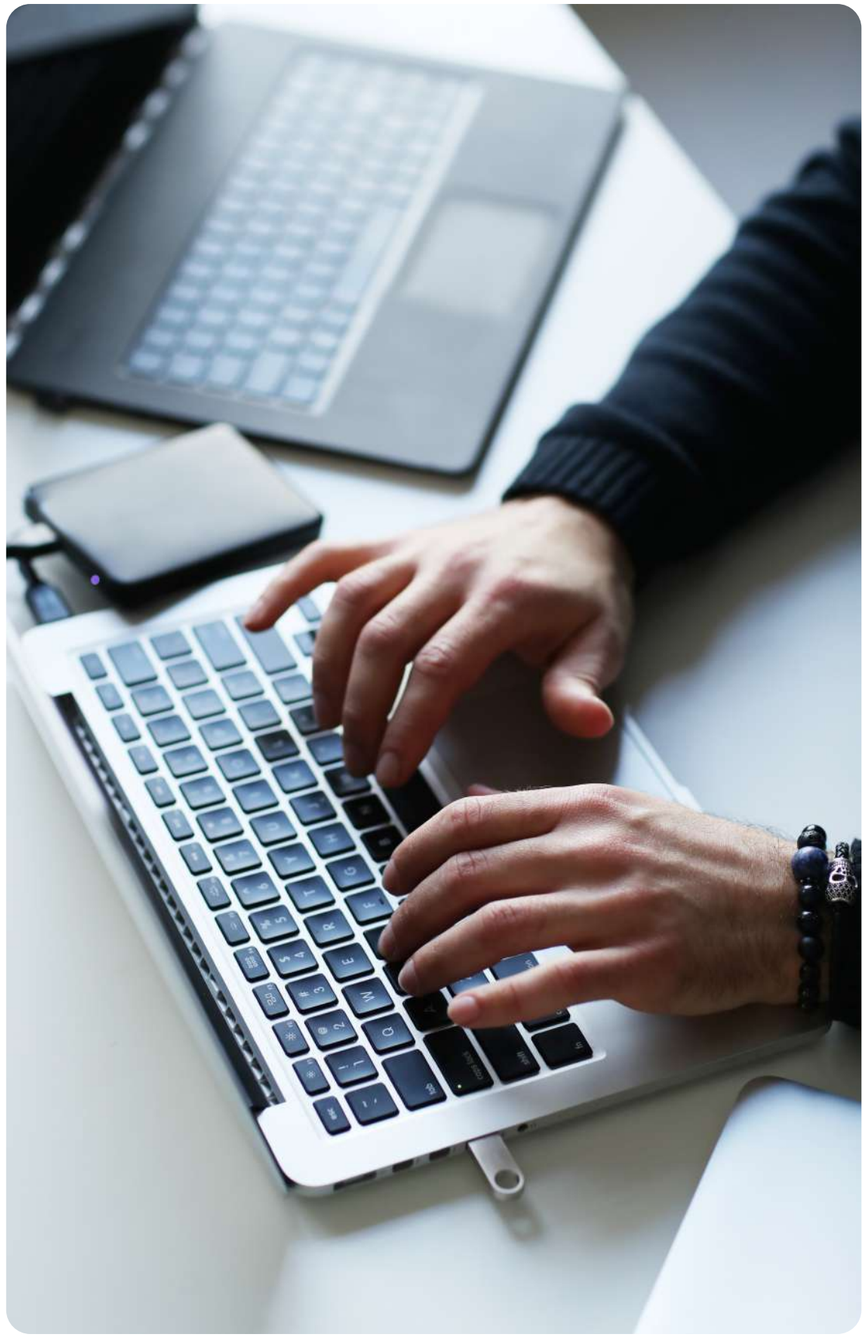


Firmy narażone na ataki

Cyberbezpieczeństwo stanowi nieodłączny element rzeczywistości dla przedsiębiorstw, niezależnie od ich branży czy wielkości. Współczesne zagrożenia atakami obejmują niemal każdego przedsiębiorcę, niezależnie od specyfiki jego działalności. Zapoznaj się z metodami podnoszenia poziomu bezpieczeństwa Twojej firmy w obszarze cyberprzestrzeni.

“70% firm w Polsce spotkało się z sytuacją, która zagrażała bezpieczeństwu danych i systemów IT przedsiębiorstwa. Jednocześnie sami przedsiębiorcy oceniają swoją cyberodporność nisko.”

Źródło: biz.gov.pl



Wzrost ryzyka cyberataków w ostatnich latach

W ostatnich latach obserwujemy alarmujący wzrost ryzyka związanego z cyberatakami. Dynamiczny rozwój technologii oraz globalna cyfryzacja sprawiają, że przedsiębiorstwa stają się coraz bardziej narażone na ataki cybernetyczne. W tym kontekście warto przyjrzeć się czynnikom, które przyczyniły się do tego wzrostu ryzyka w ostatnich latach i zrozumieć, jakie wyzwania stawiają przed nami dzisiejsze realia cyberprzestrzeni.

Praca zdalna

Wzrost praktyk pracy zdalnej i hybrydowej w ostatnich latach wprowadził nowe wyzwania i dynamicznie zmienił krajobraz bezpieczeństwa.
W odpowiedzi na pandemię wywołanej wirusem COVID-19 - 72% ankietowanych małych firm na całym świecie stwierdziło, że przyspieszyło swoje projekty transformacji cyfrowej.

Tak szybkie przyjęcie technologii sprawiło, że wiele małych firm jest podatnych na zagrożenia cybernetyczne. Pracując z różnych lokalizacji i korzystając z różnych urządzeń, pracownicy zdalni stają się potencjalnym celem dla ataków.

Prawie jedna trzecia incydentów związanych z cyberbezpieczeństwem w małych firmach doprowadziła do naruszenia danych w 2020 r., a dane logowania zostały naruszone w 44% potwierdzonych naruszeń.
Zdalne miejsca pracy wymagają dostępu do poufnych danych firmowych (w tym danych logowania) z różnych lokalizacji, co wymaga odpowiedniego zabezpieczenia.

Globalna cyfryzacja

Globalna cyfryzacja, będąca integralną częścią współczesnego biznesu, znacząco zwiększa ryzyko cyberataków. Rozprzestrzenianie się technologii cyfrowej na globalną skalę sprawia, że przedsiębiorstwa z różnych branż stają się bardziej podatne na złożone zagrożenia cybernetyczne.

W świecie, w którym firmy przechodzą na modele działania oparte na danych, każda organizacja staje się potencjalnym celem dla atakujących. Wzrost liczby systemów online, platform internetowych i zastosowań technologii IoT (Internet of Things) stwarza nowe punkty dostępu, które mogą być wykorzystane przez cyberprzestępców.

W tej rzeczywistości, gdzie dane są kluczowym aktywem, konieczność skutecznej ochrony przed atakami cybernetycznymi staje się imperatywem dla każdej organizacji, niezależnie od jej wielkości czy dziedziny działania. Wartościowe informacje i poufne dane stają się celem ataków, co podkreśla wagę odpowiednich strategii bezpieczeństwa w erze globalnej cyfryzacji.

Przykładowe rodzaje ataków powodujących wyciek danych w firmach.

Phishing

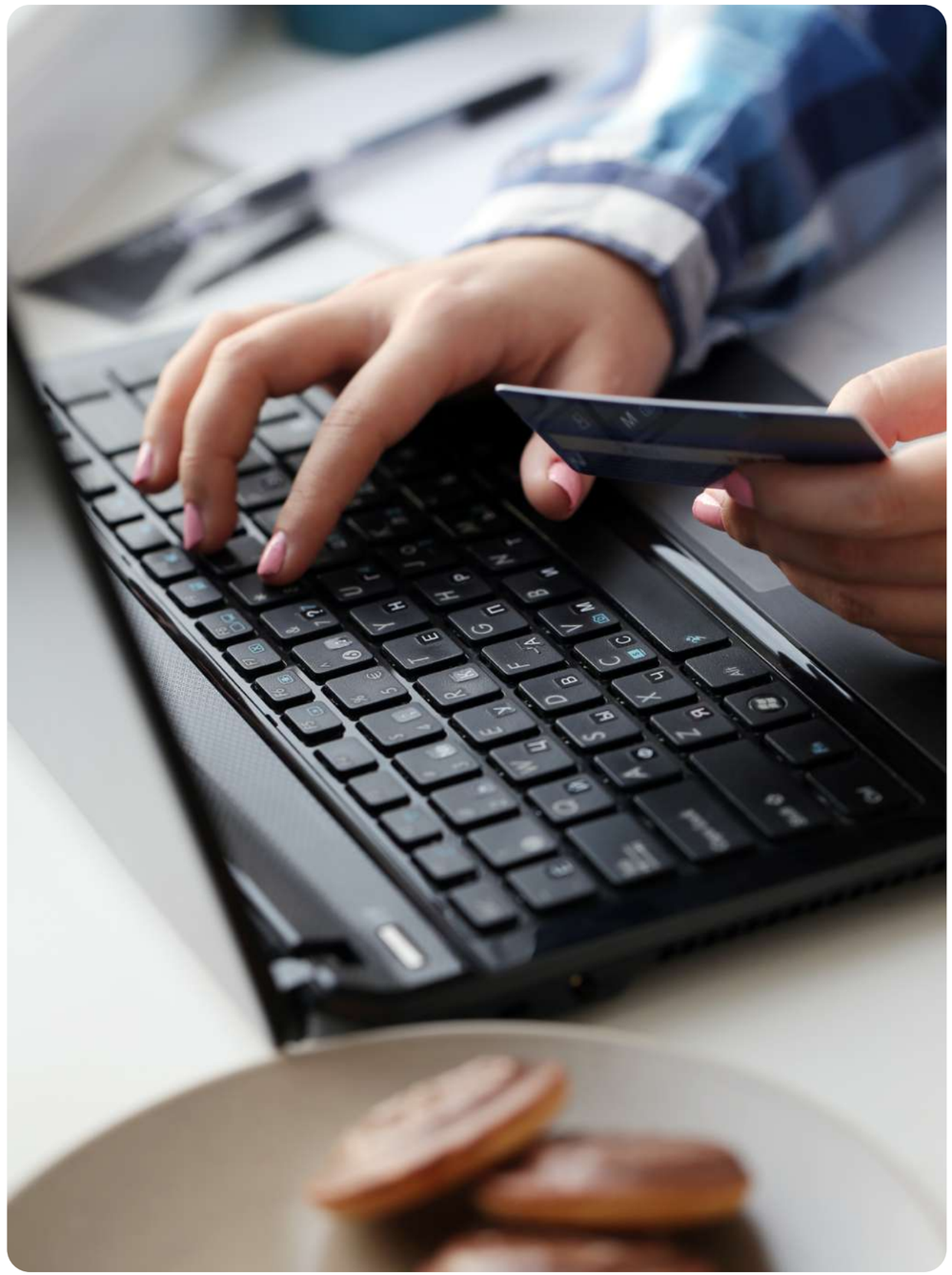
Phishing to forma cyberoszustwa, w której atakujący podszywa się pod zaufaną osobę, instytucję lub organizację, aby nakłonić ofiarę do ujawnienia wrażliwych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe.

Najczęściej odbywa się to za pośrednictwem fałszywych e-maili, wiadomości SMS, stron internetowych lub wiadomości w mediach społecznościowych, które wyglądają na autentyczne.

Celem phishingu jest wyłudzenie danych, które mogą być wykorzystane do kradzieży tożsamości, przejęcia konta lub innych działań o charakterze przestępczym.

Aby się chronić, warto zachować ostrożność, weryfikować autentyczność wiadomości i unikać klikania podejrzanych linków.

Warto również stosować menedżery haseł, które automatycznie uzupełniają dane logowania tylko na stronach, których adresy URL dokładnie odpowiadają zapisanym danym. To chroni użytkownika przed wprowadzeniem haseł na fałszywych stronach, które próbują podszywać się pod zaufane witryny.



Podstawowe cechy ataku typu phishing

Podrabianie tożsamości

Phisherzy często podszywają się pod znane i zaufane instytucje, takie jak banki, firmy, instytucje rządowe czy serwisy internetowe. Często ich ataki wydają się bardzo autentyczne.

Wiadomości e-mailowe

Jednym z powszechnych środków phishingu są fałszywe wiadomości e-mailowe. Phisherzy wysyłają e-maile, udając, że pochodzą od zaufanych źródeł, i proszą ofiary o podanie poufnych informacji, jak numery kart kredytowych czy hasła.

Strony phishingowe

Phisherzy tworzą fałszywe strony internetowe, które naśladują prawdziwe serwisy, aby przekonać ofiary do wprowadzenia swoich danych. Często używają podobnych adresów URL czy domen, aby sprawić, by strony wyglądały autentycznie.

Ataki smishingowe

Smishing to odmiana phishingu, w której atakujący używają wiadomości tekstowych (SMS) do oszustw. Ofiary otrzymują fałszywe wiadomości z prośbą o podanie informacji osobistych.

Ataki spear phishing

W przypadku spear phishingu atakujący skupiają się na konkretnych osobach czy organizacjach. Tworzą bardziej spersonalizowane i precyzyjne ataki, bazując na informacjach zdobytych na temat swoich celów.

Ataki społecznościowe

Phisherzy wykorzystują także media społecznościowe, aby podszywać się pod znajomych, firmy czy instytucje. Przesyłają linki do fałszywych stron, zachęcając do kliknięcia i podania poufnych informacji.

Aby unikać phishingu, ważne jest zachowanie ostrożności przy otwieraniu wiadomości e-mail, klikaniu w linki czy udostępnianiu poufnych informacji online. Edukacja użytkowników oraz stosowanie dodatkowych środków bezpieczeństwa, takich jak filtrowanie antyphishingowe, są kluczowe dla skutecznej ochrony przed tym rodzajem cyberataków.

Bruteforce

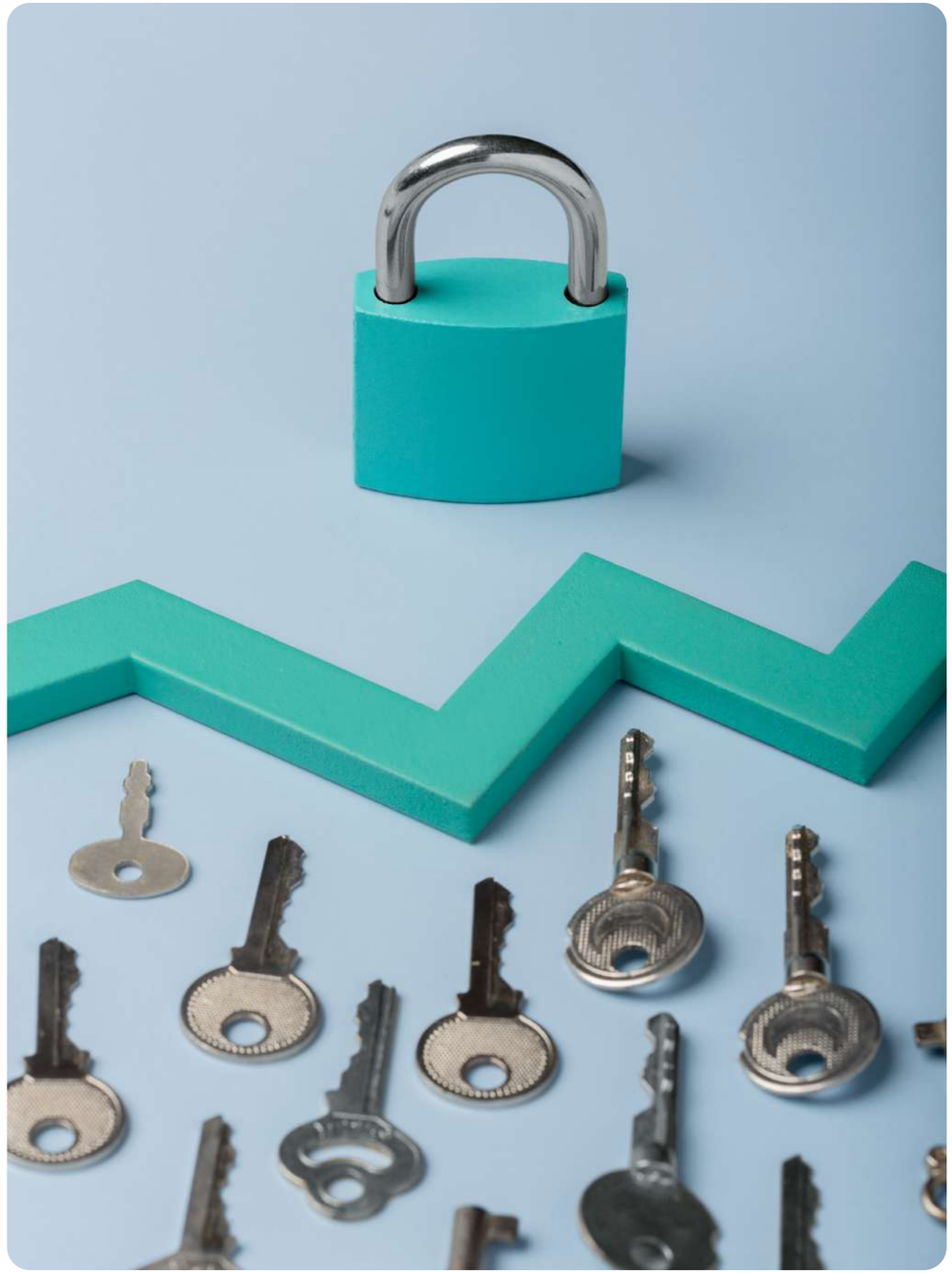
Brute force (atak siłowy) to metoda ataku na systemy informatyczne polegająca na próbie odgadnięcia haseł, kluczy szyfrujących lub innych danych uwierzytelniających poprzez systematyczne testowanie wszystkich możliwych kombinacji.

Atakujący używa w tym celu specjalistycznego oprogramowania, które automatycznie generuje i sprawdza różne warianty, aż do znalezienia prawidłowego rozwiązania.

Brute force jest skuteczny, ale często czasochłonny, zwłaszcza gdy zabezpieczenia są silne i wykorzystują długie, złożone hasła.

Aby się przed nim chronić, stosuje się m.in. mechanizmy ograniczające liczbę prób logowania, blokady czasowe, uwierzytelnianie wieloskładnikowe (MFA) oraz hasła o dużej złożoności

Menedżery haseł generują długie, losowe i unikalne hasła, które są trudne lub wręcz niemożliwe do odgadnięcia metodą siłową. Dzięki temu nawet jeśli atakujący spróbuje tej techniki, czas potrzebny na złamanie hasła będzie niewspółmiernie długi.



Podstawowe cechy ataku typu bruteforce

Niezliczona liczba prób

Atakujący dokonuje wielu prób logowania, testując różne kombinacje haseł, aby uzyskać dostęp do konta. Ta metoda opiera się na testowaniu wszystkich możliwych kombinacji.

Słabe hasła są łatwe do złamania

Atak ten jest szczególnie skuteczny w przypadku słabych haseł, takich jak proste sekwencje znaków, słowa ze słownika czy powszechne kombinacje.

Wzrost skuteczności przy słabych zabezpieczeniach

Jeśli system nie ma odpowiednich zabezpieczeń, takich jak blokada konta po kilku nieudanych próbach, atak brute force staje się bardziej skuteczny.

Stosowanie automatycznych programów

Atak brute force jest często prowadzony za pomocą automatycznych programów, które szybko i systematycznie testują różne hasła bez udziału człowieka.

Zagrożenie dla kont online

Ataki brute force mogą być skierowane przeciwko kontom online, takim jak konta e-mailowe, profile na stronach społecznościowych czy nawet konta bankowe.

Zastosowanie słownika

Wariantem ataku brute force jest atak przy użyciu słownika, w którym atakujący testuje popularne hasła, słowa ze słownika czy kombinacje znanego tekstu.

Aby skutecznie chronić się przed atakami brute force, ważne jest stosowanie silnych haseł, które są trudne do odgadnięcia, oraz implementacja dodatkowych środków bezpieczeństwa. Te mogą obejmować blokady po kilku nieudanych próbach logowania, zastosowanie wielopoziomowej weryfikacji tożsamości, monitorowanie aktywności, aby wykryć podejrzane działania, a także wykorzystywanie menedżerów haseł które pomagają w generowaniu i zapamiętywaniu unikalnych haseł. Edukacja użytkowników na temat bezpiecznych praktyk hasłowych również odgrywa kluczową rolę w ochronie przed tego rodzaju atakami.

Keylogging

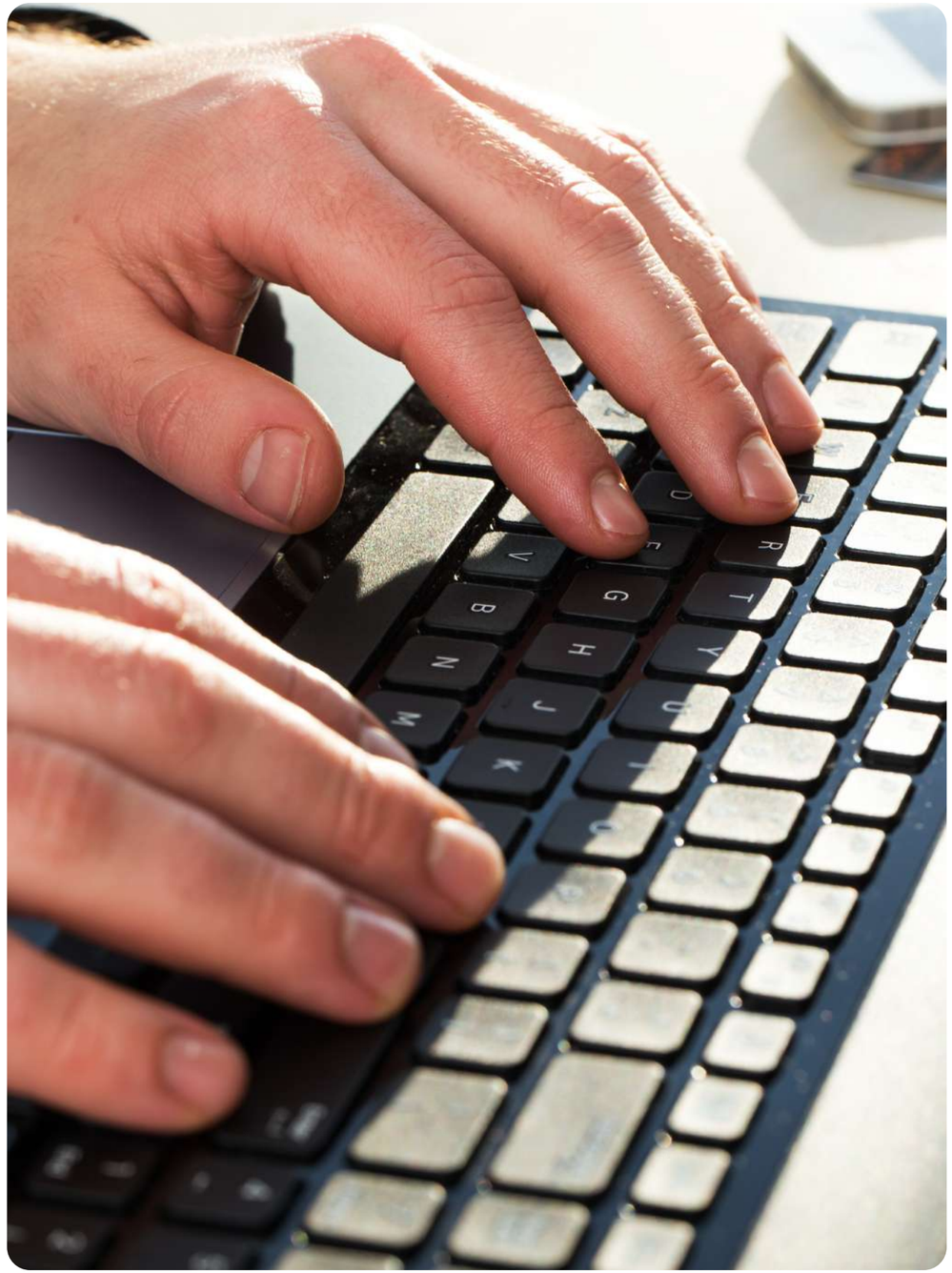
Keylogging to technika śledzenia i rejestrowania naciśnięć klawiszy na klawiaturze, stosowana zazwyczaj przez cyberprzestępców w celu zdobycia poufnych informacji, takich jak hasła, dane logowania czy informacje finansowe.

Działanie keyloggera polega na przechwytywaniu w czasie rzeczywistym każdego wpisywanego znaku, a następnie przesyłaniu tych danych do atakującego.

Keyloggery mogą mieć formę oprogramowania (np. złośliwe aplikacje instalowane na urządzeniu) lub sprzętu (np. niewielkie urządzenia podłączane między klawiaturą a komputerem).

Aby się przed nimi chronić, warto stosować aktualne oprogramowanie antywirusowe, unikać instalowania nieznanych programów i korzystać z bezpiecznych środowisk do logowania, takich jak uwierzytelnianie wieloskładnikowe.

Przy korzystaniu z menedżera haseł użytkownik często nie wpisuje ręcznie haseł – są one wprowadzane automatycznie, co minimalizuje ryzyko przechwycenia wprowadzanych danych przez keylogger.



Podstawowe cechy ataku z wykorzystaniem keyloggera

Niewidoczność dla użytkownika

Keylogger działa w ukryciu i jest zazwyczaj niewidoczny dla użytkownika. Atakujący starają się utrzymać keyloggera w tle, aby ofiary nie miały świadomości o ich istnieniu.

Celowe ataki na dane finansowe

Ataki z wykorzystaniem keyloggerów często mają na celu pozyskanie danych finansowych, takich jak numery kart kredytowych czy informacje o kontach bankowych.

Różne formy ataku

Keyloggery mogą mieć formę sprzętową (fizyczne urządzenia podłączane do komputera) lub programową (aplikacje działające w systemie operacyjnym).

Ataki na komputery i urządzenia mobilne

Keyloggery mogą być skierowane zarówno na komputery stacjonarne, jak i urządzenia mobilne, które są używane do wprowadzania informacji za pomocą klawiatury ekranowej.

Rejestrowanie wszystkich działań na klawiaturze

Keylogger rejestruje wszystkie klawisze wciśnięte przez użytkownika, zbierając informacje o wprowadzanych hasłach, wiadomościach e-mail, danych logowania czy innych tekstach.

Zdalne przesyłanie danych

Zebrane dane są często przesyłane do atakującego za pomocą Internetu. Może to odbywać się poprzez e-mail, FTP, HTTP lub innych metod transmisji danych.

Ochrona przed atakami keyloggerów obejmuje regularne skanowanie systemu antywirusowego, unikanie klikania w podejrzane linki czy załączniki, korzystanie z oprogramowania antymalware oraz menedżerów haseł, a także świadomość użytkowników na temat zagrożeń i praktyk bezpieczeństwa online. Współczesne narzędzia bezpieczeństwa często wykrywają i blokują działanie keyloggerów, jednak regularne aktualizacje i monitorowanie są kluczowe w utrzymaniu skutecznej ochrony.

Inne czynniki zagrażające bezpieczeństwu danych.



Nieprzestrzeganie firmowej polityki haseł (lub jej brak)

Brak konsekwentnego przestrzegania polityki haseł stwarza potencjalne luki w obronie. Użytkownicy, którzy stosują słabe hasła lub niezmienne kombinacje, narażają organizację na ryzyko łatwego dostępu przez potencjalnych atakujących do wielu zasobów firmowych, co może mieć tragiczne konsekwencje dla przedsiębiorstwa.

Niedostateczna ochrona danych

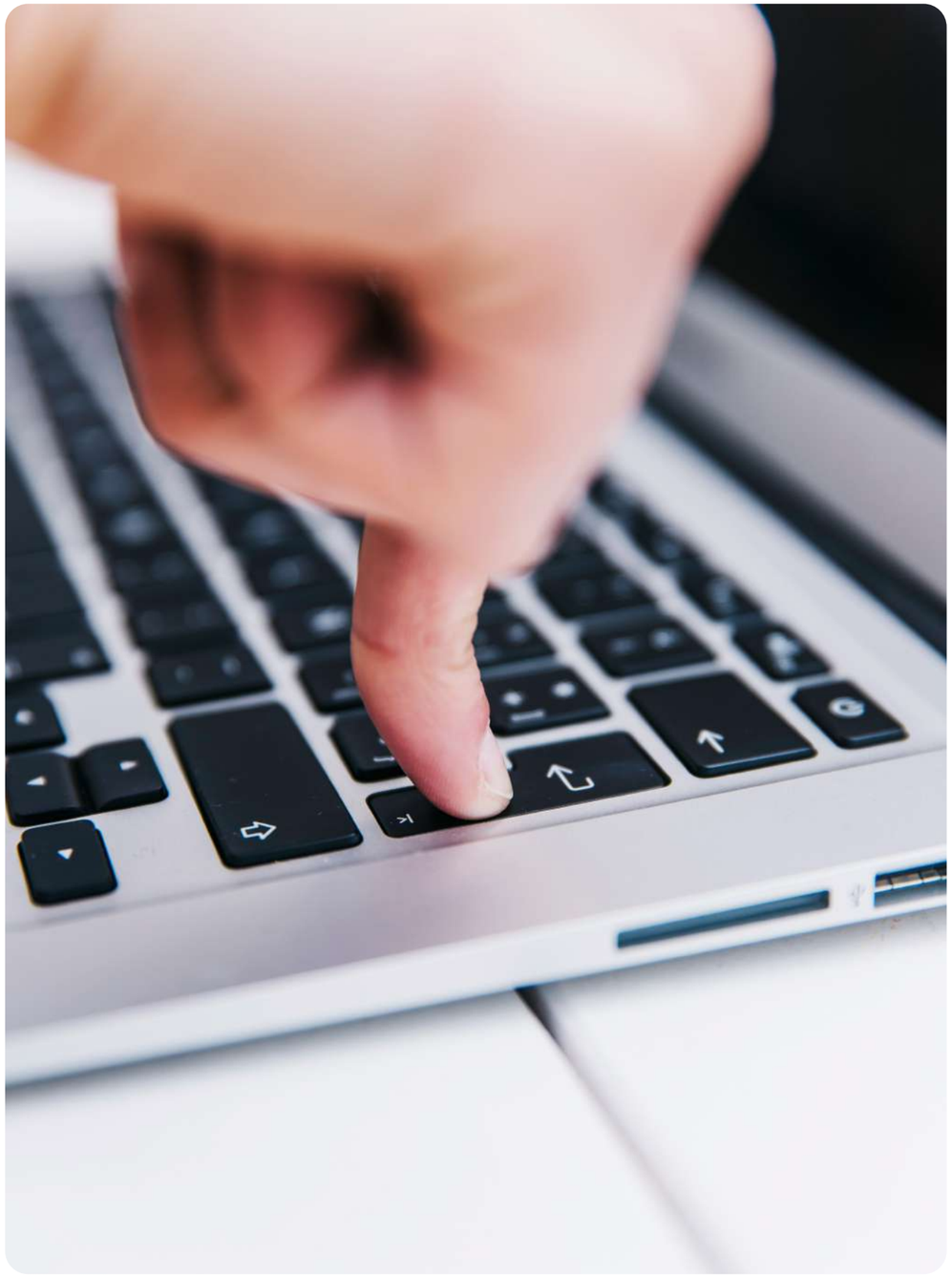
Brak skutecznych mechanizmów ochrony danych, takich jak szyfrowanie i odpowiednie zarządzanie dostępem oraz udostępnianiem, sprawia, że informacje firmowe są bardziej podatne na kradzież i nieautoryzowany dostęp.

Brak odpowiednich uprawnień

Zbyt szeroki dostęp do danych dla pracowników, którzy go nie potrzebują, może prowadzić do nadużyć. Zasada najmniejszych uprawnień polega na przyznawaniu pracownikom tylko tych uprawnień, które są absolutnie niezbędne do wykonywania ich codziennych zadań.

Brak szkoleń dla pracowników

Niewystarczające szkolenie pracowników w zakresie cyberbezpieczeństwa sprawia, że stanowią oni potencjalne ogniwo słabe w łańcuchu obronnym. Nieświadomi pracownicy mogą popełniać błędy, takie jak klikanie w podejrzane linki czy otwieranie złośliwych załączników.



Jakie są konsekwencje wycieku danych w firmie?

Główne konsekwencje

Pierwszym widocznym efektem cyberataków jest utrudnienie lub nawet całkowity paraliż funkcjonowania firmy. Pracownicy i właściciele często tracą dostęp do kluczowych danych i narzędzi, co może objawiać się na przykład niemożnością zalogowania się do skrzynki pocztowej czy uzyskania dostępu do dysku w chmurze. Takie sytuacje nie tylko zakłócają codzienną pracę, ale mogą również wpływać na realizację strategicznych celów biznesowych.

Nie wszystkie skutki ataku są jednak widoczne od razu. Niepokojącymi sygnałami może być spowolnione działanie urządzeń i aplikacji, nagłe pojawianie się lub znikanie plików i folderów, a także rozsyłanie spamu z firmowych komputerów czy telefonów. Takie objawy często pozostają niezauważone, co zwiększa ryzyko dalszych strat.

Cyberataki niosą ze sobą również poważne konsekwencje finansowe:

a. Przerwy w działalności firmy oznaczają realne straty – według danych NASK aż dwie trzecie firm, które padły ofiarą cyberataku, odnotowały wyraźny spadek przychodów.

b. Dodatkowo koszty mogą generować utrata lub uszkodzenie danych, konieczność przywracania systemów czy naprawy sprzętu i infrastruktury. W niektórych przypadkach powrót do pełnej sprawności wymaga zatrudnienia dodatkowych specjalistów, co wiąże się z kolejnymi wydatkami.

W dłuższej perspektywie cyberatak może negatywnie wpłynąć na wizerunek firmy, zmniejszyć zaufanie klientów i partnerów biznesowych, a nawet zaszkodzić jej pozycji na rynku.

Straty finansowe dla firm wynikające z incydentów naruszenia bezpieczeństwa danych.

Średnie koszty incydentów i naruszeń dla firm w 2020 r.:

Liczba pracowników	Koszt
1-9	7 000$
10-49	17 000$
50-249	50 000$
249-999	133 000$
1000+	504 000$

W oparciu o dane z ośmiu krajów.
Źródło: Hiscox, “Hiscox Cyber Readiness Report,” 2020

inlockly

Przyczyny i skutki potencjalnego wycieku danych w Twojej firmie.

Jak zniwelować ryzyko wycieku danych w firmie?



12 najlepszych praktyk zarządzania hasłami dla pracowników.

1. Używaj różnych i silnych haseł dla każdego systemu i konta.
2. Nie używaj danych osobowych (w tym imion zwierząt domowych i niczego, co można odgadnąć z mediów społecznościowych) do tworzenia haseł.
3. Nie używaj słów słownikowych z żadnego języka.
4. Używaj najdłuższych możliwych haseł, nigdy nie krótszych niż 12 znaków.
5. Wymagaj co najmniej dwóch metod uwierzytelniania tożsamości użytkownika za pomocą uwierzytelniania dwuskładnikowego (2FA) lub uwierzytelniania wieloskładnikowego (MFA), gdy tylko jest to możliwe.
6. Aktualizuj hasła do wszystkich kont, które zostały naruszone w wyniku incydentu związanego z bezpieczeństwem.
7. Nie zapisuj haseł i nie zostawiaj ich na biurku lub przyklejonych do komputera.
8. Nie przechowuj haseł w przeglądarce internetowej.
9. Wdrożenie silnej, firmowej polityki i systemu egzekwowania, który zapobiega używaniu słabych haseł.
10. Usuń konta i aplikacje, które nie są już używane.
11. Zmień domyślne hasła dla ważnych systemów, takich jak zdalnie dostępne urządzenia lub wszystko, co ma kontakt z Internetem.
12. Nie przesyłaj współpracownikom haseł do kont współdzielonych niebezpiecznymi metodami, takimi jak czaty tekstowe, wiadomości email czy notatki - zawsze korzystaj z szyfrowanego udostępniania np. za pomocą menedżera haseł.

5 dodatkowych zasad dla administratorów

1. Używaj szyfrowania podczas przechowywania lub udostępniania haseł.
2. Wdróż zaawansowane metody uwierzytelniania 2FA/MFA (takich jak aplikacje wierzytelniające na telefony komórkowe lub klucze sprzętowe).
3. Zmieniaj hasła do kont współdzielonych i odwołuj indywidualne konta po odejściu pracownika z firmy.
4. Dodaj dodatkowe zabezpieczenia dla kont uprzywilejowanych - na przykład poprzez wdrożenie rozwiązania do zarządzania tożsamością (IAM), które egzekwuje bardziej rygorystyczne zasady dla tych użytkowników.
5. Edukuj pracowników, wykonawców i innych użytkowników, aby nie używali ponownie haseł firmowych do kont osobistych.

Zarządzanie dostępami dla użytkowników i zespołów w firmie

Menedżer haseł to nieocenione wsparcie dla zespołów w firmie, które pomaga im bezpiecznie wykonywać codzienne obowiązki. Wraz z rozwojem organizacji i pojawianiem się nowych działów oraz pracowników, menedżer haseł staje się niezastąpionym narzędziem w zarządzaniu poufnymi danymi i kontami.

Poniżej znajduje się kilka przykładów głównych obszarów funkcjonalnych, które mogą skorzystać na lepszym zarządzaniu hasłami.

Sprzedaż i obsługa klienta

Zespoły sprzedażowe codziennie korzystają z aplikacji, takich jak platformy CRM, które umożliwiają zarządzanie relacjami z klientami. Przechowują one dane osobowe klientów, czyli informacje pozwalające na ich identyfikację. Ochrona tych danych jest kluczowa dla budowania i utrzymania zaufania klientów.

Kadry (HR)

Dane osobowe pracowników, takie jak numery identyfikacyjne czy daty urodzenia, są niezwykle cenne dla cyberprzestępców. Zespoły HR, jako strażnicy tych danych, często stają się celem cyberataków. Dodatkowo, osoby odpowiedzialne za wdrażanie nowych pracowników zarządzają wieloma danymi uwierzytelniającymi – czasem dziesiątkami lub setkami. Menedżer haseł wspiera działy HR, chroniąc poufne informacje i ułatwiając proces wdrażania nowych pracowników.

Finanse

Dział finansowy realizuje kluczowe zadania, takie jak księgowość, zarządzanie przepływami pieniężnymi, prognozowanie finansowe czy pozyskiwanie kapitału. Te działania wiążą się z dostępem do wielu poufnych informacji finansowych przechowywanych w różnych systemach i na kontach. Ochrona tych danych jest niezbędna, aby zapewnić bezpieczeństwo firmy.

Technologia (IT)

W małych firmach zespół IT jest często niewielki, a obowiązki administratora bywają dzielone między pracowników z innych działów. Lista zadań jest zwykle bardzo długa – od ochrony witryny internetowej przed włamaniami, przez wdrażanie i wycofywanie pracowników z aplikacji, aż po radzenie sobie z incydentami bezpieczeństwa i resetowanie haseł. Menedżer haseł pomaga usprawnić te procesy, jednocześnie wzmacniając poziom ochrony i promując kulturę bezpieczeństwa w firmie.

Marketing

Zespół marketingu korzysta z wielu narzędzi cyfrowych, od mediów społecznościowych po aplikacje do projektowania i zarządzania projektami. Pracownicy często dzielą się loginami w sposób niezabezpieczony, co zwiększa ryzyko włamań. Menedżer haseł pomaga chronić te dane i zapobiegać ich nie odpowiedniemu wykorzystaniu.

Płace

Pracownicy działu płac obsługują dane osobowe i finansowe całego personelu, co czyni ich częstym celem cyberataków. Ochrona tych informacji jest kluczowa, aby zapewnić bezpieczeństwo firmy i jej pracowników.

Zamówienia i dostawcy

Oprócz danych pracowników i klientów, ważne jest również chronienie poufnych informacji dostarczanych przez dostawców. Mogą to być m.in. numery identyfikacyjne freelancerów, konta bankowe firmowe czy inne wrażliwe dane wymagane w procesie współpracy. Odpowiednia ochrona tych informacji pozwala zespołowi ds. zaopatrzenia utrzymać zaufanie wartościowych partnerów biznesowych.



Nasze rozwiązanie - aplikacja Inlockly™ na wiele platform.

RODO ZGODNOŚĆ

CCPA ZGODNOŚĆ

Czym jest aplikacja Inlockly™?

Aplikacja Inlockly™ to narzędzie z grupy menedżerów haseł, który przechowuje wszystkie hasła w jednym bezpiecznym miejscu, umożliwiając jednocześnie łatwe zarządzanie loginami i tworzenie długich, losowych i unikalnych haseł. Wystarczy zapamiętać tylko jedno hasło - hasło główne do aplikacji Inlockly™.

Menedżer haseł automatycznie synchronizuje wszystkie hasła na wielu urządzeniach, dzięki czemu można uzyskać do nich dostęp i zarządzać nimi z dowolnego miejsca.

Stosujemy najsilniejsze dostępne szyfrowanie, umożliwiamy logowanie się do kont za pomocą kilku kliknięć oraz oferujemy szereg dodatkowych korzyści.

Jak nasza aplikacja chroni przed poznanymi wcześniej zagrożeniami?

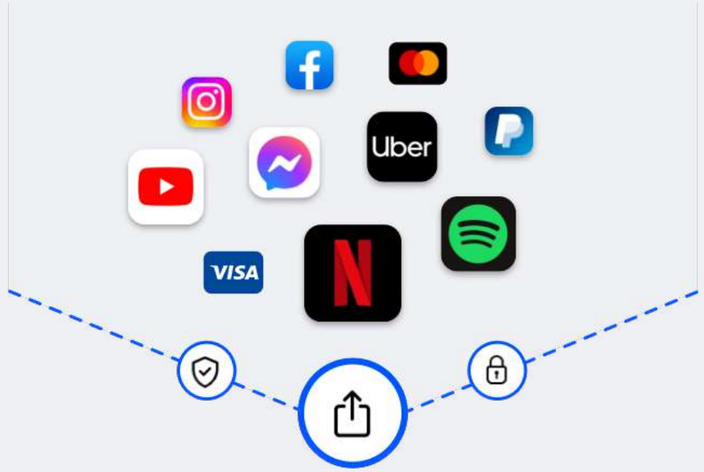
Inlockly™ znacząco ułatwia wszystkim pracownikom zachowanie najlepszych praktyk w zakresie bezpieczeństwa haseł i zarządzania dostępami, co zmniejsza ryzyko wystąpienia wycieku danych poprzez poznane wcześniej ataki.

- **Ochrona przed phishingiem**
- **Ochrona przed keyloggingiem**
- **Ochrona przed atakami brute force**
- **Pomoc w przestrzeganiu polityki haseł**
- **Bezpieczne udostępnianie danych pracowniczych**
- **Zarządzanie uprawnieniami i kontrola dostępu**

Ochrona przed phishingiem

Inlockly™ pełni istotną rolę w ochronie przed phishingiem poprzez kilka kluczowych funkcji i praktyk, takich jak:





Ukrywanie danych logowania na niezaufanych witrynach

Aplikacja Inlockly™ automatycznie wypełnia formularze logowania na stronach internetowych. To eliminuje ryzyko wpisywania danych logowania przez użytkownika na fałszywych stronach phishingowych. Dane logowania są ściśle powiązane z adresem domeny internetowej, a adresy te są automatycznie porównywane z adresem na którym znajduje się użytkownik - jeżeli nie są zgodne - dane zostają ukryte.

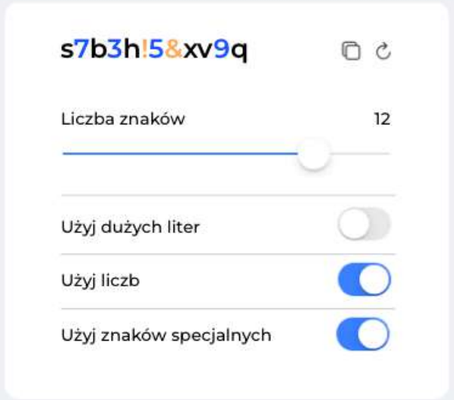
Przechowywanie innych wrażliwych danych

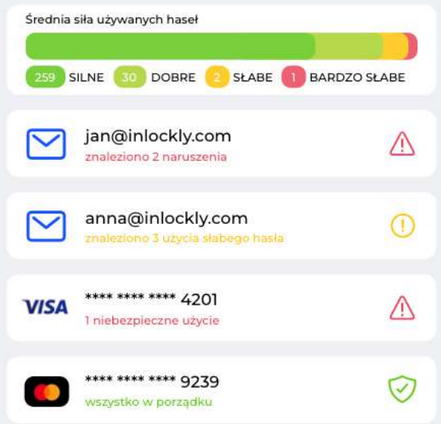
Inlockly™ przechowuje nie tylko hasła, ale także inne wrażliwe dane, takie jak numery kart płatniczych, notatki firmowe czy dane osobowe, a to wszystko w bezpieczny i szyfrowany sposób.

Dzięki wbudowanemu filtrowi adresów internetowych, aplikacja ostrzega użytkownika, gdy witryna nie jest zaufana, chroniąc informacje przed wyciekiem podczas ataków phishingowych.

Ochrona przed atakami brute force

Inlockly™ chroni przed atakami typu brute force poprzez zastosowanie kilku kluczowych mechanizmów bezpieczeństwa:





Generowanie i przechowywanie silnych i niepowtarzalnych haseł

Inlockly™ umożliwia generowanie i przechowywanie silnych, losowych haseł dla każdego konta. Te hasła są zazwyczaj długie, zawierają różne znaki, co znacznie utrudnia próby złamania hasła poprzez atak brute force. Takie frazy są ciężkie do zapamiętania bez menedżera haseł, dlatego aplikacja Inlockly™ zapamięta je za Ciebie i automatycznie uzupełni przy próbie logowania na zaufanych witrynach.

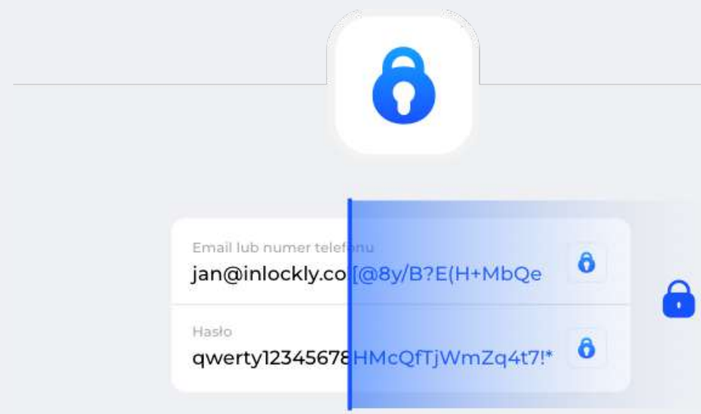
Ostrzeżenia o słabych hasłach

Inlockly™ automatycznie oblicza siłę hasła i ostrzega użytkowników przed stosowaniem słabych fraz, co motywuje do korzystania z bardziej bezpiecznych kombinacji.

Ochrona przed keyloggingiem

Inlockly™ pomaga w ochronie przed keyloggingiem, czyli rejestrowaniem klawiszy przez złośliwe oprogramowanie, poprzez zastosowanie następującego środka bezpieczeństwa:





Automatyczne wypełnianie formularzy

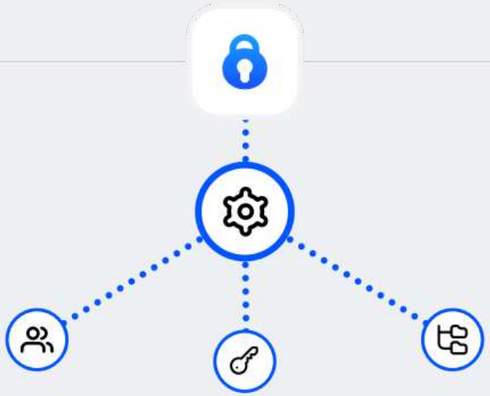
Menedżer haseł automatycznie wypełnia pola formularzy logowania, eliminując konieczność wprowadzania haseł za pomocą klawiatury. To niweluje ryzyko przechwycenia haseł poprzez keyloggera.

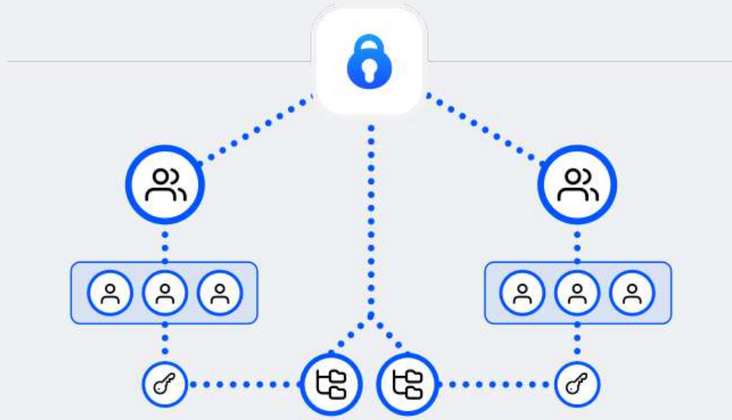
Szyfrowanie danych

Dane przechowywane są w zaszyfrowanej formie, zarówno w pamięci lokalnej, jak i w chmurze. Szyfrowanie uniemożliwia dostęp do prywatnych danych, w tym haseł, w postaci czytelnej dla człowieka.

Bezpieczne udostępnianie danych pomiędzy pracownikami

Menedżer haseł może znacząco wspomagać bezpieczne udostępnianie danych pomiędzy pracownikami poprzez wprowadzenie kilku kluczowych funkcji i praktyk:





Udostępnianie bezpośrednio z menedżera

Menedżer haseł umożliwia udostępnianie danych dostępowych bezpośrednio z aplikacji, eliminując konieczność przesyłania ich poprzez niezabezpieczone kanały komunikacyjne. Pracownicy mogą udostępniać między sobą dostęp do poufnych informacji bez konieczności jakiekolwiek przesyłania.

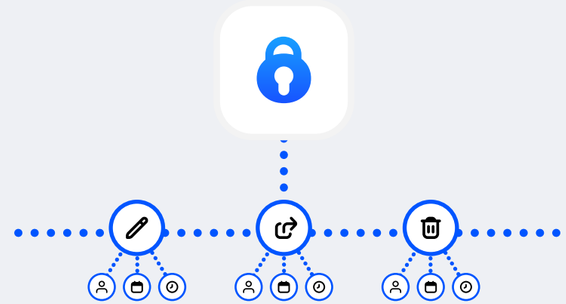
Zarządzanie uprawnieniami

Menedżer haseł pozwala na precyzyjne zarządzanie uprawnieniami dostępu do haseł. Administratorzy mogą określać, kto ma dostęp do jakich zasobów i na jakich warunkach, co zwiększa kontrolę nad udostępnianiem informacji.

Bezpieczne udostępnianie danych pomiędzy pracownikami

Menedżer haseł może znacząco wspomagać bezpieczne udostępnianie danych pomiędzy pracownikami poprzez wprowadzenie kilku kluczowych funkcji i praktyk:





Bezpieczne udostępnianie hasła zewnętrznym partnerom

W przypadku współpracy z zewnętrznymi partnerami czy dostawcami, menedżer haseł umożliwia szyfrowane udostępnianie danych dostępowych, eliminując potrzebę przesyłania ich za pośrednictwym niebezpiecznych metod, takich jak wiadomości tekstowe.

Historia i śledzenie działań

Menedżer haseł oferuje funkcje śledzenia działań i historii udostępniania. To umożliwia monitorowanie, kto i kiedy miał dostęp do konkretnych danych, co może być przydatne w przypadku audytów bezpieczeństwa.

Co sprawia, że aplikacja Inlockly™ jest bezpieczna?

Bezpieczeństwo Twojej firmy to nasz priorytet.

Podejście z którego korzystamy na co dzień to "prywatność w fazie projektowania". Oznacza to, że każda decyzja projektowa rozpoczyna się z myślą o bezpieczeństwie i prywatności użytkownika oraz jego danych.

Informacje i dane przechowywane w Inlockly™ są szyfrowane i tylko Ty posiadasz klucz (na swoim urządzeniu) pozwalający na ich odszyfrowanie. Inlockly™ jest zaprojektowany tak, aby chronić użytkownika przed naruszeniami i innymi zagrożeniami. Nawet programiści i inni pracownicy Inlockly™ nie mają możliwości podejrzeć lub udostępnić chronionych danych i informacji poufnych użytkownika.

Wyłącznie Ty możesz uzyskać dostęp do swoich prywatnych danych przechowywanych w Inlockly™.

Twoje dane w Inlockly™ są w pełni zaszyfrowane w celu zapewnienia bezpieczeństwa. Korzystamy z zaawansowanych technik szyfrowania i zabezpieczeń takich jak AES-256-GCM oraz Argon2id, aby mieć pewność, że tylko Ty posiadasz dostęp do swoich informacji.

RODO
ZGODNOŚĆ

CCPA
ZGODNOŚĆ

Z myślą o bezpieczeństwie Twoich danych

Twoje hasło główne

Chroni Twoje dane na zalogowanym urządzeniu. Tylko Ty znasz swoje hasło główne. Nigdy nie zostaje one przesłane do serwera Inlockly™.

Twoje klucze szyfrujące

Tworzone są lokalnie na Twoim urządzeniu i zabezpieczone dzięki hasłu głównemu. Klucze szyfrujące zabezpieczają dane w chmurze.

Automatyczne czyszczenie schowka

Inlockly™ automatycznie wyczyści schowek po użyciu skopiowanych wrażliwych danych takich jak loginy i hasła.

SafetyMeter™ - prywatny ochroniarz

SafetyMeter™ to narzędzie informujące Cię o wykrytych potencjalnych zagrożeniach i naruszeniach bezpieczeństwa Twoich danych.

Automatyczne blokowanie urządzenia

Po dłuższym braku aktywności Inlockly™ automatycznie wyczyści pamięć i poprosi Cię o ponowne uwierzytelnienie.

Wydaliśmy raport bezpieczeństwa

W pełni udokumentowaliśmy nasz projekt oraz mechanizmy zabepieczeń, który dokładnie opisuje działanie najważniejszych punktów aplikacji. Każdy może się z nim zapoznać na naszej stronie internetowej pod adresem www.inlockly.com.

inlockly

Wypróbuj przez 14 dni za darmo

Aplikacja Inlockly™ na Twoim urządzeniu:



RODO ZGODNOŚĆ

CCPA ZGODNOŚĆ

Twój kod rabatowy:

EBOOK10

10% zniżki na pierwszą transakcję

Odwiedź nas na www.inlockly.com