Jak zdalnie wyczyścić (lub zablokować) laptopa lub komputer z systemem Windows 10 i 11?

Zdalne wyczyszczenie laptopa lub komputera PC może pomóc w ochronie danych w przypadku zgubienia lub kradzieży komputera. Jednak generalnie najlepiej jest uzupełnić go o pełne szyfrowanie dysku, ponieważ zdalne wymazywanie ma kilka ograniczeń. Wyjaśnię zalety obu i jak najlepiej chronić swoje dane.

Wiele organizacji i osób zaczęło stosować podstawowe środki bezpieczeństwa, takie jak wymaganie silniejszych haseł, wdrażanie uwierzytelniania dwuskładnikowego i zarządzanie kontrolą dostępu. Ale często zapomina się o ochronie na najgorsze scenariusze. Jednym z głównych przeoczeń jest **to, co się dzieje, gdy ktoś zgubi laptopa lub komputer zostanie skradziony**.

Jeśli nie zostaną wdrożone odpowiednie zabezpieczenia, osoby atakujące mogą skończyć z wszystkimi danymi na urządzeniu - tajemnicami osobistymi, własnością intelektualną, informacjami finansowymi, cennymi danymi firmy, wrażliwymi danymi klientów i nie tylko.

Stanowi to ogromne ryzyko zarówno dla osób, jak i organizacji. **Jednym z rozwiązań jest skonfigurowanie zdalnego czyszczenia na urządzeniach**. Dzięki temu administratorzy mogą usuwać dane, nawet jeśli komputer został zgubiony lub skradziony (choć istnieją pewne ograniczenia). Innym przydatnym środkiem bezpieczeństwa jest **wdrożenie pełnego szyfrowania dysku**, aby złodziej nie mógł uzyskać dostępu do żadnych danych na laptopie, chyba że uda mu się również ukraść klucz.

Każda z tych technik może być bardziej skomplikowana niż się wydaje na początku, a każda z nich ma swoje wady i zalety. Z tego powodu istnieją pewne przypadki użycia, w których jedna opcja jest lepsza od drugiej lub oba mechanizmy można połączyć, jeśli poziom zagrożenia jest wystarczająco wysoki.

1. Co to jest zdalne czyszczenie?

Zdalne wymazywanie umożliwia usuwanie danych z laptopa lub komputera bez konieczności przebywania przed urządzeniem. Jest to kluczowa funkcja, którą zarówno osoby fizyczne, jak i firmy powinny rozważyć wdrożenie na wszystkich komputerach zawierających wrażliwe lub cenne dane.

Należy to wcześniej skonfigurować, ale jeśli włączone są funkcje zdalnego czyszczenia, właściciel może usunąć dane i uniemożliwić atakującemu kradzież informacji lub wykorzystanie danych do dalszych cyberataków. Dzięki temu zdalne czyszczenie może być cennym narzędziem do zapobiegania naruszeniom danych.

Jeśli rozumiesz już znaczenie zdalnego wymazywania i innych mechanizmów bezpieczeństwa, takich jak pełne szyfrowanie dysku, zapoznaj się z poniższymi sekcjami, aby dowiedzieć się, jak je skonfigurować. Jeśli nadal nie masz pewności, jakiego rodzaju atakom mogą zapobiec, przejdź do sekcji **Dlaczego należy włączyć zdalne czyszczenie lub pełne szyfrowanie dysku?** sekcji, aby zobaczyć, jakie szkody mogą wystąpić, gdy te środki nie są na miejscu.

2. Jak zdalnie wyczyścić laptopa?

Różne programy mogą zdalnie wyczyścić komputer. W tym pokazie **użyje Prey**, ponieważ jest to oprogramowanie typu open source i nie musisz płacić za jego konfigurację, chociaż jeśli urządzenie zostanie skradzione i zdecydujesz się je wyczyścić, będziesz musiał zapłacić za subskrypcję pro na tym etapie. Należy pamiętać, że Prey należy skonfigurować z wyprzedzeniem - gdy laptop został już zgubiony lub skradziony, jest już za późno na zainstalowanie oprogramowania do zdalnego czyszczenia.

3. Zanim Twoje urządzenie zostanie zgubione lub skradzione

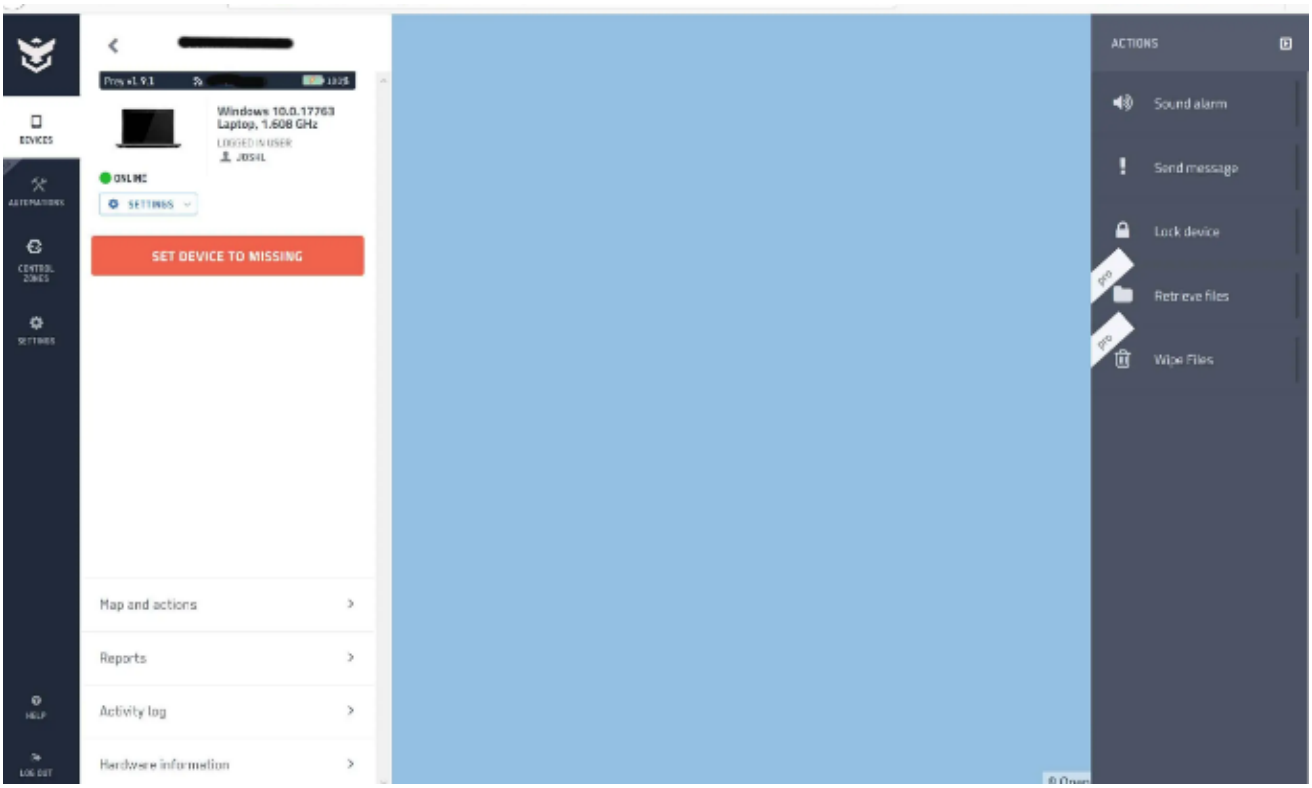
Aby rozpocząć, przejdź do strony pobierania Prey i wybierz odpowiednią wersję dla swojego komputera lub urządzenia. W tym pokazie będziemy używać 64-bitowej wersji systemu Windows. Po kliknięciu na pobrany plik naciśnij **Zapisz plik** w wyświetlonym oknie dialogowym:

Po zakończeniu pobierania pliku otwórz go, aby uruchomić kreatora instalacji. Gdy dojdziesz do ekranu powitalnego, kliknij **Dalej**, a następnie **Zgadzam się**, gdy pojawi się umowa licencyjna. Na następnym ekranie wybierz folder docelowy, w którym chcesz zainstalować Prey, lub pozostaw go jako opcję domyślną. Kliknij **Zainstaluj**.

Kiedy kreator zakończy instalację, upewnij się, że zaznaczyłeś pole wyboru, aby uruchomić Prey, a następnie kliknij **Zakończ**. Spowoduje to wyświetlenie następującej strony w Twojej przeglądarce internetowej:

Zakładając, że konfigurujesz Prey po raz pierwszy, kliknij **NOWY UŻYTKOWNIK**, a następnie wpisz swoje imię i nazwisko, adres e-mail i hasło w wyświetlonych polach. Kliknij pole w reCAPTCHA, aby udowodnić, że nie jesteś robotem, a także pola wyboru wskazujące, że masz ukończone 16 lat i zapoznałeś się z regulaminem. Kliknij niebieski przycisk **ZAREJESTRUJ SIĘ** pod nimi.

Spowoduje to uruchomienie panelu sterowania Prey, który pokaże ostatnią znaną lokalizację urządzenia:



Zwróć uwagę, że na tym zrzucie ekranu mapa została przeniesiona na środek oceanu ze względu na ochronę prywatności. Zwykle pokaże twój obszar z polem, które odnotowuje twoją ostatnią znaną lokalizację.

Po uruchomieniu Prey oferuje szereg funkcji, takich jak usługi lokalizacyjne, zdalne blokowanie i zdalne czyszczenie, z których można korzystać w razie potrzeby.

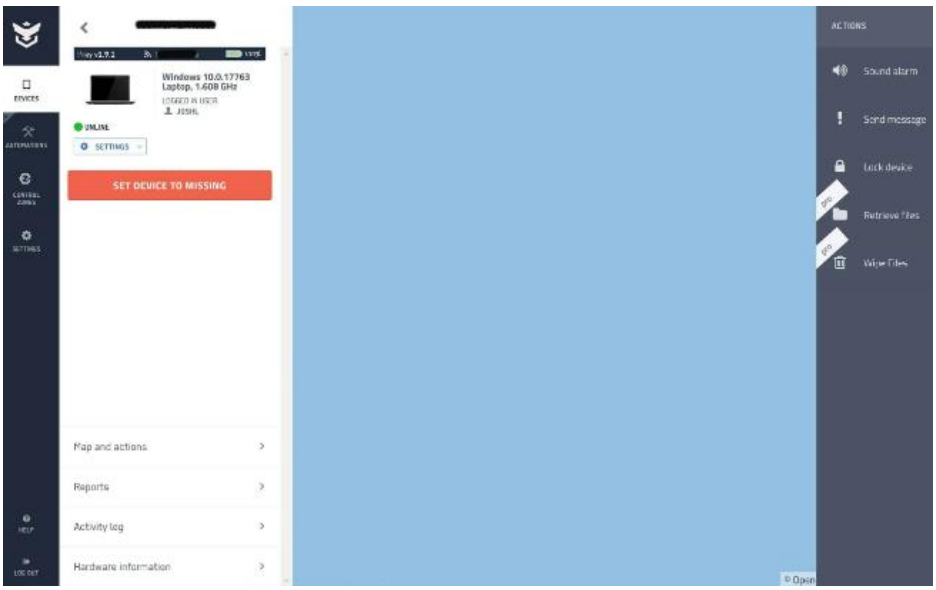
4. Po zgubieniu lub kradzieży urządzenia

Załóżmy, że doszło do tragedii, a Twój laptop został zgubiony lub skradziony. Jedyną oszczędną łaską jest to, że miałeś dalekowzroczność, aby zainstalować zdalne narzędzie do czyszczenia, takie jak Prey, aby ograniczyć potencjalne uszkodzenia. Pierwszym krokiem jest wejście na stronę Prey, podanie swoich danych i zalogowanie się:

Po zalogowaniu kliknij brakujące urządzenie. Pokaże, kiedy ostatnio był połączony z Internetem i gdzie się znajdował. Jeśli masz szczęście, że zostałeś okradziony przez nieudolnego złodzieja, połączą się z Internetem, ujawniając lokalizację urządzenia.

Następnie możesz wykorzystać te informacje, aby wyśledzić komputer lub przekazać go policji, aby pomóc im w dochodzeniu. Dane o lokalizacji są również przydatne w przypadkach, gdy urządzenie zostało po prostu zgubione - jeśli nadal jest połączone z Internetem. Panel sterowania Prey znacznie ułatwia jego odnalezienie.

Jeśli urządzenie zostało skradzione, ważne **jest, aby ograniczyć złodziejowi dostęp do plików komputera**. W prawej kolumnie znajduje się kilka różnych opcji:



Jeśli chcesz zdalnie wyczyścić urządzenie i trwale usunąć pliki, kliknij opcję **Zdalne czyszczenie** na dole kolumny. Niestety ta funkcja nie jest dostępna w bezpłatnym abonamencie, więc aby wyczyścić urządzenie, musisz subskrybować Prey Pro.

Jeśli nie zarejestrowałeś się jeszcze w Prey Pro i naprawdę potrzebujesz zdalnego czyszczenia komputera, kliknij **Aktualizuj swój plan** w wyskakującym okienku i skorzystaj z łączy, aby wyczyścić urządzenie. Spowoduje to usunięcie danych z komputera, o ile jest on nadal podłączony do Internetu.

Jeśli chcesz skonfigurować zdalne czyszczenie w przypadku kradzieży, ale nie chcesz rejestrować się w Prey Pro, istnieje szereg innych alternatyw oprogramowania. Zarówno Microsoft 365, jak i Microsoft Enterprise Mobility + Security są dostarczane z usługą **Intune**, którą można skonfigurować z wyprzedzeniem, aby można było zdalnie wyczyścić zgubione lub skradzione urządzenia. Inne firmy, takie jak Absolute i Meraki, również oferują rozwiązania do zdalnego czyszczenia.

5. Ograniczenia zdalnego czyszczenia

Zdalne wymazywanie wydaje się idealnym rozwiązaniem zapewniającym bezpieczeństwo danych w najgorszych przypadkach, ale jego zastosowania są w rzeczywistości bardziej ograniczone niż mogłoby się wydawać. Jednym z istotnych problemów jest opóźnienie między potencjalną kradzieżą

a zdalnym czyszczeniem. Innym problemem jest to, że urządzenie musi być połączone z Internetem, aby zdalne czyszczenie działało.

6. Czas między kradzieżą a wyczyszczeniem

Kiedy coś zostaje skradzione, często nie zauważamy tego od razu. Mogą minąć godziny, dni, a nawet tygodnie, zanim zdamy sobie sprawę, że nasz komputer został skradziony. To opóźnienie jest krytyczne, ponieważ sprytnemu złodziejowi może zająć tylko kilka minut, aby uzyskać dostęp do danych ze skradzionego laptopa.

Nawet w rzadkich przypadkach, gdy jesteś świadkiem kradzieży laptopa i możesz ścigać się, aby się zalogować i zdalnie wyczyścić komputer, złodziej może uzyskać dostęp do danych przed tobą. W mniej sprzyjających okolicznościach mogli mieć dni na przeglądanie akt i dostęp do wszystkiego, czego pragną. Niestety, zdalne czyszczenie nie może zrobić nic, aby powstrzymać złodzieja, który uzyskał dostęp do danych przed jego wykonaniem.

7. Urządzenie musi być online

Innym ograniczeniem zdalnego czyszczenia jest to, że skradzione urządzenie musi być w trybie online, aby mogło działać. Każdy złodziej, który wie, co robi, zatrzyma laptopa w trybie offline właśnie z tych powodów - nie chcą, aby urządzenie było śledzone ani dane, aby zostały wyczyszczone. Oznacza to, że możesz nigdy nie mieć szansy na skorzystanie z funkcji zdalnego czyszczenia, której konfiguracja wymaga tak dużego wysiłku.

Jeśli urządzenie jest podłączone do Internetu po kradzieży, to prawdopodobnie złodziej jest amatorem lub po prostu kradnie sam laptop, aby go sprzedać. W takich przypadkach jest mało prawdopodobne, że atakują one dane komputera, więc zdalne czyszczenie może nie być konieczne.

8. Czy dane faktycznie są usuwane?

Odzyskiwanie danych po ich wyczyszczeniu lub usunięciu pozostaje tematem, który budzi wiele dyskusji. Możliwość odzyskania danych zależy od szeregu czynników, w tym od metody użytej do wyczyszczenia dysku, rodzaju dysku (nowoczesny SSD czy starszy HDD) oraz od zaawansowania technologicznego potencjalnego atakującego.

W świetle współczesnych badań i postępu technologicznego, ogólnie uważa się, że odpowiednie metody nadpisywania danych są skuteczne w zapobieganiu odzyskaniu danych przez nieuprawnione osoby. Jednakże, w przypadku dysków SSD, proces ten może być bardziej skomplikowany ze względu na ich wewnętrzną architekturę i sposób działania. Technologie takie jak TRIM w dyskach SSD mogą również wpływać na możliwość odzyskania danych.

Jeśli chodzi o potencjalnych atakujących, to z biegiem lat narzędzia do odzyskiwania danych stały się bardziej zaawansowane. W związku z tym, w przypadku szczególnie wrażliwych danych, zaleca się stosowanie wielokrotnego nadpisywania, fizyczne zniszczenie nośnika lub korzystanie z szyfrowania sprzętowego, które może zapewnić dodatkową warstwę ochrony.

Podsumowując, w 2024 roku, jednokrotne wyczyszczenie danych za pomocą odpowiedniego oprogramowania w większości przypadków powinno zapobiec ich odzyskaniu przez nieautoryzowane osoby. Niemniej jednak, w obliczu zaawansowanych ataków i w przypadku dysków SSD, zaleca się dodatkowe środki ostrożności.

9. Ochrona skradzionych urządzeń za pomocą pełnego szyfrowania dysku

Szyfrowanie pełnego dysku (FDE) pozostaje kluczowym elementem ochrony danych na zgubionych lub skradzionych laptopach. W 2024 roku, FDE nadal jest preferowaną metodą ochrony, ponieważ zapewnia stałą ochronę danych bez względu na to, czy urządzenie jest podłączone do Internetu, czy nie. Oto zaktualizowane informacje na temat FDE i jego implementacji w systemie Windows:

Szyfrowanie Pełnego Dysku (FDE):

- **Zabezpieczenie danych:** FDE zapewnia, że wszystkie dane na dysku są zaszyfrowane, co uniemożliwia dostęp osobom nieupoważnionym bez odpowiedniego klucza.
- **Ochrona przed nieautoryzowanym dostępem:** Nawet jeśli laptop zostanie zgubiony lub skradziony, dane pozostają bezpieczne, ponieważ są niedostępne bez klucza szyfrującego.
- **Nie wymaga połączenia internetowego:** FDE jest skuteczne bez względu na status połączenia z Internetem, co oznacza, że dane są chronione nawet wtedy, gdy zdalne czyszczenie nie jest możliwe.

Implementacja FDE w Windows:

- **BitLocker:** W systemach Windows Pro, Enterprise i Education, BitLocker jest wbudowaną funkcją, która umożliwia szyfrowanie dysków. Wymaga ona modułu TPM (Trusted Platform Module) dla najlepszej ochrony, ale istnieją metody umożliwiające jego użycie nawet bez TPM.
- **VeraCrypt:** Dla użytkowników systemu Windows Home lub tych, którzy preferują alternatywne rozwiązania, VeraCrypt oferuje darmowe i otwarte oprogramowanie do szyfrowania dysków. VeraCrypt jest ceniony za swoją transparentność i niezależność od dużych korporacji.

W obecnym roku, zaleca się stosowanie FDE jako standardowej praktyki ochrony danych, szczególnie w środowiskach korporacyjnych i dla osób, które przechowują wrażliwe informacje na swoich urządzeniach. Dodatkowo, w miarę rozwoju technologii, użytkownicy powinni być świadomi nowych metod i narzędzi szyfrowania, które mogą oferować jeszcze lepszą ochronę danych.

10. Konfigurowanie pełnego szyfrowania dysku za pomocą funkcji BitLocker

Proces szyfrowania dysku za pomocą funkcji BitLocker w systemie Windows:

1. **Logowanie jako Administrator:** Zaloguj się do systemu Windows przy użyciu konta z uprawnieniami administratora.

2. **Uruchomienie BitLocker:** Przejdź do Panelu sterowania i wybierz opcję ‘Szyfrowanie dysków funkcją BitLocker’. Kliknij ‘Włącz funkcję BitLocker’, a system sprawdzi, czy komputer spełnia wymagania, w tym obecność układu TPM.

3. **Wybór Metody Autoryzacji:** Gdy BitLocker będzie gotowy do użycia, wybierz metodę autoryzacji – zaleca się użycie silnego hasła.

4. **Tworzenie Silnego Hasła:** Użyj silnego, unikalnego hasła i zapisz je w bezpiecznym miejscu. Unikaj prostych lub powtarzalnych haseł, które mogą osłabić ochronę szyfrowania.

5. **Opcje Odzyskiwania Klucza:** Microsoft oferuje różne opcje na wypadek zapomnienia klucza. Zaleca się zapisanie klucza odzyskiwania na nośniku USB lub wydrukowanie go i przechowywanie w bezpiecznym miejscu.

6. **Zakres Szyfrowania:** Wybierz, czy chcesz zaszyfrować cały dysk lub tylko używane miejsce. Dla nowych dysków zaleca się szyfrowanie tylko używanego miejsca, natomiast dla dysków już w użyciu – szyfrowanie całego dysku.

7. **Tryb Szyfrowania:** Wybierz 'Nowy tryb szyfrowania' przeznaczony dla stałych dysków twardych.

8. **Restart i Szyfrowanie:** Po konfiguracji BitLocker poprosi o restart komputera. Po ponownym uruchomieniu i wprowadzeniu hasła rozpocznie się proces szyfrowania.

9. **Przechowywanie Hasła:** Przechowuj hasło w bezpiecznym miejscu, ponieważ jest ono niezbędne do odblokowania zaszyfrowanego dysku.

Dostępne mogą być dodatkowe opcje szyfrowania i zabezpieczeń, które warto rozważyć w zależności od indywidualnych potrzeb i wymagań systemu. Zawsze aktualizuj system operacyjny i oprogramowanie zabezpieczające, aby korzystać z najnowszych funkcji ochrony danych.

11. Ograniczenia pełnego szyfrowania dysku

Szyfrowanie pełnego dysku (FDE) nadal jest jednym z najważniejszych elementów strategii bezpieczeństwa danych, ale jak każda technologia, ma swoje ograniczenia i wymaga odpowiedniego zarządzania. Informacje na temat FDE i bezpieczeństwa haseł:

Zarządzanie Hasłami:

- **Kompleksowość:** Używanie skomplikowanych haseł jest kluczowe. Powinny one zawierać różne znaki, takie jak litery, cyfry i symbole.
- **Unikalność:** Każde konto powinno mieć unikalne hasło, aby kompromitacja jednego nie prowadziła do ryzyka dla innych.
- **Menedżery Haseł:** Korzystanie z menedżerów haseł może pomóc w zarządzaniu silnymi i unikalnymi hasłami, jednocześnie zapewniając ich bezpieczne przechowywanie.
- **Bezpieczeństwo Fizyczne:** Hasła nie powinny być zapisywane w miejscach łatwo dostępnych dla osób nieupoważnionych.
- **Inżynieria Społeczna:** Świadomość zagrożeń związanych z inżynierią społeczną i odpowiednie szkolenia mogą pomóc w ochronie przed atakami tego typu.

Bezpieczeństwo Algorytmów Szyfrowania:

- **Równowaga między Bezpieczeństwem a Wydajnością:** Algorytmy szyfrowania muszą znaleźć równowagę między bezpieczeństwem a wydajnością. Zbyt skomplikowane algorytmy mogą negatywnie wpływać na wydajność systemu.

- **Postęp Technologiczny:** Z czasem technologia się rozwija, a to, co kiedyś było uważane za bezpieczne, może stać się podatne na ataki. Na przykład, algorytm DES został zastąpiony przez AES z uwagi na większe bezpieczeństwo.

AES-256 jako Standard:

- **Obecny Standard:** AES-256 jest uważany za solidny standard szyfrowania symetrycznego, trudny do złamania nawet przez najbardziej zaawansowane organizacje.

- **Przyszłość AES:** Podobnie jak DES w przeszłości, istnieje możliwość, że w przyszłości AES-256 może zostać pokonany w wyniku postępu technologicznego i kryptoanalizy.

Długoterminowe Bezpieczeństwo Danych:

- **Wyczyszczenie Dysków:** W przypadkach, gdy dane muszą pozostać bezpieczne przez bardzo długi czas, wyczyszczenie dysków może być bardziej skuteczne niż FDE.

- **Przechowywanie Zaszyfrowanych Danych:** Istnieją przesłanki, że niektóre organizacje mogą przechowywać zaszyfrowane dane w oczekiwaniu na przyszłe możliwości ich złamania.

Podsumowując, FDE wciąż jest ważnym narzędziem w ochronie danych, ale wymaga ono ścisłego przestrzegania dobrych praktyk zarządzania hasłami i świadomości potencjalnych przyszłych zagrożeń związanych z postępem technologicznym. Warto również zwrócić uwagę na nowe technologie szyfrowania, które mogą pojawić się w przyszłości, oferując jeszcze lepsze zabezpieczenia.

12. Łączenie zdalnego czyszczenia z pełnym szyfrowaniem dysku

Połączenie zdalnego czyszczenia i pełnego szyfrowania dysku (FDE) jest uważane za solidną strategię ochrony danych, szczególnie dla informacji, które mają długoterminową wartość:

- **Pełne Szyfrowanie Dysku (FDE):** FDE jest standardową praktyką w ochronie danych, zapewniającą, że wszystkie informacje na dysku są zaszyfrowane i dostępne tylko dla osób z odpowiednim kluczem.

- **Zdalne Czyszczenie:** W przypadku zgubienia lub kradzieży urządzenia, zdalne czyszczenie umożliwia administratorom usunięcie danych, uniemożliwiając nieautoryzowany dostęp.

- **Połączenie Obydwu Metod:** Używanie zarówno FDE, jak i zdalnego czyszczenia zapewnia warstwową ochronę. Złodziej nie uzyska dostępu do danych bez hasła, a zdalne czyszczenie może być zastosowane, jeśli urządzenie połączy się z Internetem.

- **Zarządzanie Hasłami:** Stosowanie silnych, unikalnych haseł i korzystanie z menedżerów haseł zmniejsza ryzyko złamania szyfrowania przez atakujących.

- **Dodatkowe Warstwy Ochrony:** Połączenie FDE i zdalnego czyszczenia daje więcej możliwości zabezpieczenia danych przed różnymi scenariuszami ataku, w tym przed zaawansowanymi technikami kryptoanalizy, które mogą pojawić się w przyszłości.

Podsumowując, w obecnym roku, najlepszą praktyką jest stosowanie zarówno FDE, jak i zdalnego czyszczenia, aby zapewnić kompleksową ochronę danych, które mają zachować swoją wartość przez

długi czas. Administratorzy powinni również regularnie przeglądać i aktualizować swoje protokoły bezpieczeństwa, aby odpowiadały one na rozwijające się zagrożenia i technologie.

13. Dlaczego należy włączyć zdalne czyszczenie lub pełne szyfrowanie dysku?

Gdy zdalne wymazywanie nie zostało włączone, a inne zabezpieczenia nie są stosowane, **osoby atakujące mogą uzyskać dostęp do wszystkiego, co znajduje się na laptopie lub komputerze**. Od masowych naruszeń danych po kradzieże IP, ten nadzór może mieć ogromny wpływ na firmy i osoby prywatne. To nie są tylko teoretyczne ataki. W przeszłości było wiele przykładów skradzionych laptopów lub innych urządzeń prowadzących do katastrof. Niektóre z nich to:

1. Naruszenie danych Veterans Affairs

Jedno z najbardziej szkodliwych naruszeń danych związanych z laptopami miało miejsce w 2006 roku. Nieszyfrowany laptop zawierający dane 26,5 miliona amerykańskich weteranów został skradziony z domu analityka danych.

Dane obejmowały numery ubezpieczenia społecznego, stopnie niepełnosprawności i inne dane osobowe. W 2009 roku Departament Spraw Weteranów zawarł ugodę z poszkodowanymi. Pozew zbiorowy początkowo żądał 1000 dolarów za każdą osobę, której dane zostały skradzione, jednak ostatecznie doszli do porozumienia na łączną wypłatę zaledwie 20 milionów dolarów.

W kontekście finansowym, ugoda na 20 milionów dolarów w 2009 roku może wydawać się niewielka w porównaniu z obecnymi standardami odszkodowań za naruszenia danych, które często osiągają setki milionów, a nawet miliardy dolarów, biorąc pod uwagę inflację i rosnącą wartość danych osobowych.

W dzisiejszych czasach, organizacje są bardziej skłonne do inwestowania w zabezpieczenia i technologie prewencyjne, aby uniknąć kosztów związanych z naruszeniami danych, które mogą obejmować nie tylko odszkodowania finansowe, ale również utratę zaufania i reputacji.

2. Kradzież MD Anderson Cancer Center

W latach 2012-2013 MD Anderson Cancer Center skradziono laptopa i dwa dyski USB. Kradzieże obejmowały niezaszyfrowane dane 34 800 pacjentów. Chociaż nie ma dowodów na to, że dostęp do danych osobowych miały osoby nieupoważnione, w 2017 r. teksańska firma została ukarana grzywną w wysokości 4,3 mln USD.

Firma odwołała się od decyzji Departamentu Zdrowia i Opieki Społecznej, ale kara została podtrzymana przez sędziego przewodniczącego. Sędzia Steven Kessel odrzucił argumenty MD Andersona, stwierdzając, że organizacja „… przez kolejne lata podejmowała tylko połowiczne i niepełne wysiłki w zakresie szyfrowania”.

Decyzją sędziego uznano, że nieistotne jest, czy dostęp do danych został uzyskany w sposób nieuprawniony. Orzekł, że firma nie zabezpieczyła danych osobowych przed ujawnieniem, narażając ją na odpowiedzialność.

W kontekście finansowym, grzywna w wysokości 4,3 mln USD nałożona na MD Anderson Cancer Center w 2017 roku może być uważana za stosunkowo niską w porównaniu z obecnymi standardami, gdzie kary mogą sięgać dziesiątek, a nawet setek milionów dolarów, w zależności od skali naruszenia i liczby dotkniętych osób.

Podsumowując, incydent w MD Anderson Cancer Center służy jako przestroga dla innych organizacji, aby nieustannie aktualizować i wzmacniać swoje protokoły bezpieczeństwa danych, aby uniknąć podobnych naruszeń i ich długoterminowych konsekwencji.

3. Kradzież laptopa Coplin Health Systems

Na początku 2018 roku jednej z firm opieki zdrowotnej w Zachodniej Wirginii skradziono jeden ze swoich laptopów z samochodu pracownika. Laptop należał do Coplin Health Systems i był chroniony hasłem, jednak dane nie były szyfrowane, ani nie włączono zdalnego czyszczenia, co pozostawiło otwartą możliwość uzyskania dostępu do danych 43 000 pacjentów.

Informacje o pacjentach obejmowały dane dotyczące zdrowia, numery ubezpieczenia społecznego i informacje finansowe. Na tym etapie nie ma dowodów na to, że hakerzy nadużywali danych, ale Coplin Health Systems nadal był zobowiązany do powiadomienia tych, których to dotyczyło, a także Biura Praw Obywatelskich Departamentu Zdrowia i Opieki Społecznej. Dzieje się tak, ponieważ laptop nie posiadał odpowiednich zabezpieczeń, a kradzież nadal stanowiła zagrożenie dla pacjentów i ich danych.

W świetle dzisiejszych standardów, Coplin Health Systems prawdopodobnie wdrożyłoby szereg środków bezpieczeństwa, takich jak:

- **Pełne Szyfrowanie Dysku (FDE):** Zapewniające, że wszystkie dane na laptopie są zabezpieczone i nieczytelne bez odpowiedniego klucza szyfrującego.
- **Zdalne Czyszczenie:** Umożliwiające administratorom zdalne usunięcie danych z urządzenia w przypadku zgubienia lub kradzieży.
- **Autoryzacja Wieloskładnikowa (MFA):** Wymagająca dodatkowego poziomu weryfikacji oprócz hasła, co zwiększa bezpieczeństwo dostępu do urządzeń.

W przypadku naruszenia danych, Coplin Health Systems musiałoby również przestrzegać nowych przepisów dotyczących ochrony danych, takich jak GDPR lub HIPAA, które wymagają od organizacji nie tylko informowania dotkniętych osób, ale także podejmowania działań naprawczych i zapobiegawczych.

Podsumowując, w 2024 roku, organizacje zdrowotne, takie jak Coplin Health Systems, są bardziej przygotowane na ryzyko związane z utratą urządzeń i mają obowiązek stosowania najlepszych dostępnych technologii i praktyk, aby chronić dane pacjentów przed nieautoryzowanym dostępem.

4. Skradziony laptop z Eir

Kradzieże laptopów są tak powszechne i szkodliwe nie tylko w Stanach Zjednoczonych. Eir, irlandzka firma telekomunikacyjna, również miała skradziony laptop pracownika w 2018 roku. Chociaż laptop miał być chroniony hasłem i zaszyfrowany, wadliwa aktualizacja zabezpieczeń z dnia poprzedzającego kradzież spowodowała, że dane laptopa zostały odszyfrowane, gdy został skradziony.

Usterka umożliwiła złodziejowi dostęp do danych 37 000 klientów Eir. Dane zawierały nazwiska, adresy e-mail, numery kont i numery telefonów, jednak firma stwierdziła, żeżadne dane finansowe nie są zagrożone.

Firma zgłosiła incydent do komisarza ds. ochrony danych, a także do dotkniętych nim klientów. Ten incydent pokazuje, jak czujne muszą być firmy, aby chronić swoje dane. Chociaż luki w zabezpieczeniach są niefortunną rzeczywistością, możliwe, że funkcja zdalnego czyszczenia mogła chronić dane przed nieautoryzowanym dostępem.

W obecnych czasach, firmy telekomunikacyjne jak Eir prawdopodobnie wdrożyłyby dodatkowe środki bezpieczeństwa, takie jak:

- **Zaawansowane Szyfrowanie:** Stosowanie silniejszych algorytmów szyfrowania, które są odporne na błędy w aktualizacjach zabezpieczeń.
- **Zdalne Czyszczenie:** Implementacja zdalnego czyszczenia, które pozwala na usunięcie danych z urządzenia w przypadku jego utraty lub kradzieży.
- **Autoryzacja Wieloskładnikowa (MFA):** Wymaganie dodatkowej weryfikacji tożsamości użytkownika, co zmniejsza ryzyko nieautoryzowanego dostępu nawet w przypadku skradzionego urządzenia.
- **Regularne Audyty Bezpieczeństwa:** Przeprowadzanie regularnych audytów bezpieczeństwa, aby wykrywać i naprawiać luki w zabezpieczeniach przed ich wykorzystaniem przez złodziei.

W kontekście zgłaszania incydentów, firmy takie jak Eir są teraz bardziej zobowiązane do szybkiego informowania zarówno organów regulacyjnych, jak i klientów o naruszeniach danych, zgodnie z obowiązującymi przepisami o ochronie danych, takimi jak GDPR.

Podsumowując, incydent związany z Eir podkreśla wagę proaktywnego podejścia do zarządzania ryzykiem cyberbezpieczeństwa i konieczność stosowania wielowarstwowych strategii ochrony danych w celu zapewnienia ich bezpieczeństwa w długoterminowej perspektywie.

5. *Kradzież laptopa kanadyjskiego Ministerstwa Zdrowia*

Pod koniec 2018 roku pracownikowi rządu w Kanadzie skradziono laptop. Niezaszyfrowany laptop został zabrany z zamkniętego samochodu i zawierał informacje zdrowotne dotyczące blisko 40 000 osób z Terytoriów Północno-Zachodnich.

Pomiędzy e-mailami a plikami laptop zawierał bardzo wrażliwe informacje zdrowotne, w tym zapisy dotyczące „… szczepień przeciwko HPV, C. difficile (zakażenia okrężnicy), wymazów, krztuśca, badań krwi na gruźlicę, infekcji przenoszonych drogą płciową i chorób opornych na antybiotyki, pośród innych."

Oprócz danych dotyczących zdrowia laptop zawierał również dane osobowe, które można wykorzystać do kradzieży tożsamości i innych przestępstw. Urządzenie najwyraźniej pozostawiono niezaszyfrowane, ponieważ był to hybrydowy tablet i laptop, które nie były kompatybilne z oprogramowaniem szyfrującym działu IT.

Laptop, który jest wymagany do obsługi tak poufnych informacji, nigdy nie powinien być udostępniany pracownikowi bez odpowiednich środków ochrony, bez względu na to, jak trudno jest

go zaszyfrować. Jeśli nie jest to możliwe, zamiast tego należy wydać bezpieczne urządzenie dla zadania.

W obecnych czasach, oczekuje się, że wszystkie urządzenia przechowujące wrażliwe dane, takie jak informacje zdrowotne, będą zabezpieczone za pomocą zaawansowanego szyfrowania i innych środków ochrony, takich jak zdalne czyszczenie i autoryzacja wieloskładnikowa (MFA).

W świetle dzisiejszych standardów, Ministerstwo Zdrowia w Kanadzie prawdopodobnie wdrożyłoby następujące środki bezpieczeństwa:

- **Pełne Szyfrowanie Dysku (FDE):** Zapewniające, że wszystkie dane na urządzeniu są zabezpieczone i nieczytelne bez odpowiedniego klucza szyfrującego.
- **Zdalne Czyszczenie:** Umożliwiające administratorom zdalne usunięcie danych z urządzenia w przypadku jego utraty lub kradzieży.
- **Autoryzacja Wieloskładnikowa (MFA):** Wymagająca dodatkowej weryfikacji tożsamości użytkownika, co zwiększa bezpieczeństwo dostępu do urządzeń.
- **Kompatybilność z Oprogramowaniem Szyfrującym:** Zapewnienie, że wszystkie urządzenia są kompatybilne z oprogramowaniem szyfrującym używanym przez organizację.

Podsumowując, incydent z kanadyjskim Ministerstwem Zdrowia podkreśla wagę nieustannego przeglądu i aktualizacji protokołów bezpieczeństwa, aby zapewnić, że nawet w przypadku kradzieży urządzenia, dane pozostaną chronione przed nieautoryzowanym dostępem.

6. *Kradzież laptopa Secret Service*

Z drugiej strony, w 2017 roku laptop służbowy agenta Secret Service został skradziony z samochodu w Nowym Jorku. Pomimo kradzieży laptop zawierał odpowiednie zabezpieczenia, aby złagodzić wszelkie potencjalne szkody.

Secret Service w pełni szyfruje laptopy swoich pracowników i nie pozwala na przechowywanie w nich żadnych tajnych informacji. Mają również możliwość zdalnego czyszczenia, dzięki czemu urządzenia stają się bezużyteczne dla atakujących. Chociaż niemożliwe jest powstrzymanie kradzieży, posiadanie kompleksowej polityki bezpieczeństwa cybernetycznego może pomóc w ograniczeniu ewentualnych szkód.

Kradzież laptopa agenta Secret Service z 2017 roku jest przykładem skuteczności stosowania zaawansowanych środków bezpieczeństwa w ochronie danych. W obecnych czasach, agencje rządowe i organizacje na całym świecie przykładają jeszcze większą wagę do zabezpieczeń cybernetycznych, aby chronić wrażliwe informacje przed nieautoryzowanym dostępem, nawet w przypadku fizycznej kradzieży urządzeń.

Przykłady znaczących przypadków kradzieży laptopów i innych urządzeń w latach 2019-2024:

1. **Ministerstwo Obrony Wielkiej Brytanii (MoD):** W ciągu ostatnich pięciu lat zgłoszono utratę ponad 1000 laptopów, 462 telefonów komórkowych, 265 pamięci USB i 183 dysków twardych zawierających wrażliwe i poufne dane[1].

2. **Rząd Wielkiej Brytanii:** Pracownicy rządowi zgubili lub mieli skradzione przynajmniej 2004 urządzenia mobilne w ciągu 12 miesięcy, w tym smartfony, laptopy i tablety[2].

3. **Departament Biznesu, Energii i Strategii Przemysłowej Wielkiej Brytanii:** W ciągu dwóch lat (2019-2020) zgłoszono utratę 234 telefonów komórkowych i 72 laptopów[3].

Te przypadki podkreślają znaczenie stosowania odpowiednich środków bezpieczeństwa, takich jak szyfrowanie i zdalne czyszczenie, aby chronić dane przed nieautoryzowanym dostępem w przypadku utraty lub kradzieży urządzeń.

Przykłady kradzieży laptopów i innych urządzeń w Polsce w latach 2019-2024 nie są szeroko dokumentowane w dostępnych źródłach. W przypadku takich zdarzeń, zazwyczaj zaleca się podjęcie następujących kroków:

- **Zgłoszenie kradzieży odpowiednim władzom:** Pierwszym krokiem jest zawsze zgłoszenie kradzieży policji.
- **Zmiana haseł:** Należy jak najszybciej zmienić hasła do wszystkich kont, które mogły być dostępne z urządzenia.
- **Powiadomienie banków i innych instytucji:** W przypadku, gdy na urządzeniu przechowywane były dane finansowe, należy jak najszybciej powiadomić odpowiednie instytucje.
- **Monitorowanie kont:** Ważne jest, aby monitorować swoje konta w mediach społecznościowych i pocztę elektroniczną pod kątem nieautoryzowanego dostępu.
- **Wykorzystanie funkcji zdalnego czyszczenia:** Jeśli urządzenie na to pozwala, warto skorzystać z opcji zdalnego czyszczenia danych.

W przypadku braku konkretnych przykładów z Polski, warto zwrócić uwagę na ogólne praktyki bezpieczeństwa, które pomagają w ochronie przed skutkami kradzieży urządzeń. Zawsze zaleca się stosowanie szyfrowania danych i regularne tworzenie kopii zapasowych, aby zminimalizować ryzyko utraty ważnych informacji.

Zdalne czyszczenie i pełne szyfrowanie dysku minimalizują ryzyko

Świadomość zagrożeń cybernetycznych i konieczność zabezpieczenia urządzeń elektronicznych jest większa niż kiedykolwiek. Organizacje na całym świecie zdają sobie sprawę, że odpowiednie zabezpieczenia są niezbędne do ochrony cennych danych przed kradzieżą i naruszeniami bezpieczeństwa.

Zdalne Czyszczenie i Pełne Szyfrowanie Dysku:

- **Zdalne Czyszczenie:** Konfiguracja zdalnego czyszczenia stała się standardową praktyką, pozwalającą na szybkie usunięcie danych z urządzenia w przypadku jego utraty lub kradzieży.
- **Pełne Szyfrowanie Dysku (FDE):** Pełne szyfrowanie dysku jest teraz powszechnie stosowane, aby zapewnić, że dane są nieczytelne bez odpowiedniego klucza szyfrującego.

Koszty vs. Korzyści:

- **Koszty Zabezpieczeń:** Chociaż konfiguracja tych zabezpieczeń może wydawać się czasochłonna lub skomplikowana, jest to niewielka cena w porównaniu z potencjalnymi kosztami związanymi z naruszeniem danych.

- **Korzyści:** Ochrona danych nie tylko chroni przed stratami finansowymi, ale także pomaga w utrzymaniu reputacji i zaufania klientów.

Zmiana Mentalności:

- **Proaktywność:** Organizacje stały się bardziej proaktywne w stosowaniu środków bezpieczeństwa, zamiast reagować po fakcie.

- **Edukacja:** Edukacja pracowników na temat cyberbezpieczeństwa stała się kluczowym elementem strategii bezpieczeństwa.

Zabezpieczenie urządzeń elektronicznych jest uważane za niezbędny element zarządzania ryzykiem w każdej organizacji. Zdalne czyszczenie i pełne szyfrowanie dysku są powszechnie akceptowanymi metodami ochrony danych, a ich implementacja jest uważana za standardową procedurę operacyjną.