IBM Security Trusteer Rapport

Podręcznik

Wersja 3.5.1403

Grudzień 2014 r.

*new threats, **new thinking***

Uwagi

Niniejsza publikacja została opracowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych. IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego:

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE **"AS IS"** BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy typograficzne. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych podmiotów zostały wprowadzone wyłącznie dla wygody użytkownika i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, zostanie uiszczona stosowna opłata.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów innych niż produkty IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. IBM nie testował tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów innych podmiotów należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych. Ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Wszelkie podane tu informacje mogą zostać zmienione, zanim opisywane produkty staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennej pracy. W celu kompleksowego ich zilustrowania podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

Licencja w zakresie praw autorskich

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym IBM.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty niniejszego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. 2004, 2014. Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Znaki towarowe

IBM, logo IBM oraz ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corp. zarejestrowanymi w wielu systemach prawnych na całym świecie. Nazwy innych produktów i usług mogą być znakami towarowymi IBM lub innych podmiotów. Aktualna lista znaków towarowych IBM jest dostępna w serwisie WWW, w sekcji "Copyright and trademark information" (Informacje o prawach autorskich i znakach towarowych), pod adresem www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript oraz wszystkie pochodne znaki towarowe są zastrzeżonymi znakami towarowymi lub znakami towarowymi Adobe Systems Incorporated w Stanach Zjednoczonych i w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Java oraz wszystkie znaki towarowe i logo dotyczące języka Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Postanowienia dotyczące ochrony prywatności

Oprogramowanie IBM, w tym rozwiązanie SaaS (Software as a Service), zwane dalej "Oferowanym Oprogramowaniem" może korzystać z informacji cookie lub z innych technologii do gromadzenia danych o używaniu produktów, do poprawienia jakości usług dla użytkowników końcowych, do dopasowania interakcji do ich oczekiwań oraz do innych celów. W wielu przypadkach Oferowane Oprogramowanie nie gromadzi informacji pozwalających na identyfikację osoby.

Więcej informacji na temat korzystania z różnych technologii, w tym z informacji cookie, do opisanych wyżej celów znajduje się w sekcji "IBM Software Products and Software-as-a-Service Privacy Statement" pod adresem http://www.ibm.com/software/info/product-privacy.

Spis treści

1. Informacje wstępne

O tym podręczniku

W tym podręczniku wyjaśniono sposób korzystania z programu IBM Security Trusteer Rapport ("**Rapport**") w sposób zapewniający optymalne wykorzystanie jego możliwości. Podręcznik jest przeznaczony dla:

- klientów banków i innych instytucji finansowych, oferujących program Rapport do bezpłatnego pobrania jako narzędzie chroniące rachunki bankowe obsługiwane za pośrednictwem Internetu;
- klientów korzystających z kart płatniczych chronionych przez program Rapport, korzystających z programu Rapport do zabezpieczenia transakcji realizowanych online za pomocą kart płatniczych.

Więcej informacji na temat programu Rapport

Jako uzupełnienie tego podręcznika dostępna jest opracowana przez IBM strona http://www.trusteer.com/support/faq, zawierająca często zadawane pytania.

Na stronie WWW zawierającej często zadawane pytania należy wprowadzić swoje pytanie w narzędziu Błyskawiczne odpowiedzi w celu uzyskania odpowiedzi na dodatkowe, mogące się pojawić pytania i wątpliwości.

Przesyłanie opinii

Opinie użytkowników są dla IBM bardzo ważne.

- Zachęcamy do przesyłania sugestii dotyczących nowych funkcji oraz udoskonaleń i wyrażania swoich opinii na temat programu Rapport.

W celu przesłania opinii na temat programu Rapport należy przejść pod adres:

http://www.trusteer.com/support/product-feedback.

Informacje o wsparciu

Informacje na temat wsparcia są dostępne w serwisie:

http://www.trusteer.com/support

Ułatwienia dostępu

Ułatwienia dostępu pomagają użytkownikom niepełnosprawnym, np. osobom z upośledzoną motoryką lub niedowidzącym, w efektywnym korzystaniu z oprogramowania. Opisywany tutaj produkt oferuje ułatwienia dostępu polegające na możliwości nawigacji w interfejsie na podstawie informacji odczytywanych na głos przez program.

Sprawdzone procedury w zakresie bezpieczeństwa

Bezpieczeństwo systemów informatycznych wymaga ochrony systemów i informacji poprzez działania prewencyjne, wykrywanie zagrożeń i reagowanie w przypadku niewłaściwego dostępu w obrębie organizacji i poza nią. Niewłaściwy dostęp może spowodować zmiany w informacjach, ich zniszczenie, wykorzystanie w niewłaściwy sposób albo też uszkodzenie systemu lub niewłaściwe wykorzystanie systemów, w tym użycie ich do zaatakowania innych systemów. Żaden system ani produkt informatyczny nie jest całkowicie bezpieczny. Żaden pojedynczy produkt, usługa czy zabezpieczenie nie gwarantują pełnej skuteczności ochrony przed niewłaściwym użyciem lub dostępem. Systemy, produkty i usługi IBM® zostały zaprojektowane jako część kompleksowego rozwiązania w zakresie zabezpieczeń, obejmującego niezbędne dodatkowe procedury operacyjne i mogącego wymagać większej skuteczności innych systemów, produktów czy usług. IBM NIE GWARANTUJE, ŻE SYSTEMY, PRODUKTY CZY USŁUGI SĄ ODPORNE NA DZIAŁANIA PODEJMOWANE PRZEZ OSOBY TRZECIE W ZŁEJ WIERZE LUB BEZPRAWNIE ANI ŻE TAKIE SYSTEMY, PRODUKTY CZY USŁUGI ZABEZPIECZĄ ORGANIZACJĘ PRZED TAKIMI DZIAŁANIAMI OSÓB TRZECICH.

2. Czym jest program Rapport?

Program Rapport to zaawansowane oprogramowanie zabezpieczające, chroniące przed wykradzeniem przez przestępców dane przesyłane przez klienta do systemu bankowości elektronicznej. Program Rapport jest stanowczo rekomendowany przez bank użytkownika jako dodatkowa — obok stosowanego przez klienta oprogramowania antywirusowego i zabezpieczającego — warstwa zabezpieczeń oprogramowania. Chroniąc połączenie klienta z Internetem i tworząc kanał bezpiecznej komunikacji z serwisem WWW banku, program Rapport blokuje próby wykradzenia przez szkodliwe oprogramowanie środków pieniężnych z konta klienta.

Krótki film wideo o charakterze wprowadzającym do programu Rapport można znaleźć pod adresem
http://www.trusteer.com/introduction-to-rapport

Z korzystania z programu Rapport nie należy rezygnować nawet w sytuacji, w której komputer i sieć są chronione za pomocą innych rozwiązań do ochrony komputera i komunikacji sieciowej. Ostatnie badania wskazują, że rozwiązania z zakresu zabezpieczeń, takie jak oprogramowanie antywirusowe czy firewall, charakteryzują się tylko częściową skutecznością wobec wymierzonych w serwisy finansowe ataków szkodliwego oprogramowania takiego jak Zeus, SpyEye, Gozi czy Torpig. Dzięki integracji z procesami zapobiegania wyłudzeniom oferowanymi przez bank program Rapport gwarantuje dodatkową warstwę zabezpieczeń, obok innych rozwiązań do ochrony komputera i komunikacji sieciowej. Program Rapport umożliwia wykrywanie najbardziej wyrafinowanych ataków o charakterze finansowym, wyświetlanie informujących o nich alertów i blokowanie takich ataków.

Program Rapport jest udostępniany klientom bezpłatnie, we współpracy z organizacją użytkownika, i umożliwia im ochronę sesji bankowości elektronicznej oraz innych serwisów WWW niezwiązanych z przedsiębiorstwem (takich jak na przykład e-commerce czy webmail).

Na ile rozpowszechnione są cyberprzestępstwa o charakterze finansowym?

W roku 2011 FBI zidentyfikowało dwadzieścia incydentów polegających na oszustwach na łączną sumę 20 mln USD, polegających na kradzieży danych uwierzytelniających do bankowości elektronicznej małej i średniej wielkości przedsiębiorstw amerykańskich i użyciu ich do zainicjowania przelewów bankowych do chińskich przedsiębiorstw z sektora handlowego. Według szacunków cyberprzestępcy okradają małe i średnie przedsiębiorstwa w Stanach Zjednoczonych i Europie na kwotę nawet 1 mld USD rocznie. Korporacyjne rachunki bankowe to szczególnie narażone na ataki cyberprzestępców cele, a liczba takich ataków stale rośnie. Jedno z największych zagrożeń wiąże się z komputerem wykorzystywanym do wykonywania operacji bankowych. Przestępcy wykorzystują dwie wyrafinowane metody dostępu do rachunków online za pośrednictwem komputera:

- **Szkodliwe oprogramowanie** — automatycznie i bez wiedzy użytkownika pobierane na jego komputer podczas korzystania z Internetu przechwytuje dane logowania i przesyła je do grupy przestępczej, a także umożliwia modyfikację bez wiedzy użytkownika realizowanych transakcji.
- **Wyłudzanie informacji** — przestępcy budują fałszywe serwisy WWW łudząco przypominające serwis WWW banku, aby skłonić użytkownika do wprowadzenia w nich danych logowania do bankowości elektronicznej, które zostaną następnie użyte do uzyskania dostępu do rachunku bankowego.

Oprogramowanie antywirusowe: fałszywe poczucie bezpieczeństwa

Jest taka rzecz, którą producenci oprogramowania antywirusowego woleliby przed Tobą ukryć: oferowane przez nich produkty nie są szczególnie skuteczne w zakresie blokowania najbardziej wyrafinowanych wirusów. Jak podaje serwis Krebs On Security, statystyki wskazują, że **oprogramowanie antywirusowe wykrywa zaledwie około 25% najbardziej popularnego szkodliwego oprogramowania** przesyłanego obecnie za pośrednictwem poczty e-mail. Dzieje się tak, ponieważ twórcy wirusów działają bardzo szybko. Zwykle w chwili, gdy oprogramowanie antywirusowe potrafi

wykryć daną, nową odmianę wirusa, jest już za późno. Jest to moment, gdy cyberprzestępcy zdobyli już dostęp do rachunków bankowych klientów.

Wykrywanie podpisów nie działa

W celu zidentyfikowania nowych wirusów (zwanych również „szkodliwym oprogramowaniem") rozwiązania antywirusowe tworzą specjalne sygnatury każdego przychodzącego pliku, a następnie porównują je ze słownikiem sygnatur znanych wirusów. Rozwiązania antywirusowe nie mogą bronić się przed szkodliwym oprogramowaniem, o ile wcześniej nie została pozyskana próbka pliku i nie zostanie opracowana sygnatura.

Problem polega na tym, że autorzy szkodliwego oprogramowania są także bardzo, bardzo przebiegli. Są oni w stanie stworzyć miliony plików — każdy z unikatowym podpisem — miesięcznie. To samo szkodliwe oprogramowanie może być maskowane w wielu różnych plikach, przy czym każdy powinien mieć własny podpis nieznany oprogramowaniu antywirusowemu.

Wykrycie nowych podpisów przez szkodliwe oprogramowanie służące do przestępstw finansowych przez programy antywirusowe może zająć wiele dni, a nawet tygodni. Jednocześnie wyłudzenie może mieć miejsce w ciągu zaledwie godzin po powstaniu nowego szkodliwego oprogramowania o nieznanym dotąd podpisie. Tak więc w chwili, gdy dostawca oprogramowania antywirusowego oczyści komputer ze szkodliwego oprogramowania, może być już za późno na zapobieżenie wyłudzeniu.

Strategia działania programu Rapport

Innowacyjna technologia IBM znakomicie sprawdza się tam, gdzie kończą się możliwości oferowane przez konwencjonalne oprogramowanie zabezpieczające. Od momentu zainstalowania program Rapport chroni urządzenie klienta i zapobiega zainfekowaniu go przez szkodliwe oprogramowanie finansowe. IBM komunikuje się też z bankiem, co pozwala zespołowi użytkownika niezwłocznie podejmować kroki w obliczu zmieniających się zagrożeń.

Program Rapport nie umożliwia wyszukiwania podpisów plików. Nie sprawdza on też samego pliku, ale jego aktywność. Program Rapport wykrywa proces instalacji szkodliwego oprogramowania i przerywa go, chroniąc komputer przed infekcją. Nawet w sytuacji, gdy dojdzie do instalacji szkodliwego oprogramowania na urządzeniu, program Rapport wykrywa i blokuje próby naruszenia ochrony przeglądarki oraz sesji bankowości elektronicznej. Blokując działalność szkodliwego oprogramowania, program Rapport zapewnia ochronę na poziomie uzupełniającym i przewyższającym możliwości programów antywirusowych. Oznacza to, że bank w ścisłej współpracy z IBM oferuje użytkownikowi i jego klientom najlepszą dostępną ochronę przed nadużyciami finansowymi.

Dodatkowa warstwa zabezpieczeń

Program Rapport zoptymalizowano pod kątem blokowania szkodliwego oprogramowania i nadużyć finansowych. Nie oznacza to jednak, że należy całkowicie zrezygnować z posiadanych rozwiązań antywirusowych. Wiele innych wirusów nadal stanowi zagrożenie. Mogą one spowalniać pracę komputera lub zakłócać pracę, nie będą natomiast podejmowały prób wyłudzenia środków finansowych. Należy nadal stosować rozwiązania antywirusowe posiadane przez użytkownika do ochrony przed wirusami tego typu.

Przed jakimi atakami chroni program Rapport?

Prawnie zastrzeżona technologia blokowania przeglądarki oferowana przez program Rapport uniemożliwia dostęp bez uprawnień do informacji wymienianych między klientami a serwisami WWW, niezależnie od tego, który ze szkodliwych programów odpowiada za zagrożenie.

Program Rapport wykazuje skuteczność w blokowaniu następujących technik:

- Wyłudzanie informacji
- Pharming lub podszywanie się pod serwery DNS
- Keylogging (Rejestrowanie naciśnięć klawiszy)

- Man-in-the-Middle (Człowiek pomiędzy)
- Man-in-the-Browser (Człowiek w przeglądarce)
- Wykonywanie zrzutów ekranów
- Przechwytywanie sesji
- Sterowane pobieranie

Wyłudzanie informacji

Atak polegający na *wyłudzeniu informacji* polega na stworzeniu przez przestępcę serwisu WWW wyglądającego identycznie jak serwis znany użytkownikowi i zaufany (na przykład serwis WWW banku użytkownika). Przestępca zachęca użytkownika do odwiedzenia serwisu WWW (na przykład przez przesłanie mu wiadomości e-mail z odsyłaczem do serwisu WWW). Przechodząc do fałszywego serwisu WWW, użytkownik wierzy, że jest to serwis prawdziwy. Po zalogowaniu się przez użytkownika do oszukańczego serwisu WWW przestępca przechwytuje jego dane uwierzytelniające, a następnie może wykorzystać je do zalogowania się w imieniu użytkownika w prawdziwym serwisie WWW.

W ramach ochrony przed atakami polegającymi na wyłudzaniu informacji program Rapport:

- Ostrzega użytkownika o próbie uzyskania dostępu do serwisu WWW, o którym wiadomo, że jest szkodliwy.
- To ostrzeżenie pojawia się przy wprowadzaniu hasła w serwisie WWW niezapewniającym bezpieczeństwa przy wprowadzaniu danych. Serwisy nieprzesyłające danych w sposób bezpieczny to serwisy wysokiego ryzyka, obejmujące uprawnione serwisy, które mogą łatwo zostać przejęte przez grupy przestępcze.
- Umożliwia automatyczne przekierowanie użytkownika do prawdziwego serwisu WWW banku lub na stronę często zadawanych pytań dotyczących wyłudzania informacji albo do serwisu z kampanią edukacyjną.

Pharming lub podszywanie się pod serwery DNS

Atak typu *pharming* lub *podszywanie się pod serwery DNS* występuje, kiedy w wyniku działań przestępczych komputer użytkownika odwiedza oszukańczy serwis WWW mimo wpisania przez użytkownika w pasku adresu przeglądarki właściwego adresu serwisu WWW. Atak ten jest realizowany przy użyciu różnych technik, takich jak zainfekowanie komputera szkodliwym oprogramowaniem lub naruszenie ochrony serwerów w sieci dostawcy usług internetowych. Po przejściu do oszukańczego serwisu WWW i próbie zalogowania się przestępca przechwytuje dane uwierzytelniające użytkownika, a następnie może wykorzystać je do zalogowania się w imieniu użytkownika w prawdziwym serwisie WWW i zainicjowania oszukańczych transakcji. Aby zabezpieczyć użytkownika przed atakami typu pharming, program Rapport weryfikuje adres IP oraz certyfikat SSL serwisu WWW przy każdej próbie nawiązania połączenia z chronionym serwisem WWW. Jeśli weryfikacja nie powiedzie się, program Rapport kończy połączenie i nawiązuje nowe połączenie z prawdziwym serwisem WWW.

Rejestrowanie naciśnięć klawiszy

Program do rejestracji naciśnięć klawiszy to szkodliwe oprogramowanie rezydujące na komputerze użytkownika w sposób dla niego niewidoczny. Program rejestrujący naciśnięcia klawiszy zapisuje znaki wprowadzane za pomocą klawiatury, a następnie przesyła te dane przestępcom. W ten sposób programy rejestrujące naciśnięcia klawiszy pozwalają przechwytywać wprowadzane przez użytkownika podczas logowania dane uwierzytelniające, numery kart płatniczych oraz inne newralgiczne informacje, i przesyłać je do przestępców, którzy mogą następnie wykorzystać te dane uwierzytelniające do zalogowania się na rachunku użytkownika, podszycia się pod niego i realizacji przestępczych transakcji. Program Rapport blokuje programy do rejestracji naciśnięć klawiszy przez szyfrowanie wprowadzanych z klawiatury znaków, uniemożliwiając odczyt newralgicznych informacji przez te programy.

Man-in-the-Middle (Człowiek pomiędzy)

Man-in-the-Middle (Człowiek pomiędzy) to zaawansowana odmiana ataków polegających na wyłudzaniu informacji i ataków typu pharming. W przypadku tego konkretnego ataku użytkownik loguje się do serwisu WWW i rozpoczyna pracę, całkowicie nieświadom, że wszystkie informacje wymieniane między nim a serwisem WWW są przekazywane do cyberprzestępców za pośrednictwem pośredniczącego serwisu WWW, który w ten sposób odczytuje prywatne informacje i ma możliwość modyfikacji transakcji użytkownika. Na przykład, jeśli użytkownik chce przesłać pewną kwotę pieniędzy określonemu odbiorcy płatności, przestępca może zmienić tożsamość odbiorcy, co spowoduje przekierowanie środków na inny rachunek bankowy.

Program Rapport uniemożliwia przekierowywanie przeglądarki przez szkodliwe oprogramowanie do oszukańczych serwisów WWW, wykorzystując do tego wiele warstw weryfikacji, takich jak weryfikacja adresów IP serwisów WWW oraz certyfikatów.

Man-in-the-Browser (Człowiek w przeglądarce)

Man-in-the-Browser (Człowiek w przeglądarce) to szkodliwe oprogramowanie przenikające do przeglądarki, niekiedy w postaci programów dodatkowych, takich jak pasek narzędzi, BHO czy wtyczka. Szkodliwe oprogramowanie tego rodzaju steruje wszystkim, co ma miejsce w przeglądarce. Gromadzi ono newralgiczne informacje, takie jak dane uwierzytelniania logowania, i przekazuje je przestępcom. Umożliwia ono także generowanie transakcji w imieniu użytkownika, na przykład przesyłanie środków pieniężnych z jego rachunku na rachunek grupy przestępczej.

Program Rapport uniemożliwia modyfikowanie danych w przeglądarce za pośrednictwem wielu mechanizmów:

- Blokuje dostęp szkodliwego oprogramowania do newralgicznych informacji jeszcze zanim zostanie ono rozpoznane.
- Identyfikuje i usuwa szkodliwe oprogramowanie, gdy tylko staje się to możliwe. Usunięcie szkodliwego oprogramowania pozwala zablokować jego przekształcenie się w wariant trudniejszy do zablokowania lub zaatakowanie

przez nie programu antywirusowego, który ma je zablokować. Co więcej, program Rapport pozwala wykryć i usunąć wiele wariantów tego samego szkodliwego oprogramowania, niezależnie od tego, jaki plik binarny jest używany w tym wariancie.

- Uniemożliwia pobranie bez wiedzy użytkownika zidentyfikowanego szkodliwego oprogramowania — nawet z uprawnionych serwisów WWW.

Wykonywanie zrzutów ekranów

Szkodliwe oprogramowanie może dysponować także mechanizmami do wykonywania zrzutów ekranów i wysyłania ich do przestępców. Zrzuty ekranów mogą przedstawiać szczegółowe dane rachunków bankowych, salda, a nawet dane uwierzytelniające, w przypadku obecności panelu klawiszy na stronie logowania serwisu WWW. Program Rapport dezaktywuje mechanizmy przechwytywania ekranu mimo, że użytkownik ma połączenie z chronionymi serwisami WWW.

Przechwytywanie sesji

Oprogramowanie do przechwytywania sesji wykrada parametry sesji użytkownika w danym serwisie WWW i wysyła te informacje do przestępcy. Następnie te parametry sesji są przez nią wykorzystywane do przejęcia kontroli nad serwisem WWW i obejścia procesu uwierzytelniania wymaganego do zalogowania się do tego serwisu WWW. Program Rapport blokuje dostęp do parametrów sesji mimo, że użytkownik ma połączenie z chronionymi serwisami WWW.

Sterowane pobieranie

W przypadku sterowanego pobierania szkodliwe oprogramowanie jest pobierane bez wiedzy użytkownika, po przejściu do serwisu WWW. Serwis ten może być uprawnionym, lecz zainfekowanym serwisem WWW, tak że szkodliwe oprogramowanie zostanie bez wiedzy użytkownika pobrane na jego komputer.

Ochrona danych Twoich klientów przez program Rapport

Po zainstalowaniu na komputerze program Rapport automatycznie chroni serwisy WWW należące do partnerów biznesowych współpracujących z IBM w celu zapewnienia przedsiębiorstwu i jego klientom najwyższego możliwego poziomu zabezpieczeń. Ochronę oferowaną przez program Rapport można także ręcznie zastosować do wszystkich pozostałych serwisów WWW, do których wymagane jest logowanie się i z którymi użytkownik wymienia newralgiczne informacje, takie jak dane osobiste czy finansowe.

Po nawiązaniu połączenia z chronionym serwisem WWW program Rapport realizuje w tle trzy ważne działania, wysoce utrudniające przestępcom atak na użytkownika:

- Program Rapport sprawdza, czy połączenie nawiązano z prawdziwym, a nie z fałszywym serwisem WWW (stworzonym przez przestępców).
- Po weryfikacji program Rapport blokuje komunikację między komputerem a chronionym serwisem WWW. Chroni to przed przechwyceniem połączenia online z bankiem przez przestępców.
- Program Rapport chroni komputer użytkownika i połączenie z Internetem, tworząc tunel umożliwiający bezpieczną komunikację z bankiem lub przedsiębiorstwem, uniemożliwiając przestępcom wykorzystanie szkodliwego oprogramowania do kradzieży danych logowania oraz modyfikacji transakcji finansowych i operacji wymiany danych.

Program Rapport zapewnia dodatkową, ważną i unikalną warstwę zabezpieczeń, umożliwiającą partnerom biznesowym lepszą ochronę newralgicznych informacji oraz reagowanie na pojawiające się zagrożenia.

Oto niektóre specyficzne sposoby ochrony komunikacji, danych i finansów użytkownika oferowane przez program Rapport:

- Bezpieczna komunikacja z chronionymi serwisami
- Ochrona danych logowania
- Ochrona sesji w przeglądarce
- Ochrona naciśnięć klawiszy

- Ochrona kart płatniczych
- Blokowanie wykonywania zrzutów ekranu
- Sprawdzanie poprawności serwisów WWW
- Blokowanie programów dodatkowych w przeglądarce
- Blokowanie modyfikowania procesów
- Ostrzeżenia dotyczące szkodliwych serwisów WWW
- Raportowanie zdarzeń nieuprawnionego dostępu
- Ochrona przed atakami nakładek

Bezpieczna komunikacja z chronionymi serwisami

Po nawiązaniu połączenia z chronionym serwisem WWW program Rapport blokuje dostęp do serwisu WWW wszelkich procesów na komputerze. Komunikacja z serwisem WWW jest bezpieczna od wszelkich prób dostępu przez szkodliwe oprogramowanie. Nawet, jeśli na komputer użytkownika przedostanie się w sposób niewidoczny nierozpoznane szkodliwe oprogramowanie, nie może ono uzyskać dostępu do newralgicznych danych w serwisie WWW ani zmodyfikować przeprowadzanych przez użytkownika transakcji.

Ochrona danych logowania

Po zalogowaniu się do chronionego serwisu WWW uwierzytelnia on użytkownika dzięki bezpiecznych danych uwierzytelniających logowania, takich jak nazwa użytkownika czy hasło. Problem polega na tym, że przestępcy dysponują szeregiem metod przechwycenia danych uwierzytelniających umożliwiających logowanie — np. przez wyłudzenie — i użycia ich do zalogowania się na konto bankowości elektronicznej.

Ochrona sesji w przeglądarce

Po zalogowaniu się do serwisu WWW zapisuje on plik tekstowy zwany plikiem cookie sesji w tymczasowej pamięci na czas trwania sesji. Plik cookie sesji identyfikuje uwierzytelnioną sesję i umożliwia wielokrotne przesyłanie newralgicznych informacji na i z serwera serwisu WWW bez konieczności ponownego logowania się.

Szkodliwe oprogramowanie może przechwytywać pliki cookie sesji i używać ich do obchodzenia uwierzytelnień oraz przejmowania sesji w serwisie WWW. W celu zabezpieczenia się przed tego typu atakami program Rapport blokuje dostęp aplikacji do plików cookie sesji w serwisach WWW partnerów.

Uwaga: Ta funkcja jest obsługiwana wyłącznie przez partnerów współpracujących z IBM w zakresie ochrony swojej komunikacji online z klientami.

Ochrona naciśnięć klawiszy

Program Rapport szyfruje naciśnięcia klawiszy przesyłane do przeglądarki i ukrywa je przed szkodliwymi komponentami oprogramowania znajdującymi się w systemie operacyjnym. Zabezpiecza to szkodliwe oprogramowanie przed odczytem naciśnięć klawiszy i przechwyceniem newralgicznych informacji, takich jak hasło czy numer karty płatniczej.

Ochrona kart płatniczych

Program Rapport ostrzega użytkownika o próbie przesłania danych kart płatniczych do lokalnych i niezabezpieczonych serwisów WWW. Ostrzeżenie to jest wyświetlane w oknie dialogowym, które pozwala na zatrzymanie przesyłania. Program Rapport aktywuje także funkcję uniemożliwiającą rejestrację naciśnięć klawiszy po wprowadzeniu numeru karty płatniczej w chronionym serwisie WWW programu Rapport lub w dowolnym chronionym (za pomocą protokołu https) serwisie zawierającym słowo kluczowe związane z kartą płatniczą taką jak Visa, Mastercard czy Amex. Ochrona przed rejestracją naciśnięć klawiszy uniemożliwia przechwycenie szczegółowych danych kart płatniczych przez szkodliwe oprogramowanie.

Uwaga: Ta funkcja jest obsługiwana wyłącznie w przypadku kart płatniczych systemów kart płatniczych objętych taką ochroną.

Blokowanie wykonywania zrzutów ekranu

Program Rapport dezaktywuje wszelkie próby wykonania zrzutu ekranu podczas wyświetlania w przeglądarce chronionego serwisu WWW. Uniemożliwia to przechwycenie przez szkodliwe oprogramowanie newralgicznych informacji przez wykonanie zrzutu ekranu.

Sprawdzanie poprawności serwisów WWW

Nawet w przypadku wpisania poprawnego adresu banku lub serwisu WWW przedsiębiorstwa szkodliwe oprogramowanie może użyć różnych metod, zwanych atakami typu pharming, do przekierowania przeglądarki do oszukańczego serwisu WWW.

Aby zabezpieczyć użytkownika przed atakami typu pharming, program Rapport weryfikuje adres IP oraz certyfikat SSL serwisu WWW przy każdej próbie nawiązania połączenia z chronionym serwisem WWW. Jeśli certyfikat SSL utracił ważność, jest niepoprawny lub został podpisany przez nieznanego wystawcę, program Rapport uaktywnia ostrzeżenie i pomaga użytkownikowi nawiązać połączenie z serwisem. Jeśli adresu IP nie ma w tabelach zaufanych adresów IP dla tego serwisu WWW, program Rapport zastępuje go znanym, poprawnym adresem IP tego serwisu WWW.

Blokowanie programów dodatkowych w przeglądarce

Po nawiązaniu połączenia z chronionym serwisem WWW program Rapport blokuje wszelkie programy dodatkowe nierozpoznawane jako uprawnione i bezpieczne. Programy dodatkowe przeglądarki to niewielkie, zwykle należące do firm trzecich, fragmenty oprogramowania znajdujące się w przeglądarce i umożliwiające sterowanie komunikacją. Ich celem jest ochrona użytkownika przed szkodliwymi programami dodatkowymi, które mogą wykradać dane logowania lub modyfikować przesyłane przez użytkownika informacje.

Blokowanie modyfikowania procesów

Program Rapport analizuje próby modyfikacji procesów przeglądarki i blokuje próby wyglądające podejrzanie. Modyfikacja procesów przeglądarki (znana również jako wprowadzanie zmian w programie) to technika przejmowania kontroli nad przeglądarką i uzyskiwania dostępu do zawartych w niej, newralgicznych danych.

Ostrzeżenia dotyczące szkodliwych serwisów WWW

Program Rapport ostrzega użytkownika o próbie uzyskania dostępu do serwisu WWW, o którym wiadomo, że jest szkodliwy.

Raportowanie zdarzeń nieuprawnionego dostępu

Program Rapport komunikuje się z serwisami WWW partnerów IBM, zapewniając dostęp do informacji o poziomie bezpieczeństwa oraz rejestrację wszelkich prób nieuprawnionego dostępu do konta bankowości elektronicznej. Pozwala to bankowi lub przedsiębiorstwu podjąć niezwłoczne czynności mające na celu eliminację zagrożeń.

Uwaga: Ta funkcja jest obsługiwana wyłącznie przez partnerów współpracujących z IBM w zakresie ochrony swojej komunikacji online z klientami.

Ochrona przed atakami nakładek

Ataki nakładek to próby przejęcia danych uwierzytelniających użytkowników końcowych przez monitorowanie dostępu użytkowników końcowych do serwisów finansowych, a następnie uruchomienie okna aplikacji w przeglądarce użytkownika. To okno aplikacji pyta o newralgiczne dane i blokuje dostęp użytkownika końcowego do uprawnionego serwisu aż do czasu ich podania. Ataki takie mogą łudząco przypominać etap procesu logowania się do uprawnionego serwisu WWW, przekonując użytkownika końcowego do podania newralgicznych danych.

Program Rapport identyfikuje ten typ ataków i może reagować na nie na szereg różnych sposobów, uniemożliwiając w ten sposób działanie szkodliwego oprogramowania i kradzież danych uwierzytelniających.

Obsługa

Program Rapport jest prosty w obsłudze. Korzystanie z niego nie wymaga dysponowania wiedzą techniczną. Program Rapport nie wymaga także przeprowadzenia dodatkowych czynności konfiguracyjnych, nie zmienia sposobu pracy użytkownika, nie powoduje modyfikacji sposobu działania przeglądarki i nie wyświetla po napotkaniu zagrożenia pytań o charakterze technicznym.

Większość z operacji realizowanych przez program Rapport jest realizowana w tle i nie zakłóca pracy użytkownika ani nie wymaga jego udziału. Program Rapport rejestruje wszystkie czynności podejmowane w celu ochrony użytkownika w raporcie o aktywności, którego wyświetlenie jest możliwe w dowolnej wybranej przez niego chwili. Szczegółowe informacje na temat poziomów ryzyka można znaleźć w raporcie o aktywności. Po napotkaniu przez program Rapport poważnego zagrożenia powiadamia on o tym fakcie użytkownika. Niektóre podejmowane w takich przypadkach czynności wymagają prostego reagowania na Ostrzeżenia programu Rapport, które są szczególnie łatwe do zrozumienia.

Sprawdzenie, które serwisy WWW są chronione przez program Rapport, nie nastręcza wielu trudności. Po prawej stronie paska adresu przeglądarki (lub w pobliżu) wyświetlana jest ikona, której kolor wskazuje, czy aktualnie odwiedzany serwis jest chroniony.

Ikona program Rapport ( ) pojawia się na pasku zadań systemu Windows, jeśli program Rapport jest uruchamiany. Kliknięcie ikony na pasku zadań powoduje otwarcie Konsoli Rapport, za pośrednictwem której można uzyskać dostęp do różnych funkcji i informacji programu Rapport.

Przy każdym użyciu nowych danych logowania w chronionym serwisie program Rapport wyświetla okno dialogowe z ofertą ochrony tych danych uwierzytelniających. To okno dialogowe pojawia się tylko przy pierwszym użyciu danych logowania.

Dodatkowe funkcje programu Rapport

Obok ochrony uzyskiwanej automatycznie przy nawiązywaniu połączenia z serwisami WWW partnerów IBM możliwe jest ręczne dodanie zabezpieczeń programu Rapport do wszystkich pozostałych używanych serwisów WWW. Więcej informacji można znaleźć w punkcie Ochrona dodatkowych serwisów WWW.

Obok ochrony serwisu WWW program Rapport oferuje także inne funkcje zabezpieczeń (wszystkie oferowane bezpłatnie):

- Skanowanie komputera w poszukiwaniu udoskonaleń zabezpieczeń umożliwiające dalsze udoskonalanie zabezpieczeń na komputerze użytkownika.
- Generowanie raportów przy próbach włamania się na rachunki bankowe.

Informacje dla zaawansowanych użytkowników

Program Rapport to aplikacja wykorzystująca w niewielkim stopniu zasoby systemowe. Szczegółowe informacje na temat wykorzystania zasobów systemowych przez program Rapport można znaleźć w punkcie Wykorzystywanie zasobów systemowych komputera PC przez program Rapport.

Program Rapport w żaden sposób nie narusza prywatności użytkownika. Więcej informacji można znaleźć w punkcie Program Rapport a prywatność użytkownika.

Program Rapport wyposażono w mechanizm autoochrony, uniemożliwiający wyłączenie lub usunięcie oprogramowania. W efekcie nie ma możliwości zatrzymania procesów programu Rapport za pośrednictwem menedżera zadań. Więcej informacji na temat zatrzymywania programu Rapport można znaleźć w punkcie Zatrzymywanie programu Rapport.

Wykorzystywanie zasobów systemowych komputera PC przez program Rapport

Działanie programu Rapport wiąże się z działaniem następujących plików:

- Pliki wykonywalne:
  - Program Files\Trusteer\Rapport\bin\RapportService.exe
  - Program Files\Trusteer\Rapport\bin\RapportMgmtService.exe
- Procesy:
  - RapportService.exe
  - RapportMgmtService.exe
- Usługi:
  - Rapport Management Service (w przypadku nieadministracyjnych kont w 64-bitowych systemach operacyjnych: RapportInjService_x64.exe)
- Sterowniki:
  - 'RapportPG.sys' (w przypadku 64-bitowych systemów operacyjnych: 'RapportPG64.sys')
  - 'RapportKELL.sys' (w przypadku 64-bitowych systemów operacyjnych: 'RapportKE64.sys')
  - 'RapportEI.sys' (w przypadku 64-bitowych systemów operacyjnych: 'RapportEI64.sys')
- Należy zapewnić około 15 MB przestrzeni w profilu użytkownika na dzienniki i ustawienia (w zależności od liczby różnych przeglądarek używanych na tym komputerze liczba ta może wzrosnąć).
- Wielkość programu to 15 MB plus przestrzeń w profilu użytkownika.

Program Rapport a ochrona prywatności

Program Rapport tworzy na komputerze zaszyfrowany podpis danych uwierzytelniania. Informacje te nie mogą posłużyć do pobrania danych uwierzytelniania i są przez program Rapport wykorzystywane wyłącznie do identyfikacji wszelkich zdarzeń wycieku danych uwierzytelniania użytkownika bez jego zezwolenia. Program Rapport wysyła anonimowe raporty na temat zdarzeń dotyczących bezpieczeństwa oraz błędów wewnętrznych do centralnego serwera. Informacje te mogą następnie posłużyć do poprawy funkcjonowania produktu i jego strategii.

Centralna usługa Rapport: potężny mechanizm zapobiegania oszustwom

Centralna usługa Rapport to usługa oferująca partnerom IBM możliwość podejmowania niezwłocznych działań w celu zapobiegania oszukańczemu działaniu na koncie użytkownika.

Każdorazowo przy wykryciu podejrzanego oprogramowania lub działania serwisu WWW program Rapport generuje zdarzenie dotyczące zabezpieczeń i wysyła je do centralnej usługi programu Rapport w celu jego analizy. Ta centralna usługa pozwala przeprowadzać rozległe testy umożliwiające określenie, czy dane działanie jest oszukańcze. Jeśli dane działanie okaże się oszukańcze, centralna usługa przekazuje do programu Rapport informację o konieczności bardziej agresywnego blokowania zagrożeń.

Uwaga: Centralna usługa Rapport jest dostępna dla banku użytkownika wyłącznie pod warunkiem, że nie wyłączy on funkcji wysyłania zdarzeń zabezpieczeń do analizy. To ustawienie jest dostępne w kreatorze konfiguracji programu Rapport i jest domyślnie włączone. Mimo włączenia tej funkcji anonimowość[1] użytkownika jest w pełni chroniona.

[1] Wszystkie informacje wysyłane z komputera do centralnej usługi programu Rapport są anonimowe i obejmują szczegóły techniczne, nie zaś prywatne dane. W przypadku powstania w programie Rapport podejrzenia naruszenia ochrony danych osobowych do banku lub przedsiębiorstwa użytkownika przesyłane jest ostrzeżenie obejmujące identyfikator pozwalający powiązać incydent z kontem użytkownika. IBM nie ma dostępu do takiego identyfikatora ani innych prywatnych informacji.

Program Rapport chroni użytkownika nawet w sytuacji rezygnacji z przesyłania zdarzeń bezpieczeństwa do analizy. Jednak wysyłanie zdarzeń do analizy pozwala na wykrycie przez program Rapport bardziej wyrafinowanych, a nawet nieznanych zagrożeń.

Niektóre przykłady zdarzeń bezpieczeństwa przesyłanych do analizy przez program Rapport to:

- Podejrzany serwis WWW
- Próby przechwycenia danych uwierzytelniających
- Próby zakłócenia przesyłania newralgicznych danych
- Podejrzane oprogramowanie

Jedną ze znaczących korzyści z posiadania centralnej usługi Rapport jest system wczesnego ostrzegania, ostrzegający bank użytkownika o wszelkich naruszeniach ochrony nazwy użytkownika lub jego hasła. Centralna usługa pozwala wykryć zagrożenia niewykryte przez oprogramowanie antywirusowe oraz pozostałe oprogramowanie zabezpieczające.

Obok zdarzeń dotyczących zabezpieczeń program Rapport wysyła od czasu do czasu dane dotyczące wewnętrznych błędów oprogramowania. Informacje te mogą pomóc IBM w identyfikacji i naprawie błędów dotyczących oprogramowania.

Czy mogę wyłączyć opcję wysyłania zdarzeń dotyczących zabezpieczeń i dzienników błędów do IBM?

Przepustowość wykorzystywaną przez tę funkcję można zmniejszyć, co pozwala wysyłać do IBM tylko zdarzenia o znaczeniu krytycznym. Takie ustawienie nie jest jednak zalecane. IBM wykorzystuje te informacje do zapewnienia najwyższego możliwego poziomu ochrony przed szkodliwym oprogramowaniem wszystkim użytkownikom serwisów finansowych korzystającym z programu Rapport. Użytkownikowi korzystającemu z aktywnej funkcji przesyłania zdarzeń dotyczących bezpieczeństwa i dzienników błędów do IBM jest zapewniana pełna anonimowość[2]. Nie jest możliwe wyłączenie przesyłania zdarzeń dotyczących bezpieczeństwa ani dzienników błędów do IBM.

W celu przesyłania do IBM tylko zdarzeń dotyczących bezpieczeństwa o znaczeniu krytycznym i dzienników błędów należy zmienić ustawienie **Wyślij zdarzenia dotyczące zabezpieczeń i błędy do analizy** z wartości **Zawsze** na wartość **Tylko zdarzenia o znaczeniu krytycznym**.

[2] Wszystkie informacje wysyłane z komputera do centralnej usługi programu Rapport są anonimowe i obejmują szczegóły techniczne, nie zaś prywatne dane. W przypadku powstania w programie Rapport podejrzenia naruszenia ochrony danych osobowych do banku lub przedsiębiorstwa użytkownika przesyłane jest ostrzeżenie obejmujące identyfikator pozwalający powiązać incydent z kontem użytkownika. IBM nie ma dostępu do takiego identyfikatora ani innych prywatnych informacji.

3. Instalowanie programu Rapport

Instalowanie programu Rapport jest szybkie i proste. Wystarczy pobrać plik instalacyjny ze strony WWW banku, uruchomić go i postępować zgodnie ze wskazówkami w standardowym kreatorze instalacji.

Dalsze instrukcje można znaleźć w punkcie Instalowanie programu Rapport w systemie Windows 8 za pośrednictwem przeglądarki Internet Explorer. Instrukcje dotyczące instalowania programu Rapport w innych przeglądarkach WWW można znaleźć na stronie WWW:
http://www.trusteer.com/support/win-install-instructions.

Jeśli program Rapport jest instalowany za pośrednictwem konta administratora systemu Windows, standardowy użytkownik może uruchomić program Rapport ze swojego konta, ale nie może zatrzymać ani rozpocząć procesu instalacji, zdeinstalować ani ponownie zainstalować programu Rapport, ani nie może zmieniać ustalonych ustawień strategii. Ograniczenie to umożliwia administratorom instalowanie programu Rapport na urządzeniach całego przedsiębiorstwa, jednocześnie uniemożliwiając wyłączanie opcji zabezpieczających przez pracowników lub modyfikowanie przez nich strategii bezpieczeństwa dotyczących wszystkich użytkowników.

Zdecydowanie zaleca się instalację programu Rapport z konta administratora, ponieważ powoduje to automatyczne rozszerzenie ochrony na wszystkich użytkowników. Ponadto nie jest możliwe instalowanie sterowników w przypadku instalowania programu Rapport ze standardowego konta użytkownika, zaś najważniejsze mechanizmy zabezpieczające programu Rapport (ochrona przed szkodliwym programowaniem i deinstalowanie go) są instalowane za pośrednictwem sterowników.

W przypadku instalowania programu Rapport ze standardowego konta użytkownika nie będzie on mógł być uruchamiany z żadnego innego konta użytkownika, a jego instalacja nie będzie możliwa na żadnym innym koncie, o ile nie zostanie on najpierw zdeinstalowany.

Skąd można pobrać program Rapport?

Będąc klientem banku lub innej organizacji oferującej program Rapport, można pobrać go ze strony WWW banku. Bank może:

- Wyświetlić sekcję zabezpieczeń na stronie WWW banku (zwykle w dolnej części strony) wraz z odsyłaczem do programu Rapport lub odsyłaczem do strony umożliwiającej pobranie oprogramowania zabezpieczającego.
- Zaoferować możliwość pobrania programu Rapport w ramach procesu logowania do konta bankowości elektronicznej lub tuż po pomyślnym zalogowaniu.

Czy program Rapport działa z moim systemem operacyjnym i przeglądarką?

Program Rapport działa z następującymi systemami operacyjnymi i przeglądarkami: http://www.trusteer.com/supported-platforms.

Dlaczego otrzymuję komunikat informujący, że program Rapport już istnieje na moim komputerze?

Jeśli wersja programu Rapport już istnieje na komputerze podczas instalowania go, w procesie instalacji wyświetlane jest następujące okno dialogowe:

Wyświetlenie tego ekranu podczas instalacji oznacza, że na komputerze jest już zainstalowany program Rapport. Ponowna instalacja programu Rapport jest całkowicie bezpieczna (wystarczy upewnić się, że nie będzie instalowana wersja starsza, niż zainstalowana obecnie).

- **Aby zainstalować program Rapport zamiast już istniejącej wersji:**

1. Wybierz opcję najlepiej wyjaśniającą przyczynę zamiaru ponownej instalacji programu Rapport.
2. Kliknij opcję **Dalej**. Proces instalacji zostanie rozpoczęty, a następnie przerwany w celu zamknięcia programu Rapport. Przed zamknięciem programu Rapport zostanie wyświetlony komunikat z prośbą o wprowadzenie kodu zabezpieczającego. Do komunikatu dołączony jest obrazek ze słowem, które należy wpisać, aby uniemożliwić wyłączenie programu Rapport przez szkodliwe oprogramowanie.
3. Wprowadź znaki widoczne na obrazku. (Nie jest rozróżniana wielkość liter).
4. Kliknij opcję **Zamknij**. Podczas zamykania programu Rapport wyświetlany jest następujący komunikat: „Należy poczekać na zamknięcie programu Trusteer Endpoint Protection". Zniknięcie tego komunikatu oznacza, że działanie programu Rapport zostało zatrzymane. Proces instalacji jest kontynuowany bez przeszkód. Po zakończeniu instalacji może zostać wyświetlony ekran z następującym komunikatem:

   Nastąpiła aktualizacja programu Trusteer Endpoint Protection do nowej wersji. Niektóre nowe funkcje programu Trusteer Endpoint Protection będą dostępne dopiero po ponownym uruchomieniu.

   Mimo wyświetlenia tego komunikatu komputer jest chroniony. Zaleca się jednak ponowne uruchomienie komputera tak szybko, jak to tylko możliwe.

W jaki sposób mogę zainstalować program Rapport we współużytkowanym środowisku pulpitu wirtualnego?

W przypadku instalowania programu Rapport w systemie operacyjnym Windows Server (2003 lub 2008) kreator instalacji wykrywa system operacyjny i instaluje wersję serwerową programu Rapport. Wersja ta obsługuje wiele sesji. Więcej informacji można znaleźć w punkcie Instalowanie programu Rapport w systemie operacyjnym Windows Server (2003 lub 2008).

Uwaga: Poniższa procedura opisuje instalację, w której program Rapport wdrożono w celu wymuszenia instalacji wersji administracyjnych. Więcej informacji na temat pozostałych opcji wdrożenia programu Rapport zawiera publikacja *Installing IBM Security Trusteer Rapport from a Standard User Account Best Practices*.

Instalowanie programu Rapport w systemie operacyjnym Windows 8 za pośrednictwem przeglądarki Internet Explorer

Ta procedura wyjaśnia sposób pobierania i instalowania programu Rapport w przypadku uruchamiania systemu operacyjnego Windows 8 i korzystania z przeglądarki Microsoft Internet Explorer. W przypadku innych przeglądarek stosowne instrukcje można znaleźć na stronie WWW: http://www.trusteer.com/support/win-install-instructions.

Aby zainstalować program Rapport:

1. Przejdź na stronę logowania swojej organizacji. Jeśli organizacja ta oferuje program Rapport do pobrania, zostanie wyświetlony ekran powitalny z przyciskiem **Pobierz teraz**.
2. Kliknij opcję **Pobierz teraz**. W dolnej części okna przeglądarki zostanie wyświetlony pasek informacyjny z pytaniem, czy plik RapportSetup.exe ma zostać uruchomiony, czy zapisany.
3. Kliknij opcję **Uruchom**. Kilka sekund później zostanie wyświetlone kolejne okno dialogowe z pytaniem: „Czy chcesz zezwolić następującemu programowi na wprowadzenie zmian na tym komputerze?”

4. Kliknij opcję **Tak**. Może zostać wyświetlone okno dialogowe z następującym komunikatem:

> *Próbujesz zainstalować program Trusteer Endpoint Protection, korzystając ze standardowego konta użytkownika systemu Windows. Przeprowadzenie instalacji z użyciem konta tego rodzaju nie pozwala na wykorzystanie zaawansowanych funkcji usuwania szkodliwego oprogramowania, dostępnych w produkcie Trusteer Endpoint Protection, i może spowodować wystawienie komputera na ryzyko. Z tego względu instalację należy przeprowadzić z użyciem uprawnień administratora.*
>
> *Aby skorzystać z uprawnień administratora w systemie Windows i kontynuować proces instalacji, należy kliknąć przycisk Instaluj.*
>
> *Jeśli komputer należy do firmy lub organizacji, może okazać się konieczny kontakt z jej działem IT.*

Ten komunikat oznacza, że użytkownik jest obecnie zalogowany za pośrednictwem standardowego konta systemu Windows. IBM zaleca instalowanie programu Rapport za pośrednictwem konta administratora.

5. Kliknij opcję **Instaluj**. Zostanie wyświetlony monit z prośbą o wprowadzenie hasła administratora.

Uwaga:	Jeśli nie możesz zainstalować programu Rapport z wykorzystaniem uprawnień administratora, możesz zamknąć to okno dialogowe. Nie zostanie wyświetlony monit o wprowadzenie hasła administratora, a instalator zostanie zamknięty.

6. Wprowadź hasło i kliknij przycisk **Tak**, aby kontynuować. Może zostać wyświetlone okno dialogowe z następującym komunikatem:

> *W związku z niniejszą instalacją mogą zostać wyświetlone okna dialogowe firewalla i oprogramowania antywirusowego z ostrzeżeniami związanymi z niniejszą instalacją.*
> *Należy zezwolić programom RapportSetup lub RapportService na kontynuowanie pracy w przypadku wyświetlenia dowolnego z tych ostrzeżeń, wybierając opcję taką jak:*
> *- Wyłącz blokadę*
> *- Tak*
> *- Zezwól*
> *- Zezwalaj*
> *Jeśli instalacja nie powiedzie się, może okazać się potrzebne czasowe wyłączenie oprogramowania antywirusowego lub zabezpieczającego i ponowienie próby instalacji. W przeciwnym wypadku oprogramowanie antywirusowe lub firewall — szczególnie w przypadku ustawienia wysokiego poziomu ochrony — mogą uniemożliwić poprawne zakończenie procesu instalacji.*

7. Kliknij przycisk **OK**. Rozpocznie się pobieranie programu Rapport.

   Zostanie wyświetlony kreator instalacji programu Trusteer Endpoint Protection Installation.

8. Jeśli chcesz, aby program Rapport był kompatybilny z lektorem ekranowym, kliknij opcję **Zaawansowane**. Zostanie wyświetlony ekran Opcje zaawansowane. Zaznacz opcję **Niedowidzę, mam problemy z rozróżnianiem kolorów i/lub korzystam z pomocy lektorów ekranowych**, a następnie kliknij przycisk **Kontynuuj**. Ten tryb umożliwia odczytywanie przez lektora ekranowego treści menu i okien dialogowych programu Rapport i eliminuje możliwość zablokowania działania lektora ekranowego przez program Rapport w oknie przeglądarki. Powoduje to także wyłączenie okien dialogowych z

zabezpieczeniami w postaci obrazka wyświetlanych przy zatrzymywaniu lub deinstalacji programu Rapport.

Uwaga:	Nie należy zaznaczać pola wyboru **Niedowidzę, mam problemy z rozróżnianiem kolorów i/lub korzystam z pomocy lektorów ekranowych**, instalując program Rapport na komputerze nieprzeznaczonym dla osób korzystających z lektora ekranowego. Ustawienie to powoduje bowiem dezaktywację niektórych funkcji zabezpieczeń.

9. Kliknij opcję **Akceptuję warunki zawarte w umowie licencyjnej**.
10. Kliknij przycisk **Instaluj**. Proces instalacji będzie kontynuowany. Po zakończeniu procesu instalacji w kreatorze zostanie wyświetlony przycisk Zakończ.
11. Kliknij przycisk **Zakończ**. Po upływie kilku sekund program Rapport otwiera nowe okno przeglądarki umożliwiające wykonanie krótkiego testu kompatybilności. Po zakończeniu testu program Rapport otwiera stronę w przeglądarce użytkownika.

Proces instalacji jest zakończony.

Instalowanie programu Rapport w systemie operacyjnym Windows Server (2003 i 2008)

Program Rapport obsługuje system operacyjny Windows Server (2003 i 2008). Program Rapport obsługuje także wiele sesji użytkownika, umożliwiając obsługę wielu profili w jednej instalacji, tak jak jest to wymagane na potrzeby współużytkowanej infrastruktury pulpitu wirtualnego. Program Rapport wykrywa fakt uruchomienia procesu instalacji na serwerze Windows Server (2003 lub 2008) i instaluje wersję serwera uwzględniającą możliwość wyłączenia wysyłania komend ponownego uruchomienia do użytkowników. Wyłączenie możliwości wysyłania komend ponownego uruchomienia do użytkowników pomaga uniknąć sytuacji, w których jeden użytkownik restartuje system dla wszystkich użytkowników na danym komputerze. Informacje na temat wyłączania możliwości wydawania komend ponownego uruchomienia można znaleźć w publikacji *IBM Security Trusteer Rapport Virtual Environment Best Practices*.

- **Aby zainstalować program Rapport w systemie operacyjnym Windows Server 2003 lub 2008:**

  1. Uruchom plik RapportSetup.exe. Plik ten można pobrać ze strony: http://www.trusteer.com/support/rapport-installation-links.
  2. Kontynuuj proces instalacji, umożliwiający pobranie kompletnego pakietu instalacyjnego oraz inicjalizację kreatora instalacji. Kreator instalacji wykrywa system operacyjny na serwerze i wyświetla ekran **Wykryto hosta w systemie operacyjnym Windows Server**.
  3. Po wyświetleniu tego ekranu kliknij opcję **Wyświetl dokument**. W przeglądarce WWW otwierana jest strona wsparcia dla przedsiębiorstw dotycząca programu Rapport, zawierająca wyjaśnienie sposobu, w jaki program Rapport pomaga chronić przedsiębiorstwa. Na stronie wsparcia firmy kliknij odsyłacz, aby wyświetlić dokument *IBM Security Trusteer Rapport Virtual Implementation Scenarios*, który udostępnia ważne informacje dotyczące implementacji programu Rapport w środowisku pulpitu wirtualnego.

4. Po zapoznaniu się z treścią dokumentu zaznacz pole wyboru **Potwierdzam zapoznanie się z dokumentem** i kontynuuj proces instalacji.

Inaczej, niż w przypadku ekranu **Wykryto hosta systemu Windows Server**, instalacja przebiega podobnie do instalacji w pozostałych systemach operacyjnych.

Jak mogę przełączyć się na konto administratora?

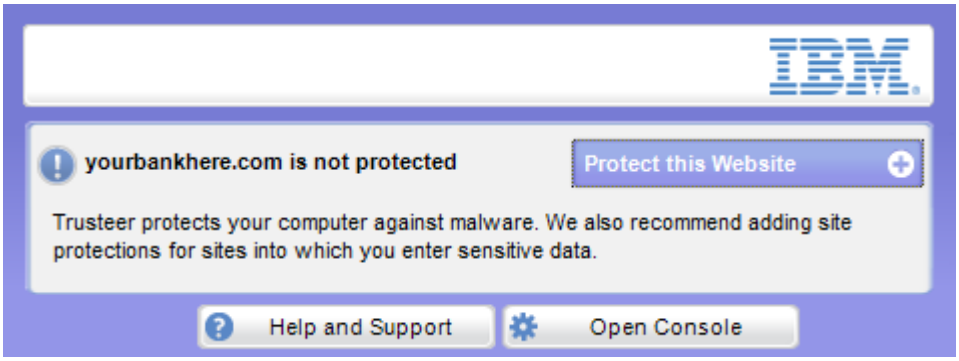
- Przełączanie się na konto administratora (system operacyjny Windows 8)
- Przełączanie się na konto administratora (system operacyjny Windows 7)
- Przełączanie się na konto administratora (system operacyjny Windows XP)

4. Pierwsze kroki

Niezwłocznie po zakończeniu instalacji program Rapport jest uruchamiany i od tego momentu wszelka komunikacja z serwisami WWW partnerów jest chroniona. Ikona programu Rapport pojawia się na pasku adresu w przeglądarce lub po jego prawej stronie. Po przejściu do serwisu WWW banku lub przedsiębiorstwa ikona programu Rapport staje się zielona, co wskazuje, że serwis jest już chroniony.

Przy pierwszym zalogowaniu się na konto bankowości elektronicznej może zostać wyświetlone okno dialogowe ochrony hasła.

Po przejściu do serwisu WWW, który nie jest chroniony przez program Rapport, ikona programu Rapport jest wyszarzona. Po kliknięciu szarej ikony programu Rapport wyświetlane jest okno dialogowe (wskaźnik statusu programu Rapport) informujące, że witryna nie jest chroniona.



Dostępne możliwości to:

- Chroń dodatkowe serwisy WWW, do których się logujesz, lub za pośrednictwem których możesz odczytać lub przesłać newralgiczne dane.
- Otwórz Konsolę Rapport. Wiele procedur w tym podręczniku rozpoczyna się od otwarcia konsoli.
- Wybierz z nagłówków tematów te, które zawierają najbardziej interesujące informacje.

- Poczuj bezpieczeństwo podczas wykonywania czynności związanych z pracą, obsługą bankową i dokonywaniem zakupów w Internecie.

Otwórz Konsolę Rapport

Konsola Rapport to portal oferujący dostęp do szeregu funkcji i informacji dotyczących programu Rapport.

Aby otworzyć Konsolę Rapport:

- Kliknij ikonę Rapport ( ) na pasku zadań. Zostanie wyświetlona Konsola Rapport.

Nie widzę ikony programu Rapport na pasku zadań

Ikona () pojawia się domyślnie na pasku zadań programu Rapport, gdy jest on uruchomiony. Istnieje możliwość ukrycia ikony (zobacz Ukrywanie i przywracanie ikony na pasku zadań). Ikona informuje, że aktywne są zabezpieczenia programu Rapport niezależne od przeglądarki. Ochrona przeglądarki obejmuje ochronę przed szkodliwym oprogramowaniem, skanowanie i usuwanie. Jeśli ikona nie pojawia się, a nie została ona ukryta odpowiednim ustawieniem w Konsoli Rapport, oznacza to, że program Rapport nie działa. Program Rapport można zatrzymać lub zdeinstalować. Aby uruchomić program Rapport po jego zatrzymaniu, należy wybrać opcje **Programy** > **Trusteer Endpoint Protection** > **Uruchom program Trusteer Endpoint Protection**.

5. Ochrona czynności dokonywanych za pośrednictwem bankowości elektronicznej

Jeśli bank użytkownika jest partnerem IBM, można pobrać program Rapport ze strony powitalnej banku i cieszyć się w pełni chronioną bankowością elektroniczną od razu po jego zainstalowaniu.

Program Rapport identyfikuje zagrożenia dla bezpieczeństwa i neutralizuje je bez udziału użytkownika. Tylko w tych przypadkach, w których program Rapport wykryje pewien poziom zagrożenia, może zostać wyświetlony monit z prośbą o potwierdzenie przez użytkownika procesu jego neutralizacji. Więcej informacji na temat reagowania na alerty i ostrzeżenia programu Rapport można znaleźć w punkcie Reagowanie na alerty i ostrzeżenia.

6. Bezpieczne korzystanie z kart płatniczych online

Program Rapport chroni użytkownika przed kradzieżą kart płatniczych w przypadku korzystania z nich online.

Program Rapport oferuje następujące funkcje zapewniające bezpieczeństwo kart należących do systemów kart płatniczych objętych taką ochroną:

- Wykrywanie czynności wprowadzania kodu BIN dla kart należących do systemów kart płatniczych objętych ochroną na stronie WWW.
- Aktywacja blokady rejestrowania naciśnięć klawiszy niezwłocznie po rozpoczęciu wprowadzania kodu BIN, w celu uniemożliwienia przechwycenia numeru karty płatniczej przez szkodliwe oprogramowanie rejestrujące naciśnięcia klawiszy.
- Powiadamianie o aktywacji blokady rejestrowania naciśnięć klawiszy.
- Ostrzeganie o ryzyku związanym z wprowadzaniem numeru karty płatniczej w podejrzanych lub niezabezpieczonych serwisach oraz oferowanie opcji zaufania witrynie/przerwania wprowadzania numeru karty.

Uwaga: Program Rapport nie uzyskuje dostępu do numerów osobistych kart płatniczych. Program Rapport rozpoznaje sekwencję cyfr na początku numeru karty, identyfikującą jej wystawcę. Jest to numer identyfikacyjny banku (ang. bank identification number, BIN).

Podczas wprowadzania numerów kart płatniczych może zostać wyświetlone ostrzeżenie o następującej treści:

> *Prawdopodobnie wprowadzasz dane karty płatniczej w serwisie WWW niezabezpieczonym lub o wysokim stopniu ryzyka. Nie zaleca się wprowadzania danych kart płatniczych w niezabezpieczonych serwisach.*

Więcej informacji na temat tego ostrzeżenia można znaleźć w punkcie Reagowanie na ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej.

Prawdopodobnie wprowadzasz dane karty płatniczej. Oprogramowanie Trusteer automatycznie zabezpiecza dane karty płatniczej przed kradzieżą online.

Więcej informacji na temat tego komunikatu można znaleźć w punkcie Reagowanie na komunikaty o zabezpieczeniu danych karty płatniczej.

7. Reagowanie na alerty i ostrzeżenia

W produkcie wyświetlane są alerty i ostrzeżenia wymagające reakcji użytkownika. Po wyświetleniu okna dialogowego należy uważnie przeczytać jego treść i wybrać odpowiednią odpowiedź. Podjęcie niezbędnych działań może mieć krytyczne znaczenie dla bezpieczeństwa użytkownika. W celu odszukania danego alertu lub ostrzeżenia należy wyszukać w niniejszym dokumencie treść komunikatu wyświetlanego na ekranie.

Reagowanie na oferty ochrony hasła

Poniższy tekst stanowi przykład oferty ochrony hasła:

> *Program Trusteer Endpoint Protection wykrył czynność wprowadzania hasła.*
> *Czy chcesz, aby program Trusteer Endpoint Protection rozpoczął ochronę tego hasła?*
> *Kliknięcie opcji „Chroń to hasło" spowoduje, że program Trusteer Endpoint Protection będzie ostrzegał użytkownika przy każdej próbie wprowadzenia tego hasła w nowym serwisie WWW, w którym nie było ono dotąd wprowadzane. Pomaga to chronić przed wyłudzeniem danych logowania przez oszukańcze serwisy WWW.*

Oferta ochrony hasła pojawia się jednokrotnie dla każdego chronionego serwisu WWW. Oferta ta pojawia się za pierwszym razem, gdy program Rapport wykryje czynność wprowadzania hasła w zabezpieczonym serwisie WWW. Komunikat ten zostanie wyświetlony na przykład, jeśli niedawno pobrano program Rapport z serwisu WWW banku, a następnie zalogowano się do tego serwisu WWW. Innym przykładem jest ręczne ustawienie ochrony dla serwisu WWW, a następnie zalogowanie się do niego.

W przypadku wprowadzenia objętego ochroną hasła w serwisie WWW, którego program Rapport nie rozpoznaje, ostrzega on użytkownika o próbie użycia hasła w innym serwisie WWW. Ostrzeżenie pomaga uniknąć wprowadzania hasła w oszukańczym serwisie WWW, co pomaga chronić przed wyłudzaniem informacji[3].

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Chroń**: Po kliknięciu przycisku **Chroń** program Rapport rozpoczyna ochronę hasła dla tego serwisu WWW. Z chwilą zmiany hasła program Rapport, nie pytając użytkownika, automatycznie zaczyna chronić nowe hasło.
- **Nie chroń**: Wybór tej opcji powoduje, że program Rapport nie chroni żadnych haseł w tym serwisie i nie oferuje ochrony haseł w przypadku ponownych odwiedzin tego serwisu.
- **Nigdy nie chroń haseł**: Powoduje wyłączenie ochrony przed wyłudzeniem informacji przez program Rapport we wszystkich serwisach WWW. Po kliknięciu opcji **Nigdy nie chroń haseł** program Rapport nie będzie wyświetlał żadnych ostrzeżeń dotyczących wprowadzania haseł i nie będzie oferował ochrony haseł w żadnym serwisie WWW

Mam wybraną ochronę niewłaściwego hasła. Co mam teraz zrobić?

Wprowadź poprawne hasło. Program Rapport zapewni jego ochronę.

Wprowadzone przeze mnie chronione hasło zawiera błąd. Co teraz?

Ponownie poprawnie wprowadź hasło. Program Rapport umożliwi ochronę poprawnego hasła.

[3] Atak polegający na wyłudzeniu informacji to próba skłonienia użytkownika do odwiedzenia fałszywego serwisu WWW, który udaje inny, wiarygodny serwis (np. należący do banku), i wprowadzenia w nim swoich danych logowania, które mogą następnie zostać wykorzystane przez przestępców do uzyskania dostępu do konta bankowości elektronicznej i popełnienia przestępstwa, na przykład wykonania przelewu środków z rachunku bankowego użytkownika.

Mam wybraną opcję całkowitej rezygnacji z ochrony haseł, a teraz chcę chronić hasła. Co mam teraz zrobić?

Jeśli wybrano rezygnację z ochrony haseł, w strategii bezpieczeństwa programu Rapport ustawiono definicję strategii. Tę strategię można zmienić.

Aby zmienić strategię ochrony haseł:

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran User Approval. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Odszukaj element sterujący **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Z listy po prawej stronie tego elementu sterującego wybierz opcję **W newralgicznych serwisach WWW partnerów i moich** w celu zresetowania strategii i przywrócenia jej ustawień domyślnych. Zaznacz opcję **W serwisach WWW partnerów**, aby oferta ochrony haseł była wyświetlana tylko w serwisach WWW partnerów.
6. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Chcę chronić moje hasło, mimo że wcześniej została przeze mnie wybrana opcja „Nie chroń". Jak mogę rozpocząć jego ochronę?

Możesz zmienić decyzję o ochronie hasła dla tego konkretnego serwisu.

- **Aby włączyć wyłączoną dla konkretnego serwisu WWW ochronę hasła:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Wyświetlona zostanie strategia zabezpieczeń nazw użytkowników i haseł dla każdego serwisu WWW.
6. Zaznacz pole wyboru **Ostrzegaj w przypadku użycia hasła w innym miejscu** dla serwisu WWW, dla którego ma zostać włączona ochrona hasła. Program Rapport zapewni ochronę hasła dla tego serwisu WWW.
7. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Dostaję alert o hasło, które nie jest już używane. Jak mogę to przerwać?

W zależności od naszych ustaleń z witrynami WWW partnerów, hasła są często chronione, nawet po ich zastąpieniu nowymi. Kontynuowanie ochrony haseł rzadko bywa problemem, ponieważ chronione hasła nie są używane do innych celów. Jeśli jednak wystąpi konieczność zaprzestania ochrony starego hasła przez program Rapport, można wyczyścić pamięć podręczną PII (ang. Personally Identifiable Information) w celu zresetowania mechanizmu ochrony hasła. Czyszczenie pamięci podręcznej powoduje zaprzestanie ochrony starego hasła przez program Rapport, lecz także powoduje wyświetlenie nowej oferty ochrony hasła przy następnych odwiedzinach chronionego serwisu WWW.

Aby wyczyścić pamięć podręczną PII:

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Wyświetlona zostanie strategia zabezpieczeń nazw użytkowników i haseł dla każdego serwisu WWW.
6. Kliknij opcję **Wyczyść pamięć podręczną**. Wszystkie ustawienia ochrony hasła zostaną usunięte, zaś strategie ochrony hasła zostaną zresetowane, co spowoduje ponowne wyświetlenie w programie Rapport oferty ochrony hasła przy kolejnej wizycie w każdym z serwisów WWW.

Mimo wpisania chronionego hasła w serwisie innym niż ten, dla którego mam ustawioną ochronę tego hasła, nie otrzymuję ostrzeżenia. Dlaczego?

Niektóre uprawnione serwisy zostały już przez program Rapport zidentyfikowane jako uprawnione. Ponieważ wpisanie hasła w tych serwisach nie prowadzi do oszustwa, program Rapport nie wyświetla w nich ostrzeżenia.

Reagowanie na ostrzeżenia dotyczące danych chronionych

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego danych chronionych:

> *Właśnie wprowadzono tekst podobny do danych logowania w serwisie: twojbanktutaj.com*
> *Otrzymujesz to ostrzeżenie, ponieważ zamierzasz przesłać swoje dane do innego serwisu WWW: swojbanktutaj.com*
> *Upewnij się, że rozpoznajesz serwis, do którego zamierzasz przesłać dane logowania. Dane dotyczące bezpieczeństwa mogą ulec kradzieży podczas przesyłania do nieznanego serwisu WWW.*

Ostrzeżenie dotyczące ochrony danych pojawia się każdorazowo podczas wprowadzania tekstu zgodnego z chronioną nazwą użytkownika/hasłem w serwisie WWW nierozpoznawanym przez program Rapport. Celem tego okna komunikatu jest sprawdzenie, czy serwis WWW, do którego aktualnie przesyłane są informacje, nie jest serwisem oszukańczym, próbującym ukraść dane uwierzytelniające od użytkownika. Działanie takie określane jest terminem *Phishing* lub wyłudzeniem informacji.

W powyższym przykładzie program Rapport sprawdza, czy serwis WWW swojbanktutaj.com (adres przykładowy) nie podszywa się pod serwis twojbanktutaj.com i nie próbuje skłonić Cię do wprowadzenia w nim Twoich danych uwierzytelniających do serwisu twojbanktutaj.com.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zaufaj temu serwisowi**: jeśli zgadzasz się na wysłanie swoich danych logowania do tego serwisu WWW i wiesz, że ten serwis WWW nie pyta o dane uwierzytelniające innego serwisu. Po kliknięciu opcji **Zaufaj temu serwisowi** ostrzeżenie nie zostanie ponownie wyświetlone w przypadku wprowadzenia tej chronionej nazwy użytkownika lub hasła w tym serwisie WWW. Jeśli wprowadzono tekst niebędący danymi logowania lub będący danymi logowania używanymi w kilku serwisach WWW, wówczas, aby zachować możliwość wprowadzania go bez wyświetlania za każdym razem alertu, można także zaznaczyć pole wyboru **Nie chroń tych danych logowania w żadnym serwisie WWW**.

Uwaga:	Sprawdzoną procedurą dotyczącą zabezpieczeń jest wybór takich haseł, które zawierają unikalne, trudne do przewidzenia frazy *oraz* nieużywanie tego samego hasła dla więcej niż jednego serwisu WWW. Postępowanie zgodnie z tą praktyką minimalizuje prawdopodobieństwo konieczności zaznaczenia pola wyboru **Nie chroń tych danych logowania w żadnym serwisie WWW**.

- **Zabierz mnie stąd!** Tę opcję należy wybrać, aby zrezygnować z wysyłania danych logowania do tego serwisu WWW. Zostanie wyświetlone okno dialogowe z monitem o wybranie serwisu, do którego użytkownik ma zostać przekierowany.

Dlaczego dostaję tak wiele ostrzeżeń dotyczących danych chronionych?

W przypadku użycia łańcucha znaków często wpisywanego jako hasło w wielu różnych witrynach użytkownik otrzymuje ostrzeżenie dotyczące danych chronionych każdorazowo przy wprowadzeniu tego łańcucha w dowolnym serwisie, do którego hasło jest chronione. Aby uniknąć podobnych, irytujących sytuacji, nie należy chronić haseł używanych regularnie. W przypadku używania tego rodzaju hasła w serwisie WWW, do/z którego przesyłane są newralgiczne dane, należy zmienić hasło na zapewniające wyższy poziom bezpieczeństwa. Hasło bezpieczne jest unikalne dla serwisu WWW, w którym jest używane, i składa się z sekwencji znaków trudnej do przewidzenia. Zwykle składa się ono z kombinacji liter, cyfr i symboli.

Mimo wpisania chronionego hasła w serwisie WWW nieobjętym ochroną przez program Rapport nie otrzymuję alertu. Dlaczego?

Program Rapport korzysta z szeregu metod rozpoznawania serwisów WWW jako uprawnionych. Jednak w przypadku podejrzeń, że program Rapport nie wyświetla w sposób prawidłowy alertów dotyczących konkretnego serwisu należy skontaktować się z działem wsparcia, korzystając z informacji w punkcie Uzyskiwanie wsparcia.

Otrzymuję ostrzeżenie dotyczące ochrony danych mimo, że nie wpisuję chronionego hasła. Dlaczego?

W przypadku niektórych chronionych serwisów WWW program Rapport chroni wszystkie hasła wprowadzone kiedykolwiek w tym serwisie po zainstalowaniu programu Rapport. Ochrona ta obejmuje stare hasła, a nawet słowa wprowadzone przypadkowo. Może być to przyczyną wyświetlania ostrzeżenia.

Reagowanie na ostrzeżenia dotyczące wprowadzania danych bez zabezpieczenia

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego wprowadzania danych bez zabezpieczenia:

> *Wszelkie informacje wprowadzone na tej stronie, w tym nazwy użytkowników i hasła, są przesyłane za pośrednictwem niezaszyfrowanego połączenia i mogą zostać łatwo odczytane przez osoby trzecie.*

To ostrzeżenie pojawia się przy wprowadzaniu hasła w serwisie WWW niezapewniającym bezpieczeństwa przy wprowadzaniu danych. Jest ono wyświetlane, aby ostrzec użytkownika przed przesyłaniem newralgicznych danych do serwisów o wysokim stopniu ryzyka, w tym do serwisów uprawnionych, które mogą łatwo zostać przejęte przez grupy przestępcze.

Po wyświetleniu tego komunikatu należy wybrać jedną z poniższych opcji:

- **Nie przesyłaj**: przerywa operację przesyłania i automatycznie przekierowuje przeglądarkę na stronę WWW IBM z wyjaśnieniem ryzyka związanego z wprowadzaniem danych do niezabezpieczonych serwisów.
- **Prześlij mimo to**: kontynuuje wprowadzanie mimo ostrzeżenia.
- **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie**: kontynuuje wprowadzanie mimo ostrzeżenia i zapisuje w programie Rapport informację o ufaniu temu serwisowi w przyszłości. Kliknięcie tego przycisku powoduje dodanie serwisu do listy serwisów uznawanych za zaufane. Program Rapport nie będzie ostrzegał o nich w przyszłości. Decydując się na usunięcie serwisu z listy, należy zapoznać się z informacjami w punkcie Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych bez zabezpieczenia.
- **Zmień ustawienia**: otwiera ekran strategii bezpieczeństwa programu Rapport i zmienia strategię **Ostrzegaj, kiedy przesyłam newralgiczne dane do niezabezpieczonych serwisów**, decydującą o wyświetlaniu lub nie podobnych ostrzeżeń.

Czy po wybraniu opcji „Ten serwis jest zaufany, nie wyświetlaj alertu ponownie" można usunąć ten serwis z listy zaufanych serwisów?

Tak, można.

➡ **Aby usunąć serwis z listy serwisów wybranych jako zaufane:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.

4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Kliknij element sterujący strategii **Ostrzegaj, kiedy przesyłam zabezpieczone dane do niezabezpieczonych serwisów**. Zostanie wyświetlony komunikat „Następujące serwisy wybrano jako zaufane:" wraz z listą serwisów, które wybrano jako zaufane.

6. Znajdź serwis wybrany jako zaufany i kliknij opcję **Usuń ten serwis** obok nazwy serwisu.

7. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Reagowanie na ostrzeżenia dotyczące wyłudzania informacji

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego wyłudzania informacji:

> *Próbujesz uzyskać dostęp do strony WWW pod adresem www.swojbanktutaj.com. Ten serwis WWW to znany serwis wyłudzający informacje, dlatego został on zablokowany przez program Trusteer, aby chronić dane użytkownika.*
> *Serwisy wyłudzające informacje są tworzone przez oszustów dążących do skłonienia użytkownika do ujawnienia newralgicznych informacji przez imitowanie serwisów uprawnionych.*
> *Wprowadzenie danych na tej stronie może skutkować kradzieżą tożsamości i stratami finansowymi.*

To ostrzeżenie pojawia się po zablokowaniu przez program Rapport serwisu WWW, który użytkownik chciał odwiedzić, ponieważ program Rapport uznał ten serwis za fałszywy i znany z wyłudzania informacji. Program Rapport wyposażono w szereg mechanizmów umożliwiających dokładne wykrycie serwisów WWW wyłudzających informacje. Ostrzeżenie to, pojawiające się po przejściu do podejrzanego serwisu

WWW, pozwala zapobiec wyłudzeniom informacji. Pojawienie się tego ostrzeżenia po kliknięciu odsyłacza do serwisu WWW oznacza, że odsyłacz jest najprawdopodobniej fałszywy, a ryzyko jest większe.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zabierz mnie stąd**: przekierowuje do poprzedniej odwiedzonej strony w przeglądarce.
- **Dlaczego ta strona była zablokowana?** Otwiera stronę WWW z wyjaśnieniem, dlaczego to ostrzeżenie zostało wyświetlone.
- **Ignoruj to ostrzeżenie**: wczytuje serwis WWW mimo zgłoszonych czynników ryzyka. Nastąpi przejście do serwisu zweryfikowanego jako serwis utworzony przez grupę przestępczą do celów oszustwa polegającego na kradzieży poufnych danych uwierzytelniających logowania do konta. W przypadku niektórych witryn wyłudzających informacje już samo wprowadzenie danych, bez naciśnięcia przycisku przesyłania, wystarcza do przechwycenia tych danych i wykorzystania ich do kradzieży lub oszustwa. Zdecydowanie zaleca się **rezygnację z wyboru tej opcji**.

Co należy zrobić, jeśli jako wyłudzający informacje został uznany serwis WWW, który uważam za uprawniony?

Jeśli serwis WWW uznany za uprawniony został oznaczony jako wyłudzający informacje, należy wykonać zrzut ekranu tego serwisu, zanotować otrzymane ostrzeżenie i otworzyć zgłoszenie na stronie http://www.trusteer.com/support/submit-ticket.

Jak mogę wyłączyć ostrzeżenia o zapobieganiu oszustwom?

➔ **Aby wyłączyć ostrzeżenia o zapobieganiu oszustwom:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.

3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Ustaw element sterujący **Ostrzegaj przy przeglądaniu szkodliwych serwisów** na wartość **Nigdy**.
6. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Reagowanie na ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej

Poniższy tekst stanowi przykład ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej:

> *Prawdopodobnie wprowadzasz dane karty płatniczej w serwisie WWW niezabezpieczonym lub o wysokim stopniu ryzyka. Nie zaleca się wprowadzania danych kart płatniczych w niezabezpieczonych serwisach.*

To ostrzeżenie pojawia się podczas wprowadzania zabezpieczonych numerów kart płatniczych na stronie WWW na dysku lokalnym lub w dowolnym niezabezpieczonym serwisie WWW. Ten komunikat jest wyświetlany z myślą o tym, aby pomóc użytkownikowi uniknąć przesyłania numerów kart płatniczych do oszukańczych serwisów lub do serwisów uprawnionych, lecz nie zapewniających odpowiedniego poziomu bezpieczeństwa.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zabierz mnie z tej strony**: tę opcję należy wybrać w przypadku rezygnacji z wysyłania danych karty do tego serwisu WWW. W przeglądarce zostanie załadowana strona startowa.
- **Ignoruj, ten serwis WWW jest zaufany**: tę opcję należy wybrać, aby przesłać dane karty do tego serwisu WWW. Okno dialogowe zostanie zamknięte, lecz program Rapport będzie nadal blokował możliwość przechwycenia danych karty płatniczej przez programy rejestrujące naciśnięcia klawiszy. Wystawca karty płatniczej otrzymuje powiadomienie o tym wyborze. Decydując się na usunięcie strony wybranej wcześniej jako zaufana, należy zapoznać się z informacjami w punkcie Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych kart płatniczych.

Uwaga:	Zignorowanie tego ostrzeżenia spowoduje wysłanie danych karty płatniczej do znanego oszukańczego serwisu WWW lub wysłanie ich do serwisu, który nie zapewnia szyfrowania i pozwala na ich ujawnienie podmiotom trzecim.

- **Zawsze ufaj tej witrynie**: program Rapport ufa obecnie tej witrynie i nie wyświetla tego ostrzeżenia ponownie przy próbie wprowadzenia przez użytkownika w tym serwisie jakiegokolwiek numeru karty płatniczej. Program Rapport będzie nadal blokował możliwość przechwycenia danych karty płatniczej przez programy rejestrujące naciśnięcia klawiszy.
- **Zrezygnuj z ochrony kart**: wyłącza funkcję ochrony kart płatniczych. Aby ponownie włączyć tę funkcję, zmień wartość ustawienia dla strategii **Chroń numery kart płatniczych przed kradzieżą** z **Nigdy** na **Zawsze**.

Uwaga:	Ochrona kart płatniczych jest włączona tylko dla systemów kart płatniczych objętych taką ochroną.

Reagowanie na komunikaty o ochronie karty płatniczej

Poniższy tekst stanowi przykład komunikatu o ochronie karty płatniczej:

Prawdopodobnie wprowadzasz dane karty płatniczej. Firma Trusteer automatycznie zabezpiecza dane karty płatniczej przed kradzieżą online.

Ten komunikat informuje użytkownika o tym, że program Rapport wykrył operację przesyłania numeru karty płatniczego do strony WWW i rozpoczął szyfrowanie danych wprowadzanych na stronie, aby uniemożliwić przechwycenie numeru karty płatniczej przez szkodliwe oprogramowanie rejestrujące naciśnięcia klawiszy. Komunikat ten jest wyświetlany po wprowadzeniu numeru chronionej karty płatniczej w chronionym serwisie WWW programu Rapport lub w dowolnym chronionym (za pomocą protokołu https) serwisie zawierającym słowo kluczowe związane z kartą płatniczą, takim jak Visa, Mastercard czy Amex.

Po wyświetleniu tego komunikatu nie trzeba już robić nic więcej. Opcjonalnie można kliknąć przycisk **OK** w celu zamknięcia okna z komunikatem. W przypadku rezygnacji okno zostanie zamknięte automatycznie po krótkim czasie.

Jeśli nie chcesz otrzymywać powiadomień o aktywacji funkcji blokującej rejestrację naciśnięć klawiszy, kliknij opcję **Nie wyświetlaj tego komunikatu ponownie**. Aby ponownie włączyć te powiadomienia, zaznacz dla strategii **Chroń numery kart płatniczych przed kradzieżą** pole wyboru **Powiadom mnie o aktywacji zabezpieczeń kart płatniczych przez program Trusteer**.

Uwaga: Ochrona kart płatniczych jest włączona tylko dla systemów kart płatniczych objętych taką ochroną.

Reagowanie na alerty o wykryciu próby wykonania zrzutu ekranu

Poniższy tekst stanowi przykład alertu dotyczącego wykrycia próby wykonania zrzutu ekranu:

Przechwycony ekran może zawierać newralgiczne dane z serwisu twojbanktutaj.com

Ten alert pojawia się, gdy na komputerze w chwili wyświetlania serwisu WWW partnera zostanie naciśnięty klawisz PrtScn. Alert pomaga zdecydować o zablokowaniu lub zezwoleniu na wykonanie zrzutu ekranu.

Klawisz PrtScn na klawiaturze służy do wykonywania zrzutów ekranu. Możliwe jest jednak aktywowanie przez szkodliwe oprogramowanie tego samego mechanizmu, aktywowanego przez ten klawisz, i przechwycenie newralgicznych informacji w celu dokonania oszustwa.

Uwaga: Ten alert jest generowany przez funkcję blokowania przechwytywania ekranu, włączaną domyślnie w serwisach WWW partnerów.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zezwalaj**: umożliwia przechwycenie ekranu za pomocą klawisza PrtScn. Tę opcję należy wybrać w przypadku celowego naciśnięcia klawisza zrzutu ekranu w celu jego przechwycenia.
- **Blokuj**: uniemożliwia przechwycenie ekranu za pomocą klawisza PrtScn. Wybierz tę opcję, jeśli klawisz PrtScn został naciśnięty nieumyślnie.

To okno dialogowe jest wyświetlane nawet wówczas, jeśli nie próbuję wykonać zrzutu ekranu zawierającego newralgiczne dane.

Zminimalizuj lub zamknij wszystkie okna przeglądarki i spróbuj ponownie.

Reagowanie na alerty dotyczące ochrony przeglądarki

Poniższy tekst stanowi przykład alertu dotyczącego ochrony przeglądarki:

Poniższy dodatek programu Internet Explorer korzysta z nieznanej metody dostępu do przeglądarki i jako taki nie podlega monitorowaniu przez program Trusteer Endpoint Protection. Ten pasek narzędzi można albo na stałe włączyć, albo zablokować.

Ten alert pojawia się, gdy program dodatkowy (taki jak pasek narzędzi lub rozszerzenie) próbuje uzyskać dostęp do informacji należących do chronionego serwisu WWW za pomocą metody, która nie jest obecnie monitorowana w programie Rapport.

Po wyświetleniu tego alertu należy wybrać jedną z poniższych opcji:

- **Zezwól na stałe**: powoduje zezwolenie na działanie programu dodatkowego w dowolnym serwisie WWW. Wybierz tę opcję, jeśli wiesz o działaniu programu dodatkowego w swojej przeglądarce, korzystasz z niego i ufasz jego źródłu.
- **Blokuj na stałe**: powoduje zablokowanie przez program Rapport działania programu dodatkowego w dowolnym serwisie WWW i powoduje anonimowe przesłanie do IBM raportu dotyczącego bezpieczeństwa o zablokowanym programie dodatkowym, umożliwiając przeanalizowanie tego faktu przez ekspertów ds. bezpieczeństwa IBM. Pozwala to IBM globalnie i na stałe zablokować program dodatkowy, jeśli zostanie on zidentyfikowany jako szkodliwy.

Czy mogę odblokować zablokowany wcześniej przez siebie program dodatkowy lub zablokować program dodatkowy, na którego działanie została wcześniej wyrażona zgoda?

➡ **Aby zmienić status programów dodatkowych, na których działanie zezwolono lub które zablokowano:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Kliknij nazwę strategii **Blokuj nieznane programy dodatkowe w przeglądarce**. Poniżej nazwy strategii zostanie wyświetlona lista wszelkich dozwolonych lub zablokowanych programów dodatkowych.
6. Przełącz status zablokowania lub zezwolenia każdego z programów dodatkowych stosownie do potrzeb.
7. Kliknij przycisk **Zapisz**. Zmiany zostaną zapisane.

Reagowanie na alerty dotyczące aktywacji funkcji usuwania szkodliwego oprogramowania

Poniższy tekst stanowi przykład alertu dotyczącego aktywacji funkcji usuwania szkodliwego oprogramowania:

> *Program Trusteer Endpoint Protection wykrył i zablokował szkodliwe oprogramowanie <nazwa_szkodliwego_oprogramowania>. Usuwanie szkodliwego oprogramowania przerwano, ponieważ dla strategii usuwania szkodliwego oprogramowania wybrano wartość „Nigdy”.*
> *NALEŻY TERAZ AKTYWOWAĆ STRATEGIĘ USUWANIA SZKODLIWEGO OPROGRAMOWANIA W CELU ZMAKSYMALIZOWANIA POZIOMU BEZPIECZEŃSTWA.*

Ten alert pojawia się po wyłączeniu strategii usuwania szkodliwego oprogramowania, po wykryciu i zablokowaniu go przez program Rapport. Alert ten ma stanowić zachętę do aktywacji przez użytkownika strategii usuwania szkodliwego oprogramowania, tak aby program Rapport mógł usunąć szkodliwe oprogramowanie. Usuwanie szkodliwego oprogramowania włączono domyślnie, lecz można je wyłączyć, korzystając ze strategii bezpieczeństwa programu Rapport.

Po wyświetleniu tego alertu należy wybrać jedną z poniższych opcji:

- **Aktywuj strategię usuwania teraz**: strategia usuwania szkodliwego oprogramowania zostaje aktywowana i program Rapport inicjuje usuwanie zablokowanego szkodliwego oprogramowania. Może zostać wyświetlone inne okno dialogowe wymagające zrestartowania komputera. Użytkownik przed kliknięciem przycisku **Zrestartuj komputer teraz** będzie miał możliwość zapisania i zamknięcia otwartych plików i aplikacji. Proces restartowania kończy usuwanie szkodliwego oprogramowania.
- **Ignoruj**: Alert ten pojawia się przy następnej próbie wykrycia szkodliwego oprogramowania przez program Rapport. Szkodliwe oprogramowanie pozostaje na komputerze, lecz jest zablokowane. Zablokowane szkodliwe oprogramowanie znajdujące się na komputerze stanowi ryzyko, ponieważ może ono zostać aktywowane w przyszłości, w sytuacji zatrzymania lub zdeinstalowania programu Rapport albo w sytuacji użycia przeglądarki nieobsługującej programu Rapport.

Reagowanie na alerty dotyczące zainicjowania usuwania szkodliwego oprogramowania

Poniższy tekst stanowi przykład alertu dotyczącego zainicjowania usuwania szkodliwego oprogramowania:

> *Program Trusteer Endpoint Protection wykrył i zablokował szkodliwe oprogramowanie <nazwa_szkodliwego_oprogramowania>; zainicjowano usuwanie szkodliwego oprogramowania.*
> *ZRESTARTUJ TERAZ KOMPUTER, ABY UKOŃCZYĆ USUWANIE*

Alert podobny do powyższego pojawia się po wykryciu i zablokowaniu przez program Rapport szkodliwego oprogramowania i przystąpieniu do usuwania go z komputera. Do ukończenia procesu usuwania szkodliwego oprogramowania przez program Rapport konieczne jest zrestartowanie komputera.

Po wyświetleniu tego alertu należy wybrać jedną z poniższych opcji:

- **Zrestartuj komputer teraz**: restartuje komputer niezwłocznie, po ukończeniu procesu usuwania szkodliwego oprogramowania. Po zrestartowaniu komputera i zalogowaniu się na swoje konto w serwisie chronionym przez program Rapport upewnij się, że ikona programu Rapport jest zielona. Alert dotyczący zainicjowania usuwania szkodliwego oprogramowania nie powinien pojawić się ponownie po zrestartowaniu komputera. Jeśli pojawi się on ponownie, należy przesłać raport dotyczący problemu z Konsoli Rapport.
- **Ignoruj**: Usuwanie szkodliwego oprogramowania zostanie zakończone przy kolejnej próbie zrestartowania komputera. Do chwili zrestartowania komputera należy unikać wszelkich newralgicznych operacji online. Program Rapport nie wyświetli ponownego alertu dotyczącego usuwania tego szkodliwego oprogramowania.
- **Zawieś wyświetlanie alertu na tydzień**: ten alert zostanie wyświetlony ponownie w ciągu tygodnia, jeśli szkodliwe oprogramowanie nie zostanie wcześniej usunięte. Jeśli w tym czasie komputer zostanie zrestartowany, proces usuwania szkodliwego oprogramowania zostanie zakończony i alert nie pojawi się ponownie.

Reagowanie na ostrzeżenia dotyczące niepoprawnego certyfikatu

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego niepoprawnego certyfikatu:

> *Ten serwis WWW korzysta z niepoprawnego certyfikatu.*
> *Zaleca się zablokowanie dostępu do tego serwisu WWW, o ile nie jest on wewnętrznym serwisem organizacji użytkownika.*

To ostrzeżenie pojawia się po przejściu do chronionego serwisu WWW, po wykryciu przez program Rapport, że certyfikat[4] serwisu WWW jest niepoprawny. Nieważny certyfikat mógł utracić ważność, może być niepoprawny lub podpisany przez nieznanego wystawcę. To ostrzeżenie jest wyświetlane, aby ostrzec użytkownika przed wysyłaniem newralgicznych danych do oszukańczych serwisów WWW.

Uwaga: To ostrzeżenie może pojawiać się na stronach WWW z poprawnymi certyfikatami, jeśli datę lub godzinę dla tego komputera ustawiono nieprawidłowo. W przypadku częstego pojawiania się tego ostrzeżenia należy sprawdzić datę i godzinę na komputerze.

Ostrzeżenie dotyczące nieważnego certyfikatu zawiera następujące informacje:

Pole na ekranie	Opis
Przyczyna błędu	Przyczyna aktywacji tego ostrzeżenia przez program Rapport. Możliwe wartości: • **Adresy są niezgodne**: adres, do którego próbowano uzyskać dostęp, i adres na certyfikacie są niezgodne. Aby certyfikat był ważny, adresy muszą być zgodne. Sprawdź oba adresy. Jeśli adres na certyfikacie wydaje się podejrzany lub niepowiązany z serwisem WWW, do którego usiłujesz uzyskać dostęp, zdecyduj o zablokowaniu dostępu. • **Nieznany podmiot podpisujący certyfikat**: podmiot, który podpisał certyfikat, jest nieznany IBM. Nie należy ufać nieznanym podmiotom podpisującym przy generowaniu ważnych certyfikatów. Banki i instytucje finansowe zawsze korzystają z certyfikatów od znanych osób podpisujących. • **Certyfikat utracił ważność**: certyfikat utracił ważność i nie jest poprawny. Serwis WWW korzystający z certyfikatu, który utracił ważność, cechuje niski poziom bezpieczeństwa. Banki i instytucje finansowe nigdy nie korzystają z certyfikatów, które utraciły ważność. Sprawdź zegar systemowy, aby upewnić się, że data na komputerze jest poprawna. Jeśli na komputerze ustawiona jest data z przyszłości, ten komunikat może być wyświetlany w wyniku błędu. • **Niepoprawny certyfikat**: Format certyfikatu jest niepoprawny.
Adres na certyfikacie	Adres na certyfikacie wyświetlanym przez ten serwis WWWW. Każdy certyfikat jest wydawany dla konkretnego adresu WWW. W serwisie WWW powinien być widoczny certyfikat z listą posiadanych adresów.
Adres we wniosku	Adres WWW, pod który przekierowywana jest przeglądarka. Jest to adres, do którego próbowano uzyskać dostęp.

[4] Certyfikat SSL to kryptograficzny certyfikat cyfrowy potwierdzający tożsamość serwisu WWW i tworzący zaszyfrowane połączenie umożliwiające przesyłanie newralgicznych danych do serwisu WWW. Symbol kłódki na pasku adresu przeglądarki lub w dolnej części przeglądarki oznacza, że połączenie między przeglądarką a serwisem WWW jest zabezpieczone protokołem SSL. Jednocześnie jednak obecność symbolu kłódki nie gwarantuje, że certyfikat jest poprawny.

Pole na ekranie	Opis
Data ważności certyfikatu	Każdy certyfikat jest ograniczony w czasie. Serwis WWW korzystający z certyfikatu, który utracił ważność, cechuje niski poziom bezpieczeństwa.
Osoba podpisująca	Podmiot, który wystawił certyfikat. Nie należy ufać certyfikatom od nieznanych podmiotów.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Blokuj dostęp**. Blokuje dostęp do serwisu. Wybierz tę opcję, jeśli serwis WWW jest serwisem o charakterze finansowym lub zakupowym, do którego użytkownicy przesyłają newralgiczne informacje.
- **Zezwalaj na dostęp**. Umożliwia dostęp do serwisu. Tę opcję można wybrać, jeśli serwis WWW znajduje się w sieci lokalnej (intranet) lub jeśli nie operuje on newralgicznymi informacjami. W przypadku zezwolenia na dostęp należy postępować z zachowaniem ostrożności i nie przesyłać do serwisu newralgicznych informacji. Pole wyboru **Nie wyświetlaj ostrzeżenia dotyczącego tego serwisu WWW ponownie** należy zaznaczyć tylko, jeśli program Rapport nie powinien wyświetlać alertów dotyczących tego serwisu w przyszłości.

Jak mogę wyłączyć tę funkcję?

Istnieje możliwość wyłączenia sprawdzania poprawności certyfikatu SSL za pomocą Konsoli Rapport. Powoduje to zatrzymanie mechanizmu sprawdzania przez program Rapport ważności certyfikatów serwisów WWW, a w efekcie przerwanie pojawiania się tych ostrzeżeń.

➡ **Aby wyłączyć sprawdzanie poprawności certyfikatu SSL:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.

4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Odszukaj element sterujący **Sprawdź poprawność certyfikatów SSL serwisu WWW**.

6. Z listy po prawej stronie tego elementu sterującego wybierz opcję **Nigdy**.

7. Kliknij przycisk **Zapisz**. Sprawdzanie poprawności certyfikatu SSL jest teraz wyłączone.

Reagowanie na standardowe ostrzeżenia dotyczące konta użytkownika

Poniższy tekst stanowi przykład standardowego ostrzeżenia dotyczącego konta użytkownika:

> *Program Trusteer Endpoint Protection zidentyfikował na tym komputerze szkodliwe oprogramowanie stwarzające wysokie ryzyko dla operacji finansowych. Zaleca się powstrzymanie od wykonywania operacji bankowych na tym konkretnym komputerze aż do chwili rozwiązania problemu lub aż do chwili ponownego zainstalowania programu Trusteer Endpoint Protection za pośrednictwem konta użytkownika systemu Windows z uprawnieniami administratora.*

To ostrzeżenie pojawia się podczas instalowania programu Rapport za pośrednictwem standardowego konta użytkownika, znanego także jako konto użytkownika z ograniczeniami (ang. Limited User Account, LUA). W przypadku zainstalowania programu Rapport za pośrednictwem standardowego konta użytkownika nie jest możliwe uruchomienie zaawansowanych funkcji usuwania szkodliwego oprogramowania i komputer może być wystawiony na ryzyko. Do zapewnienia pełnej ochrony komputera program Rapport wymaga uprawnień administratora.

Należy spróbować zainstalować program Rapport ponownie, korzystając z uprawnień administratora. W przypadku braku uprawnień administratora należy skontaktować się z administratorem IT.

Więcej informacji można znaleźć na stronie:
http://manage.trusteer.com/support/what-admin-mode-windows

Reagowanie na powiadomienia dotyczące raportu o aktywności

Poniższy tekst stanowi przykład powiadomienia dotyczącego tygodniowego raportu o aktywności:

Okresowy raport o aktywności jest gotowy.

To powiadomienie pojawia się raz na tydzień w przypadku wybrania w Konsoli Rapport opcji generowania tygodniowego raportu o aktywności.

Po wyświetleniu tego powiadomienia należy wybrać jedną z poniższych opcji:

- **Otwórz raport**: otwiera Konsolę Rapport i wyświetla tygodniowy raport o aktywności.
- **Zamknij**: zamyka alert i nie wyświetla raportu o aktywności. Raport o aktywności można jednak wyświetlić w dowolnej chwili.

Minął ponad tydzień, a nadal nie otrzymuję powiadomienia o dostępności Tygodniowego raportu o aktywności. Dlaczego?

Tygodniowy raport o aktywności pojawia się tylko, jeśli w ciągu ostatniego tygodnia miało miejsce co najmniej jedno zdarzenie. Istnieje możliwość, że nie zarejestrowano żadnych zdarzeń.

Reagowanie na komunikaty o potwierdzeniu aktualizacji kodu

W przypadku włączenia na komputerze kontroli konta użytkownika (funkcja zabezpieczeń dostępna w systemach Windows 8 i Windows 7) od czasu do czasu podczas automatycznej aktualizacji programu Rapport może być widoczny następujący komunikat:

Ukończenie procesu aktualizacji oprogramowania wymaga zastąpienia przez program Trusteer Endpoint Protection plików aplikacji. W systemie operacyjnym może zostać wyświetlone okno dialogowe z potwierdzeniem. Kliknij przycisk potwierdzania, aby pomyślnie ukończyć proces aktualizacji.

W przypadku wyświetlenia tego komunikatu kliknij przycisk **OK**. Następnie może zostać wyświetlone okno dialogowe Kontrola konta użytkownika z informacją o konieczności dysponowania uprawnieniami do kontynuowania procesu aktualizacji programu Rapport. Po wyświetleniu komunikatu Kontrola konta użytkownika należy kliknąć przycisk **Kontynuuj** w celu ukończenia procesu aktualizacji.

Uwaga: Jeśli komunikat z potwierdzeniem aktualizacji kodu pojawia się często, należy przesłać wniosek o wsparcie na stronie: http://www.trusteer.com/support/submit-ticket.

Reagowanie na ostrzeżenia dotyczące trybu zgodności z lektorem ekranowym

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego trybu zgodności z lektorem ekranowym:

Program Trusteer Endpoint Protection jest obecnie zainstalowany w trybie zgodności z lektorem ekranowym. Aktywowanie tej strategii może spowodować wyłączenie niektórych lektorów ekranowych. Czy na pewno chcesz aktywować tę strategię?

To ostrzeżenie pojawia się, jeśli program Rapport jest zainstalowany w trybie zgodności z lektorem ekranowym, podczas próby włączenia jednej z następujących strategii bezpieczeństwa:

- **Blokuj wykonywanie zrzutów ekranu**
- **Blokuj dostęp do informacji w przeglądarce**

Te strategie są domyślnie wyłączone, jeśli program został zainstalowany w trybie zgodności z lektorem ekranowym. Włączenie którejkolwiek z tych strategii może spowodować zakłócenia w działaniu oprogramowania lektora ekranowego, uniemożliwiając mu odczytywanie stron WWW oraz opcji menu i okien dialogowych programu Rapport.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Aktywuj strategię**. Tę opcję należy wybrać w przypadku pewności co do zamiaru włączenia strategii, jeśli nie ma ryzyka, że uniemożliwi to korzystanie z lektorów ekranowych w programie Rapport.

Uwaga:	Jeśli nie ma potrzeby korzystania z lektorów ekranowych, należy zainstalować program Rapport ponownie, nie wybierając trybu zgodności z lektorem ekranowym. Przed ponowną instalacją należy usunąć wszystkie foldery powiązane z programem Rapport. Wskazówki dotyczące usuwania folderów można znaleźć tutaj: http://www.trusteer.com/support/remove-rapport-folders

- **Anuluj**. Tę opcję należy wybrać, aby anulować operację aktywacji strategii.

Reagowanie na alerty dotyczące ponownej instalacji w trybie administratora

Poniższy tekst stanowi przykład alertu dotyczącego ponownej instalacji w trybie administratora:

> *Program Trusteer Endpoint Protection zainstalowano uprzednio za pośrednictwem konta o ograniczonych uprawnieniach użytkownika. W celu zmaksymalizowania bezpieczeństwa zaleca się ponowne zainstalowanie programu Trusteer Endpoint Protection z konta użytkownika dysponującego uprawnieniami administratora.*

Ten alert wskazuje, że usługodawca udostępniający program Rapport ograniczył w ostatnim czasie możliwość instalowania programu Rapport do kont z uprawnieniami administratora systemu Windows. Program Rapport został zainstalowany za pośrednictwem standardowego konta użytkownika. Dostawca zaleca obecnie

zdeinstalowanie programu Rapport za pośrednictwem standardowego konta użytkownika, na którym zainstalowano program Rapport, a następnie ponowną instalację programu Rapport za pośrednictwem konta administratora. Po zainstalowaniu programu Rapport za pośrednictwem konta administratora stanie się on aktywny na wszystkich kontach użytkowników systemu Windows na komputerze.

Konto administratora systemu Windows jest kontem użytkownika systemu Windows, które umożliwia dokonywanie zmian mających wpływ na ustawienia wszystkich lub wybranych użytkowników danego komputera. Zmiany te uwzględniają ustawienia zabezpieczeń, procesy instalacji oprogramowania i dostęp do plików. Mimo że każdy komputer z systemem Windows ma konto administratora, Microsoft zaleca korzystanie ze standardowego konta użytkownika przy zwykle wykonywanych operacjach.

Po wyświetleniu tego alertu należy wybrać jedną z następujących opcji:

- **Zamknij**. Następuje zamknięcie alertu. Następnie można ponownie zainstalować program Rapport, korzystając z poniższej procedury.
- **Wyświetl alert po 7 dniach**. Alert zostaje zamknięty, a następnie jest wyświetlany ponownie po upływie siedmiu dni w celu przypomnienia użytkownikowi o konieczności przeprowadzenia ponownej instalacji.

➡ **Aby ponownie zainstalować program Rapport:**

1. Zdeinstaluj program Rapport, korzystając z tego samego standardowego konta użytkownika, które było używane do zainstalowania programu Rapport:
   - Deinstalowanie programu Rapport (Windows 8 i Windows 7)
   - Deinstalowanie programu Rapport (Windows XP)

Uwaga:	W oknie dialogowym Deinstalowanie programu IBM Security Trusteer Endpoint Protection należy zaznaczyć pole wyboru **Usuń ustawienia wszystkich użytkowników**. Jest to niezbędne do zapewnienia bezproblemowej ponownej instalacji.

2. Przełącz się na konto administratora:
   - Przełączanie się na konto administratora (system operacyjny Windows 8)
   - Przełączanie się na konto administratora (system operacyjny Windows 7)
   - Przełączanie się na konto administratora (system operacyjny Windows XP)
3. Należy pobrać najnowszą wersję programu Rapport od swojego usługodawcy; w tym celu:
   a. Przejdź na stronę http://www.trusteer.com/support/rapport-installation-links.
   b. Odszukaj odpowiedni dla swojego usługodawcy (banku, przedsiębiorstwa lub innej organizacji, która zaoferowała Ci program Rapport) odsyłacz do pliku do pobrania.
   c. Kliknij odsyłacz do pliku instalacyjnego do pobrania.
   d. Po wyświetleniu monitu zapisz plik na komputerze.
   e. Uruchom plik, aby go zainstalować. Pełną instrukcje instalacji można znaleźć w sekcji Instalowanie programu Rapport.

Przełączanie się na konto administratora (system operacyjny Windows 8)

Aby przełączyć się na konto administratora, potrzebne są nazwa użytkownika i hasło dla konta administratora. Jeśli nie znasz nazwy użytkownika ani hasła dla konta administratora, musisz zwrócić się do administratora z prośbą o zmianę rodzaju swojego konta lub zainstalowanie programu Rapport.

➡ **Aby przełączyć się na konto użytkownika o uprawnieniach administratora:**

1. Na ekranie **Start** kliknij ikonę konta.
2. Klikając, wybierz użytkownika, na którego konto chcesz się przełączyć.

Nie wiem, czy konto, którego używam, jest kontem administratora

Jeśli nie masz pewności, czy konto użytkownika jest kontem administratora, czy standardowym kontem użytkownika, możesz sprawdzić typ konta, przełączając się na nie, a następnie wykonując poniższe czynności.

- **Jeśli komputer należy do domeny:**

  1. Kliknij **Start**.
  2. Kliknij opcję **Panel sterowania**.
  3. Kliknij opcję **Konta użytkowników**.
  4. Kliknij opcję **Konta użytkowników**.
  5. Kliknij opcję **Zarządzaj kontami użytkowników**.
  6. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Nazwa użytkownika jest podświetlona, zaś typ konta jest wyświetlony w kolumnie Grupa.

- **Jeśli komputer należy do grupy roboczej:**

  1. Kliknij **Start**.
  2. Kliknij opcję **Panel sterowania**.
  3. Kliknij opcję **Konta użytkowników i bezpieczeństwo rodzinne**.
  4. Kliknij opcję **Konta użytkowników**.
  5. Kliknij opcję **Zarządzaj innym kontem**. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika.) Typ konta jest wyświetlany pod nazwą użytkownika.

Przełączanie się na konto administratora (system operacyjny Windows 7)

Aby przełączyć się na konto administratora, potrzebne są nazwa użytkownika i hasło dla konta administratora. Jeśli nie znasz nazwy użytkownika ani hasła dla konta administratora, musisz zwrócić się do administratora z prośbą o zmianę rodzaju swojego konta lub zainstalowanie programu Rapport.

- **Aby przełączyć się na konto użytkownika o uprawnieniach administratora:**

1. Kliknij **Start**.
2. Kliknij strzałkę obok opcji **Zamknij**.
3. Kliknij opcję **Przełącz użytkownika**.
4. Naciśnij kombinację klawiszy **Ctrl+Alt+Delete**, a następnie kliknij konto użytkownika, na które chcesz się przełączyć.

Nie wiem, czy konto, którego używam, jest kontem administratora

Jeśli nie masz pewności, czy konto użytkownika jest kontem administratora, czy standardowym kontem użytkownika, możesz sprawdzić typ konta, przełączając się na nie, a następnie wykonując poniższe czynności.

- **Jeśli komputer należy do domeny:**

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj kontami użytkowników**.
6. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Nazwa użytkownika jest podświetlona, zaś typ konta jest wyświetlony w kolumnie Grupa.

- **Jeśli komputer należy do grupy roboczej:**

  1. Kliknij **Start**.
  2. Kliknij opcję **Panel sterowania**.
  3. Kliknij opcję **Konta użytkowników i bezpieczeństwo rodzinne**.
  4. Kliknij opcję **Konta użytkowników**.
  5. Kliknij opcję **Zarządzaj innym kontem**. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Typ konta jest wyświetlany pod nazwą użytkownika.

Przełączanie się na konto administratora (system operacyjny Windows XP)

Aby przełączyć się na konto administratora, potrzebne są nazwa użytkownika i hasło dla konta administratora. Jeśli nie znasz nazwy użytkownika ani hasła dla konta administratora, musisz zwrócić się do administratora z prośbą o zmianę rodzaju swojego konta lub zainstalowanie programu Rapport.

- **Aby przełączyć się na konto użytkownika o uprawnieniach administratora:**

  - Jeśli włączono opcję Szybkie przełączanie (opcja domyślna w przypadku systemów operacyjnych Windows XP Home Edition i Professional na komputerach wyposażonych w ponad 64 MB pamięci RAM):

    1. Kliknij **Start**.
    2. Kliknij opcję **Wyloguj**.
    3. Kliknij opcję **Przełącz użytkownika**. Zostanie wyświetlony ekran logowania systemu operacyjnego Windows XP wraz z liczbą programów dla każdego użytkownika pod nazwą użytkownika.
    4. Klikając, wybierz użytkownika, na którego konto chcesz się przełączyć.
    5. Wpisz hasło, a następnie kliknij strzałkę, aby zalogować się na komputerze.

- Jeśli opcja Szybkie przełączanie jest wyłączona lub nie jest obsługiwana (w przypadku komputerów z systemem operacyjnym Windows XP Professional będących częścią domeny):

  1. Zrestartuj komputer
  2. Zaloguj się, korzystając z nazwy użytkownika i hasła użytkownika o uprawnieniach administratora.

Nie wiem, czy konto, którego używam, jest kontem administratora

Jeśli nie masz pewności, czy konto użytkownika jest kontem administratora, czy standardowym kontem użytkownika, możesz sprawdzić typ konta, przełączając się na nie, a następnie wykonując poniższe czynności.

Jeśli komputer należy do domeny:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj kontami użytkowników**.
6. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Nazwa użytkownika jest podświetlona, zaś typ konta jest wyświetlony w kolumnie Grupa.

Jeśli komputer należy do grupy roboczej:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników i bezpieczeństwo rodzinne**.
4. Kliknij opcję **Konta użytkowników**.

5. Kliknij opcję **Zarządzaj innym kontem**. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Typ konta jest wyświetlany pod nazwą użytkownika.

8. Dostosowywanie programu Rapport

Można zmienić język Konsoli Rapport oraz okien dialogowych oraz ukryć ikonę programu Rapport pojawiającą się obok paska adresu przeglądarki, a także ukryć ikonę programu Rapport wyświetlaną na pasku zadań.

Ukrywanie i przywracanie ikony programu Rapport na pasku adresu

Domyślnie ikona programu Rapport zawsze pojawia się na pasku adresu przeglądarki lub po jego prawej stronie. Ikona ma kolor zielony, jeśli serwis WWW w przeglądarce jest chroniony przez program Rapport, a kolor szary, jeśli serwis WWW w przeglądarce nie jest chroniony przez program Rapport.

Poza wskazaniem chronionych serwisów WWW można kliknąć ikonę programu Rapport i wybrać opcję **Chroń ten serwis WWW**, aby włączyć ochronę niechronionego serwisu.

Ikonę tę można ukryć, jeśli jest to preferowane. Gdy ikona programu Rapport jest ukryta, program Rapport kontynuuje udostępnianie tego samego zabezpieczenia dla chronionych serwisów WWW, lecz nie jest widoczne, które serwisy WWW są chronione, i nie można zdecydować o włączeniu ochrony dla niechronionego serwisu WWW.

Wyświetlaniem lub ukrywaniem ikony można sterować z poziomu Konsoli Rapport. Jeśli ikona jest ukryta, dostęp do Konsoli Rapport można uzyskać wyłącznie z menu Start systemu Windows.

Aby ukryć ikonę programu Rapport:

1. Otwórz Konsolę Rapport.
2. W obszarze Ustawienia produktu panelu kontrolnego, obok statusu **Ikona na pasku adresu** kliknij opcję **ukryj**. Zostanie wyświetlone okno komunikatu następującej treści:

   Aby zmiany odniosły skutek, może być konieczne zamknięcie i ponowne otwarcie przeglądarki.

3. Kliknij przycisk **OK**. Status **Ikona na pasku adresu** zmieni się na ukryty i zostanie wyświetlony odsyłacz **pokaż**.

   Ikona jest teraz ukryta lub zostanie ukryta po zrestartowaniu przeglądarki.

Aby przywrócić ikonę:

- Kliknij przycisk **pokaż**.

Ukrywanie i przywracanie ikony na pasku zadań

Domyślnie ikona programu Rapport ( ) pojawia się na pasku zadań zawsze, gdy program Rapport jest uruchomiony.

Ikona informuje, że aktywne są zabezpieczenia programu Rapport niezależne od przeglądarki. Ochrona ta obejmuje ochronę przed szkodliwym oprogramowaniem, skanowanie i usuwanie go. Aby otworzyć Konsolę Rapport, należy kliknąć ikonę Rapport.

Ikonę tę można ukryć, jeśli jest to preferowane. Mimo że ikona programu Rapport jest ukryta, program Rapport zapewnia ten sam poziom ochrony.

Wyświetlaniem lub ukrywaniem ikony można sterować z poziomu Konsoli Rapport. Jeśli ikona jest ukryta, dostęp do Konsoli Rapport można uzyskać wyłącznie z menu Start systemu Windows.

Aby ukryć ikonę programu Rapport wyświetlaną na pasku zadań:

1. Otwórz Konsolę Rapport.
2. W obszarze Ustawienia produktu panelu kontrolnego obok statusu **Ikona na pasku zadań** kliknij opcję **ukryj**. Status **Ikona na pasku zadań** zmieni się na ukryty i zostanie wyświetlony odsyłacz **pokaż**.

   Ikona jest teraz ukryta na pasku zadań.

Aby przywrócić ikonę:

- Kliknij przycisk **pokaż**.

Zmiana języka interfejsu

Domyślnie Konsola Rapport i wszystkie pozostałe okna dialogowe są wyświetlane w języku angielskim. Język interfejsu Konsoli Rapport i okien dialogowych można również zmienić na jeden z kilku innych języków.

Aby zmienić język Konsoli Rapport:

1. Otwórz Konsolę Rapport.
2. W obszarze Ustawienia produktu panelu kontrolnego kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.
3. Z listy **Język** wybierz język. Zostanie wyświetlony następujący komunikat.

   Zmiany odniosą skutek w pełni po zamknięciu wszystkich okien przeglądarki.
   Przełączyć język i ponownie uruchomić konsolę Trusteer Endpoint Protection?

4. Kliknij przycisk **OK**. Konsola Rapport zostanie ponownie załadowana w wybranym języku.

9. Wyświetlanie informacji o aktywności programu Rapport

Mechanizmy ochrony programu Rapport są aktywowane przez kilka typów zdarzeń. Niektóre z tych zdarzeń to zdarzenia uprawnione, przypominające zdarzenia powodowane przez szkodliwe oprogramowanie. Inne zdarzenia mogą być inicjowane przez szkodliwe oprogramowanie znajdujące się na komputerze. Każde zdarzenie jest zliczane i rejestrowane w raporcie aktywności wyświetlanym w dowolnej chwili. Raport przedstawia aktywność z ostatnich siedmiu dni. Licznik zdarzeń można zresetować lub zatrzymać, albo włączyć lub wyłączyć okno dialogowe z propozycją przedstawienia tygodniowego raportu aktywności, pojawiające się na ekranie na początku każdego tygodnia.

Wyświetlanie raportu o aktywności

Tygodniowy raport o aktywności przedstawia liczbę zdarzeń wyzwolonych przez każdy z mechanizmów ochrony programu Rapport w ciągu ostatnich siedmiu dni. Raport ten służy wyłącznie do celów informacyjnych. Nie jest niezbędne wykonywanie żadnych czynności, ponieważ program Rapport blokuje wszystkie zdarzenia mogące doprowadzić do ujawnienia danych. Raport o aktywności jest wyświetlany automatycznie w ciągu 12 godzin po zainstalowaniu programu Rapport.

Fakt, że raport o aktywności zawiera zdarzenia, nie oznacza jeszcze obecności na komputerze szkodliwego oprogramowania ani faktu odwiedzin oszukańczego serwisu. Oznacza tylko, że oprogramowanie lub odwiedzone serwisy naruszają strategię bezpieczeństwa ustanowioną przez właścicieli chronionych serwisów WWW lub przez IBM. Na przykład możliwe, że używane oprogramowanie próbowało wykonać zrzut ekranu wyciągu bankowego lub odczytać informacje wprowadzone w serwisie WWW bankowości elektronicznej. To naruszenie strategii spowodowało zablokowanie przez program Rapport możliwości dostępu tego oprogramowania do newralgicznych informacji.

Aby w dowolnej chwili wyświetlić tygodniowy raport o aktywności:

1. Otwórz Konsolę Rapport.
2. W obszarze **Tygodniowy raport o aktywności** panelu kontrolnego kliknij opcję **Pełny raport**. Zostanie wyświetlony Tygodniowy raport o aktywności.

   Raport zawiera dziewięć liczników dla dziewięciu kategorii zdarzeń. Kategorie raportu o aktywności zawierają listę różnych typów zdarzeń napotkanych przez program Rapport i zażegnanych podczas przeglądania Internetu.
3. Klikając nazwę każdego licznika, można wyświetlić opis zdarzenia bezpieczeństwa, za którego zliczanie on odpowiada, oraz listę zliczonych zdarzeń danej kategorii.

Uwaga:	Nie należy się martwić, jeśli nie wszystkie informacje przedstawione w niniejszym raporcie są jasne, ponieważ ma on charakter nieco specjalistyczny. Przedstawione w nim informacje nie wymagają podjęcia jakichkolwiek czynności przez użytkownika. Raport można bezpiecznie zamknąć i nie trzeba do niego wracać. Jest on zachowywany wyłącznie do wglądu w przyszłości, na potrzeby użytkowników analizujących działanie programu Rapport w dłuższym okresie czasu.

Konfigurowanie raportu o aktywności

Dostępna jest opcja umożliwiająca automatyczne wyświetlanie raportu o aktywności co siedem dni. Raport jest wyświetlany po raz pierwszy automatycznie po upływie 12 godzin od instalacji programu Rapport. Domyślnie raport nie pojawia się co tydzień, lecz można go w dowolnej chwili wyświetlić w Konsoli Rapport.

Wyczyszczenie danych zawartych w tygodniowym raporcie o aktywności powoduje wyzerowanie wszystkich liczników zdarzeń. Wyłączenie tygodniowego raportu o aktywności powoduje zatrzymanie wszystkich liczników zdarzeń.

Aby skonfigurować raport o aktywności:

1. Otwórz Konsolę Rapport.
2. W obszarze **Tygodniowy raport o aktywności** panelu kontrolnego kliknij opcję **Pełny raport**. Zostanie wyświetlony Tygodniowy raport o aktywności.

Można teraz:

- Włączyć tygodniowy raport o aktywności, zaznaczając pole wyboru **Automatycznie prezentuj ten raport na początku każdego tygodnia**. Co siedem dni będzie wyświetlane okno dialogowe z propozycją wyświetlenia tego raportu.
- Czyszczenie raportu o aktywności.
- Wyłączanie raportu o aktywności.

Czyszczenie raportu o aktywności

Aby wyczyścić raport o aktywności:

1. Kliknij opcję **Wyczyść raport**. Zostanie wyświetlony ekran z potwierdzeniem.
2. Kliknij przycisk **OK**. Wszystkie liczniki zostaną zresetowane.

Wyłączanie raportu o aktywności

Aby wyłączyć tygodniowy raport o aktywności:

1. Kliknij opcję **Wyłącz raport**. Zostanie wyświetlony ekran z potwierdzeniem.
2. Kliknij przycisk **OK**. Liczniki zdarzeń są czyszczone, zaś tygodniowy raport o aktywności jest wyłączany. W obszarze Tygodniowy raport o aktywności panelu kontrolnego jest teraz wyświetlany komunikat „Raport o aktywności jest wyłączony". Raport można włączyć ponownie, klikając opcję **Włącz raport o aktywności**.

10. Skanowanie komputera w poszukiwaniu udoskonaleń zabezpieczeń

Aktualizacja oprogramowania na komputerze ma kluczowe znaczenie dla bezpieczeństwa. Nowe zagrożenia pojawiają się stale i przedsiębiorstwa zajmujące się oprogramowaniem regularnie aktualizują swoje programy tak, aby uwzględniały one poprawki związane ze słabymi punktami zabezpieczeń i innymi defektami. Niektóre programy są szczególnie wrażliwe na ataki, gdy nie są regularnie aktualizowane.

Program Rapport skanuje zawartość komputera co trzy dni w celu upewnienia się, że zainstalowano na nim program antywirusowy. Ponadto sprawdza on także, czy na komputerze dostępne są aktualne wersje programu antywirusowego i pozostałych programów, takich jak Adobe Flash, Adobe Reader, Java czy Skype. Raport Sprawdzone procedury dotyczące zabezpieczeń zawiera listę programów, które program Rapport uznał za nieaktualne, oraz sposób ich aktualizacji. Istnieje możliwość uzyskania dostępu do raportu Sprawdzone procedury dotyczące zabezpieczeń za pośrednictwem Konsoli Rapport.

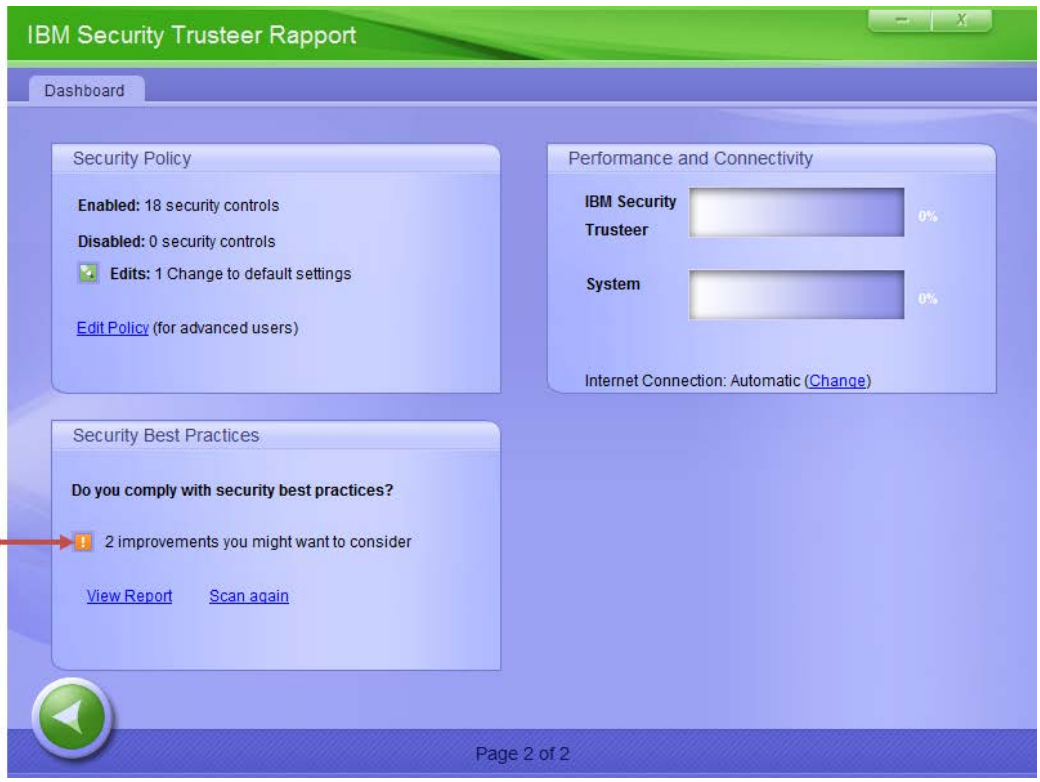
Uruchamianie operacji ręcznego skanowania

Mimo, że program Rapport zapewnia regularne skanowanie komputera, możliwe jest uruchomienie ponownego skanowania, gdy tylko jest to potrzebne.

- **Aby przeskanować zawartość komputera pod kątem udoskonaleń zabezpieczeń:**

1. Otwórz Konsolę Rapport.

2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony drugi ekran panelu kontrolnego, zawierający w dolnej części po lewej stronie podsumowanie Sprawdzone procedury dotyczące zabezpieczeń.



Podsumowanie wyników ostatniego skanowania

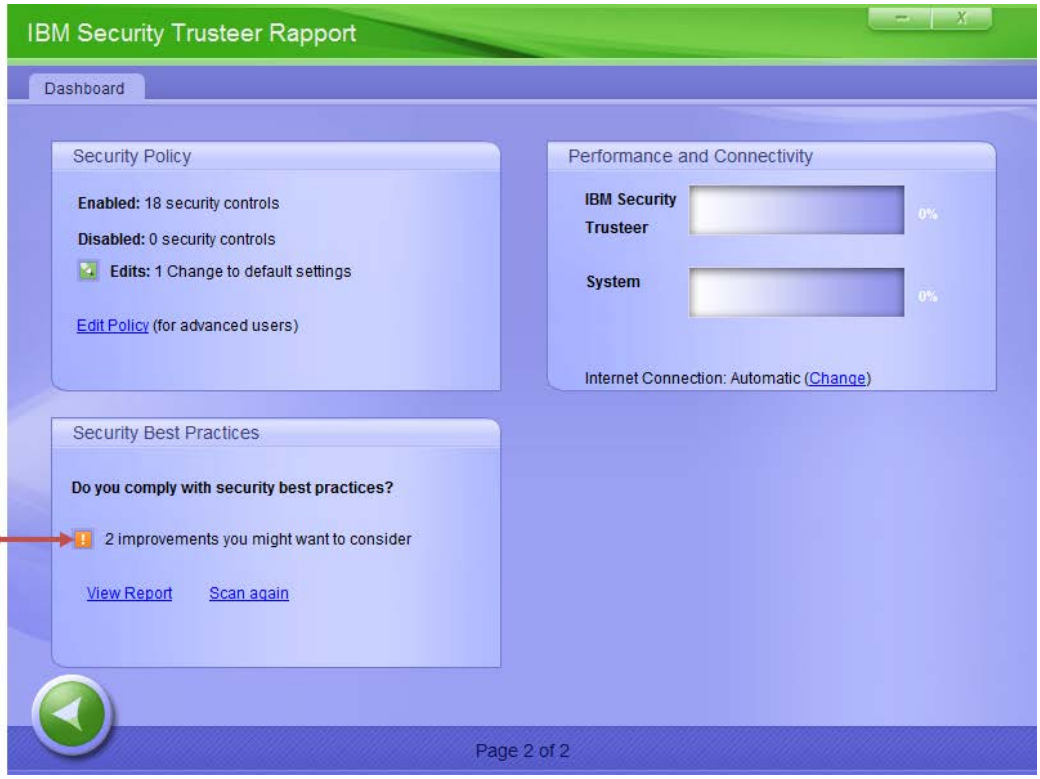
3. W obszarze Sprawdzone procedury dotyczące zabezpieczeń panelu kontrolnego kliknij opcję **Skanuj ponownie**. Gdy trwa skanowanie, odsyłacz **Skanuj ponownie** znika, a zamiast niego pojawiają się słowa „Trwa skanowanie... ”. Po zakończeniu skanowania ponownie pojawia się odsyłacz **Skanuj ponownie**, a wyniki skanowania są aktualizowane.

Wyświetlanie raportu Sprawdzone procedury dotyczące zabezpieczeń

Raport Sprawdzone procedury dotyczące zabezpieczeń zawiera listę programów, które program Rapport uznał za nieaktualne, oraz sposób ich aktualizacji.

➔ **Aby wyświetlić raport Sprawdzone procedury dotyczące zabezpieczeń:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony drugi ekran panelu kontrolnego, zawierający w dolnej części po lewej stronie podsumowanie Sprawdzone procedury dotyczące zabezpieczeń.



Podsumowanie wyników ostatniego skanowania

3. Kliknij opcję **Wyświetl raport**. Zostanie wyświetlona karta Sprawdzone procedury dotyczące zabezpieczeń, zawierająca raport z wszystkimi problemami dotyczącymi zabezpieczeń, wykrytymi podczas skanowania.

4. Kliknij każdy z problemów dotyczących zabezpieczeń. Wyświetlony zostanie pełny opis ryzyka, jakie stwarza ten problem, oraz zalecenie dotyczące czynności, jakie należy podjąć w celu jego zażegnania.

11. Zarządzanie chronionymi serwisami i hasłami

Program Rapport udostępnia informacje dotyczące serwisów WWW i haseł chronionych w Konsoli Rapport. Konsoli Rapport można użyć w celu usunięcia serwisów WWW i haseł.

Istnieją dwie kategorie chronionych serwisów WWW:

- **Zaufane serwisy WWW partnerów**. Są to serwisy WWW należące do partnerów IBM. Zaufani partnerzy współpracują bezpośrednio z IBM w celu zapewnienia optymalnej strategii zabezpieczeń do swoich zastosowań. Uzyskując dostęp do serwisu WWW partnera, użytkownik zyskuje automatyczną ochronę. Nie jest możliwe usunięcie ochrony programem Rapport dla tych serwisów WWW. Liczba chronionych serwisów partnerskich nie powoduje żadnego obciążenia dla systemu.

  Zaufane serwisy WWW partnerów oferują również dodatkowe mechanizmy wsparcia:

  - Partnerzy IBM mają dostęp do programu Trusteer Management Application, który umożliwia im definiowanie konfiguracji strategii zabezpieczeń oraz opracowywanie szczegółowych raportów dotyczących zainfekowanych urządzeń.
  - Partnerzy IBM otrzymują szczegółowe powiadomienia o zdarzeniach występujących na urządzeniach użytkowników końcowych. Partnerzy mogą subskrybować te raporty o zdarzeniach (źródła) oraz podejmować czynności w oparciu o te zdarzenia, a w razie potrzeby kontaktować się z użytkownikami końcowymi.
  - Partnerzy IBM mają dostęp do zespołu ds. analiz zabezpieczeń IBM i mogą w ścisłej współpracy z zespołem uzyskiwać wskazówki krok po kroku ułatwiające użytkownikom końcowym usuwanie infekcji.
  - Partnerzy IBM mają dostęp do usług wsparcia dotyczącego oprogramowania IBM Trusteer, gdy tylko zaistnieje potrzeba rozwiązania problemu, wystosowania zapytania, rozwiązania kwestii dotyczącej

kompatybilności, skonfigurowania klienta programu Rapport oraz w ramach bieżącej edukacji klienta.

- **Serwisy WWW dodane ręcznie**. Są to serwisy WWW dodane przez użytkownika ze względu na korzyści płynące z ochrony zapewnianej przez program Rapport podczas nawiązywania z nimi połączenia. Nie obowiązuje żadne ograniczenie co do liczby serwisów, jaką można objąć ochroną. IBM zaleca aktywację ochrony dla programu Rapport we wszystkich dodatkowych serwisach WWW, za pośrednictwem których użytkownik przesyła dane prywatne i osobowe lub wszelkie inne newralgiczne informacje. Przykłady serwisów WWW, których ochrona może być wskazana, to:
  - Rachunki bankowe online
  - Rachunki funduszy inwestycyjnych
  - Rachunki brokerskie online
  - Sklepy internetowe
  - Serwisy e-mail z interfejsem WWW (takie jak Outlook, Yahoo! Mail i Gmail)
  - Serwisy sieci społecznościowych (takie jak Facebook, Orkut czy Linkedin)
  - Aplikacje ubezpieczeniowe
  - Serwisy osobistych informacji medycznych
  - Serwisy zakupowe online (takie jak eBay, Amazon, Walmart.com czy Target.com)

  Istnieje możliwość usunięcia ochrony przez program Rapport z tych serwisów WWW przez usunięcie ich z listy.

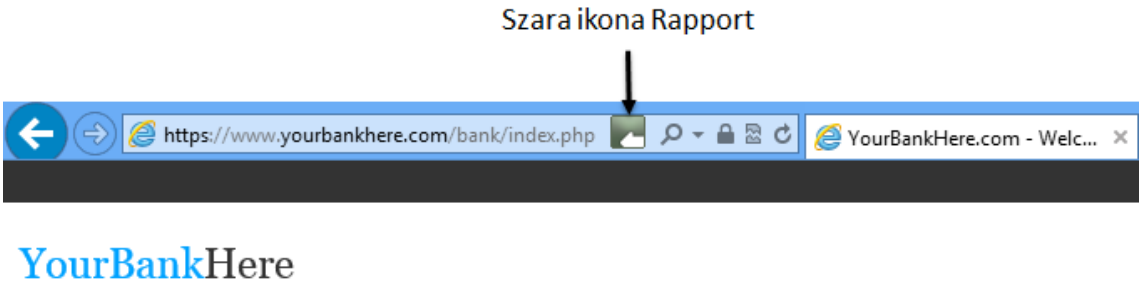
Uwaga:	W przypadku niektórych instalacji programu Rapport opcja ręcznego ustawienia ochrony serwisów WWW jest wyłączona.

W obszarze Zaufane serwisy Konsoli Rapport wyświetlana jest liczba serwisów WWW należących do każdej z obecnie chronionych kategorii. Istnieje możliwość wyświetlenia listy i opisu chronionych serwisów WWW naszych partnerów. W tym celu należy kliknąć opcję **Zaufane serwisy WWW partnerów**. Można także wyświetlić listę serwisów WWW dodanych ręcznie przez kliknięcie opcji **Ręcznie dodane serwisy WWW**.

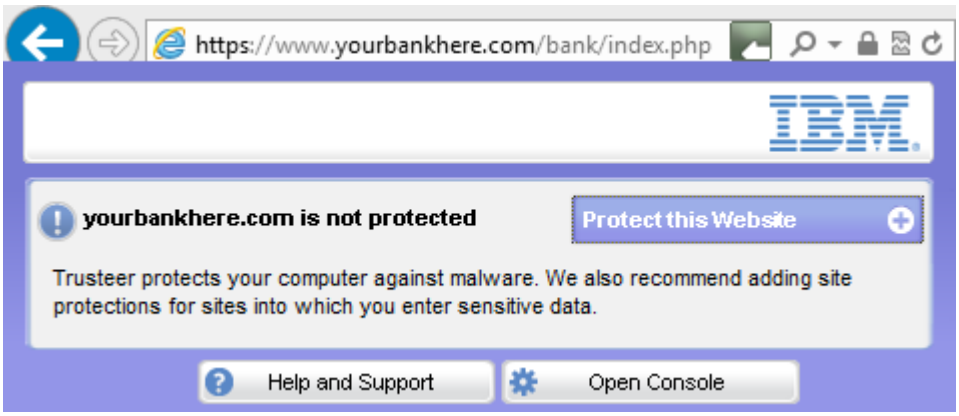
Ochrona dodatkowych serwisów WWW

- **Aby chronić dodatkowy serwis WWW:**

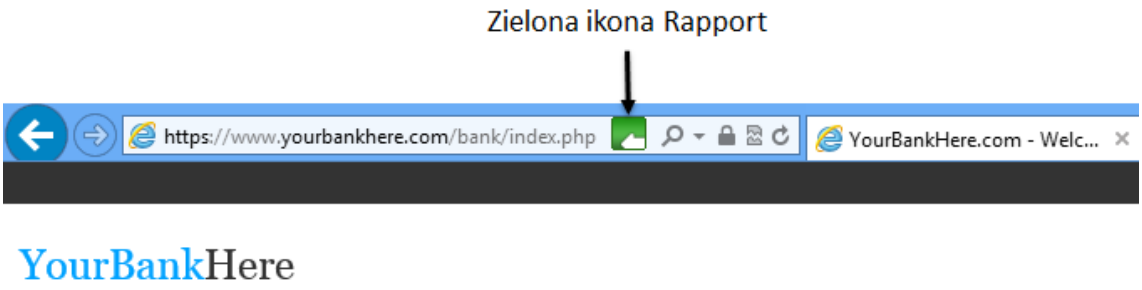
1. Przejdź do serwisu WWW, który chcesz chronić. Jeśli nie włączono jeszcze programu Rapport w celu ochrony tego serwisu WWW, ikona programu Rapport na pasku adresu jest wyszarzona.



2. Kliknij szarą ikonę programu Rapport na pasku adresu. Zostanie wyświetlone okno dialogowe.



3. W oknie dialogowym kliknij opcję **Chroń ten serwis WWW**. Ikona programu Rapport na pasku adresu przyjmuje kolor zielony, co oznacza, że ten serwis WWW jest teraz chroniony przez program Rapport.



Ikona jest wyświetlana domyślnie. Można również ukryć ikonę programu Rapport.

Dlaczego ikona programu Rapport nie pojawia się w mojej przeglądarce?

Jeśli ikona programu Rapport nie pojawia się w przeglądarce użytkownika, są trzy możliwe przyczyny:

- Wybrano ukrycie ikony na pasku adresu. Program Rapport nadal zapewnia ochronę, lecz ikona nie jest widoczna. Można przywrócić wyświetlanie ikony. Więcej informacji na temat ukrywania i przywracania ikony programu Rapport można znaleźć w sekcji Ukrywanie i przywracanie ikony programu Rapport na pasku adresu.
- Program Rapport nie obsługuje przeglądarki użytkownika. Listę obecnie obsługiwanych przeglądarek można znaleźć pod adresem: http://www.trusteer.com/support/supported-platforms.
- Program Rapport został zatrzymany i nie działa. Można uruchomić program Rapport ponownie. Więcej informacji można znaleźć w sekcji Uruchamianie programu Rapport.

Usuwanie chronionych serwisów WWW

➔ **Aby usunąć ręcznie dodane serwisy WWW:**

1. Otwórz Konsolę Rapport.
2. W obszarze Zaufane serwisy WWW kliknij opcję **Przeglądaj zaufane serwisy WWW**. Zostanie wyświetlona karta Zaufane serwisy WWW.
3. Kliknij opcję **Serwisy WWW dodane ręcznie**. Zostanie wyświetlona lista wszystkich ręcznie dodanych serwisów WWW.
4. Kliknij odsyłacz **usuń** obok serwisu WWW na tej liście. Zostanie wyświetlony ekran z potwierdzeniem.
5. Kliknij przycisk **OK**. Serwis WWW zostanie usunięty z listy. Ikona programu Rapport będzie teraz wyszarzona po przejściu do usuniętego serwisu WWW, co będzie oznaczać, że nie jest on już chroniony.

Zarządzanie chronionymi nazwami użytkowników i hasłami

Po zaakceptowaniu propozycji programu Rapport ochrony hasła w chronionym serwisie nie tylko zapewnia on ochronę hasła, lecz także chroni wszelkie przyszłe hasła wprowadzane w tej witrynie. Program Rapport zapamiętuje wybór użytkownika o ochronie hasła lub jej braku dla każdego serwisu. Nie oferuje on ponownej ochrony hasła po przejściu do tego serwisu, o ile użytkownik nie wyczyści pamięci podręcznej ochrony haseł. Konsola Rapport wskazuje, dla których serwisów WWW jest obecnie włączona ochrona haseł programu Rapport. W razie potrzeby możliwe jest wyłączenie ochrony hasła dla dowolnego chronionego serwisu WWW. Można także wyczyścić pamięć podręczną ochrony hasła, powodującą skasowanie wszystkich mechanizmów ochrony haseł i decyzji o ochronie haseł.

Uwaga: W przypadku niektórych serwisów WWW partnerów IBM program Rapport chroni nie tylko hasła, ale i nazwy użytkowników. Konsola Rapport wskazuje także strategię ochrony nazwy użytkownika dla serwisu WWW.

Aby wyłączyć ochronę hasła dla chronionego serwisu WWW:

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Przewiń w dół listy mechanizmów zabezpieczeń, aż do odszukania opcji **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**.

6. Kliknij opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Wyświetlona zostanie strategia zabezpieczeń nazw użytkowników i haseł dla każdego serwisu WWW.

7. Usuń zaznaczenie pola wyboru **Ostrzegaj w przypadku użycia hasła w innym miejscu** dla serwisu WWW, dla którego ma zostać wyłączona ochrona hasła. Program Rapport nie będzie zapewniał ochrony hasła tego serwisu WWW.

Uwaga:	Klikniecie opcji **Wyczyść pamięć podręczną** powoduje wyczyszczenie wszystkich ustawień ochrony hasła i zresetowanie wszystkich strategii ochrony hasła, co spowoduje ponowne wyświetlenie w programie Rapport oferty ochrony hasła przy kolejnej wizycie w każdym z serwisów WWW.

8. Kliknij przycisk **Zapisz**. Zmiany zostaną zapisane.

12. Modyfikowanie strategii bezpieczeństwa programu Rapport

Uwaga: Modyfikowanie strategii bezpieczeństwa programu Rapport to czynność przeznaczona dla zaawansowanych użytkowników.

Funkcje zabezpieczeń programu Rapport nie wymagają żadnych czynności konfiguracyjnych, można jednak dokonać zmian w pewnej liczbie funkcji w celu dostosowania ich do swoich potrzeb.

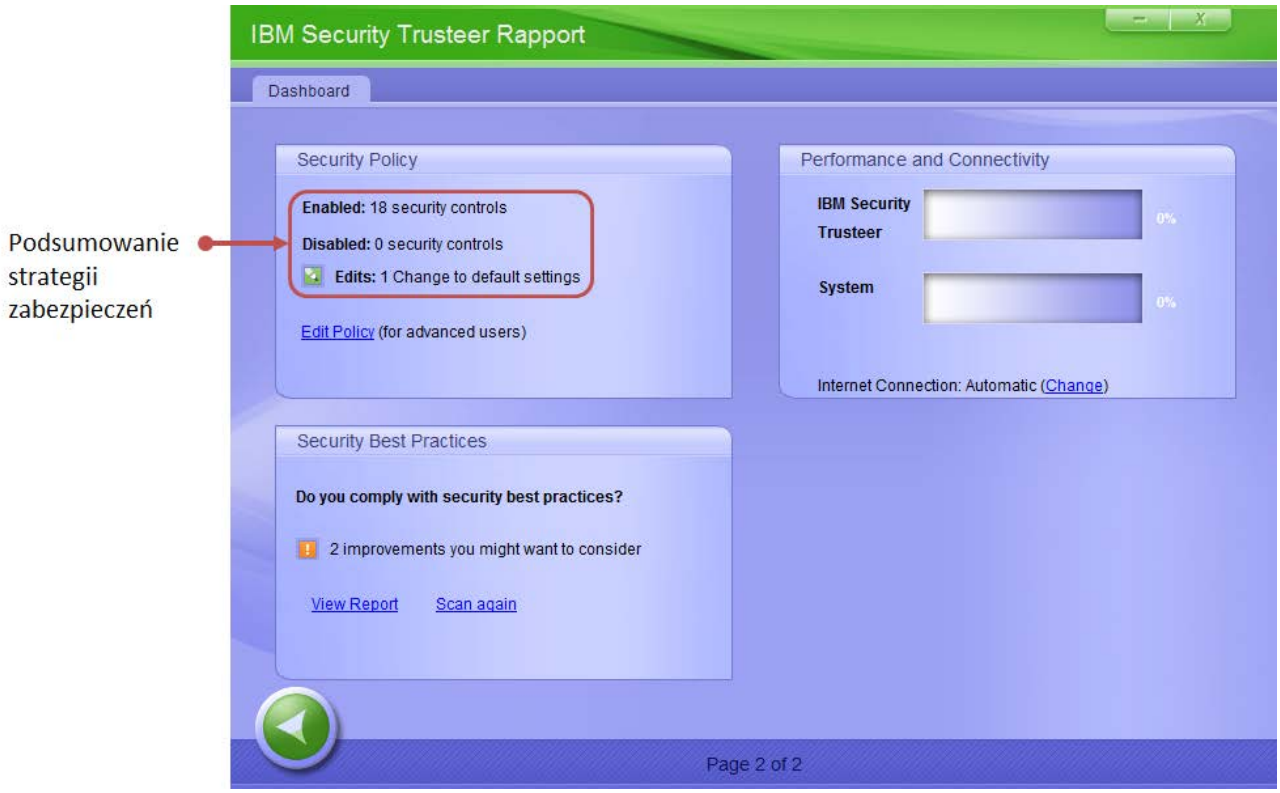
Wyświetlanie podsumowania dotyczącego strategii bezpieczeństwa

W Konsoli Rapport wyświetlane jest podsumowanie strategii bezpieczeństwa. Podsumowanie zawiera liczbę aktywnych oraz liczbę nieaktywnych mechanizmów zabezpieczeń.

Aby wyświetlić podsumowanie strategii bezpieczeństwa:

1. Otwórz Konsolę Rapport.

2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony drugi ekran panelu kontrolnego, zawierający podsumowanie strategii zabezpieczeń w obszarze Strategia zabezpieczeń.



Podsumowanie strategii zabezpieczeń obejmuje następujące informacje:

Pole na ekranie	Opis
Włączone	Liczba obecnie włączonych mechanizmów zabezpieczeń.
Wyłączone	Liczba obecnie wyłączonych mechanizmów zabezpieczeń.
Zmiany	Liczba zmian dokonanych w strategii domyślnej.

Modyfikowanie mechanizmów zabezpieczeń

Strategia zabezpieczeń programu Rapport oferuje najwyższy poziom zabezpieczeń przy jednoczesnej minimalizacji możliwych konfliktów z programami uprawnionymi. Na przykład blokowanie zrzutów ekranu jest ustawiane domyślnie w celu ochrony wyłącznie serwisów WWW partnerów. Wynika to z faktu, że zrzuty ekranów są wykonywane przez wiele produktów uprawnionych, zaś IBM preferuje interferencje z oprogramowaniem wykonującym zrzuty ekranu wyłącznie tam, gdzie ma to newralgiczne znaczenie dla systemu bankowości elektronicznej lub zabezpieczeń korporacyjnych.

Strategię bezpieczeństwa programu Rapport można zmieniać, modyfikując poszczególne mechanizmy zabezpieczeń. Modyfikacja strategii zabezpieczeń może pomóc we włączeniu uprawnionego zadania zablokowanego przez domyślną strategię zabezpieczeń lub rozwiązać problem z kompatybilnością z inną aplikacją dotyczącą zabezpieczeń. Wszelkie modyfikacje wprowadzone w domyślnej strategii mają na celu redukcję poziomu ochrony zapewnianej przez program Rapport. Przystąpienie do zmiany strategii zabezpieczeń wymaga świadomości związanego z tym ryzyka.

Uwaga: Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany w tym ustawieniu można wprowadzić wyłącznie po zalogowaniu się z konta administratora.

➔ **Aby zmienić mechanizmy zabezpieczeń:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.

4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Wybierz żądane ustawienie z menu po prawej stronie mechanizmu, który chcesz zmienić. Przed zmianą dowolnego z ustawień upewnij się, że masz świadomość istotności wprowadzanej zmiany w poziomie ochrony zapewnianej przez program Rapport. Więcej informacji na temat mechanizmów strategii zabezpieczeń, dostępnych opcji i wszelkich informacji dodatkowych można znaleźć w punkcie Informacje na temat mechanizmów strategii zabezpieczeń. Możliwe ustawienia to:

   - **Zawsze**: mechanizm jest stale włączony i nie jest zależny od zawartości serwisu WWW.
   - **Nigdy**: mechanizm jest stale wyłączony.
   - W serwisach WWW partnerów: mechanizm jest dostępny dla serwisów WWW partnerów i bazuje na strategii ustalonej przez właściciela serwisu WWW. Serwisy WWW partnerów współpracują bezpośrednio z IBM w celu zapewnienia optymalnej strategii zabezpieczeń.
   - **W newralgicznych serwisach WWW partnerów i moich**: mechanizm jest dostępny dla serwisów WWW partnerów oraz chronionych serwisów WWW dodanych ręcznie.

   Klikanie poszczególnych nazw mechanizmów powoduje wyświetlenie ich opisów oraz wszelkich ich funkcji.

   Aby przywrócić wszystkim ustawieniom wartości domyślne, należy kliknąć opcję **Przywróć wartości domyślne**.

Uwaga:	Jeśli program Rapport zainstalowano w trybie dla użytkowników niedowidzących, wówczas domyślne wartości dla ustawień **Blokuj wykonywanie zrzutów ekranu** oraz **Blokuj dostęp do informacji w przeglądarce** to **Nigdy**.

6. Kliknij przycisk **Zapisz**. Zmiany w strategii zostaną zapisane. W przypadku niektórych zmian, aby odniosły one skutek, niezbędne jest ponowne uruchomienie przeglądarki lub komputera.

Uwaga: Jeśli program Rapport zainstalowano w trybie zgodności z lektorem ekranowym i aktywowano strategię **Blokuj wykonywanie zrzutów ekranu** lub **Blokuj dostęp do informacji w przeglądarce**, wówczas wyświetlany jest komunikat zawierający następujący tekst:

Program Trusteer Endpoint Protection jest obecnie zainstalowany w trybie zgodności lektora ekranowego. Aktywowanie tej strategii może spowodować wyłączenie niektórych lektorów ekranowych. Czy na pewno chcesz aktywować tę strategię?

Uwaga: Aby aktywować strategię, kliknij opcję **Aktywuj strategię**. Aby zrezygnować z aktywacji strategii z uwagi na potencjalne ryzyko dezaktywacji lektorów ekranowych, kliknij opcję **Anuluj**.

Informacje na temat mechanizmów strategii zabezpieczeń

Przystępując do modyfikowania strategii zabezpieczeń programu Rapport, należy mieć świadomość istotności wprowadzanych zmian w poziomie ochrony zapewnianej przez program Rapport.

Blokuj wykonywanie zrzutów ekranu

Opis

Powoduje dezaktywację wszelkich prób wykonania zrzutu ekranu podczas wyświetlania chronionego serwisu WWW. Programy na komputerze użytkownika próbujące wygenerować zrzut ekranu, generują czarny obraz.

Celem jest zapobieżenie przechwyceniu ekranu zawierającego newralgiczne informacje przez szkodliwe oprogramowanie.

Opcje

- **Nigdy**. Umożliwia wykonywanie zrzutów ekranu przez cały czas. (Niektóre operacje, takie jak zatrzymanie programu Rapport, skutkują wyświetleniem komunikatu o potwierdzeniu działania zabezpieczeń, którego nie można przechwycić nawet, jeśli dla tego mechanizmu zabezpieczeń wybrano opcję „Nigdy".)
- **W serwisach WWW partnerów** (domyślnie). Blokuje wszystkie operacje wykonywania zrzutów ekranu na komputerze tylko w przypadku otwarcia w przeglądarce dowolnego serwisu WWW partnera.
- **W newralgicznych serwisach WWW partnerów i moich**. Blokuje wszystkie operacje wykonywania zrzutów ekranu na komputerze tylko w przypadku otwarcia w przeglądarce chronionego serwisu WWW (dodanego ręcznie lub partnera).

Dodatkowe informacje

Komenda Zrzut ekranu jest obsługiwana w sposób odmienny od pozostałych mechanizmów wykonywania zrzutów ekranu. Naciśnięcie klawisza PrtScn powoduje wyświetlenie przez program Rapport komunikatu Alert o wykryciu próby wykonania zrzutu ekranu z prośbą do użytkownika o zablokowanie lub zezwolenie na działanie mechanizmu wykonywania zrzutów ekranu.

Nawet, jeśli trzeba wykonać zrzuty ekranu na komputerze, wyłączenie tej funkcji nie jest konieczne. Funkcja blokowania zrzutów ekranu programu Rapport nie zabezpiecza mechanizmów wykonywania zrzutów ekranu przed wykonaniem zrzutów ekranu, gdy nie są wyświetlane chronione serwisy WWW. Domyślnie funkcja blokowania zrzutów ekranu ma zastosowanie wyłącznie do chronionych serwisów WWW partnerów. Nawet, gdy wykonywanie zrzutów ekranu jest zablokowane, istnieje możliwość wykonania zrzutu ekranu za pomocą klawisza PrtScn na klawiaturze. W przypadku użycia klawisza PrtScn zostanie wyświetlone okno dialogowe programu Rapport, w którym można zablokować wykonywanie zrzutów ekranów lub zezwolić na nie. Kliknięcie przycisku **Zezwól** powoduje wykonanie zrzutu ekranu.

Stąd blokadę wykonywania zrzutów ekranu należy wyłączyć wyłącznie w razie potrzeby wykonania zrzutów ekranów wyświetlanych w serwisach WWW partnerów, za pomocą mechanizmu wykonywania zrzutów ekranów innego niż klawisz PrtScn na klawiaturze. Po zakończeniu wykonywania zrzutów ekranu można ponownie włączyć funkcję blokowania wykonywania zrzutów ekranu w celu przywrócenia zapewnianej przez nią ochrony.

W przypadku zablokowania użytkownika przez program Rapport podczas próby wykonania zrzutu fragmentu ekranu niebędącego chronionym serwisem WWW należy zminimalizować wszystkie otwarte przeglądarki lub zamknąć wszystkie okna i karty zawierające chronione strony WWW. Następnie można już bez problemów wykonać zrzut ekranu.

Sprawdzaj poprawność certyfikatów SSL serwisu WWW

Opis

Po przejściu do chronionego serwisu WWW program Rapport sprawdza certyfikat SSS serwisu. Jeśli certyfikat utracił ważność, jest nieprawidłowy lub został podpisany przez nieznanego wystawcę, program Rapport uaktywnia Ostrzeżenie o nieważności certyfikatu wymagające działania ze strony użytkownika. Sprawdzanie poprawności certyfikatów SSL przez program Rapport jest silniejsze, niż mechanizm sprawdzania poprawności przeglądarki, i powinno być stosowane w przypadku serwisów WWW partnerów, nawet jeśli przeglądarka generuje ostrzeżenia o nieważności certyfikatów.

Celem jest zabezpieczenie użytkownika przed przechodzeniem do fałszywych serwisów WWW.

Opcje

- **Nigdy**. Nie sprawdza certyfikatów SSL serwisów WWW.
- **W serwisach WWW partnerów** (domyślnie). Sprawdza certyfikaty SSL używane w serwisach WWW partnerów po ich odwiedzeniu.

- **W newralgicznych serwisach WWW partnerów i moich**. Sprawdza certyfikaty SSL używane w serwisach WWW partnerów i dodanych ręcznie po ich odwiedzeniu.

Opis

Informacje o tym, jak reagować na ostrzeżenie o nieważnym certyfikacie, można znaleźć w punkcie Reagowanie na ostrzeżenie o nieważnym certyfikacie.

Istnieje możliwość wyczyszczenia pamięci podręcznej programu Rapport z niepoprawnych certyfikatów, dla których wcześniej udzielono autoryzacji. Po wyczyszczeniu pamięci podręcznej certyfikaty, które usunięto z pamięci podręcznej, generują ostrzeżenie w przypadku przejścia do serwisu WWW, który z nich korzysta.

W celu wyczyszczenia pamięci podręcznej z nieważnych certyfikatów należy kliknąć opcję **Wyczyść pamięć podręczną** poniżej listy rozwijanej Sprawdzaj poprawność certyfikatów SSL serwisu WWW.

Blokuj nieznane programy dodatkowe przeglądarki

Opis

Blokuje nierozpoznane programy dodatkowe przeglądarki. Programy dodatkowe przeglądarki (znane również jako paski narzędzi lub BHO) to niewielkie (zwykle należące do firm trzecich) fragmenty oprogramowania znajdujące się w przeglądarce i umożliwiające sterowanie komunikacją. Większość programów dodatkowych przeglądarki (takich jak pasek narzędzi Google) to programy uprawnione. Istnieją jednak także szkodliwe programy dodatkowe.

Celem jest ochrona użytkownika przed szkodliwymi programami dodatkowymi, które mogą wykradać dane logowania lub modyfikować przesyłane przez użytkownika informacje.

Opcje

- **Nigdy**. Zezwala na wszystkie programy dodatkowe przeglądarki we wszystkich serwisach.

- **W serwisach WWW partnerów**. Blokuje nierozpoznane programy dodatkowe przeglądarki, gdy użytkownik jest połączony z serwisem WWW partnera.
- **W newralgicznych serwisach WWW partnerów i moich** (domyślnie). Blokuje nierozpoznane programy dodatkowe przeglądarki, gdy użytkownik jest połączony z serwisem WWW partnera lub chronionym serwisem WWW dodanym ręcznie.

Dodatkowe informacje

W konsoli wyświetlana jest lista nieznanych programów dodatkowych wykrytych przez program Rapport i zablokowanych podczas połączenia z chronionym serwisem WWW. Istnieje możliwość ręcznego odblokowania konkretnych programów dodatkowych, o których wiadomo, że są bezpieczne, po zaznaczeniu pola wyboru **Zezwól** dla każdego programu dodatkowego.

Blokuj dostęp do informacji w przeglądarce

Opis

Blokuje procesy na komputerze umożliwiające dostęp do serwisów WWW przez wykorzystanie interfejsu API programowania DOM. Procesy te mogą odczytywać newralgiczne informacje lub modyfikować realizowane przez użytkownika transakcje. Program Rapport blokuje te procesy niezależnie od tego, czy są one uprawnione, czy szkodliwe.

Celem takiego działania jest zapobieżenie nieuprawnionemu odczytowi newralgicznych informacji przez szkodliwe procesy lub modyfikacji transakcji użytkownika.

Opcje

- **Nigdy**. Nie blokuje dostępu procesów do serwisów WWW.
- **W serwisach WWW partnerów** (domyślnie). Blokuje procesy, gdy użytkownik jest połączony z serwisem WWW partnera.

- **W newralgicznych serwisach WWW partnerów i moich**. Blokuje procesy, gdy użytkownik jest połączony z serwisem WWW partnera lub chronionym serwisem WWW dodanym ręcznie.

Dodatkowe informacje

Typowy przykład to programy do zarządzania hasłami, które zapamiętują hasła użytkowników i wprowadzają je automatycznie na stronach logowania. Program Rapport blokuje dostęp takich programów do danych, ponieważ są to dane o newralgicznym znaczeniu i programy takie mogłyby paść ofiarą ataków szkodliwego oprogramowania wykradającego dane uwierzytelniające do serwisów finansowych użytkownika. Nie należy używać takich produktów w finansowych serwisach WWW. Niektóre uprawnione programy mogą uzyskiwać dostęp do tych informacji i są blokowane przez program Rapport w serwisach WWW partnerów.

Blokuj dostęp do newralgicznych plików cookie serwisu WWW

Opis

Blokuje dostęp aplikacji do plików cookie, takich jak pliki cookie sesji ustawione przez właściciela serwisu WWW partnera jako newralgiczne pliki cookie.

Celem jest zapobieżenie przejęciu przez pliki cookie sesji użytkownika w serwisie WWW.

Opcje

- **Nigdy**. Nie blokuj dostępu aplikacji do newralgicznych plików cookie.
- **W serwisach WWW partnerów** (domyślnie). Blokuje dostęp do newralgicznych plików cookie po nawiązaniu połączenia z serwisem WWW partnera.

Dodatkowe informacje

IBM musi zapoznać się z informacjami cookie serwisu WWW, zanim będzie możliwe skonfigurowanie programu Rapport w celu ich ochrony. W przeciwnym wypadku może wystąpić konflikt z serwisem WWW. Z tej przyczyny tego typu ochrona jest dostępna wyłącznie dla serwisów WWW partnera.

Sprawdzaj poprawność adresów IP serwisów WWW

Opis

Sprawdza poprawność adresów IP serwisów WWW względem tabel translacji zaufanych adresów IP. Po przejściu do chronionego serwisu WWW program Rapport sprawdza adres IP serwisu względem listy znanych dobrych adresów dla tego serwisu WWW. Jeśli adresu IP nie ma na liście, program Rapport zastępuje go znanym, poprawnym adresem IP serwisu WWW.

Celem jest ochrona użytkownika przed nawiązaniem połączenia z oszukańczym serwisem WWW wskutek ataku typu pharming[5].

Opcje

- **Nigdy**. Nie sprawdza poprawności adresów IP względem tabel zaufanych adresów IP.
- **W serwisach WWW partnerów**. Sprawdza adresy IP serwisów WWW względem tabel zaufanych adresów IP przy nawiązywaniu połączeń z serwisami WWW partnerów.
- **W newralgicznych serwisach WWW partnerów i moich** (domyślnie). Sprawdza adresy IP serwisów WWW względem tabel zaufanych adresów IP przy nawiązywaniu połączeń z serwisami WWW partnerów i chronionymi serwisami WWW dodanymi ręcznie.

[5] Ataki typu pharming to próby przekierowania ruchu z serwisu WWW do innych serwisów, które się pod niego podszywają.

Dodatkowe informacje

Funkcja czyszczenia pamięci podręcznej dla tego mechanizmu nie jest obecnie obsługiwana.

Aktywuj zastępowanie znaków

Opis

Szyfruje wszystkie naciśnięcia klawiszy przesyłane do przeglądarki, uniemożliwiając ich rozpoznanie przez oprogramowanie do rejestracji naciśnięć klawiszy.

Ma to na celu udaremnienie rejestracji odczytu naciśnięć klawiszy przez oprogramowanie i przechwycenia newralgicznych informacji, takich jak hasła.

Opcje

- **Nigdy**. Nie szyfruje naciśnięć klawiszy.
- **W serwisach WWW partnerów**. Szyfruje naciśnięcia klawiszy, gdy użytkownik jest połączony z serwisem WWW partnera.
- **W newralgicznych serwisach WWW partnerów i moich** (domyślnie). Szyfruje naciśnięcia klawiszy, gdy użytkownik jest połączony z serwisem WWW partnera lub chronionym serwisem WWW dodanym ręcznie.

Dodatkowe informacje

Ta funkcja może kolidować z innymi programami uniemożliwiającymi rejestrację naciśnięć klawiszy i powodować generowanie nieprawidłowych naciśnięć klawiszy. Stąd, jeśli na komputerze działa inny program blokujący rejestrację naciśnięć klawiszy (na przykład stanowiący składnik oprogramowania antywirusowego), może zaistnieć potrzeba wyłączenia tej funkcji. Alternatywnie można także wyłączyć aktywny program blokujący rejestrację naciśnięć klawiszy.

Jeśli ta strategia jest wyłączona, a nie została wyłączona przez użytkownika, oznacza to, że program Rapport wykrył konflikt między konfiguracją sprzętu lub oprogramowania a programem Rapport. Aby uniknąć konfliktu, program Rapport wyłączył ten mechanizm.

Aktywuj zastępowanie znaków na poziomie jądra

Opis

Szyfruje wszystkie naciśnięcia klawiszy przesyłane do przeglądarki i ukrywa jej przed szkodliwymi komponentami oprogramowania (znanymi jako programy rejestrujące naciśnięcia klawiszy jądra) w systemie operacyjnym.

Zamiana znaków na poziomie jądra to silniejsza wersja zamiany znaków. Po włączeniu zamiany znaków na poziomie jądra program Rapport szyfruje naciśnięcia klawiszy na poziomie jądra systemu, uniemożliwiając programom rejestrującym naciśnięcia klawiszy odczyt naciśnięć klawiszy na dowolnym etapie komunikacji między klawiaturą a przeglądarką WWW. Jeśli opcja *Aktywuj zastępowanie znaków* jest wyłączona, wyłączona jest także opcja *Aktywuj zastępowanie znaków na poziomie jądra*, nawet jeśli dla strategii ustawiono wartość **zawsze**. Opcja *Aktywuj zastępowanie znaków na poziomie jądra* stanowi uzupełnienie opcji *Aktywuj zastępowanie znaków*, czyniąc ją silniejszą, lecz nie może ona działać niezależnie.

Ma to na celu udaremnienie naciśnięć klawiszy przez szkodliwe oprogramowanie do ich rejestracji i przechwycenia w ten sposób newralgicznych informacji, takich jak numery kart płatniczych.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Blokuj nieuprawnione moduły w przeglądarce

Opis

Monitoruje pliki DLL wczytywane do przeglądarek i uniemożliwia ładowanie szkodliwych plików do przeglądarki.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Ponieważ to zabezpieczenie działa po uruchomieniu przeglądarki, chroni ono wszystkie serwisy WWW, nie rozróżniając między serwisami partnerów a serwisami dodanymi ręcznie.

Ostrzegaj przy przeglądaniu szkodliwych serwisów

Opis

Ostrzega użytkownika o próbie uzyskania dostępu do serwisu WWW, o którym wiadomo, że jest szkodliwy.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW

Opis

Hasła wprowadzone w newralgicznych serwisach WWW są klasyfikowane przez program Rapport jako informacje pozwalające na identyfikację osoby. W przypadku serwisów WWW partnerów program Rapport może klasyfikować dodatkowe informacje, takie jak nazwa użytkownika, jako pozwalające na identyfikację osoby, w oparciu o strategię wybraną przez właściciela serwisu WWW. Program Rapport oferuje

ochronę hasła przy pierwszej próbie zalogowania się do chronionego serwisu WWW. Wybór ochrony haseł powoduje utworzenie strategii ochrony haseł dla danego serwisu. Podczas przeglądania stron WWW i wprowadzenia tekstu zgodnego z hasłem w innych serwisach WWW program Rapport analizuje te serwisy WWW. Jeśli są one nieznane, program Rapport aktywuje ostrzeżenie wymagające reakcji ze strony użytkownika. Więcej informacji można znaleźć w punkcie Reagowanie na ostrzeżenia dotyczące danych chronionych.

Celem jest ochrona użytkownika przed działaniem oszukańczych serwisów WWW, próbujących ukraść informacje pozwalające na identyfikację osoby: przed atakami znanymi jako wyłudzenia informacji[6].

Opcje

- **Nigdy**. Program Rapport nie oferuje ochrony hasła przy logowaniu się do serwisu WWW po raz pierwszy ani nie ostrzega użytkownika w przypadku wprowadzania haseł w nierozpoznawanych serwisach WWW.
- **W serwisach WWW partnerów**. Program Rapport oferuje ochronę hasła przy logowaniu się do serwisu WWW partnera po raz pierwszy oraz, w przypadku kliknięcia opcji **Wyczyść pamięć podręczną**, po kliknięciu po raz pierwszy opcji **Wyczyść pamięć podręczną**. Dla każdego serwisu, dla którego wybrano ochronę hasła, program Rapport ostrzega użytkownika przy próbie wprowadzenia chronionego hasła do nierozpoznanego serwisu WWW.

[6] Atak polegający na wyłudzeniu informacji to próba skłonienia użytkownika do odwiedzenia fałszywego serwisu WWW, który udaje inny, wiarygodny serwis (np. należący do banku), i wprowadzenia w nim swoich danych logowania, które mogą następnie zostać wykorzystane przez przestępców do uzyskania dostępu do konta bankowości elektronicznej i popełnienia przestępstwa, na przykład wykonania przelewu środków z rachunku bankowego użytkownika.

- **W newralgicznych serwisach WWW partnerów i moich** (domyślnie). Program Rapport oferuje ochronę hasła przy logowaniu się po raz pierwszy do dowolnego serwisu WWW partnera lub dodanego ręcznie, oraz jeśli kliknięto opcję **Wyczyść pamięć podręczną**, po kliknięciu po raz pierwszy opcji **Wyczyść pamięć podręczną**. Dla każdego serwisu, dla którego wybrano ochronę hasła, program Rapport ostrzega użytkownika przy próbie wprowadzenia chronionego hasła do nierozpoznanego serwisu WWW.

Dodatkowe informacje

Strategie ochrony hasła i nazwy użytkownika dla poszczególnych serwisów WWW można wyświetlić, klikając opcję **Ostrzegaj, gdy dane logowania są używane w nieznanych serwisach WWW**.

Aby wyłączyć ochronę hasła lub nazwy użytkownika dla konkretnego serwisu WWW, należy wyczyścić to pole wyboru. Program Rapport nie będzie ostrzegał użytkownika o wprowadzeniu tego hasła lub identyfikatora użytkownika w nieznanych serwisach WWW.

Można także wyczyścić pamięć podręczną chronionych informacji pozwalających na identyfikację osoby. Po wyczyszczeniu pamięci podręcznej program Rapport przestaje chronić hasła. Wyczyszczenie pamięci podręcznej powoduje ponadto zresetowanie wszystkich decyzji dotyczących ochrony haseł dla wszystkich chronionych serwisów WWW. Przy pierwszym zalogowaniu się do każdego chronionego serwisu WWW po wyczyszczeniu pamięci podręcznej program Rapport ponownie oferuje ochronę hasła. W celu wyczyszczenia pamięci podręcznej należy kliknąć opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**, a następnie kliknąć opcję **Wyczyść pamięć podręczną**.

Blokuj modyfikację procesów przeglądarki

Opis

Blokuje próby modyfikacji procesów przeglądarki. Modyfikacja procesów przeglądarki (znana również jako wprowadzanie zmian w programie) to technika przejmowania kontroli nad przeglądarką i uzyskiwania dostępu do zawartych w niej, newralgicznych danych. Technika ta jest wykorzystywana nie tylko przez szkodliwe oprogramowanie, lecz także przez niektóre programy uprawnione. Program Rapport analizuje każdą próbę modyfikacji procesu i blokuje te próby, które wyglądają podejrzanie.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Ponieważ to zabezpieczenie działa po uruchomieniu przeglądarki, chroni ono wszystkie serwisy WWW, nie rozróżniając między serwisami partnerów a serwisami dodanymi ręcznie.

Chroń program Trusteer Endpoint Protection przed nieuprawnionym usunięciem

Opis

Chroni sam program Rapport przed nieuprawnionym usunięciem lub zmodyfikowaniem. Program Rapport chroni własne procesy przed zakończeniem, swoje pliki przed usunięciem lub zmodyfikowaniem oraz swoje klucze rejestru przed usunięciem lub zmodyfikowaniem. W efekcie niemożliwe jest wykonanie prostych operacji, takich jak zakończenie procesu programu Rapport czy usunięcie jego plików. Program Rapport chroni przed usunięciem ich z komputera przez szkodliwe oprogramowanie.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Program Rapport może i powinien zostać usunięty za pośrednictwem panelu sterowania, zgodnie z opisem w sekcji Deinstalowanie programu Rapport.

Wczesna ochrona przeglądarki

Opis

Rozpoczyna ochronę przeglądarki na najwcześniejszym możliwym etapie po jej uruchomieniu.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Ponieważ to zabezpieczenie działa po uruchomieniu przeglądarki, chroni ono wszystkie serwisy WWW, nie rozróżniając między serwisami partnerów a serwisami dodanymi ręcznie.

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Wyślij zdarzenia dotyczące zabezpieczeń i błędy do analizy

Opis

Każdorazowo przy wykryciu podejrzanego oprogramowania lub aktywności serwisu WWW program Rapport generuje zdarzenie dotyczące zabezpieczeń i wysyła je do centralnej usługi programu Rapport umożliwiającej jej analizę. Ta centralna usługa pozwala przeprowadzać rozległe testy umożliwiające określenie, czy dana aktywność jest oszukańcza. Jeśli okaże się ona oszukańcza, wówczas centralna usługa programu Rapport przekazuje do programu Rapport informację o konieczności bardziej agresywnego blokowania zagrożeń. Obok zdarzeń związanych z bezpieczeństwem program Rapport wysyła od czasu do czasu dane dotyczące wewnętrznych błędów oprogramowania. Informacje te mogą pomóc IBM w identyfikacji i naprawie błędów dotyczących oprogramowania. Wszystkie informacje wysyłane z komputera do centralnej usługi programu Rapport są anonimowe i obejmują szczegóły techniczne, nie zaś prywatne dane.

Wyłączenie tej funkcji może znacząco obniżyć bezpieczeństwo. W przypadku wystąpienia realnego zagrożenia dla bezpieczeństwa online funkcja ta pozwala zaalarmować właściciela zaatakowanego serwisu WWW, np. bank lub przedsiębiorstwo, umożliwiając mu podjęcie kroków mających na celu zabezpieczenie newralgicznych danych i funduszy.

Opcje

- **Tylko zdarzenia o znaczeniu krytycznym**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Więcej informacji na temat strategii IBM dotyczącej ochrony prywatności oraz praktyk IBM w zakresie danych użytkownika można znaleźć pod adresem http://www.trusteer.com/support/privacy-policy oraz http://www.trusteer.com/support/end-user-license-agreement.

Usuń szkodliwe oprogramowanie

Opis

Program Rapport usuwa pewne typy szkodliwego oprogramowania z komputera użytkownika. Jest to ważna, dodatkowa warstwa zabezpieczeń, stanowiąca uzupełnienie możliwości programu Rapport w zakresie ochrony newralgicznych danych przed dostępem szkodliwego oprogramowania.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Uwaga:	W przypadku niektórych instalacji programu Rapport tego ustawienia nie można wyłączyć.

Chroń numery kart płatniczych przed kradzieżą

Opis

Ostrzega przy próbie wprowadzenia danych kart płatniczych do lokalnych i niezabezpieczonych serwisów WWW. Ostrzeżenie to jest wyświetlane w oknie dialogowym, które pozwala na zatrzymanie przesyłania.

Aktywuje program uniemożliwiający rejestrację naciśnięć klawiszy po wprowadzeniu numeru karty płatniczej w chronionym serwisie WWW programu Rapport lub w dowolnym chronionym (za pomocą protokołu HTTPS) serwisie zawierającym słowo

kluczowe związane z kartą płatniczą, takim jak Visa, Mastercard czy Amex. Ma to na celu uniemożliwienie przechwycenia danych karty płatniczej przez szkodliwe oprogramowanie rejestrujące naciśnięcia klawiszy.

Funkcja ta chroni użytkownika przed kradzieżą karty płatniczej, pomagając użytkownikowi uniknąć przesyłania numerów kart płatniczych do serwisów wyłudzających informacje lub do serwisów uprawnionych, lecz nie zapewniających odpowiedniego poziomu bezpieczeństwa, a także eliminując możliwość przechwycenia danych kart płatniczych przez szkodliwe oprogramowanie.

To zabezpieczenie jest dostępne wyłącznie dla systemów kart płatniczych objętych taką ochroną.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Serwisy wymienione na liście „Następujące serwisy wybrano jako zaufane" to dowolne serwisy, które wybrano jako zaufane, klikając opcję **Ignoruj, ten serwis jest zaufany** w oknie dialogowym ostrzeżenia o wykryciu operacji wprowadzania danych karty płatniczej.

Aby usunąć konkretny serwis z listy zaufanych serwisów, kliknij opcję **Usuń ten serwis** obok serwisu, który chcesz usunąć. Aby usunąć wszystkie serwisy, kliknij opcję **Usuń wszystkie serwisy**.

Jeśli nie chcesz otrzymywać powiadomień o aktywacji funkcji programu Rapport blokującej rejestrację naciśnięć klawiszy, usuń zaznaczenie pola wyboru **Powiadom mnie o aktywacji zabezpieczeń kart płatniczych przez program Trusteer** (opcja domyślnie jest włączona).

Jeśli nie chcesz otrzymywać ostrzeżeń dotyczących wprowadzania danych karty płatniczej do lokalnych i niezabezpieczonych serwisów WWW, usuń zaznaczenie opcji **Wyświetl alert, jeśli program Trusteer Endpoint Protection wykryje operację wprowadzania danych karty płatniczej o wysokim ryzyku** (opcja domyślnie jest włączona).

Ostrzegaj mnie, kiedy przesyłam zabezpieczone dane do niezabezpieczonych serwisów

Opis

To ostrzeżenie pojawia się przy wprowadzaniu hasła w serwisie WWW niezapewniającym bezpieczeństwa przy wprowadzaniu danych. Jest ono wyświetlane, aby ostrzec użytkownika przed przesyłaniem newralgicznych danych do serwisów o wysokim stopniu ryzyka, w tym do serwisów uprawnionych, które mogą łatwo zostać przejęte przez grupy przestępcze.

Opcje

- **Nigdy**
- **Zawsze** (domyślnie)

Dodatkowe informacje

Jeśli program Rapport zainstalowano za pośrednictwem konta administratora systemu Windows, zmiany tego ustawienia można wprowadzić wyłącznie po zalogowaniu się na konto administratora.

Serwisy wymienione na liście „Następujące serwisy wybrano jako zaufane" to dowolne serwisy, które wybrano jako zaufane, klikając opcję **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie** w oknie dialogowym ostrzeżenia o wykryciu operacji wprowadzania danych bez zabezpieczenia lub klikając opcję **Ten serwis jest zaufany** w oknie dialogowym ostrzeżenia o ochronie informacji.

Aby usunąć konkretny serwis z listy zaufanych serwisów, kliknij opcję **Usuń ten serwis** obok serwisu, który chcesz usunąć. Aby usunąć wszystkie serwisy, kliknij opcję **Usuń wszystkie serwisy**.

13. Rozwiązywanie problemów

Problem z programem Rapport? Pod adresem http://www.trusteer.com/support/faq można znaleźć listę często zadawanych pytań dotyczących rozwiązywania problemów.

Aby dowiedzieć się, jak można uzyskać wsparcie, należy zapoznać się z punktem Uzyskiwanie wsparcia. W poniższych sekcjach można znaleźć informacje o tym, jak wykonać niektóre procedury niezbędne przy rozwiązywaniu problemów.

Uwaga:	Zawsze istnieje możliwość wyłączenia programu Rapport bez konieczności usuwania programu Rapport z komputera, w celu sprawdzenia, czy dany problem dotyczy programu Rapport. Należy unikać usuwania programu Rapport podczas rozwiązywania problemów. Zatrzymanie programu Rapport ma ten sam skutek i umożliwia IBM szybkie i efektywne rozwiązanie problemów podczas kontaktu z działem wsparcia.

Zatrzymywanie programu Rapport

Zatrzymanie programu Rapport powoduje szybkie i proste zatrzymanie funkcji programu bez jego deinstalowania. Program Rapport można zatrzymać w celu sprawdzenia, czy jest on przyczyną doświadczanych problemów. W celu ponownego uruchomienia programu Rapport należy uruchomić program Rapport. Nie ma potrzeby jego reinstalowania.

W przypadku wystąpienia problemu i podejrzenia, że jego przyczyną może być program Rapport, należy spróbować zatrzymać program Rapport. Jeśli problem nie ustąpi mimo zatrzymania programu Rapport, oznacza to, że prawdopodobieństwo, iż to program Rapport jest przyczyną problemu, jest nikłe. Jeśli problem zniknie po zatrzymaniu programu Rapport, oznacza to, że program Rapport jest prawdopodobnie przynajmniej w części przyczyną problemu.

IBM nie zaleca deinstalowania programu Rapport. Przed podjęciem ostatecznej decyzji o deinstalacji programu Rapport należy skontaktować się z działem wsparcia IBM Trusteer w celu uzyskania pomocy. Więcej informacji można znaleźć w punkcie Uzyskiwanie wsparcia.

Uwaga: Jeśli program Rapport zainstalowano z konta administratora systemu Windows, wówczas można zatrzymać program Rapport wyłącznie po zalogowaniu się z konta administratora.

➔ **Aby zatrzymać program Rapport:**

1. Zapisz dane i zamknij wszystkie otwarte okna.

Uwaga: Nie zatrzymuj programu Rapport, jeśli otwarte jest okno przeglądarki. Zatrzymanie programu Rapport przy otwartym oknie przeglądarki może spowodować awarię.

2. Z menu Start systemu Windows wybierz opcje **Programy** > **Trusteer Endpoint Protection** > **Zatrzymaj program Trusteer Endpoint Protection**. Zostanie wyświetlony komunikat zabezpieczający z prośbą o potwierdzenie. Wraz z komunikatem wyświetlany jest obrazek zawierający kilka znaków do przepisania. Ma to na celu zabezpieczenie przed wyłączeniem programu Rapport przez szkodliwe oprogramowanie.
3. Wprowadź znaki widoczne na obrazku.
4. Kliknij opcję **Zamknij**. Podczas zamykania programu Rapport wyświetlany jest następujący komunikat: „Należy poczekać na zamknięcie programu Trusteer Endpoint Protection.” Zniknięcie tego komunikatu oznacza, że działanie programu Rapport zostało przerwane. Można także dodatkowo sprawdzić, że program Rapport nie działa. W tym celu należy otworzyć okno przeglądarki i upewnić się, że ikona programu Rapport nie jest wyświetlana po prawej stronie paska adresu.

Uruchamianie programu Rapport

Uruchomienie programu Rapport powoduje wznowienie jego pracy, jeśli wcześniej został on zatrzymany.

Uwaga: Jeśli program Rapport zainstalowano z konta administratora systemu Windows, wówczas można uruchomić program Rapport wyłącznie po zalogowaniu się z konta administratora.

Aby uruchomić program Rapport:

Z menu Start wybierz opcje **Programy** > **Trusteer Endpoint Protection** > **Uruchom program Trusteer Endpoint Protection**. Zostanie wyświetlony komunikat „Należy poczekać na uruchomienie programu Trusteer Endpoint Protection". Zniknięcie tego komunikatu oznacza, że program Rapport został ponownie uruchomiony. Można sprawdzić, czy program Rapport działa, sprawdzając ikonę programu Rapport na pasku zadań ().

Uzyskiwanie wsparcia

Usługi wsparcia dla programu IBM Trusteer są stale dostępne. IBM oferuje szereg opcji wsparcia:

- Jeśli na komputerze zainstalowano program Rapport i nie występują problemy z nawiązywaniem połączeń, można rozpocząć zgłaszanie problemu za pośrednictwem Konsoli Rapport. Zobacz punkt Wysyłanie raportu dotyczącego problemu użytkownika. Po zgłoszeniu problemu za pośrednictwem Konsoli Rapport program Rapport przesyła do IBM wniosek o wsparcie z raportem dotyczącym problemu oraz ważne pliki dzienników ułatwiające IBM znalezienie rozwiązania problemu.
- Jeśli program Rapport nie jest zainstalowany lub jeśli nie można przesłać za jego pośrednictwem wniosku o wsparcie, należy skorzystać z formularza na stronie http://www.trusteer.com/support/submit-ticket. Należy uwzględnić możliwie najwięcej informacji zarówno na temat problemu, jak i komputera, w tym systemu operacyjnego, przeglądarki, zaobserwowanego działania oraz inne stosowne szczegółowe dane.
- W przypadku napotkania problemów z wydajnością, połączeniem, stabilnością lub innych problemów dotyczących przeglądarki należy kliknąć odsyłacz „Live Support" dostępny pod adresem http://www.trusteer.com/support w celu uruchomienia czatu online z przedstawicielem działu wsparcia.

Uwaga: W przypadku pytań dotyczących programu Rapport, jeśli nie występuje żaden konkretny problem, należy przeszukać niniejszy podręcznik lub skorzystać z usługi Błyskawiczne odpowiedzi na stronie WWW: http://www.trusteer.com/support/faq.

Odblokowywanie uprawnionych programów dodatkowych przeglądarki

Jeśli niektóre strony WWW nie są wyświetlane prawidłowo i zachodzi podejrzenie, że uprawniony program dodatkowy może być blokowany, można sprawdzić, czy program Rapport nie blokuje tego programu dodatkowego.

➔ **Aby odblokować uprawniony program dodatkowy w przeglądarce:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Blokuj nieznane programy dodatkowe w przeglądarce**. Zostanie wyświetlona lista zablokowanych programów dodatkowych. Obok nazwy każdego z zablokowanych programów dodatkowych znajduje się pole wyboru **Zawsze zezwalaj na działanie tego programu dodatkowego**.
6. Zaznacz pole wyboru **Zawsze zezwalaj na działanie tego programu dodatkowego** dla zablokowanego programu dodatkowego, na którego działanie chcesz zezwolić.

7. Kliknij przycisk **Zapisz**. Program dodatkowy jest teraz odblokowany.

Wyłączanie blokady rejestrowania naciśnięć klawiszy

Funkcja blokowania rejestrowania naciśnięć klawiszy programu Rapport może kolidować z innymi programami do rejestracji naciśnięć klawiszy i generować nieprawidłowe naciśnięcia klawiszy. Stąd, jeśli na komputerze działa inny program blokujący rejestrację naciśnięć klawiszy (na przykład stanowiący składnik oprogramowania antywirusowego), może zaistnieć potrzeba wyłączenia tej funkcji. Alternatywnie można także wyłączyć aktywny program blokujący rejestrację naciśnięć klawiszy.

➡ **Aby wyłączyć funkcję blokowania rejestracji naciśnięć klawiszy:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Z listy obok pola **Aktywuj zastępowanie znaków** wybierz opcję **Nigdy**. Zostanie wyświetlony następujący komunikat:

   Po ustawieniu dla opcji Aktywuj zastępowanie znaków wartości Nigdy program Trusteer Endpoint Protection nie chroni kart płatniczych. Można przywrócić wartości domyślne, włączyć zastępowanie znaków albo wyłączyć ochronę kart płatniczych tak, aby ustawienia były spójne.

6. Kliknij przycisk **OK**.
7. Z listy obok pola **Aktywuj zastępowanie znaków na poziomie jądra** wybierz opcję **Nigdy**.
8. Kliknij przycisk **Zapisz**. Zostanie wyświetlony komunikat z informacją, że zmiany odniosą skutek po zrestartowaniu komputera.
9. Kliknij przycisk **OK**.
10. Zrestartuj komputer. Funkcja blokowania rejestrowania naciśnięć klawiszy programu Rapport jest wyłączona.

Cofanie przypadkowych autoryzacji

W przypadku niektórych ostrzeżeń programu Rapport możliwa jest autoryzacja serwisów WWW lub certyfikatów nierozpoznawanych przez program Rapport jako uprawnione. Po dokonaniu autoryzacji serwisu WWW lub certyfikatu użytkownik nie jest ponownie ostrzegany w przypadku tego samego serwisu WWW lub certyfikatu, ponieważ jest on już zapisany w pamięci podręcznej. W razie przypadkowej autoryzacji serwisu WWW lub certyfikatu istnieje możliwość wyczyszczenia pamięci podręcznej, tak że ten sam serwis lub certyfikat spowoduje wygenerowanie ostrzeżenia przy ponownej próbie nawiązania połączenia.

Usuwanie autoryzowanych nieważnych certyfikatów SSL

Po wykryciu przez program Rapport, że certyfikat[7] serwisu WWW jest niepoprawny program Rapport wyświetla Ostrzeżenie o nieważności certyfikatu, aby ostrzec użytkownika przed wysłaniem newralgicznych danych do oszukańczych serwisów WWW. Po zaznaczeniu opcji **Nie wyświetlaj ostrzeżenia dotyczącego tego serwisu WWW ponownie** w oknie dialogowym Ostrzeżenie o nieważnym certyfikacie certyfikat serwisu WWW, z którym nawiązywane jest połączenie, jest dodawany do pamięci podręcznej zawierającej autoryzowane nieważne certyfikaty. Wyczyszczenie pamięci podręcznej powoduje usunięcie autoryzacji dla wszelkich certyfikatów znajdujących się w pamięci podręcznej i powoduje, że program Rapport ostrzega użytkownika ponownie podczas próby ponownych odwiedzin w tych samych serwisach WWW.

➔ **Aby skasować autoryzowane nieważne certyfikaty SSL:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

[7] Certyfikat SSL to kryptograficzny certyfikat cyfrowy potwierdzający tożsamość serwisu WWW i tworzący zaszyfrowane połączenie umożliwiające przesyłanie newralgicznych danych do serwisu WWW. Symbol kłódki na pasku adresu przeglądarki lub w dolnej części przeglądarki oznacza, że połączenie między przeglądarką a serwisem WWW jest zabezpieczone protokołem SSL. Jednocześnie jednak obecność symbolu kłódki nie gwarantuje, że certyfikat jest poprawny.

5. Kliknij opcję **Sprawdź poprawność certyfikatów SSL serwisu WWW**. Informacje o tym mechanizmie pojawią się poniżej, wraz z odsyłaczem umożliwiającym **wyczyszczenie pamięci podręcznej**.
6. Kliknij opcję **Wyczyść pamięć podręczną** po rozwinięciu bloku informacji. Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**. Pamięć podręczna zostanie wyczyszczona.

Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych kart płatniczych

Po wykryciu przez program Rapport faktu wprowadzenia numeru karty płatniczej na stronie WWW na dysku lokalnym lub w dowolnym niezabezpieczonym serwisie WWW program Rapport wyświetli ostrzeżenie o wykryciu operacji przesyłania karty płatniczej. Ten komunikat jest wyświetlany, aby zapobiec przesłaniu numeru karty płatniczej do serwisu WWW wyłudzającego informacje lub do serwisu uprawnionego, lecz nie zapewniającego odpowiedniego poziomu bezpieczeństwa. Kliknięcie opcji **Ignoruj, ten serwis WWW jest zaufany** w oknie dialogowym ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej serwis WWW jest dodawany do listy serwisów wybranych jako zaufane i użytkownik nie jest ponownie ostrzegany przy wprowadzaniu numeru karty płatniczej do tego serwisu. Można usunąć serwis z tej listy.

➡ **Aby usunąć serwisy wybrane jako zaufane na potrzeby wprowadzania danych kart płatniczych:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.

3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.

4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Kliknij opcję **Chroń numery kart płatniczych przed kradzieżą**. Wszystkie serwisy wybrane jako zaufane są wymienione na liście w rozwijanym obszarze. W rozwijanym obszarze znajduje się lista serwisów, które wybrano jako zaufane przez kliknięcie opcji **Ignoruj, ten serwis jest zaufany** w oknie dialogowym ostrzeżenia o wykryciu operacji wprowadzania danych karty płatniczej.

6. Kliknij opcję **Usuń ten serwis** dla każdego serwisu, który chcesz usunąć z listy, lub kliknij opcję **Usuń wszystkie serwisy**, aby usunąć wszystkie zaufane serwisy. Zostanie wyświetlony ekran z potwierdzeniem.

7. Kliknij przycisk **OK**.

Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych bez zabezpieczenia

Po wykryciu przez program Rapport faktu wprowadzenia hasła do serwisu WWW, który nie przesyła danych w sposób bezpieczny, program Rapport wyświetla ostrzeżenie dotyczące wprowadzania danych bez zabezpieczenia. Jest ono wyświetlane, aby ostrzec użytkownika przed wprowadzaniem newralgicznych danych do serwisów o wysokim stopniu ryzyka, w tym do serwisów uprawnionych, które mogą łatwo zostać przejęte przez grupy przestępcze.

Kliknięcie opcji **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie** w tym oknie dialogowym powoduje, że serwis WWW jest dodawany do listy serwisów WWW wybranych jako zaufane i użytkownik nie jest ostrzegany ponownie w przypadku wprowadzenia numeru karty płatniczej do tego serwisu. Można usunąć serwis z tej listy.

- **Aby usunąć niezabezpieczone serwisy WWW wybrane wcześniej jako zaufane:**

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

   Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij element **Ostrzegaj, kiedy przesyłam zabezpieczone dane do niezabezpieczonych serwisów**. Wszystkie serwisy wybrane jako zaufane są wymienione na liście w rozwijanym obszarze. W rozwijanym obszarze wyświetlane są serwisy, które wybrano jako zaufane, klikając opcję **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie** w oknie dialogowym ostrzeżenia o wykryciu operacji wprowadzania danych bez zabezpieczenia lub klikając opcję **Ten serwis jest zaufany** w oknie dialogowym ostrzeżenia o ochronie informacji.
6. Kliknij opcję **Usuń ten serwis** dla każdego serwisu, który chcesz usunąć z listy, lub kliknij opcję **Usuń wszystkie serwisy**, aby usunąć wszystkie zaufane serwisy. Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**.

Usuwanie serwisów WWW, dla których zezwolono na wysyłanie danych logowania

Po wprowadzeniu tekstu zgodnego z chronionym hasłem do nieznanego serwisu WWW w programie Rapport wyświetlane jest Ostrzeżenie dotyczące danych chronionych. Jeśli wybrano ignorowanie tego ostrzeżenia, serwis staje się serwisem autoryzowanym i program Rapport nie ostrzega użytkownika przy wprowadzaniu chronionego hasła do tego serwisu WWW. Autoryzowane w ten sposób serwisy WWW są przechowywane w pamięci podręcznej. Wyczyszczenie pamięci podręcznej powoduje usunięcie takich wcześniej dokonanych autoryzacji.

Po przypadkowym kliknięciu opcji **Ignoruj to ostrzeżenie** w oknie dialogowym Ostrzeżenie o danych chronionych może okazać się potrzebne skasowanie autoryzowanych serwisów WWW zapisanych w pamięci podręcznej, do których zezwolono na wysyłanie danych logowania. Wyczyszczenie pamięci podręcznej nie powoduje cofnięcia operacji przesyłania hasła, które miały już miejsce, lecz powoduje zresetowanie nieznanego statusu serwisów WWW, które zostały przypadkowo autoryzowane.

- **Aby wyczyścić pamięć podręczną autoryzowanych serwisów WWW, dla których zezwolono na wysyłanie danych logowania:**

  1. Otwórz Konsolę Rapport.
  2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
  3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
  4. Wprowadź znaki widoczne na obrazku.

     Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Przewiń w dół do pozycji **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**, a następnie kliknij nazwę mechanizmu. Informacje o tym mechanizmie pojawią się poniżej, wraz z odsyłaczem umożliwiającym **wyczyszczenie pamięci podręcznej**.
6. Kliknij opcję **Wyczyść pamięć podręczną** po rozwinięciu bloku informacji. Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**. Pamięć podręczna zostanie wyczyszczona.

Postępowanie w przypadku błędów

Po wyświetleniu błędu programu Rapport, jeśli potrzebne są pewne informacje na jego temat, należy zapoznać się z poniższymi informacjami.

Postępowanie w przypadku błędów aktualizacji

Poniższy tekst stanowi przykład błędu dotyczącego aktualizacji programu Rapport:

> *Program Trusteer Endpoint Protection nie mógł odebrać aktualizacji. Kliknij przycisk OK, aby skonfigurować nazwę użytkownika i hasło serwera proxy.*

Ten błąd występuje, jeśli program Rapport nie mógł nawiązać połączenia z Internetem w celu sprawdzenia dostępności aktualizacji. Ten błąd może wystąpić w przypadku nawiązania połączenia z siecią Internet za pośrednictwem serwera proxy, gdy program Rapport nie mógł automatycznie wykryć szczegółowych danych serwera proxy.

➡ **W przypadku odebrania tego błędu:**

1. Kliknij przycisk **OK**. Zostanie otwarta Konsola Rapport z kartą Połączenie internetowe.
2. Wybierz opcję **Użyj serwera proxy**. Wprowadź w podanym polu nazwę serwera proxy lub adres IP.

3. W polu **Port** wprowadź port TCP, który ma być używany do nawiązania połączenia z serwerem proxy.
4. Jeśli serwer proxy użytkownika wymaga uwierzytelnienia, wprowadź nazwę użytkownika w polu **Nazwa użytkownika serwera proxy** i hasło w polu **Hasło serwera proxy**.
5. Kliknij opcję **Zastosuj ustawienia**.
6. Kliknij opcję **Sprawdź połączenie**, aby po skonfigurowaniu serwera proxy sprawdzić, czy program Rapport ma połączenie z Internetem.

Postępowanie w przypadku błędów instalatora programu Rapport

Proces instalowania programu Rapport przebiega dwustopniowo:

1. Użytkownik pobiera plik RapportSetup.exe (plik programu startowego).
2. Po uruchomieniu tego pliku przez użytkownika pobierany jest plik instalacji pełnej. Jeśli proces pobierania nie powiedzie się, co zdarza się niekiedy w przypadku obecności firewalla blokującego pobieranie, może zostać wyświetlony komunikat o błędzie „Błąd podczas wyodrębniania pakietu konfiguracji programu Rapport".

Aby rozwiązać ten problem, należy pobrać pełny pakiet konfiguracyjny z następującego serwisu WWW: http://www.trusteer.com/support/install-troubleshooting.

Poniższy tekst stanowi przykład błędu dotyczącego instalowania programu Rapport:

> *Niestety pobranie pakietu programu instalacyjnego nie było możliwe. Kliknij przycisk „OK", aby zamknąć okno konfiguracji. Nastąpi automatyczne przejście do strony pobierania, na której można bezpośrednio pobrać pakiet programu instalacyjnego i zainstalować go. Jeśli problem nie ustąpi, należy sprawdzić ustawienia sieciowe i firewall.*

Ten błąd pojawia się podczas instalacji programu Rapport, jeśli instalator programu Rapport nie mógł pobrać pełnego pakietu programu instalacyjnego.

W przypadku wyświetlenia tego błędu kliknij przycisk **OK**. Zostanie wyświetlony serwis WWW IBM. Pełny pakiet programu instalacyjnego można pobrać z serwisu WWW: http://www.trusteer.com/support/install-troubleshooting.

Uwaga: Jeśli instrukcje dostępne w serwisie WWW nie okażą się pomocne, należy skorzystać z usług wsparcia dla programu IBM Trusteer pod adresem http://www.trusteer.com/support/submit-ticket.

Postępowanie w przypadku błędów dotyczących deinstalacji

Poniższy tekst stanowi przykład błędu, jaki może wystąpić podczas procesu deinstalowania:

Niektóre z plików programu Trusteer Endpoint Protection są zablokowane przez inne oprogramowanie. Jeśli przeglądarka jest otwarta, należy ją zamknąć, a następnie podjąć próbę zdeinstalowania programu Trusteer Endpoint Protection. Jeśli problem nie ustąpi, należy zapoznać się z treścią serwisu http://rapport.trusteer.com/installer/troubleshoot_uninstall

Ten komunikat pojawia się w przypadku zablokowania któregokolwiek z plików programu Rapport przez inny program podczas próby zdeinstalowania programu Rapport.

W przypadku wyświetlenia tego błędu należy postępować zgodnie z instrukcjami podanymi w oknie dialogowym. Istnieje także możliwość pobrania narzędzia Safe Uninstall, którego można użyć do zdeinstalowania programu Rapport; narzędzie można pobrać w serwisie WWW: http://www.trusteer.com/support/uninstall-troubleshooting.

Uwaga: Jeśli instrukcje zamieszczone w serwisie WWW nie okażą się pomocne, należy przesłać odpowiednie zgłoszenie do działu wsparcia (adres: http://www.trusteer.com/support/submit-ticket).

Konfigurowanie serwera proxy na potrzeby automatycznych aktualizacji

Program Rapport automatycznie łączy się z Internetem w celu sprawdzenia dostępności aktualizacji i pobrania strategii bezpieczeństwa. Większość konfiguracji serwera proxy jest wykrywana automatycznie przez program Rapport bez dokonywania jakichkolwiek zmian w konfiguracji. Jednak, jeśli z nieznanej przyczyny program Rapport nie może automatycznie wykryć serwera proxy, konieczna jest jego konfiguracja.

Aby skonfigurować serwer proxy:

1. Otwórz Konsolę Rapport.
2. W panelu kontrolnym kliknij opcję  . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Wydajność i połączenia, obok pola Połączenie internetowe, kliknij opcję **Zmień**. Zostanie wyświetlona karta Połączenie internetowe.
4. Wybierz opcję **Użyj serwera proxy**. Wprowadź w podanym polu nazwę serwera proxy lub adres IP.
5. W polu **Port** wprowadź port TCP, który ma być używany do nawiązania połączenia z serwerem proxy.
6. Jeśli serwer proxy użytkownika wymaga uwierzytelnienia, wprowadź nazwę użytkownika w polu **Nazwa użytkownika serwera proxy** i hasło w polu **Hasło serwera proxy**.
7. Kliknij opcję **Zastosuj ustawienia**.
8. Kliknij opcję **Sprawdź połączenie**, aby po skonfigurowaniu serwera proxy sprawdzić, czy program Rapport ma połączenie z Internetem.

Wysyłanie przez użytkownika raportu o problemie

W przypadku korzystania przez użytkownika z funkcji raportowania problemów dotyczących programu Rapport wysyła on raport techniczny zawierający ważne pliki wewnętrzne dzienników programu Rapport wraz z opisem problemu. Ten raport techniczny może pomóc IBM w identyfikacji i rozwiązywaniu problemów. Jest to najlepszy sposób zgłaszania problemów, ponieważ daje on IBM wyczerpujące informacje dotyczące problemu użytkownika, ułatwiające IBM zapewnienie mu optymalnego wsparcia.

Uwaga: Informacje zawarte w plikach dzienników to dane techniczne, niezawierające informacji newralgicznych ani osobistych.

➔ **Aby zgłosić problem:**

1. Otwórz Konsolę Rapport. Zostanie wyświetlony panel kontrolny.
2. W obszarze Pomoc i wsparcie kliknij opcję **Zgłoś problem**. Zostanie wyświetlona karta Zgłoś problem.
3. W polu **Imię i nazwisko** opcjonalnie wprowadź swoje imię i nazwisko.
4. W polu **Adres e-mail** wprowadź swój adres e-mail. IBM prześle na ten adres rozwiązanie zgłoszonego problemu.
5. W polu **Opis problemu** wprowadź pełny opis problemu. Podaj możliwie dokładne dane.
6. Kliknij przycisk **Prześlij**. Podczas przesyłania raportu o problemie przez program Rapport w prawym dolnym rogu ekranu wyświetlany jest poniższy komunikat.

   Program Trusteer Endpoint Protection wysyła raport o problemie...

   Po wysłaniu raportu wyświetlany jest komunikat z potwierdzeniem, że raport został przesłany.

   Ostatni wniosek o wsparcie został pomyślnie przesłany do programu Trusteer.

Przedstawiciel IBM skontaktuje się z użytkownikiem za pośrednictwem poczty elektronicznej w celu udzielenia pomocy w rozwiązaniu tego problemu.

Kopiowanie identyfikatora programu Trusteer Endpoint Protection

W przypadku zwrócenia się o pomoc do działu wsparcia dla programu IBM Trusteer może okazać się konieczne podanie numeru identyfikatora programu Trusteer Endpoint Protection. Numer identyfikatora programu Trusteer Endpoint Protection można skopiować z obszaru Ustawienia produktu w Konsoli.

Aby skopiować identyfikator programu Trusteer Endpoint Protection:

1. Otwórz Konsolę Rapport. Zostanie wyświetlony panel kontrolny.
2. W obszarze Ustawienia produktu kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.
3. Kliknij opcję **Kopiuj identyfikator Trusteer Endpoint Protection**. Identyfikator programu Trusteer Endpoint Protection zostanie zapisany w schowku na komputerze.
4. W oknie wiadomości e-mail naciśnij kombinację klawiszy Ctrl+V, aby wkleić identyfikator programu Trusteer Endpoint Protection do swojej wiadomości e-mail.

Wysyłanie plików dzienników programu Rapport do IBM

Jeśli pracownik działu wsparcia dla programu IBM Trusteer poprosi o odszukanie na komputerze plików dzienników programu Rapport i wysłanie ich do IBM w celu ułatwienia rozwiązania problemu, użytkownik powinien wykonać procedurę podaną na stronie WWW: http://www.trusteer.com/support/gathering-rapport-logs.

Problemy dotyczące instalacji

IBM udostępnia krótki i prosty proces instalacji, nie wymagający od użytkownika końcowego dysponowania żadną wiedzą techniczną. Jednak w niektórych przypadkach użytkownicy mogą napotkać problemy związane z próbą instalacji programu Rapport.

Nieukończony proces deinstalowania

Jeśli program Rapport zdeinstalowano, to aby zainstalować go ponownie, należy najpierw zrestartować komputer. W razie próby ponownej instalacji bez zrestartowania komputera po jego zdeinstalowaniu wyświetlany jest następujący komunikat:

> *Nie można teraz zainstalować programu Trusteer Endpoint Protection. Ponów próbę po ponownym uruchomieniu komputera. Jeśli problem nie ustąpi, skontaktuj się z działem wsparcia pod adresem http://www.trusteer.com/support, podając następujący kod referencyjny: PREVUNIS.*

Aby rozwiązać ten problem, zrestartuj komputer i spróbuj ponownie.

Utknięcie instalacji na etapie „Wybór miejsca docelowego" (tylko komputery Mac)

Kreator instalacji na komputerze Mac umożliwia użytkownikom wybór lokalizacji docelowej, w której ma zostać zainstalowany program Rapport. W niektórych przypadkach użytkownicy nie mogą kontynuować po dotarciu do tego etapu i przycisk **Kontynuuj** jest niedostępny.

Oznacza to, że użytkownicy korzystają ze starszej, nieobsługiwanej wersji systemu operacyjnego Mac OS X. Program Rapport można zainstalować wyłącznie w systemie operacyjnym Mac OS X 10.6 Snow Leopard lub nowszym. Listę obsługiwanych platform można znaleźć pod adresem: http://www.trusteer.com/support/supported-platforms.

Błąd instalacji systemu Windows 1638

Jeśli użytkownik podejmie próbę zainstalowania nowej wersji programu Rapport, a na komputerze jest już zainstalowana bardzo stara jego wersja, może zostać wyświetlony komunikat o błędzie „Podczas instalowania tego pakietu wystąpił błąd. Instalator dla Windows zwrócił błąd „1638".

- **Aby rozwiązać ten problem:**

  1. Usuń wszystkie foldery programu Rapport zgodnie z następującym opisem: http://www.trusteer.com/support/remove-rapport-folders.
  2. Uruchom program narzędziowy w celu wykonania procedury czyszczącej systemu Windows: http://support.microsoft.com/mats/Program_Install_and_Uninstall.
  3. Zrestartuj komputer i spróbuj ponownie.

Błąd instalacji systemu Windows 16xx

Odebranie przez użytkownika komunikatu o błędzie podobnego do opisanego w komunikacie Błąd instalacji w systemie Windows 1638 zwykle oznacza problem z instalatorem systemu Windows.

- **Aby rozwiązać ten problem w przypadku systemu operacyjnego Windows XP, Windows Vista lub Windows Server:**

  1. Przeprowadź aktualizację instalatora systemu Windows: http://www.microsoft.com/download/details.aspx?id=8483.
  2. Zrestartuj komputer i spróbuj ponownie zainstalować program Rapport.

- **Aby rozwiązać ten problem w przypadku systemu operacyjnego Windows 7 lub Windows 8:**

  1. Sprawdź, czy włączono usługę instalatora:

     a. Otwórz listę usług, otwierając okno „Uruchom" (klawisz Windows + „R") i uruchom następującą komendę:

```
services.msc
```

b. Odszukaj na liście usługę Instalator Windows, kliknij ją prawym przyciskiem myszy, a następnie kliknij opcję **Właściwości**. Upewnij się, że jako **Typ uruchomienia** wybrano opcję **Ręczny**.

c. Zrestartuj komputer i sprawdź, czy problem ustąpił.

2. Jeśli problem nie ustąpi, spróbuj zarejestrować Instalatora dla Windows:

a. Otwórz okno komend „Uruchom" (klawisz systemu Windows + „R") i uruchom następującą komendę:

```
msiexec /unreg
```

b. Po wyświetleniu komunikatu z potwierdzeniem kliknij przycisk **OK**.

c. Otwórz okno komend „Uruchom" (klawisz systemu Windows + „R") i uruchom następującą komendę:

```
msiexec /regserver
```

d. Po wyświetleniu komunikatu z potwierdzeniem kliknij opcję OK.

e. Zrestartuj komputer i spróbuj ponownie.

3. Jeśli problem nie ustąpi, otwórz wiersz komend, korzystając z uprawnień administratora, i uruchom następującą komendę:

```
sfc.exe /scannow
```

4. Po zakończeniu procesu spróbuj ponownie zainstalować program Rapport.

System Windows nie obsługuje podpisów cyfrowych

W przypadku braku lub uszkodzenia pliku crypt32.dll może zostać wyświetlony następujący komunikat o błędzie: „Ta wersja systemu Windows nie obsługuje podpisów cyfrowych.". Plik crypt32.dll jest ważnym plikiem systemu Windows. Jeśli go brak lub jest on uszkodzony, użytkownik może napotykać trudności podczas instalowania innych programów.

Użytkownik powinien skontaktować się z firmą Microsoft w celu pobrania brakującego pliku.

Instalacja zakończona przedwcześnie

W niektórych przypadkach użytkownicy mogą doświadczać problemów związanych z instalowaniem programu Rapport. Proces instalacyjny rozpoczyna się wówczas normalnie, lecz na pewnym etapie pasek postępu zostaje zresetowany i w kreatorze instalacji wyświetlany jest następujący komunikat:

> *Kreator instalacji programu Trusteer Endpoint Protection w wyniku błędu przedwcześnie zakończył działanie. System nie został zmodyfikowany. W celu zainstalowania tego programu w późniejszym czasie należy ponownie uruchomić Kreatora instalacji. Kliknij przycisk Zakończ, aby zamknąć Kreatora instalacji.*

Istnieje szereg możliwych przyczyn tego błędu. Wykonaj kroki poniższej procedury, aż do rozwiązania problemu.

Aby rozwiązać ten problem:

1. Usuń wszystkie foldery programu Rapport zgodnie z następującym opisem: http://www.trusteer.com/support/remove-rapport-folders.
2. Zrestartuj komputer i spróbuj ponownie.
3. Jeśli problem nie ustąpi, upewnij się, że na komputerze znajdują się następujące pliki systemowe:
   a. c:\windows\system32\srclient.dll
   b. c:\windows\system32\winspool.drv
   c. W systemie Windows XP: c:\windows\system32\wbem\framedyn.dll
   d. W systemie Windows Vista/7/8: c:\windows\system32\framedyn.dll

   Jeśli brak któregokolwiek z powyższych plików, użytkownik powinien skontaktować się z firmą Microsoft w celu pobrania brakujących plików systemowych.

4. Spróbuj utworzyć skrót internetowy na komputerze:

   a. Kliknij pulpit prawym przyciskiem myszy, a następnie kliknij opcje **Nowy > Skrót**.

   b. Wpisz adres http://www.trusteer.com.

   c. Kliknij opcje **Dalej > Zakończ**.

   Jeśli ten sposób nie działa, oznacza to, że system operacyjny może blokować wiele rodzajów instalacji. W takim przypadku użytkownik powinien skontaktować się z działem wsparcia firmy Microsoft w celu rozwiązania problemu.

5. Kliknij prawym przyciskiem myszy opcję Mój komputer, a następnie kliknij opcję **Właściwości > karta Zaawansowane > Zmienne środowiskowe**. Odszukaj zmienną PATH i upewnij się, że pole **Wartość zmiennej** zaczyna się od łańcucha:

   ```
   %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;
   ```

   Jeśli zmienna PATH nie zaczyna się od tego łańcucha, dodają ją na początku pola.

   Jeśli zmienna PATH nie istnieje, utwórz ją, przechodząc do opcji **Zmienne systemowe > Nowa**. Nadaj nazwę zmiennej **PATH** i skopiuj poprzedzający ją łańcuch do pola **Wartość zmiennej**.

   Kliknij przycisk **OK** we wszystkich otwartych menu i spróbuj ponownie zainstalować program Rapport.

6. Jeśli problem nie ustąpi, eskaluj go, kontaktując się z zespołem działu wsparcia dla programu IBM Trusteer:
   http://www.trusteer.com/support.

Ikona programu Rapport

Domyślnie ikona programu Rapport zawsze pojawia się na pasku adresu przeglądarki lub po jego prawej stronie. Ikona ma kolor zielony, jeśli serwis WWW w przeglądarce jest chroniony przez program Rapport, i ma kolor szary, jeśli serwis WWW w przeglądarce nie jest zabezpieczony przez program Rapport.

Powszechny problem napotykany przez użytkowników to brak ikony programu Rapport.

➔ **Aby rozwiązać ten problem na komputerze PC:**

1. Zrestartuj komputer. Po zainstalowaniu programu Rapport ikona nie pojawi się, dopóki komputer nie zostanie zrestartowany.
2. Upewnij się, że użytkownik korzysta z obsługiwanej przeglądarki. Więcej informacji można znaleźć pod adresem http://www.trusteer.com/support/supported-platforms.
3. Upewnij się, że użytkownik korzysta z najnowszej wersji programu Rapport. Więcej informacji można znaleźć w punkcie Sprawdzanie statusu aktualizacji programu Rapport.
4. Sprawdź, czy na komputerze występują jakiekolwiek konflikty z innymi programami. Listę kompatybilnego oprogramowania zabezpieczającego można znaleźć pod adresem: http://www.trusteer.com/support/compatibility-other-security-software.

Uwaga:	Nie każdy konflikt ma związek z ikoną programu Rapport. Kliknięcie nazwy programu na liście oprogramowania powoduje wyświetlenie rodzaju konfliktu, jaki może ono powodować, oraz sposobu jego rozwiązania.

5. Upewnij się, że użytkownik nie ukrył ikony programu Rapport. Więcej informacji można znaleźć w punkcie Ukrywanie i przywracanie ikony programu Rapport na pasku adresu.

6. Jeśli problem nie ustąpi, użytkownik powinien przesłać raport o problemie. Zobacz punkt Wysyłanie raportu dotyczącego problemu użytkownika.

Aby rozwiązać ten problem na komputerze Mac:

1. Zrestartuj komputer. Po zainstalowaniu programu Rapport ikona nie pojawi się, dopóki komputer nie zostanie zrestartowany.
2. Upewnij się, że użytkownik korzysta z obsługiwanej przeglądarki. Więcej informacji można znaleźć pod adresem http://www.trusteer.com/support/supported-platforms.
3. Upewnij się, że użytkownik korzysta z najnowszej wersji programu Rapport. Wersja programu Rapport jest wyświetlana w Konsoli Rapport na stronie **Ustawienia produktu**.
4. Sprawdź, czy na komputerze występują jakiekolwiek konflikty z innymi programami. Listę kompatybilnego oprogramowania zabezpieczającego można znaleźć pod adresem: http://www.trusteer.com/support/compatibility-other-security-software.

Uwaga:	Nie każdy konflikt ma związek z ikoną programu Rapport. Kliknięcie nazwy programu na liście oprogramowania powoduje wyświetlenie rodzaju konfliktu, jaki może ono powodować, oraz sposobu jego rozwiązania.

5. Spróbuj wymusić zamknięcie przeglądarki (CMD+Q), a następnie ponownie otworzyć ją i sprawdzić, czy zostanie wyświetlona ikona. Jeśli ikona zostanie wyświetlona, należy skonfigurować przeglądarkę, tak aby nie była ona uruchamiana automatycznie po uruchomieniu komputera:
   a. W systemie operacyjnym Snow Leopard (10.6): wybierz opcje **Preferencje systemowe > Konta > Elementy logowania**. Jeśli przeglądarka WWW znajduje się na liście, usuń ją.
   b. W systemach operacyjnych Lion i Mountain Lion (10.7 i 10.8): wybierz opcje **Preferencje systemowe > Użytkownicy i grupy > Rzecz otwierana podczas logowania**. Jeśli przeglądarka znajduje się na liście, usuń ją.

c. Nie zaznaczaj pola wyboru **Otwórz okna ponownie podczas logowania** podczas zamykania lub ponownego uruchamiania komputera.

d. Zrestartuj komputer i sprawdź, czy ikony nadal brakuje.

6. Jeśli problem nie ustąpi, użytkownik powinien przesłać raport o problemie. Zobacz punkt Wysyłanie raportu dotyczącego problemu użytkownika.

Problemy dotyczące ekranu powitalnego

Użytkownicy mogą skarżyć się na pojawianie się, podczas próby zalogowania się do konta bankowości elektronicznej, ekranu powitalnego programu Rapport. Istnieje szereg powodów pojawiania się ekranu powitalnego; stąd ważne jest rozpoznanie, kiedy ten komunikat się pojawia, oraz czy program Rapport jest zainstalowany.

Ekran powitalny pojawia się, mimo że program Rapport nie jest zainstalowany

Na większości ekranów powitalnych użytkownicy mogą kliknąć przycisk **Nie, dziękuję** lub **Przypomnij mi później**. Po kliknięciu przez użytkownika opcji **Przypomnij mi później** ekran powitalny pojawia się ponownie w przedziałach skonfigurowanych przez bank przy implementacji ekranu powitalnego na stronie WWW. Uważa się za normalną sytuację, w której ekran powitalny pojawia się raz w tygodniu; jeśli jednak pojawia się on codziennie lub przy każdym logowaniu, może to oznaczać problem.

➔ **Aby rozwiązać ten problem:**

1. Upewnij się, że w przeglądarce ustawiono opcję zapisywania lub zezwalania na informacje cookie. http://www.trusteer.com/support/i-keep-getting-offered-download-rapport.

2. Upewnij się, że w przeglądarce nie ustawiono opcji usuwania plików cookie po jej zamknięciu:

   a. Internet Explorer: wybierz **Opcje internetowe > Ogólne**. Upewnij się, że pole wyboru **Usuń historię przeglądania przy zakończeniu** nie jest zaznaczone.

b. Google Chrome: wybierz **Ustawienia > Prywatność > Ustawienia treści**. Upewnij się, że pole wyboru **Zachowuj dane lokalne tylko do zamknięcia przeglądarki** nie jest zaznaczone.

c. Mozilla Firefox: wybierz **Narzędzia > Opcje > Prywatność**. Upewnij się, że nie jest wybrana opcja **Program Firefox nie będzie pamiętał historii**.

3. Spróbuj usunąć pliki cookie i zalogować się ponownie. Przy pierwszej próbie zostanie wyświetlony ekran powitalny, lecz po kliknięciu opcji **Nie, dziękuję** ekran powitalny nie zostanie wyświetlony ponownie.

4. Jeśli problem nie ustąpi, eskaluj go, kontaktując się z zespołem działu wsparcia dla programu IBM Trusteer: http://www.trusteer.com/support.

Ekran powitalny pojawia się, mimo że program Rapport jest już zainstalowany

Ekran powitalny normalnie rozpoznaje, czy program Rapport jest już zainstalowany, i pojawia się tylko, jeśli nie został on zainstalowany. Podczas rozwiązywania problemów związanych z ekranem powitalnym należy zawsze najpierw sprawdzić, czy program Rapport jest zainstalowany i czy działa prawidłowo.

➡ **Rozwiązywanie problemów na komputerze PC:**

1. Zrestartuj komputer i spróbuj ponownie.

2. Upewnij się, że użytkownik korzysta z najnowszej wersji programu Rapport. Więcej informacji można znaleźć w punkcie Sprawdzanie statusu aktualizacji programu Rapport.

3. Upewnij się, że ikona programu Rapport pojawia się na pasku adresu przeglądarki. Więcej informacji można znaleźć na stronie http://www.trusteer.com/support/how-can-i-tell-rapport-working.

   a. Jeśli ikona nie jest wyświetlana, należy zapoznać się z punktem Ikona programu Rapport.

b. Jeśli ikona jest wyświetlana, lecz jest wyszarzona w chronionym serwisie, należy eskalować problem do zespołu działu wsparcia dla programu IBM Trusteer: http://www.trusteer.com/support.

c. Jeśli ikona jest wyświetlana i jest zielona oraz wyświetlany jest ekran powitalny, należy kontynuować wykonywanie tej procedury.

4. Zrestartuj przeglądarkę i spróbuj ponownie.

5. Jeśli problem nie ustąpi, spróbuj usunąć pliki cookie z przeglądarki i sprawdzić, czy ekran powitalny nadal się pojawia. http://www.trusteer.com/support/i-keep-getting-offered-download-rapport.

6. Jeśli problem nie ustąpi, może to oznaczać, że jest on związany z połączeniem sieciowym:

   a. Dodaj adres ekranu powitalnego do zaufanych serwisów przeglądarki Internet Explorer: wybierz opcje **Narzędzia > Opcje internetowe > Zabezpieczenia > Zaufane witryny**, kliknij opcję **Witryny**, a następnie dodaj witrynę.

   b. Poproś użytkownika o przejście do adresu ekranu powitalnego. Jeśli w przeglądarce wyświetlany jest komunikat o błędzie 403-zabronione, oznacza to, że firewall, filtr WWW lub serwer proxy blokują wyświetlanie ekranu powitalnego. Aby wyeliminować blokadę, należy dodać adres ekranu powitalnego do usługi, która go blokuje.

7. Jeśli problem nie ustąpi, użytkownik powinien przesłać raport o problemie. Zobacz punkt Wysyłanie raportu dotyczącego problemu użytkownika.

- **Rozwiązywanie problemów na komputerze Mac:**

1. Zrestartuj komputer i spróbuj ponownie.

2. Upewnij się, że użytkownik korzysta z najnowszej wersji programu Rapport. Wersja programu Rapport jest wyświetlana w Konsoli Rapport na stronie **Ustawienia produktu**.

3. Upewnij się, że ikona programu Rapport pojawia się na pasku adresu przeglądarki. Więcej informacji można znaleźć na stronie http://www.trusteer.com/support/how-can-i-tell-rapport-working.

   a. Jeśli ikona nie jest wyświetlana, należy zapoznać się z punktem Ikona programu Rapport.

   b. Jeśli ikona jest wyświetlana, lecz jest wyszarzona w chronionym serwisie, należy eskalować problem do zespołu działu wsparcia dla programu IBM Trusteer: http://www.trusteer.com/support.

   c. Jeśli ikona jest wyświetlana i jest zielona oraz wyświetlany jest ekran powitalny, należy kontynuować wykonywanie tej procedury.

4. Spróbuj wymusić zamknięcie przeglądarki (CMD+Q), a następnie ponownie otworzyć ją i sprawdzić, czy zostanie wyświetlony ekran powitalny. Jeśli ekran powitalny zostanie wyświetlony, należy skonfigurować przeglądarkę, tak aby nie była ona uruchamiana automatycznie po uruchomieniu komputera:

   a. W systemie operacyjnym Snow Leopard (10.6): wybierz opcje **Preferencje systemowe > Konta > Elementy logowania**. Jeśli przeglądarka WWW znajduje się na liście, usuń ją.

   b. W systemach operacyjnych Lion i Mountain Lion (10.7 i 10.8): wybierz opcje **Preferencje systemowe > Użytkownicy i grupy > Rzecz otwierana podczas logowania**. Jeśli przeglądarka znajduje się na liście, usuń ją.

   c. Nie zaznaczaj pola wyboru **Otwórz okna ponownie podczas logowania** podczas zamykania lub ponownego uruchamiania komputera.

   d. Zrestartuj komputer i sprawdź, czy ekran powitalny nadal jest wyświetlany.

5. Jeśli problem nie ustąpi, użytkownik powinien przesłać raport o problemie. Zobacz punkt Wysyłanie raportu dotyczącego problemu użytkownika.

Problemy z wydajnością

Jeśli komputer spełnia wymagania systemowe dla programu Rapport, jego zainstalowanie nie wpływa na wydajność systemu.

Spowolnione działanie komputera lub przeglądarki WWW

W rzadkich przypadkach program Rapport może spowodować, że komputer będzie reagował z opóźnieniem. Takiego spowolnienia użytkownik doświadcza, otwierając przeglądarkę lub przechodząc do innych serwisów WWW. IBM traktuje takie problemy poważnie; jednak po zainstalowaniu każdego nowego programu zabezpieczającego spodziewane jest takie niewielkie spowolnienie. Ponieważ spowolnienie działania może niekiedy okazać się trudne do wykrycia lub analizy, należy zawsze najpierw sprawdzać, czy spowolnienie rzeczywiście dotyczy programu Rapport.

1. W tym celu należy zatrzymać na próbę program Rapport i przez kilka minut normalnie korzystać z komputera, aby zaobserwować, czy spowolnienie występuje wyłącznie podczas działania programu Rapport. Następnie można uruchomić program Rapport w celu sprawdzenia, czy komputer zaczyna reagować wolniej.

   Informacje na temat uruchamiania i zatrzymywania programu Rapport można znaleźć w punktach Uruchamianie programu Rapport oraz Zatrzymywanie programu Rapport.

Uwaga:	Zatrzymanie programu Rapport nie wpływa na działanie przeglądarki. Jeśli spowolnienie nie ustąpi, oznacza to, że problem nie jest związany z programem Rapport.

2. Upewnij się, że w komputerze dostępna jest wystarczająca ilość pamięci RAM:

   a. Naciśnij kombinację klawiszy Windows+R, aby otworzyć okno dialogowe Uruchom, a następnie wpisz:

```
msinfo32
```

   b. Kliknij przycisk **OK**.

c. W oknie **Informacje o systemie**, w okienku nawigacji, kliknij **Podsumowanie systemu**, zaś w okienku szczegółów odszukaj wpisy **Całkowity rozmiar pamięci fizycznej** i **Dostępna pamięć fizyczna**.

   Jeśli komputer ma mniej niż 1 GB całkowitej pamięci fizycznej lub mniej niż 100 MB dostępnej pamięci fizycznej, uruchomienie programu Rapport nie jest możliwe.

3. Jeśli w komputerze dostępna jest wystarczająca ilość pamięci RAM, zaś spowolnienie jest związane z programem Rapport, eskaluj problem do zespołu wsparcia dla programu IBM Trusteer: http://www.trusteer.com/support.

Wysokie zużycie mocy obliczeniowej procesora lub pamięci

Program Rapport zwykle korzysta z dwu usług, które zawsze pojawiają się w menedżerze zadań: RapportService.exe i RapportMgmtService.exe.

W poniższej tabeli przedstawiono normalne zużycie pamięci i mocy obliczeniowej procesora dla tych usług:

	Użycie pamięci (MB)	Użycie mocy obliczeniowej procesora (%)
RapportService.exe	Do 40	0-1
RapportMgmtService.exe	Do 30	0-1

Krótkotrwałe, nagłe skoki zużycia mocy obliczeniowej procesora są zjawiskiem normalnym podczas operacji takich, jak otwieranie przeglądarki, logowanie się na konto czy otwieranie Konsoli Rapport. Użytkownicy końcowi mogą jednak niekiedy skarżyć się na nadmierne użycie przez program Rapport zasobów systemowych.

Jeśli klient skarży się na wysokie zużycie mocy obliczeniowej procesora lub pamięci, należy sprawdzić następujące dane:

- Czy problem dotyczy usługi RapportService.exe albo RapportMgmtService.exe?
- Czy występuje duże zużycie mocy obliczeniowej procesora, czy pamięci?
- Jak wiele mocy obliczeniowej lub pamięci wykorzystuje ten proces?

Jeśli zużycie mocy jest nadmierne, należy eskalować problem do zespołu działu wsparcia dla programu IBM Trusteer:
http://www.trusteer.com/support.

Problemy związane ze współdziałaniem

Program Rapport wykorzystuje wielowarstwowy system zabezpieczeń, blokujący na szereg sposobów działanie szkodliwego oprogramowania na przeglądanych stronach WWW. Niestety, niekiedy dochodzi do konfliktów tych mechanizmów zabezpieczeń z uprawnionymi programami. W przypadku wystąpienia konfliktu można zdecydować o edycji lub wyłączeniu odpowiednich strategii bezpieczeństwa. Więcej informacji można znaleźć w punkcie Modyfikowanie mechanizmów zabezpieczeń.

Uwaga: Jeśli mechanizmy zabezpieczeń programu Rapport zostały wyłączone, dane użytkownika nie są chronione. Mimo że użytkownik jest chroniony przez wszystkie pozostałe warstwy ochrony, najwyższy poziom bezpieczeństwa zapewnia pozostawienie domyślnych ustawień strategii. W przypadku braku pewności co do dokonywanych zmian możliwe jest przywrócenie ustawień domyślnych przez kliknięcie opcji **Przywróć wartości domyślne**.

Programy do zarządzania hasłami

Procesy na komputerze użytkownika mogą uzyskiwać dostęp do przeglądarki i odczytywać newralgiczne informacje lub modyfikować realizowane przez użytkownika transakcje. W przypadku połączenia z chronioną witryną WWW program Rapport blokuje możliwość uzyskania dostępu do przeglądarki przez procesy niezależnie od tego, czy dany proces jest szkodliwy, czy nie. Niestety, blokowanie dostępu procesów do przeglądarki może powodować blokowanie przez program Rapport prób uzyskania dostępu do przeglądarki przez uprawnione programy, takie jak programy do zarządzania hasłami czy porównywania odcisków palców.

Jeśli program do zarządzania hasłami przerwał pracę po zainstalowaniu programu Rapport, należy wyłączyć strategię **Blokuj dostęp do informacji w przeglądarce**.

Oprogramowanie do wykonywania zrzutów ekranu

Program Rapport blokuje próby wykonania zrzutów ekranu po przejściu przez użytkownika do chronionych serwisów WWW. Programy na komputerze użytkownika próbujące wygenerować zrzut ekranu generują czarny obraz. Szkodliwe oprogramowanie może próbować przechwycić ekran zawierający newralgiczne informacje (np. dane osobowe). W przypadku próby ręcznego wykonania zrzutu ekranu z poziomu chronionego serwisu program Rapport wyświetla komunikat umożliwiający zatwierdzenie tego zrzutu ekranu. Niestety próby zablokowania zrzutów ekranu mogą powodować blokowanie uprawnionych narzędzi oraz programów do wykonywania zrzutów ekranu. Ponadto niektóre narzędzia do udostępniania ekranu oraz narzędzia dostępu zdalnego korzystające z technologii wykonywania zrzutów ekranu mogą być zablokowane.

Jeśli narzędzie do wykonywania zrzutów ekranu lub narzędzie dostępu zdalnego jest zablokowane lub jest w nim wyświetlany pusty albo czarny ekran, należy wyłączyć strategię **Blokuj wykonywanie wykonywania zrzutów ekranu**.

Tryb dla osób niedowidzących (lektory ekranowe lub narzędzia do powiększania)

Niektóre z mechanizmów zabezpieczeń programu Rapport mogą być w konflikcie z technikami wspomagającymi pracę użytkowników niedowidzących, takimi jak lektory ekranowe czy narzędzia do powiększania. Ponadto wszelkie zmiany w ustawieniach programu Rapport wymagają przedstawienia przez użytkownika kodu CAPTCHA, będącego kodem zabezpieczeń niemożliwym do odczytania przez programy działające automatycznie.

Aby umożliwić tym klientom korzystanie z dodanych zabezpieczeń oferowanych przez program Rapport, do programu dołączono instalację wersji przeznaczonej dla osób niedowidzących. Zainstalowanie programu Rapport w tym trybie powoduje automatyczne wyłączenie strategii, które mogą być w konflikcie z tymi technikami wspomagającymi.

Aby zainstalować program Rapport w trybie dla użytkowników niedowidzących, pobierz i uruchom w zwykły sposób plik instalacyjny programu Rapport. W kreatorze instalacji kliknij opcję **Zaawansowane** i zaznacz pole wyboru **Niedowidzę, mam problemy z rozróżnianiem kolorów i/lub korzystam z pomocy lektorów ekranowych**. Kliknij opcję **Kontynuuj** i kontynuuj proces instalacji.

Pozostałe problemy

W przypadku napotkania problemu z programem Rapport nieujętego w niniejszej sekcji rozwiązywania problemów należy podjąć próbę wykonania następujących ogólnych kroków dotyczących rozwiązywania problemów:

1. Zrestartuj komputer i sprawdź, czy problem ustąpił.
2. Upewnij się, że na komputerze uruchomiono zaktualizowaną wersję programu Rapport.
    a. W przypadku użytkowników komputerów PC więcej informacji można znaleźć w punkcie Sprawdzanie statusu aktualizacji programu Rapport.
    b. W przypadku użytkowników komputerów Mac wersja programu Rapport jest wyświetlana w Konsoli Rapport na stronie **Ustawienia produktu**.
    c. Jeśli aktualizacja programu Rapport jest dostępna, należy pobrać jej najnowszą wersję, zrestartować komputer i sprawdzić, czy problem został rozwiązany. Więcej informacji można znaleźć w punkcie http://www.trusteer.com/support/rapport-installation-links.
3. Sprawdź, czy na komputerze są zainstalowane inne programy oraz czy mogą być one w konflikcie z programem Rapport.
    Więcej informacji można znaleźć pod adresem http://www.trusteer.com/support/compatibility-other-security-software.

4. Jeśli problem wystąpi podczas korzystania z określonej przeglądarki WWW, należy upewnić się, że ta przeglądarka jest obsługiwana i że używana jest jej najnowsza wersja.
   Więcej informacji można znaleźć pod adresem http://www.trusteer.com/support/supported-platforms.
5. W przypadku podejrzeń, że to nie program Rapport jest źródłem problemów, należy spróbować zatrzymać program Rapport i sprawdzić, czy problem nie ustąpił. Można także spróbować uruchomić program Rapport w celu sprawdzenia, czy problem nie uległ wznowieniu.
6. Jeśli problem nie ustąpi, eskaluj go, kontaktując się z zespołem działu wsparcia dla programu IBM Trusteer:
   http://www.trusteer.com/support.

14. Aktualizowanie programu Rapport

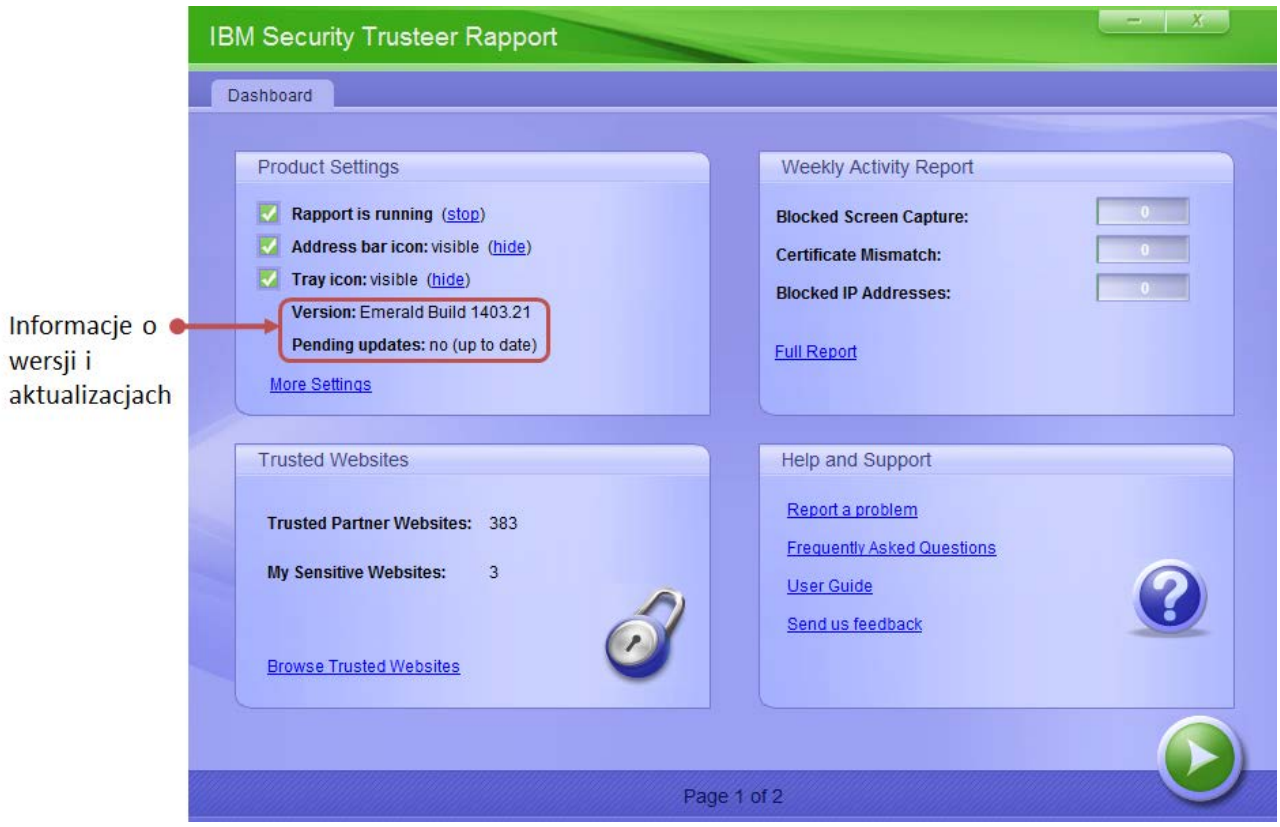
Regularne aktualizacje mają kluczowe znaczenie dla skuteczności działania programu Rapport. Z tego względu aktualizacje programu Rapport są wykonywane automatycznie. Aktualizacje pojawiają się niezależnie i bez wiedzy użytkownika. Można jednak zaktualizować program Rapport ręcznie odpowiednio do potrzeb oraz wyłączyć automatyczne aktualizacje.

Sprawdzanie statusu aktualizacji programu Rapport

Informacje związane ze statusem aktualizacji programu Rapport są wyświetlane w obszarze Ustawienia produktu Konsoli Rapport.

➡ **Aby sprawdzić status aktualizacji programu Rapport:**

1. Otwórz Konsolę Rapport. Obszar Ustawienia produktu zostanie wyświetlony w górnym lewym roku panelu kontrolnego.



Pole **Oczekujące aktualizacje** informuje użytkownika o dostępności oczekujących aktualizacji oraz o tym, czy wersja programu Rapport jest aktualna. Jeśli ostatnia pobrana aktualizacja wymaga zrestartowania systemu, aby możliwe było jej zastosowanie, w tym polu wyświetlana jest wartość *tak*.

2. Opcjonalnie kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu, zawierająca dodatkowe informacje.

   Poniższe pola wyświetlania podlegają aktualizacji:

   - **Ostatnie zapytanie o aktualizacje**. Data i godzina ostatniego przesłania przez program Rapport zapytania o nowe aktualizacje.
   - **Automatyczne aktualizacje oprogramowania**. Informacja o tym, czy automatyczne aktualizacje są włączone, czy wyłączone. Domyślnie aktualizacje są włączone. Aby mieć pewność co do otrzymywania wszystkich aktualizacji, należy pozostawić dla tego ustawienia wartość domyślną.

Ręczne aktualizowanie programu Rapport

Program Rapport jest domyślnie aktualizowany automatycznie. Można także zaktualizować program Rapport ręcznie.

➔ **Aby ręcznie zaktualizować program Rapport:**

1. Otwórz Konsolę Rapport. Obszar Ustawienia produktu zostanie wyświetlony w górnym lewym roku panelu kontrolnego.

2. Kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.

3. Kliknij opcję **sprawdź teraz w poszukiwaniu aktualizacji**. Program Rapport dokonuje sprawdzenia w poszukiwaniu aktualizacji. Kiedy program Rapport sprawdza dostępność aktualizacji, postęp jest wskazywany przez tekst pojawiający się poniżej pól wyświetlania. Poniższa lista zawiera opis możliwych wyników sprawdzania w poszukiwaniu aktualizacji:

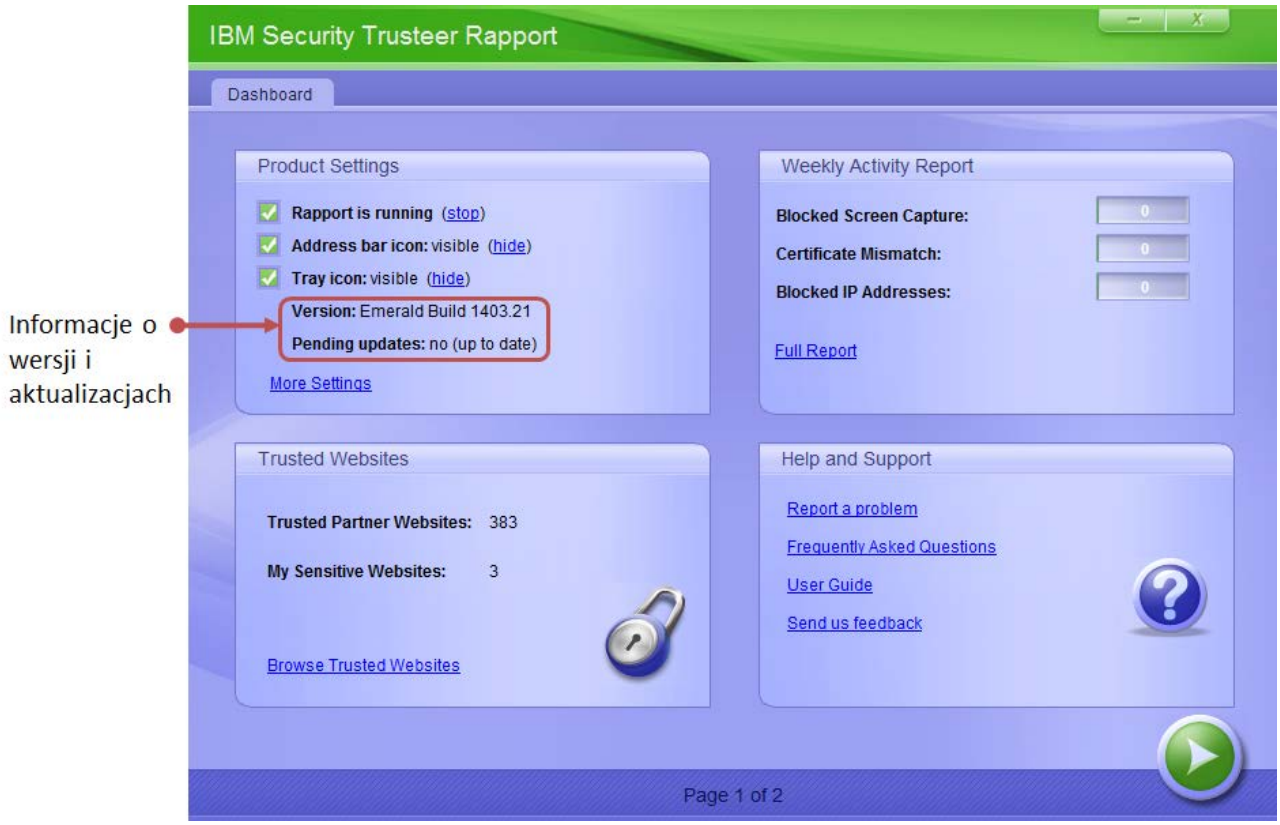
- Program Rapport nie wykrywa oczekujących aktualizacji. Wyświetlany jest komunikat: „Najnowsza konfiguracja programu Rapport została już uruchomiona."
- Program Rapport wykrywa i pobiera, a następnie instaluje aktualizację. Wyświetlany jest komunikat: „Konfiguracja została zaktualizowana. Uruchomiona jest teraz najnowsza wersja konfiguracji programu Rapport." Liczba w polu wyświetlania **Plik konfiguracyjny** jest zwiększana.
- Program Rapport wykrywa i pobiera aktualizację, która ma zostać zastosowana przy ponownym uruchomieniu komputera. Wyświetlany jest następujący komunikat: „Aktualizacja oprogramowania jest gotowa. Konfiguracja została zaktualizowana." Wartość w polu **Oczekujące aktualizacje** zmienia się na „tak (aby zastosować, zrestartuj komputer)".
- Program Rapport wykrywa i pobiera więcej niż jedną aktualizację. Niektóre aktualizacje są stosowane niezwłocznie, inne zaś zostaną zastosowane po zrestartowaniu komputera. Wyświetlany jest następujący komunikat: „Aktualizacja oprogramowania jest gotowa. Konfiguracja została zaktualizowana." Liczba w polu wyświetlania **Plik konfiguracyjny** jest zwiększana. Wartość w polu **Oczekujące aktualizacje** zmienia się na „tak (aby zastosować, zrestartuj komputer)".

Wyłączanie automatycznych aktualizacji

Domyślnie aktualizacje programu Rapport są wykonywane automatycznie. Aktualizacje pojawiają się niezależnie i bez wiedzy użytkownika. Regularne aktualizacje mają kluczowe znaczenie dla skuteczności działania programu Rapport. Aktualizacje automatyczne można wyłączyć, lecz w takim przypadku program Rapport nie będzie aktualizowany.

➔ **Aby wyłączyć automatyczne aktualizacje:**

1. Otwórz Konsolę Rapport. Obszar Ustawienia produktu zostanie wyświetlony w górnym lewym roku panelu kontrolnego.



2. Kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.

3. Usuń zaznaczenie pola wyboru **Automatyczne aktualizacje oprogramowania**. Zostanie wyświetlona karta Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek zawierający kilka znaków do przepisania. Ma to na celu zabezpieczenie przed uzyskaniem dostępu do Konsoli i wyłączeniem programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.
5. Kliknij przycisk **OK**. Automatyczne aktualizacje są teraz wyłączone. Podczas, gdy automatyczne aktualizacje są wyłączone, program Rapport nie jest aktualizowany do czasu jego ręcznej aktualizacji. Więcej informacji można znaleźć w sekcji Ręczne aktualizowanie programu Rapport.

15. Deinstalowanie programu Rapport

Zdecydowanie zaleca się zdeinstalowanie programu Rapport. W przypadku trudności z programem Rapport należy przesłać wniosek o wsparcie na stronie http://www.trusteer.com/support/submit-ticket. Na czas rozwiązywania problemu można zatrzymać program Rapport bez deinstalowania go.

Program Rapport oferuje tyko jedną metodę deinstalacji, co pozwala chronić go przed nieuprawnioną deinstalacją.

Uwaga: Jeśli program Rapport zainstalowano z konta administratora systemu Windows, wówczas można zdeinstalować go wyłącznie po zalogowaniu się z konta administratora.

Deinstalowanie programu Rapport (Windows 8 i Windows 7)

Deinstalowanie programu Rapport (Windows XP)

Uwaga: W przypadku napotkania trudności przy deinstalowaniu programu Rapport oraz w celu uzyskania informacji na temat deinstalowania programu Rapport za pomocą narzędzia do bezpiecznej deinstalacji należy zapoznać się z informacjami pod adresem: http://www.trusteer.com/support/uninstalling-rapport-using-safeuninstall-utility.

Co oznacza pole wyboru Usuń ustawienia wszystkich użytkowników na ekranie podczas deinstalowania?

Pole wyboru **Usuń ustawienia wszystkich użytkowników** pojawiające się w oknie dialogowym Deinstalowanie programu IBM Security Trusteer Endpoint Protection powoduje usunięcie wszystkich zmian wprowadzonych w programie Rapport, w tym dodanych serwisów oraz haseł, na których ochronę się zdecydowano. Po zaznaczeniu tego pola wyboru, jeśli użytkownik zdecyduje się na ponowne zainstalowanie programu Rapport w przyszłości, program nie zapamięta żadnych z wprowadzonych zmian.

Deinstalowanie programu Rapport (Windows 8 i Windows 7)

- **Aby zdeinstalować program Rapport:**

1. Otwórz Panel sterowania.
2. W menu **Programy** kliknij opcję **Deinstalowanie programu**.
3. Kliknij dwukrotnie pozycję Trusteer Endpoint Protection na liście programów. Zostanie wyświetlony komunikat z prośbą o potwierdzenie.
4. Kliknij przycisk **Tak**. Zostanie wyświetlone okno dialogowe programu Rapport przedstawiające najnowsze zdarzenia, których program Rapport pomyślnie zapobiegł.
5. Kliknij przycisk **Kontynuuj**. Zostanie wyświetlone kolejne okno dialogowe, oferujące pomoc w zakresie problemów technicznych z programem Rapport. Aby kontynuować deinstalowanie, należy zamknąć wszystkie otwarte pliki i aplikacje.
6. Kliknij opcję **Nie; zdeinstaluj teraz**. Program Rapport ukończy proces deinstalowania. Po zakończeniu procesu deinstalowania zostanie otwarte nowe okno przeglądarki z prośbą o opinię o programie Rapport oraz kilkoma prostymi pytaniami.

Deinstalowanie programu Rapport (Windows XP)

- **Aby zdeinstalować program Rapport:**

1. Otwórz Panel sterowania.
2. Kliknij opcję **Dodaj/usuń programy**.
3. Odszukaj na liście programów pozycję Trusteer Endpoint Protection i kliknij przycisk **Zdeinstaluj/Zmień** obok programu Trusteer Endpoint Protection. Zostanie wyświetlony komunikat z prośbą o potwierdzenie.

4. Kliknij przycisk **Tak**. Zostanie wyświetlone okno dialogowe programu Rapport przedstawiające najnowsze zdarzenia, których program Rapport pomyślnie zapobiegł.
5. Kliknij przycisk **Kontynuuj**. Zostanie wyświetlone kolejne okno dialogowe, oferujące pomoc w zakresie problemów technicznych z programem Rapport. Aby kontynuować deinstalowanie, należy zamknąć wszystkie otwarte pliki i aplikacje.
6. Kliknij opcję **Nie; zdeinstaluj teraz**. Program Rapport ukończy proces deinstalowania. Po zakończeniu procesu deinstalowania zostanie otwarte nowe okno przeglądarki z prośbą o opinię o programie Rapport oraz kilkoma prostymi pytaniami.

16. Aktualizowanie programu Rapport

Aby przeprowadzić aktualizację programu Rapport do nowej wersji, należy zainstalować nową wersję bez uprzedniego deinstalowania poprzedniej. Proces instalowania jest taki sam, jak w przypadku standardowej instalacji, obejmuje jednak kilka dodatkowych kroków.

Instrukcje instalacji można znaleźć w sekcji Instalowanie programu Rapport. W trakcie procesu instalowania wyświetlany jest następujący ekran:

Ten ekran pojawia się podczas instalowania nowej wersji bez deinstalowania istniejącej. Po wyświetleniu tego ekranu wybierz opcję **Tak - chcę tylko przeprowadzić aktualizację**. Kliknij przycisk **Dalej** i kontynuuj proces instalowania jak zwykle.

Uwaga:	Jeśli program Rapport został już zainstalowany z konta administratora systemu Windows, wówczas można zainstalować program Rapport bez deinstalowania bieżącej wersji wyłącznie po zalogowaniu się z konta administratora.

W trakcie procesu instalowania zostanie wyświetlony komunikat zabezpieczający z prośbą o potwierdzenie:

Ten ekran zostanie wyświetlony, ponieważ kreator instalacji wymaga zamknięcia istniejącej wersji programu Rapport w celu zainstalowania nowej wersji. Z uwagi na zabezpieczenie przed możliwością wyłączenia programu Rapport przez szkodliwe oprogramowanie każde jego zamknięcie wymaga potwierdzenia przez użytkownika. Po wyświetleniu tego ekranu należy wprowadzić znaki widoczne na obrazku i kliknąć przycisk **Zamknij**. Proces instalacji jest kontynuowany jak zwykle.

Po zakończeniu procesu instalowania w oknie komunikatu może zostać wyświetlony następujący tekst:

> *Nastąpiła aktualizacja programu Trusteer Endpoint Protection do nowszej wersji. Niektóre nowe funkcje programu Trusteer Endpoint Protection będą dostępne dopiero po ponownym uruchomieniu.*

Mimo wyświetlenia tego komunikatu komputer jest chroniony. Zaleca się jednak ponowne uruchomienie komputera tak szybko, jak to tylko możliwe.