# 5. ZARZĄDZANIE DANYMI: BEZPIECZEŃSTWO I PRYWATNOŚĆ

## CASE STUDY

**Wprowadzenie**
W dniu 12 maja 2017 r. nastąpił największy atak ransomware na całym świecie. Atak wykorzystywał exploit o nazwie EternalBlue - słabość w systemie NSA opublikowaną przez ShadowBrokers.
Gdy komputer został zainfekowany WannaCry, szyfrował on wszystkie dane. Program wyświetlał ekran żądający okupu w postaci wirtualnego Bitcoina w celu uzyskania ponownego dostępu. Wysokość okupu rosła z czasem aż do końca odliczania, kiedy wszystkie pliki miały zostać zniszczone.
Wannacry wpłynęło na ponad 200 000 systemów firm, agencji rządowych i osób prywatnych w ponad 150 krajach. W rezultacie duże organizacje, takie jak National Health Services (NHS)[1] w Wielkiej Brytanii i Renault-Nissan, musiały wstrzymać produkcję w niektórych obszarach. Dotyczyło to również wielu dużych firm, w tym Telefonica, FedEx, Deutsche Bahn, Santander i KPMG.

Dlaczego ten atak okazał się tak silny?

- Po pierwsze, chodziło o sposób, w jaki się rozprzestrzenia. Najczęstszą drogą infekcji konwencjonalnego ataku ransomware było rozprzestrzenianie go się za pośrednictwem wiadomości e-mail typu phishing i odwiedzanie odpowiedniej strony internetowej. Ransomware był dystrybuowany jako poczta elektroniczna, aby zachęcić użytkowników do kliknięcia w załącznik, lub w formie włamania się na serwer sieciowy i zamaskowania go jako reklama, więc gdy użytkownik odwiedzał witrynę, komputer użytkownika stawał się zainfekowany. Oprogramowanie ransomware WannaCry miało cechy robaka, który jest dystrybuowany autonomicznie przez sieć bez żadnych działań ze strony użytkownika. Każdy komputer z systemem Windows bez odpowiedniej poprawki był podatny na infekcję.
- Po drugie, niechronione systemy operacyjne. Jednym z najważniejszych czynników było to, że duża liczba komputerów nie miała zainstalowanej poprawki Microsoftu lub działała na wersji systemu Windows, dla której nie było w ogóle łatki.

**Lekcje**
Liderzy nie zauważyli tego, aby powstrzymać i zminimalizować potencjał cyberataków muszą upewnić się, że ich systemy operacyjne są stale aktualizowane i łatane we wszystkich sieciach.

## EKSPOZYCJA

### 1. BEZPIECZEŃSTWO DANYCH

Eksperci ostrzegają, że WannaCry to dopiero początek, a liczby potwierdzają ten pogląd.

Wśród właścicieli małych firm panuje błędne przekonanie, że hakerzy są zainteresowani tylko atakowaniem dużych przedsiębiorstw. W rzeczywistości hakerzy kochają MŚP. Te mniejsze firmy zwykle mniej koncentrują się na bezpieczeństwie i nie mają budżetów na bezpieczeństwo IT, jakie

[1] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

mają duże przedsiębiorstwa. Nie mają środków na opłacenie analityków bezpieczeństwa ani wewnętrznych pracowników IT.[2]

**Rodzaje zagrożeń**
Naruszenie danych to incydent, w którym wrażliwe lub chronione w inny sposób informacje są uzyskiwane bez upoważnienia. Może to wyczerpać skromne zasoby, jakimi dysponują MŚP i zmniejszyć zaufanie konsumentów do nich. Krótko mówiąc, brak zabezpieczeń może Cię doprowadzić do bankructwa.

## 2. PRYWATNOŚĆ DANYCH

**Dlaczego prywatność ma znaczenie?**

**1. Ograniczenie władzy.** Prywatność jest ograniczeniem siły rządowej, a także siły firm z sektora prywatnego. Im więcej ktoś o nas wie, tym większą władzę może mieć nad nami. Dane osobowe są wykorzystywane do podejmowania bardzo ważnych decyzji w naszym życiu. Dane osobowe mogą być wykorzystane do wpłynięcia na naszą reputację; mogą być wykorzystywane do wpływania na nasze decyzje i kształtowania naszego zachowania. Może być wykorzystywany jako narzędzie do sprawowania nad nami kontroli. W niewłaściwych rękach dane osobowe mogą zostać wykorzystane do wyrządzenia nam wielkiej szkody.[3]

**2. Swobody.** Prywatność jest kluczem do wolności myśli i wypowiedzi i pomaga chronić naszą zdolność do obcowania z innymi ludźmi. Kluczowym elementem wolności zrzeszania się jest możliwość robienia tego z poszanowaniem prywatności. Prywatność jest kluczowym elementem demokratycznego społeczeństwa.

**3. Prawa do drugiej szansy.** Wiele osób nie jest statycznych; zmieniają się i dorastają przez całe życie. Ogromną tego zaletą jest możliwość uzyskania drugiej szansy, aby móc pokonać przeszkodę odkryć siebie na nowo. Prywatność pielęgnuje tę zdolność. Pozwala ludziom rosnąć i dojrzewać bycia związanym wszystkimi niemądrymi rzeczami, które mogli zrobić w przeszłości

**Ochrona danych różni się od prywatności danych**

- Prywatność to skomplikowana kwestia związana z prawami i swobodami zapisanymi w prawie. Ochrona danych różni się od prywatności danych. Ochrona polega na zabezpieczeniu danych przed nieautoryzowanym dostępem. Prywatność danych dotyczy autoryzowanego dostępu – kto go posiada i kto go definiuje. Ochrona danych jest zasadniczo kwestią techniczną, podczas gdy prywatność danych jest kwestią prawną.
- Technologia sama w sobie nie może zapewnić prywatności danych osobowych. Większość protokołów ochrony prywatności jest nadal podatna na ataki upoważnionych osób, które mają dostęp do danych. Ciężar spoczywający na tych upoważnionych osób dotyczy przede wszystkim prawa do prywatności, a nie technologii.

**RODO**

2 https://www.telegraph.co.uk/business/cybersecurity-for-small-business/fraud-prevention/

3 https://teachprivacy.com/10-reasons-privacy-matters/



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

- RODO to rozporządzenie w prawie UE dotyczące ochrony danych i prywatności wszystkich indywidualnych obywateli Unii Europejskiej (UE) i Europejskiego Obszaru Gospodarczego (EOG). Dotyczy to również przekazywania danych osobowych poza obszarami UE i EOG.[4]
- Ma to na celu pociągnięcie firm do odpowiedzialności za ochronę danych osobowych, które są coraz częściej wykradane w dzisiejszym cyfrowym świecie.
- Obowiązkiem krajowych organów regulacyjnych - w Wielkiej Brytanii, biura komisarza ds. Informacji - jest egzekwowanie przepisów wobec spółek podlegających ich jurysdykcji.
- Kary: zgodnie z RODO organy regulacyjne mogą ukarać firmę aż do wysokości 4% rocznej sprzedaży, choć jak dotąd większość grzywien była znacznie niższa, zwykle mniejsza niż 1 milion USD.

Dane osobowe powinny być:

- przetwarzane zgodnie z prawem, uczciwie i w sposób przejrzysty;
- gromadzone do określonych, wyraźnych i zgodnych z prawem celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami; („Ograniczenie celu”);
- adekwatne, odpowiednie i ograniczone do tego, co jest konieczne w związku z celami, dla których są przetwarzane („minimalizacja danych”);
- dokładne i, w razie potrzeby, aktualizowane („dokładność”);
- przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, w których dane osobowe są przetwarzane („ograniczenie przechowywania”);
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem, przy użyciu odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

**Case study British Airways**

- Dane pół miliona pasażerów zostały udostępnione w trakcie cyberataku pomiędzy 21 sierpnia a 5 września 2018 roku. Firma rozwiązała problem naruszenia witryny i aplikacji 6 września, po czym powiadomiono policję.
- Biuro komisarza ds. Informacji (ICO) stwierdziło, że różnego rodzaju informacje zostały upublicznione z powodu złych warunków bezpieczeństwa, w tym tych dotyczących danych do logowania, karty płatniczej i rezerwacji podróży, a także danych dotyczących nazwiska i adresu.
- Linie lotnicze będą musiały zapłacić ponad 183 miliony funtów (230 milionów dolarów) za brak właściwej ochrony danych klientów. Była to największa kara zainicjowana przez krajowe organy regulujące prywatność w całej UE od czasu wejścia w życie RODO.[5]

## 3.ETYKA DANYCH

Potęga danych jest tak wielka i może mieć tak duży wpływ na nasze życie, że powinniśmy sobie wyobrażać dane nie jako X i Y, ale jako cyfrową duszę. Pojęcie „cyfrowej duszy” zostało opisane jako elektroniczna reprezentacja ciebie. Stworzenie modelu własności i kontroli nad tym pomysłem jest dużym wyzwaniem dla firm przechowujących dane, a także dla osób fizycznych i organów regulacyjnych.

4 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
5 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

**Teoria "Pathetic dot" Lawrence'a Lessiga**
Teoria "Pathetic dot" zwana także teorią nowej szkoły chicagowskiej została wprowadzona przez Lawrcence'a Lessiga w artykule opublikowanym w 1998 roku, a spopularyzowana dzięki książce z 1999 roku pt. *Code and Other Laws of Cyberspace*. Jest to społeczno-ekonomiczna teoria regulacji.[6] Omawia ona sposób, w jaki życie jednostek jest regulowane przez cztery siły: prawo, normy społeczne, rynek I architekturę (infrastrukturę techniczną).

Teoria podkreśla, że kod komputerowy jest tylko jedną z metod regulacyjnych, które mogą zmieniać zachowanie, a zatem zrozumienie innych mechanizmów, takich jak prawo, normy i etyka, ma zasadnicze znaczenie dla budowania technologii, które nie powodują niepożądanych zachowań.

Etyka danych polega na wyjściu poza prawodawstwo i zrozumieniu interakcji między rynkami, normami i kodeksem, aby upewnić się, że etycznie korzystamy z danych osób. Musimy wykraczać poza samą zgodność, wykorzystywać dane w najlepszy możliwy sposób dla wszystkich zainteresowanych.

**Trzy tematy przewodnie**
**Zgoda.** Zgoda jest tym, o czym wiele osób myśli, gdy mowa o etyce technologicznej. Zgodnie z RODO wymogi dotyczące zgody zostały zaostrzone, aby wymagać pozytywnego i jednoznacznego działania w celu „wyrażenia zgody". Nie jest to już jednorazowa decyzja, ale bieżąca kwestia, którą należy uważnie monitorować. Osoby fizyczne mogą wycofać swoją zgodę w dowolnym momencie bez żadnych konsekwencji. Mechanizmy wycofywania zgody powinny być tak proste, jak mechanizmy wyrażania zgody. Osoby muszą mieć realny wybór w zakresie wyrażenia zgody. Jeśli nie będą mieli wyboru, zgoda nie zostanie uznana za dobrowolną i nie będzie ważna.

**Udostępnianie danych.**
Silne praktyki etyczne i ograniczania ryzyka wykluczają udostępnianie danych bez zgody osób, których te dane dotyczą. Wykluczają również udostępnianie danych stronom, którym nie udzielono dostępu. Jednak efektywne wykorzystanie danych wymaga ich udostępniania - zwłaszcza w erze cyfrowego biznesu, przy rosnącej gospodarce platformowej. Coraz więcej organizacji współpracuje, aby tworzyć nowe oferty, a nawet nowe branże. Współpraca ta wymaga powszechnego i stałego udostępniania danych, przynosząc nowe i trudne do przewidzenia ryzyko. Ryzyko to potęguje fakt, że gdy zbiory danych osiągną wystarczająco duży rozmiar, anonimowość staje się mitem. Gdy agregowane są dodatkowe zbiory danych, osoby można stosunkowo łatwo zidentyfikować (Accenture[7]).

**Algorytmiczna rozliczalność i stronniczość.** Sposoby, w jakie algorytmy klasyfikacji mogą być dostosowywane lub oceniane w celu złagodzenia potencjalnych problemów ze stronniczością lub przejrzystością. Od lat dziesiątki raportów organizacji takich jak ProPublica ujawniają skalę dyskryminacji algorytmicznej w ocenie ryzyka przestępczego, policji predykcyjnej, kredytowaniu, zatrudnianiu i innych dziedzinach.
Stronniczość może być problemem ludzkim, ale wzmocnienie tego zjawiska jest problemem technicznym - matematycznie wytłumaczalnym i kontrolowanym produktem ubocznym szkolenia modeli.

6 https://en.wikipedia.org/wiki/Pathetic_dot_theory
7 https://www.accenture.com/_acnmedia/pdf-22/accenture-data-ethics-pov-web.pdf



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

**To, że algorytm jest sprawiedliwy, nie oznacza, że jest rzetelnie używany.** Praktycy powinni podjąć działania, dokładnie analizując algorytmiczne podejście do łagodzenia uprzedzeń. Naszym obowiązkiem jest krytyczne dojście do tego, kto korzysta z tych technologii, na czyj koszt, i zabranie głosu w sprawie tego, w jaki sposób należy korzystać z naszych modeli.

**Przykłady stronniczości algorytmów**
Oprogramowanie do rozpoznawania twarzy jest coraz częściej wykorzystywane w egzekwowaniu prawa - i jest kolejnym potencjalnym źródłem stronniczości rasowej i płciowej. W lutym tego roku Joy Buolamwini z Massachusetts Institute of Technology odkrył, że trzy najnowsze rozwiązania w zakresie sztucznej inteligencji rozpoznające płeć, pochodzące z IBM Microsoft i chińskiej firmy Megvii, mogą poprawnie zidentyfikować płeć osoby na zdjęciu w 99 procentach przypadków – ale tylko w przypadku białych mężczyzn. W przypadku ciemnoskórych kobiet dokładność spadła do zaledwie 35 procent.
Zwiększa to ryzyko fałszywej identyfikacji kobiet i mniejszości. Ponownie, prawdopodobnie zależy to od danych, na których algorytmy są trenowane: jeśli zawierają znacznie więcej białych mężczyzn niż czarnych kobiet, lepiej będą identyfikować białych mężczyzn. IBM szybko ogłosił, że przekwalifikował swój system na nowy zestaw danych, a Microsoft powiedział, że podjął kroki w celu poprawy dokładności.
Źródło: New Scientist: https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/#ixzz5vqEWBlh2

## 4. ZARZĄDZANIE INFORMACJAMI

Naruszenia danych to problem, dlatego klienci coraz częściej domagają się, aby więcej uwagi poświęcić etyce pracy z danymi, więc musimy potraktować zarządzanie danymi poważniej. Firmy muszą mieć awaryjny plan, ale przede wszystkim powinny zapobiegać takim sytuacjom.

Nie istnieje jedno rozwiązanie, które pasowało by wszystkim firmom I do wszystkich problemów.

Definicja: „… specyfikacja praw decyzyjnych i ram odpowiedzialności w celu zachęcania do pożądanych zachowań w zakresie wyceny, tworzenia, przechowywania, użytkowania, archiwizacji i usuwania informacji.” (Logan, 2010). Innymi słowy, zawiera zestaw zasad i wskazówek dotyczących sposobu przetwarzania danych lub informacji w organizacji. (Cytowany w Rising, Kristensen, Tjerrild-Hansen, 2014)[8]

Cele
1. Maksymalizacja wartości informacji dla organizacji poprzez zapewnienie, że informacje są wiarygodne, bezpieczne i dostępne do podejmowania decyzji
2. Ochrona informacji, aby ich wartość dla organizacji nie została zmniejszona przez technologię lub błąd ludzki, utratę terminowego dostępu, niewłaściwe użycie lub nieszczęśliwe wypadki.

Dlaczego mówimy o zarządzaniu informacją, a nie zarządzaniu danymi?
„Mówiąc wprost, dane odnoszą się do surowych, niezorganizowanych faktów. Pomyśl o danych jak o pakietach wpisów gromadzonych i przechowywanych bez kontekstu. Gdy kontekst zostanie przypisany danym poprzez połączenie dwóch lub więcej elementów w sposób nadający znaczenie, stają się one informacją.” Lebanthal

[8] https://web.stanford.edu/class/msande238/projects/2014/GainIT.pdf



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

**4. Ocena ryzyka**

Ocena ryzyka pomaga zrozumieć obszary, które należy chronić; obszary, w których możesz być najbardziej narażony i potencjalne czarne scenariusze. Zacznij od audytu posiadanych danych I informacji, które są najcenniejsze. Następnie sprawdź, w jaki sposób przechowujesz te dane, kto ma do nich dostęp, i jak są one chronione przez technologię i procesy, aby zrozumieć, gdzie możesz być najbardziej zagrożony. Jeśli nie masz pewności, czy właściwie przeprowadzasz ocenę ryzyka, możesz rozważyć zatrudnienie eksperta, który zrobi to za Ciebie.

**Efektywny plan działania powinien zawierać następujące element:**

- Twoja odpowiedź prawna: musisz opisać, w jaki sposób poradzisz sobie z aspektami prawnymi naruszenia, na przykład informując biuro komisarza ds. Informacji (ICO) o problemie i broniąc swojej firmy przed wszelkimi roszczeniami z tytułu zaniedbania.
- Obsługa zapytań ze strony mediów: Twoja firma może być w centrum uwagi mediów po naruszeniu, więc bądź przygotowany na wszelką komunikację zewnętrzną na temat tego, co się stało i jak sobie z tym poradzisz. Prawdopodobnie będziesz potrzebował doświadczenia i wiedzy w zakresie PR, aby to zrobić skutecznie.
- Dowiedz się, co się wydarzyło: musisz mieć pod ręką ekspertów kryminalistyki IT, aby dowiedzieć się, co spowodowało naruszenie; aby szybko naprawić problem i upewnić się, że się nie powtórzy.
- Informuj klientów: w zależności od bazy klientów i skali naruszenia możesz otrzymać wiele nieprzyjemnych telefonów! Musisz być przygotowany na efektywne zarządzanie tą formą komunikacją.

**ZWRÓĆ UWAGĘ**
**Cyberbezpieczeństwo**

Jeśli masz do czynienia z konsekwencjami naruszenia ochrony danych, twoją ostatnią linią obrony jest wodoszczelna i specjalistyczna polisa ubezpieczenia cybernetycznego. Ubezpieczając cię za ewentualne naruszenie przepisów o ochronie danych (jeżeli prawo na takie ubezpieczenie zezwala) i twoją odpowiedzialność za przetwarzanie danych, może również zapewnić ochronę przed wymuszeniem, kosztami naprawy systemu, a także wydatkami PR i stratami finansowymi z powodu przestoju systemu.

**Niektóre kluczowe aspekty, na które należy zwrócić uwagę, to:**

- Biuro komisarza ds. Informacji (ICO) może nałożyć grzywny w wysokości do 500 000 funtów za naruszenie ustawy o ochronie danych. Polisa ubezpieczenia cybernetycznego Digital Risks pokryje koszty powiadomień, opłaty prawne, a w niektórych przypadkach samą karę (jeżeli jest to prawnie ubezpieczone).
- Pokryje koszty, które mogą obejmować koszty naprawy systemu, utracone dochody, gdy system jest wyłączony, a nawet płatności okupu dla hakerów.
- Ochroni Twoją witrynę, blogi i media społecznościowych pod kątem naruszenia praw autorskich lub znaków towarowych, zniesławienia itp.



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

# STUDIUM PRZYPADKU



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej.
Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

CYBERNET SECURITY CENTER
UNDER THE MINISTRY OF
DEFENSE

GENERATION DATA
USING DATA FOR PROFIT

# BEZPIECZEŃSTWO W SERWISIE FACEBOOK

## Studium przypadku bezpieczeństwa w serwisie Facebook


**Dlaczego Twoje dane osobowe mogą być przydatne?**

• Dają bezpośrednie informacje o Tobie:

o kontakty; o zdjęcia; o inne dane (gdzie byłeś, kiedy, gdzie mieszkasz, gdzie pracujesz, jakie są Twoje zainteresowania itd.);

• Dają informacje na temat osób, z którymi się komunikujesz;

• Pozwalają na wystawianie fałszywych ocen, komentarzy;



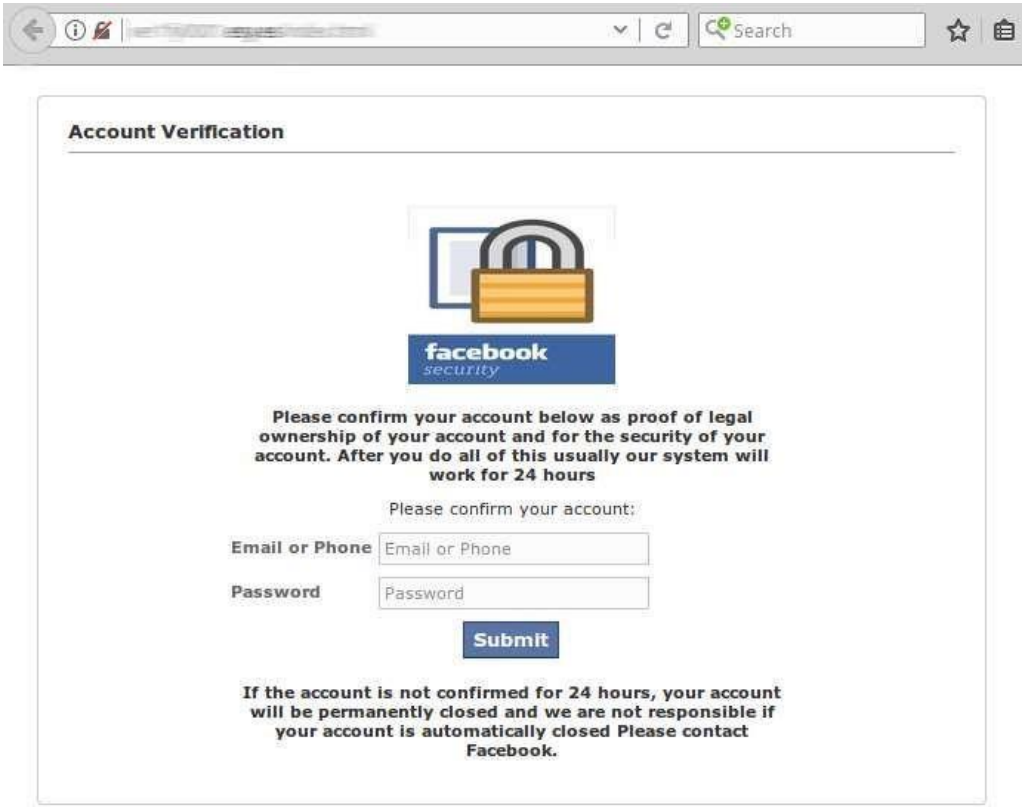
Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

• Pozwalają na administrowanie stronami i grupami, którymi zarządzasz na Facebooku.

Szczególną uwagę przywiązuje się do grup, stron i osób na Facebooku - zwłaszcza tych, które mają znaczną liczbę obserwujących. Skradzione strony i konta Facebooka są złośliwie sprzedawane stronom trzecim, wykorzystywane w celach reklamowych i innych.

**W jaki sposób przechwytywane są konta na Facebooku?**

• Najczęściej kradzione są konta chronione hasłem;
• Dane logowania pochodzą z innych źródeł (e-mail, inne konta online);
• Dane logowania są gromadzone na urządzeniach publicznych i publicznie dostępnych bezpłatnych sieciach bezprzewodowych (darmowe Wi-Fi);
• Login skradziony przez socjotechnikę (wysyłając fałszywe e-maile z linkami do phishingu na Facebooku)




**Rysunek 1**. Przykładem inżynierii społecznej jest fałszowanie stron



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

Odpowiedzialność za nieautoryzowane logowanie do konta Facebook.

Odpowiedzialność za takie działania została opisana w art. 198 1 (1) i 198 2 (1) Kodeksu karnego Republiki Litewskiej.

*Artykuł 198 1. Nielegalny dostęp do systemu informacyjnego*

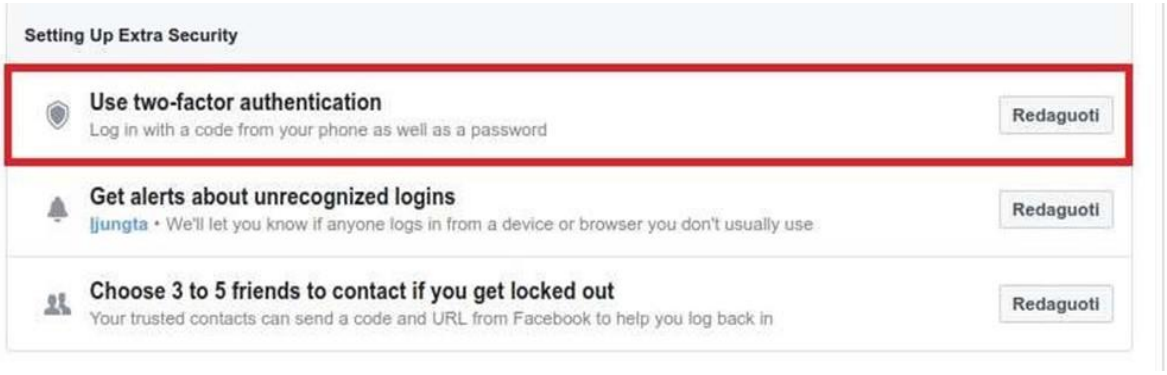
*Kto nielegalnie uzyskał dostęp do systemu informatycznego lub jego części naruszając środki bezpieczeństwa systemu informacyjnego podlega karze robót publicznych lub grzywien, aresztowaniu lub pozbawieniu wolności na okres do dwóch lat.*

*Artykuł 198 2. Nieuprawnione usuwanie urządzeń, oprogramowania, haseł, kodów i innych danych*

*Każdy, kto do celów przestępczych lub w inny sposób wyprodukował, przetransportował, importował, sprzedawał, udostępniał lub w inny sposób rozpowszechniał, nabywał lub posiadał urządzenia lub oprogramowanie bezpośrednio przeznaczone lub przystosowane do popełniania przestępstw, a także hasła, kody lub inne podobne dane do logowania do systemu informacyjnego lub jego części, podlega karze robót publicznych, grzywny lub karze więzienia na okres do trzech lat.*

Zalecenia dotyczące zapobiegania włamaniom

- Użyj bezpiecznego hasła (zaleca się, aby hasło składało się z co najmniej 9 znaków, w tym wielkich i małych liter, cyfr i znaków interpunkcyjnych);
- Nie ujawniaj nikomu swojego hasła;
- Nie używaj tego samego hasła, którego używasz do innych kont;
- Nie loguj się na swoje konto na urządzeniach publicznych;
- Unikaj umieszczania nadmiernych informacji w sieciach społecznościowych;
- Użyj uwierzytelniania dwuskładnikowego (Ustawienia ➔ Bezpieczeństwo i logowanie)




**Rysunek 2.** Skonfiguruj uwierzytelnianie dwuskładnikowe



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

- Skonfiguruj, aby odbierać wiadomości e-mail. Powiadamiaj o nieudanych logowaniach do swojego konta (Ustawienia ➔ Bezpieczeństwo i logowanie).

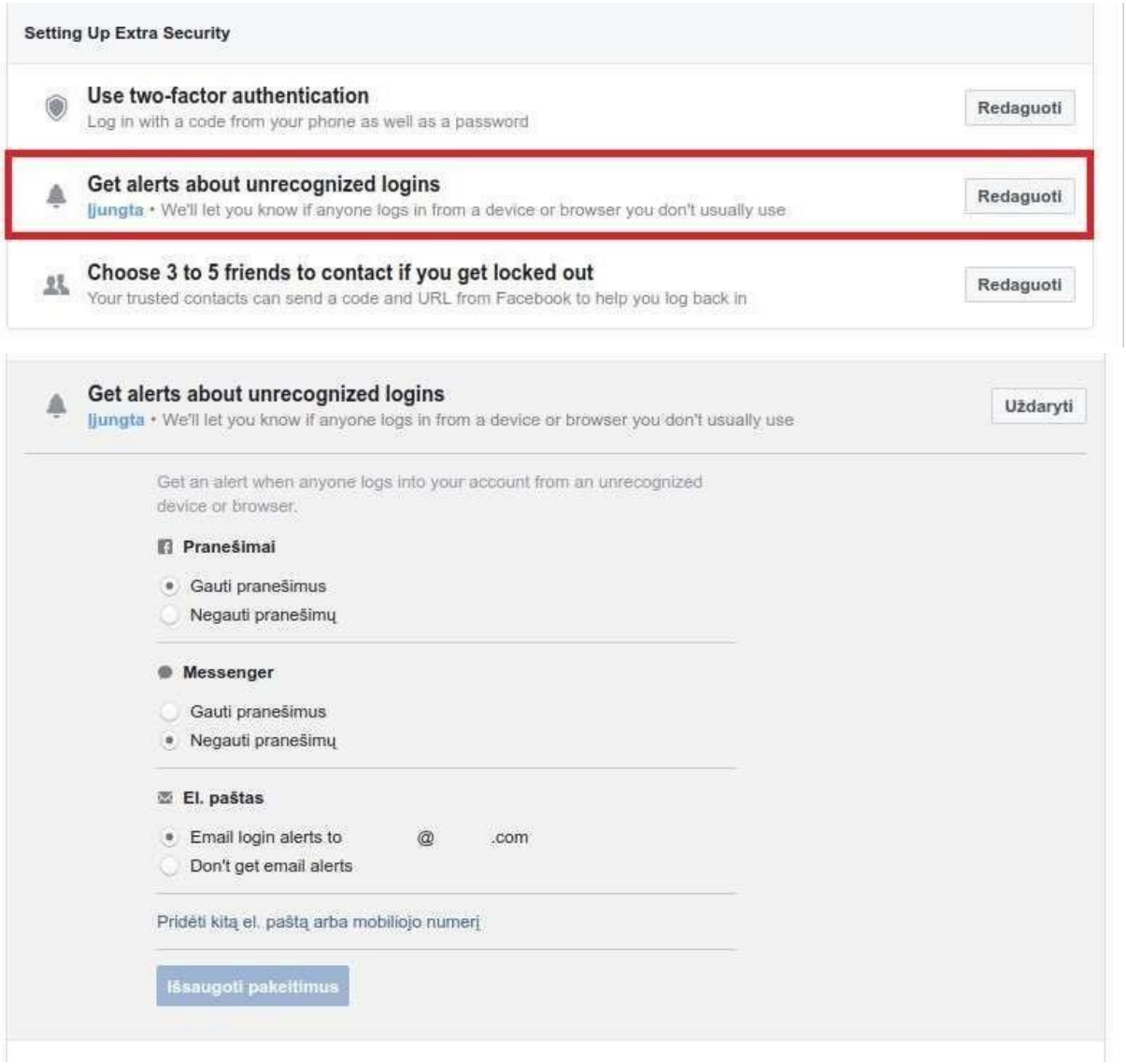



**Figure 3**. Powiadomienia o nieudanym logowaniu do konta

Co powinienem zrobić, jeśli zauważę podejrzaną aktywność lub stracę konto na Facebooku?
Jeśli podejrzewasz, że osoby trzecie uzyskały dostęp do Twojego konta:
• Zmień swoje hasło tak szybko, jak to możliwe;



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

• Sprawdź podejrzane połączenia (Ustawienia ➔ Zabezpieczenia i połączenia), odłącz następujące urządzenia, gdy zostaną zauważone:


**Rysunek 4.** Urządzenia, które są podłączone do Twojego konta

- Jeśli nie możesz się zalogować, spróbuj odzyskać hasło przy pomocy wiadomości e-mail.
- Możesz zgłosić utracone konto na stronie https://www.facebook.com/hacked
- Jeśli nie możesz odzyskać konta, możesz skontaktować się z instytucją porządku publicznego



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

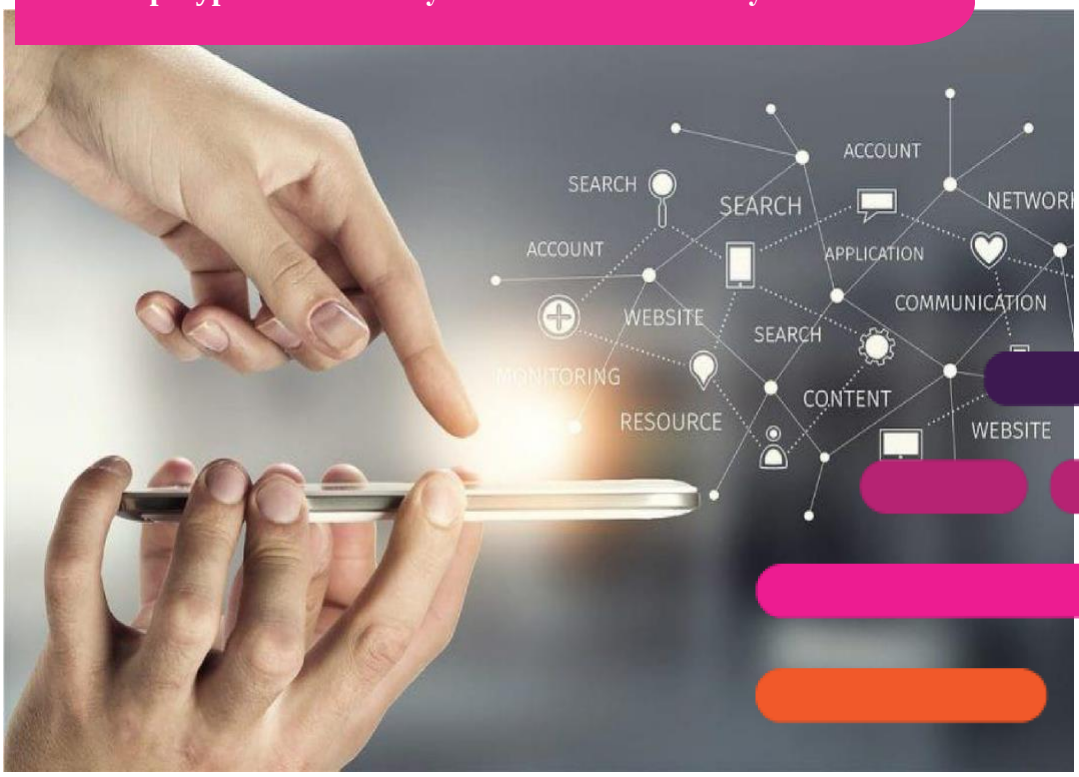
GENERATION DATA

USING DATA FOR PROFIT

CYBERNET SECURITY CENTER
UNDER THE MINISTRY OF DEFENSE

# WYSYŁANIE WIADOMOŚCI MAILOWYCH ZE SZKODLIWYM OPROGRWAMOWANIEM DO FIRM NA LITWIE

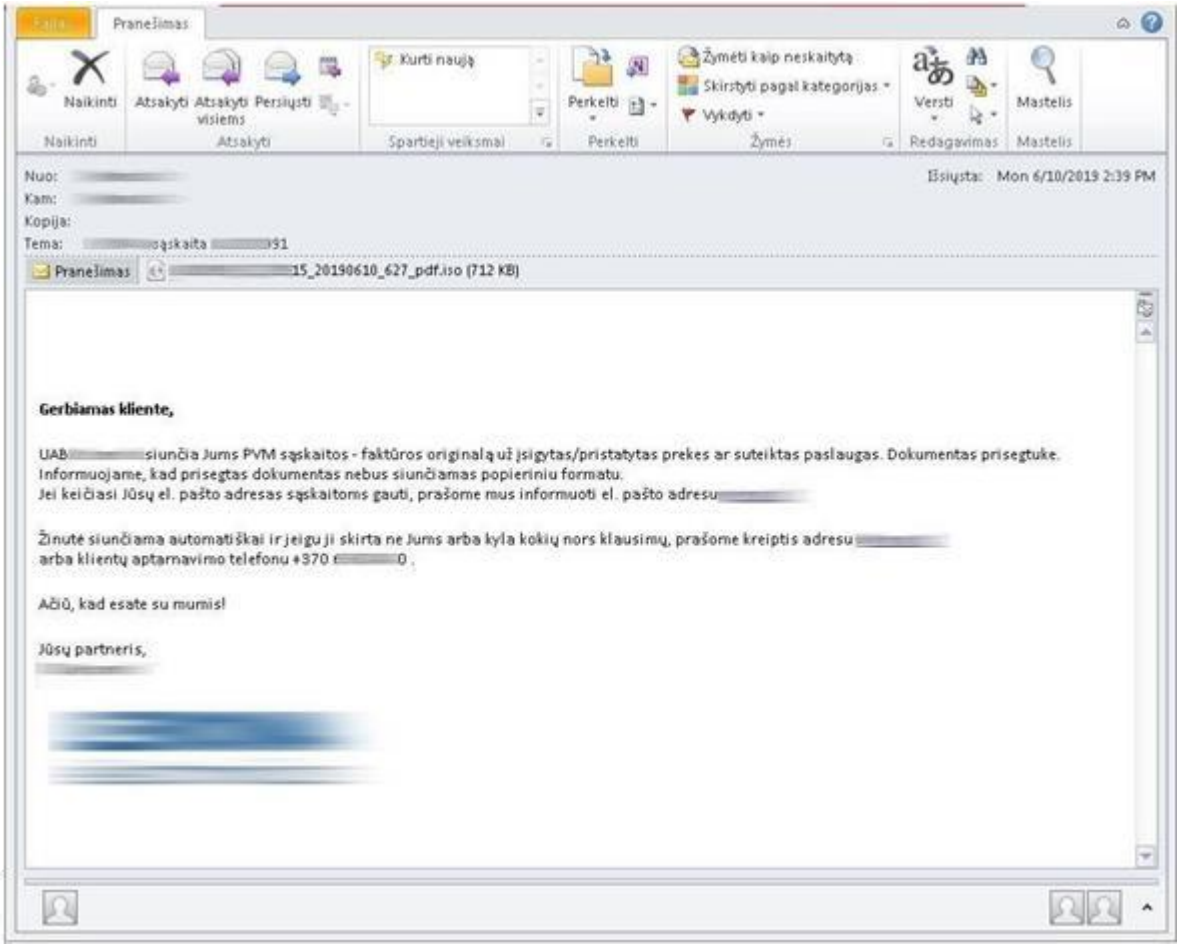
**Studium przypadku szkodliwych wiadomości mailowych**






Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

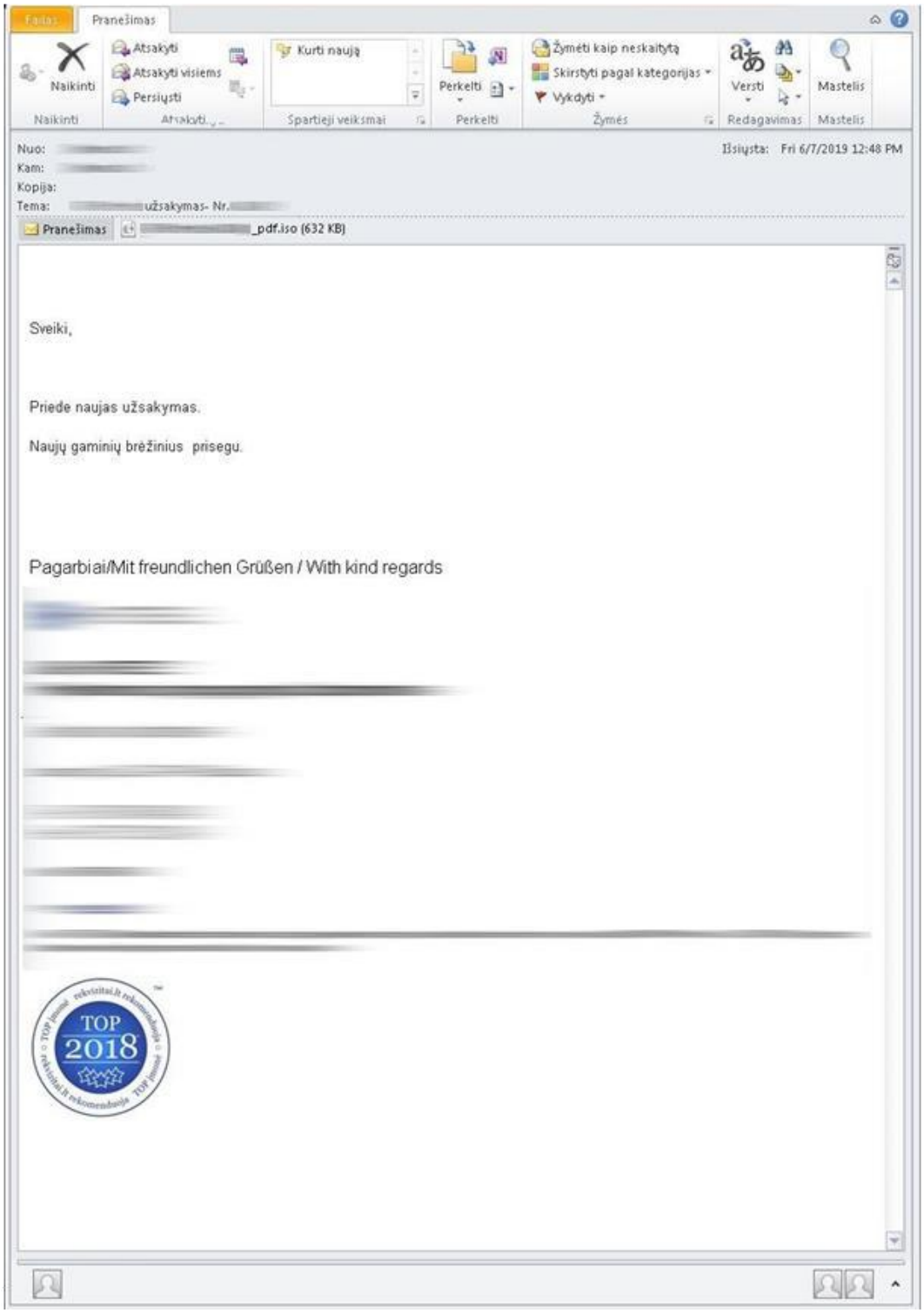
Narodowe Centrum Bezpieczeństwa Cybernetycznego przy Ministerstwie Obrony Narodowej informuje, że na Litwie rozpowszechniane są wiadomości e-mail ze złośliwym kodem. W ostatnich dniach Centrum odnotowało przypadki fałszowania wiadomości e-mail znanych firm litewskich i zagranicznych, adresów e-mail, ich logo i informacji kontaktowych.




**Rysunek 1**. Fałszywy e-mail jako przykład listu symulującego dostawcę



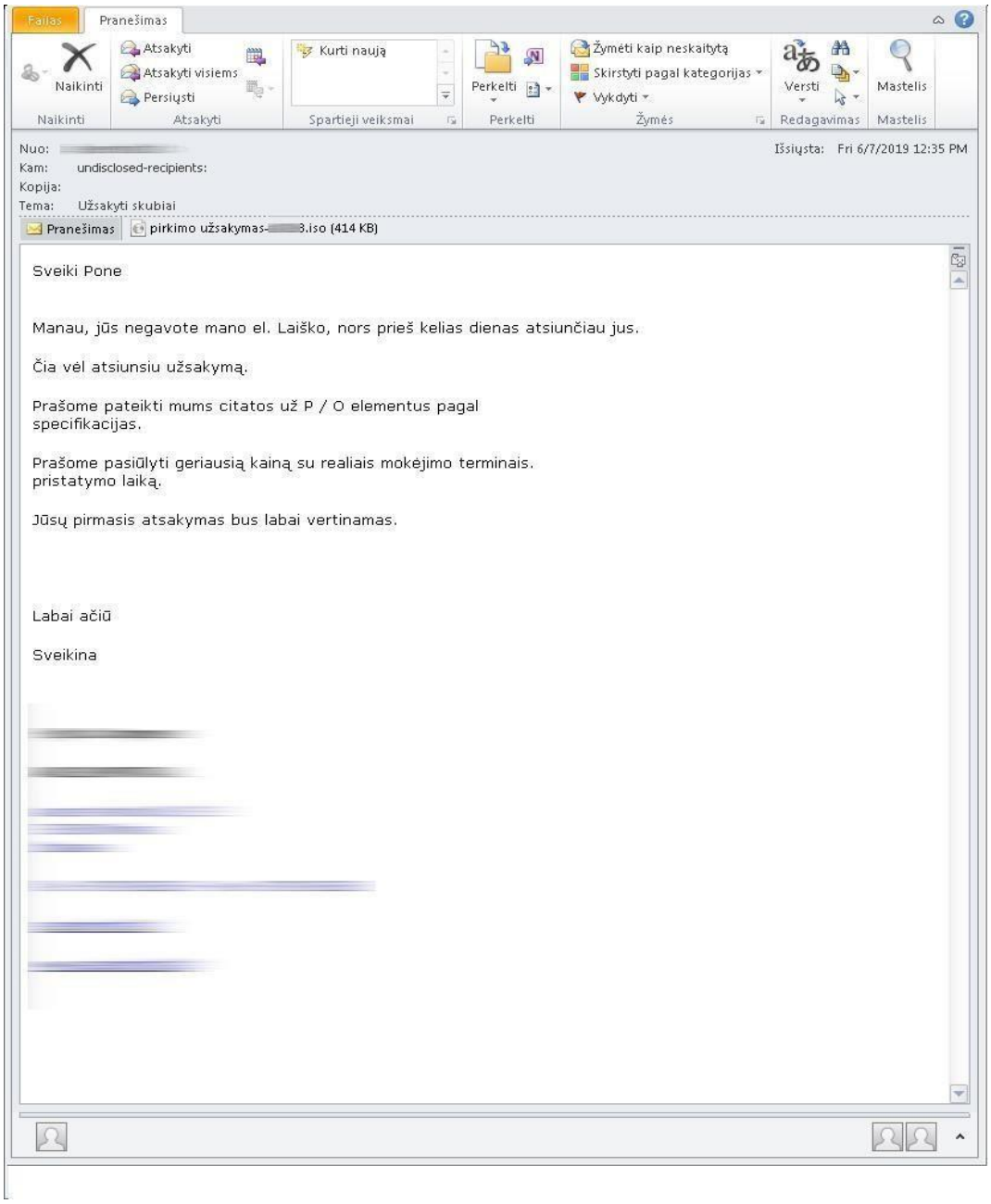
Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.




**Rysunek 2.** Fałszywy e-mail jako przykład listu symulującego dostawcę



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.




**Rysunek 3**. Fałszywy e-mail jako przykład listu symulującego dostawcę

Złośliwy kod jest przechowywany w plikach .iso dołączonych do wiadomości e-mail. Załączony plik zawiera plik wykonywalny .exe. Po otwarciu załącznika i uruchomieniu pliku wykonywalnego .exe złośliwe oprogramowanie próbuje zebrać osobiste dane użytkownika z komputera, pobiera nazwę komputera, próbuje ustalić, czy dostęp do komputera można uzyskać zdalnie (lub włączyć funkcję Pulpitu zdalnego) i wysyła informacje do zdalnego serwera.



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.

Tekst listu jest zwykle pisany w języku litewskim. Wiadomość wydaje się realistyczna dla odbiorcy, ponieważ jest wysyłana od znanego i zaufanego adresata, ale w rzeczywistości jest sfałszowana.

**Rekomendacje**

Sprawdź nagłówek wiadomości, aby zobaczyć, kto jest prawdziwym nadawcą wiadomości (pole „from"). Analizując nagłówek, należy spojrzeć na pierwszy od dołu parametr „Received". Ten parametr powie Ci, z którego serwera wysłano wiadomość e-mail. Jeśli pole „From" to sender@imone.com, pole „Received" powinno również zawierać adres „imone.com". W przypadku tego oszustwa pole „Received" pokazuje zupełnie inne dane niż miejsce, z którego wiadomość została wysłana. Zobacz także: rysunek. 4.


**Rysunek 4**. Fałszywy e-mail, prawdziwy nadawca wiadomości

W zależności od klientów poczty e-mail, możliwość wyświetlania nagłówków jest różna. Pamiętaj, że cyberprzestępcy regularnie rozpowszechniają również inny złośliwy kod, który wykorzystuje luki w zabezpieczeniach różnych programów, więc zalecamy regularną aktualizację programu antywirusowego, systemu operacyjnego i innego oprogramowania, którego używasz.

Aby zapobiec spamowi, zalecamy włączenie i prawidłowe skonfigurowanie funkcji SPF (Sender Policy Framework). Z tej funkcji należy korzystać z większą ostrożnością, ponieważ nieprawidłowe ustawienia mogą powodować, że niektóre wiadomości nie będą dostarczane do adresatów.

Przypominamy, że kluczem jest nieustanne zwracanie uwagi i krytyczne podejście do poczty przychodzącej.



Projekt został zrealizowany przy wsparciu finansowym Komisji Europejskiej. Niniejsza publikacja odzwierciedla jedynie poglądy autora, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie zawartych w niej informacji.