Systemy Logistyczne Wojsk nr 44/2016

DYNAMIKA CYBERPRZESTĘPSTW I ICH SKUTKI PRAWNE DLA PRZEDSIĘBIORSTW

THE DYNAMICS OF CYBERCRIME AND ITS LEGAL CONSEQUENCES FOR COMPANIES

Remigiusz Kozłowski
remigiuszk@poczta.fm

Rafał Adamek
r_adamek@toya.net.pl

Jakub Jabłoński
jablon.jak@gmail.com

Uniwersytet Łódzki
Wydział Zarządzania
Katedra Logistyki

Streszczenie: Współczesny świat w coraz większym stopniu opiera się na elektronicznym przepływie informacji. Polska nie jest tu wyjątkiem. Technologia ta to jednak nie tylko korzyści ale także zagrożenia. Cyberprzestępstwa stanowią poważny i rosnący problem, z którym muszą się zmierzyć zarówno system prawny poszczególnych krajów jak i wspólnot międzynarodowych, a także osoby prywatne i przedsiębiorstwa. Celem artykułu jest przedstawienie specyfiki i skali problemów przedsiębiorstw związanych z cyberprzestępczością ze szczególnym uwzględnieniem kradzieży danych objętych ustawą o ich ochronie.

Abstract:. The modern world increasingly relies on electronic information flow. Poland is no exception. This technology brings not only the benefits but also risks. Cybercrimes are a serious and growing problem, that must be faced by both legal systems of countries and international communities as well as individuals and businesses. The aim of this article is to present the specific nature and scale of problems related to businesses cybercrime, with special regard to data theft protected by the law of their protection.

Słowa kluczowe: cyberprzestępstwa, bezpieczeństwo danych, cyberbezpieczeństwo.

Key words: cybercrime, data security, cybersecurity.

1.WSTĘP

Gospodarki wszystkich krajów coraz bardziej opierają się na elektronicznym przepływie informacji. Można stwierdzić, że dalszy rozwój przedsiębiorstw a dzięki temu także całych gospodarek jest uwarunkowany zapewnieniem bezpieczeństwa obrotu gospodarczego opartego na wykorzystaniu nowych technologii teleinformatycznych. W nowoczesnych rozwiązaniach stosowanych m.in. w łańcuchach dostaw koniecznością staje się coraz szersze korzystanie z technologii informatycznych w celu sprostania wyzwaniom coraz bardziej konkurencyjnego rynku (Kochański, 2014). Nowe technologie niosą ze sobą nie tylko korzyści ale także powodują szereg problemów (Kozłowski, Matejun, 2015). Cyberprzestępstwa stanowią poważny i rosnący problem, z którym muszą się zmierzyć zarówno system prawny

poszczególnych krajów jak i wspólnot międzynarodowych. Przestępstwa takie jak np. nielegalne przejęcie i upublicznienie danych objętych ustawą o ochronie danych osobowych mogą w bardzo istotny sposób zaszkodzić przedsiębiorstwu.

Celem artykułu jest przedstawienie specyfiki i skali problemów przedsiębiorstw związanych z cyberprzestępczością ze szczególnym uwzględnieniem kradzieży danych objętych ustawą o ich ochronie.

Artykuł został przygotowany w oparciu o przegląd wybranych pozycji literatury przedmiotu oraz analizy raportów Komendy Głównej Policji, Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz raporty firm konsultingowych badających zjawiska cyberprzestępstw w skali globalnej. Analizy tych raportów zostały wzbogacone informacjami z praktyki gospodarczej. Na podstawie tak zebranych informacji oraz analiz sformułowano wnioski i zalecenia do zastosowania w celu ograniczenia zjawiska cyberprzestępczości.

1. ZAKRES DANYCH OBJĘTYCH OCHRONĄ, ADMINISTROWANIE NIMI I SKUTKI ZANIEDBAŃ

Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6 ust. 1 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych). Artykuł 7 pkt. 4 ustawy o ochronie danych osobowych definiuje administratora danych jako organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 tejże ustawy decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych może być zatem podmiot niepubliczny realizujący zadania publiczne, osoba fizyczna lub prawna, jednostki organizacyjne niebędące osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Mając na uwadze powyższe niniejsza ustawa wskazuje, iż każdy z przedsiębiorców jest administratorem danych, a dane którymi administruje i podlegają ochronie ustawowej to między innymi dane zarówno pracownicze jak i dane fizycznych kontrahentów.

Administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą (art. 26 ust. 1 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych). W niniejszej ustawie zawarto także konsekwencje zaniedbań w ochronie danych:

- „kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega

grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2" (ust. 1 art. 51 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych) ,

- „jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku" (ust. 2 art. 51 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych),
- „Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku" (art. 52 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych).

Zatem każdy administrator danych jest ustawowo związany odpowiedzialnością karną, za zabezpieczenie ich przez osobami nieuprawnionymi w tym również kradzieżą czy potocznie zwanym „wyciekiem". Administrator danych w tym również każdy przedsiębiorca zgodnie z art. 31 ust. 1 ustawy – może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie posiadanych przez siebie danych. Tym samym cedując odpowiedzialność za ich bezpieczeństwo na związany pisemną umową podmiot.

Kierując się powyższym chronionymi danymi przechowywanymi przez przedsiębiorców są informacje dotyczące ich kontrahentów w tym zawartych z nimi umów ale również dane zarówno pracowników. Pociągnięcie do odpowiedzialności karnej przedsiębiorcy za niedopełnienie nałożonych analizowaną ustawą obowiązków dotyczących dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, mogą skutkować zasądzeniem grzywny oraz finansowych zadośćuczynień. Skutki tego w szczególność dla małych i średnich firmach mogą być bardzo dotkliwe a nawet powodować ich upadek. Rozpoczęcie postępowania przygotowawczego, przez organy ścigania w kierunku wymienionych wyżej przepisów art. 51 i art. 52 analizowanej ustawy, nie tylko może wygenerować koszty w postaci grzywien i pieniężnego zadośćuczynienia ale również koszty adwokackie jak i sądowe.

2. ZNACZENIE OCHRONY DANYCH DLA FUNKCJONOWANIA I ROZWOJU PRZEDSIĘBIORSTW

Przedsiębiorstwo, tak jak prywatny użytkownik danych zobowiązane jest do przestrzegania przepisów przedstawionych w pierwszym podrozdziale niniejszego artykułu. Jest to o tyle ważne, że w przypadku firm zakres danych jest o wiele większy, niż w przypadku osoby prywatnej, a utrata danych będzie o wiele dotkliwsza.

W dobie powszechnego dostępu do Internetu, przesyłania wszystkich dokumentów drogą elektroniczną czy też ich archiwizacji w postaci „chmury", bezpieczeństwo danych stało się elementem przewagi konkurencyjnej firmy. Dane osobowe stały się też jednym z celów działalności przestępczości cybernetycznej.

Elementem zwiększającym przewagę konkurencyjną jest w pierwszej kolejności zadowolenie klienta oraz zaufanie jakim darzy organizację. Klient, udostępniając swoje dane osobowe, chce być przekonany, że te dane poufne nie zostaną przekazane osobom trzecim. Utrata takich danych niesie ze sobą ogromny, negatywny wpływ na wizerunek firmy oraz zaufanie klienta. Jest to o tyle ważne, że według badań Komisji Europejskiej, przeprowadzonych w 2015 roku, jedynie 15% badanych osób uważa, że ma całkowitą kontrolę nad swoimi danymi, natomiast nawet 31% jest zdania, że nie ma żadnej kontroli (Special Eurobarometer 431 – Data Protection).

Kolejna możliwość uzyskania lub stracenia, przewagi konkurencyjnej to własne dane, przepisy, rozwiązania czy know-how firmy. Mogą one stać się celem szpiegostwa gospodarczego (Latusek-Jurczak, 2012). Wiele organizacji posiada tajemnice handlowe, które przyczyniają się do utrzymania lepszej pozycji na tle konkurentów. Takie firmy mogą stać się celem ataków nieuczciwego konkurenta, bądź hakera, a nawet nielojalnego pracownika, który będzie chciał następnie sprzedać zdobyte dane. Znany jest przypadek, gdy jeden z pracowników Coca-Coli usiłował sprzedać jej tajny przepis firmie Pepsi. Pepsi natychmiast powiadomiło swojego konkurenta oraz FBI (www.foxnews.com). Na szczęście jej główny konkurent okazał się uczciwy, ale w innym wypadku taki przeciek, nieudaremniony, może doprowadzić nawet do upadku firmy.

W dzisiejszym świecie na popularności, w ogromnym stopniu zyskały formy elektronicznych narzędzi komunikacji. Upowszechniły się one już nie tylko wśród prywatnych użytkowników Internetu, ale również wśród firm. Wiadomości elektroniczne, takie jak e-mail zastąpiły już niemal całkowicie starsze formy, takie jak listy oraz faksy, a częściowo nawet rozmowę telefoniczną. Często pracownicy jednego projektu nie widząc się na własne oczy, przesyłają między sobą dane za pomocą różnego rodzaju komunikatorów lub w postaci wideokonferencji. To upowszechnienie się tej formy komunikacji stwarza niebezpieczeństwo utraty przesyłanych danych. Wielu użytkowników nieświadomie zamieszcza treści, które mogą zostać wykorzystane w niewłaściwy sposób. Wielokrotnie, nie zdają sobie sprawy, z faktu, że dane te mogą łatwo zostać przejęte. U wielu osób, na ich skrzynce internetowej da się odnaleźć numer PESEL, numery dowodów, adres zamieszkania, wiele haseł do innych portali czy nawet numer oraz PIN karty kredytowej. To samo odnosi się do kont firmowych. Wiele

firm organizuje z tego powodu specjalne szkolenia dla pracowników, mające zwiększyć ich świadomość. Najprostszym sposobem zabezpieczenie, może być użycie szyfrowanych połączeń, ale nie jest to rozwiązanie w 100% skuteczne.

3. CHARAKTERYSTYKA PRZESTĘPCZOŚCI KOMPUTEROWEJ – WYBRANE PRZYKŁADY

Najczęściej wśród przestępczości komputerowej występuje oszustwo komputerowe. Artykuł 287 Kodeksu Postępowania Karnego definiuje je jako: „Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5" (Kodeks Karny art. 287 § 1). W wypadku mniejszej wagi przestępstwa tego typu, sprawca podlega tylko grzywnie albo karze ograniczenia wolności lub jej pozbawienia do roku (Kodeks Karny art. 287 § 2). Natomiast w sytuacji, gdy oszustwo komputerowe zostało popełnione na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego (Kodeks Karny art. 287 § 3).

Najczęściej spotykanymi sytuacjami problemowymi, które dotyczą administratorów danych osobowych są kolokwialnie zwane „kłopotliwe zwolnienia pracownicze". I nie dotyczy to tylko i wyłącznie zwolnienia pracowników mających bezpośredni dostęp do informacji chronionych ustawą o ochronie danych czyli zatrudnionych jako kadra kierownicza, na stanowisku księgowej lub w dziale human resources (HR). W obecnym czasie, gdy dostęp do technologii teleinformatycznych jest powszechny i swobodny dotyczy to niemal każdego pracownika firmy. Przeważnie takie osoby nie mają podpisanych stosownych aneksów do umów o pracę, dotyczących danych osobowych chronionych ustawą, a dokładnie umów mających na celu zabezpieczenie pracodawcy w jedyny możliwy w tym przypadku sposób – zabezpieczeniem finansowym. Zgodnie z obowiązującym prawem za kolokwialnie tzw. „wyciek danych osobowych", nawet jeżeli sprawcą będzie pracownik firmy – odpowiada administrator tych danych, którym przeważnie jest pracodawca.

Ustawa o ochronie danych osobowych nie mówi nic na temat przestępczego wejścia w posiadanie danych chronionych tą ustawą a co za tym idzie zwolnienia z odpowiedzialności za ich udostępnienie osobom nieupoważnionym, nawet w przypadku ich utraty w przestępczy sposób. Przykładowo pracodawca, który jest administrator danych osobowych, poniesie od-

powiedzialności zgodnie z ustawą w sytuacji, w której zwolniony pracownik, po uprzednim wejściu w sposób legalny, np. pracownik HR kopiujący sobie dane wszystkich pracowników lub w sposób nielegalny, dowolny inny pracownik przełamujący zabezpieczenia informatyczne firmowych komputerów lub instalujący program szpiegowski na firmowym komputerze, wszedł w posiadanie danych osobowych chronionych ustawą a następnie udostępni takie dane na zewnątrz firmy. Nieważnym w tym przypadku będzie fakt wykorzystania udostępnionych danych przez osoby trzecie, czytać nieupoważnionym, które nie mają prawa zaznajamiać się z udostępnionymi danymi - zgodnie z ust. 1 art. 51 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, istotą przepisu jest samo umożliwienie dostępu do danych chronionych ustawą osobą nieupoważnionym a nie ich wykorzystanie czy to w sposób legalny czy nielegalny.

Poniżej zostanie wykazany stopień zagrożenia zaistnieniem takiej sytuacji. Odchodzący pracownik wykorzystuje w celu zaszkodzenia swojemu pracodawcy kopiuje posiadaną przez niego bazę pracowniczą, łącznie z danymi chronionymi ustawą i udostępnia tak sklonowaną bazę udostępnia na stronach internetowych. W obecnych czasach ludzie często są „słabi moralnie" i zachowują się nieetyczne, prymitywnie „odgrywając się" na byłym pracodawcy.

Udostępnienie danych pracowników firmy na stronach internetowych przez zwolnionego pracownika w tym również własnych danych, tak by nie rzucać na siebie podejrzeń, powoduje nieuchronne konsekwencje finansowe, a w najgorszym wypadku jeszcze prawne. Obecnie umieszczenie danych w Internecie w sposób taki by nie można było ustalić skąd te dane zostały umieszczone nie jest czymś skomplikowanym – wystarczy skorzystać z serwerów Proxy, stron należących do państw wschodnich lub ogólnodostępnej sieci Wi-Fi np. hipermarketu.

Po ujawnieniu opisywanego wcześniej wycieku danych sytuacja może rozwinąć się w dwojaki sposób. Właściciel danych może skontaktować się z administratorem tych danych i podjąć rozmowy dotyczące materialnego zadość uczynienia takiemu incydentowi – tym samym uzgadniając, iż w przypadku wszczęcie postępowania karnego z art. 51 ust. 1 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oświadczy, iż dane te umieścił tam sam jaki ich właściciel. Ta umowa, jest jedynie dżentelmeńską umową – która w żaden sposób nie może być potwierdzona pisemnie z uwag na fakt, iż sporządzenie pisemnej umowy dotyczącej powyższego załatwienia sprawy, jest jednoznacznym przyznaniem się do naruszenia przepisów ustawy o ochronie danych osobowych – takie rozwiązanie może okazać się

najmniej kosztowne w przypadku dobrze prowadzonej firmy i pozytywnych relacji pomiędzy pracownikiem a pracodawcą.

Zgodnie z art. 304 par. 1 KPK – każdy dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu ma społeczny obowiązek zawiadomić o tym Prokuratora lub Policję (Ustawa z dnia 6 czerwca 1997 r - Kodeks Postępowania Karnego). Przestępstwem ściganym z urzędu jest określone w art. 51 ust. 1 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Tak złożone zawiadomienie wszczyna postępowanie sprawdzające, które w późniejszym etapie przechodzi w postępowanie przygotowawcze. W momencie przejścia postępowania sprawdzającego w przygotowawcze, administrator danych, który nie zachował należytych środków i starań do zabezpieczenia tych informacji po pewnym czasie stanie się stroną postępowania - to jest osobą podejrzaną, której przedstawiono zarzut z art. 51 ust. 1 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Przedstawienie zarzutu skutkować może, zgodnie z wskazaną karą przytaczanego przepisu grzywną, ograniczeniem lub pozbawieniem wolności oraz, w zależności od wniesionych roszczeń przez osoby, których dane zostały udostępnione osobą nieupoważnionym, określeniem kary nawiązki na korzyść tych osób.

W celu uniknięcia powyżej scharakteryzowanych sytuacji większość umów zawartych z pracownikami, którzy mają dostęp do poufnych informacji firmy w tym danych osobowych chronionych ustawą zawierają klauzulę art. 100 par. 2 pkt 4 Kodeksu Pracy - dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę – zwane potocznie „lojalki", które przy średniej klasy prawniku ze strony pracownika nic nie znaczą, a wyciągnięcie na podstawie tak zawartej umowy konsekwencji prawnych jest praktycznie niemożliwe. Wystarczy, że pracownik wykaże, iż zaczerpnął informacje z innego źródła np.: Internetu i cała mistyczna osłona pracodawcy określona w art. 100 par. 2 pkt 4 Kodeksu Pracy (www.prawo.money.pl) rozmywa się jak mgła.

Jedynym skutecznym rozwiązaniem są umowy cywilnoprawne zawierane na zasadach określonych w Kodeksie Cywilnym w części: Wykonanie zobowiązań i skutki ich niewykonania (Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny, www.prawo.money.pl). Tak zawarte umowy, jednoznacznie określają odpowiedzialność stron umowy za niedotrzymanie jej warunków a w ich zakresie może znajdować się wszystko w granicach polskiego prawa np. jednoznaczne określenie konsekwencji za określone zachowania w tym wykorzystanie danych, również danych chronionych ustawą należących do pracodawcy – administratora danych.

4. DYNAMIKA ANALIZOWANYCH PRZESTĘPSTW W ŚWIETLE DANYCH POLICJI

Według danych Komendy Głównej Policji za okres od 2004 do 2014 roku dotyczących przestępczości komputerowej, w tym oszustw komputerowych wskazują wzrost oszustw komputerowych aż o 552 % (www.statystyka.policja.pl). W poniższej tabeli zamieszczono szczegółowe dane dotyczące powyżej wymienionych przestępstw w podziel na poszczególne lata.

Tabela 1. Liczba postępowań wszczętych oraz stwierdzonych przestępstw w latach 2004 – 2014

ROK	liczba postępowań wszczętych	liczba przestępstw stwierdzonych
2004	229	390
2005	326	568
2006	285	444
2007	322	492
2008	472	404
2009	673	978
2010	838	623
2011	1012	1364
2012	1285	1351
2013	1768	1573
2014	2567	2154

Źródło: Ststystyka Policji, za: www.statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63977,Oszustwo-komputerowe-art-287.html z dn. 01.05.2016

Analizując dane w powyższej tabeli należy podkreślić, że przestępstwa stwierdzone to ogół czynów, których charakter jako przestępstw został potwierdzony w wyniku postępowania przygotowawczego. Natomiast postępowania wszczęte to postępowanie w którym organ ścigania wydał postanowienie o wszczęciu postępowania przygotowawczego (www.prawo.wiedza.diaboli.pl). Dodatnia różnica pomiędzy ilością postępowań wszczętych a stwierdzonych bierze się z faktu, iż w jednym wszczętym postępowaniu może być zawartych

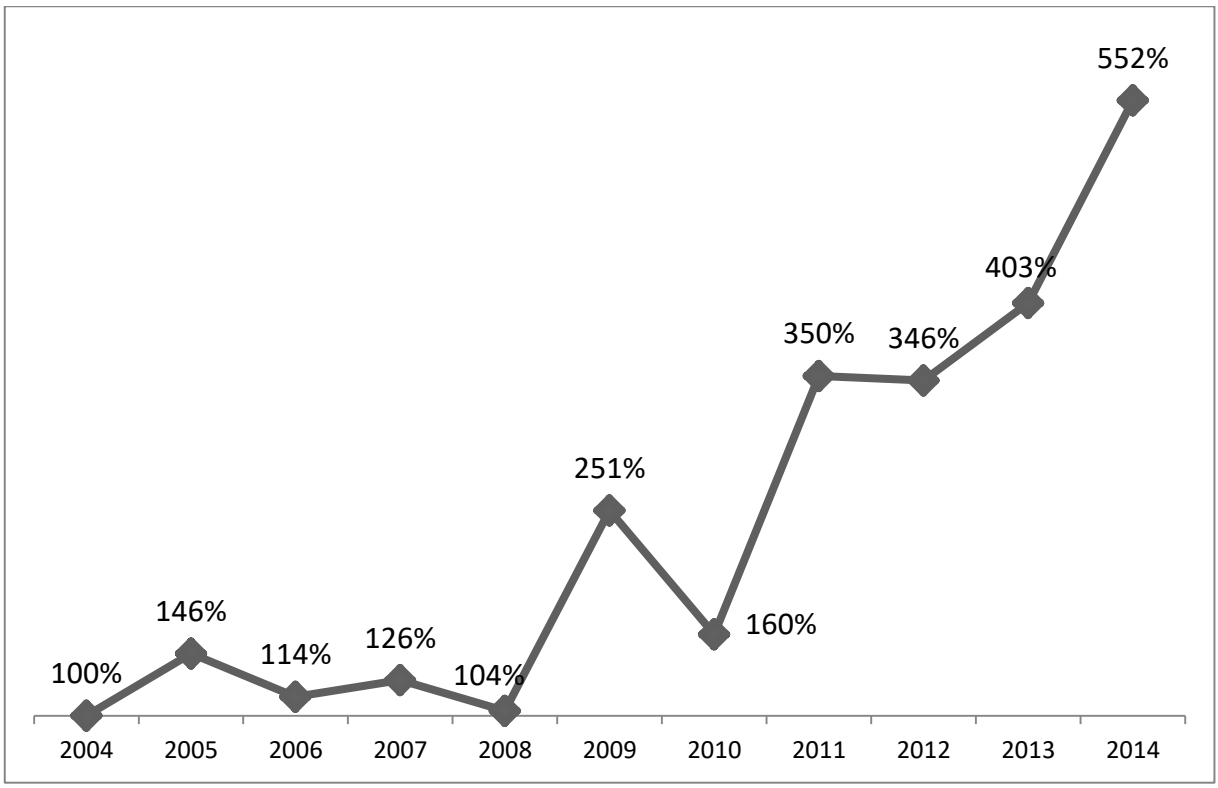
kilka stwierdzonych czynów przestępczych, które trzeba oddzielnie wykazać w celu ukarania za nie sprawcy.

Niekiedy w praktyce również zdarza się, iż pomimo wszczętego postępowania sprawdzającego nie uda się zebrać materiału dowodowego mogącego potwierdzić zaistnienie przestępstwa stąd ujemna różnica pomiędzy ilością postępowań stwierdzonych a ilością wszczętych postępowań przygotowawczych.

Analizując dane z powyższej tabeli wyraźnie widać wzrost zarówno liczby postępowań wszczętych jak i liczby przestępstw stwierdzonych. Dane te należy poddać dalszym analizom co zostało uczynione i w efekcie przedstawiono dynamikę stwierdzonych przestępstw na wykresie poniżej. Na wykresie tym zamieszczono szczegółowe dane dotyczące w podziale na poszczególne lata w okresie 2004-2014, przyjmując za rok bazowy rok 2004.

Należy również zwrócić uwagę na pojęcie „ciemnej liczby" przestępstw, to jest czynów o znamionach opisanych w ustawach, które nie zostały zgłoszone przez pokrzywdzonych organom ścigania z różnych powodów (www.zielona-gora.po.gov.pl). Częstym, a za razem mylnym przeświadczeniem pokrzywdzonych przestępstwem oszustwa komputerowego jest, pochylenie się nad łatwiejszym według nich porozumieniem z osobą, która weszła w przestępny sposób w posiadanie danych firmy, aby je odzyskać. To mylne przekonanie powoduje, że taki przedsiębiorca naraża się na kolejne ataki stając się łatwym źródłem dochodu. Takie zachowanie jest jednym z elementów wpływających na wielkość „ciemnej liczby" przestępstw i w długofalowej perspektywie przedsiębiorstwa generuje większe straty, zarówno finansowe jak i koszty prawne. Wszczęcie postępowania przygotowawczego, ma za zadanie nie tylko ujęcie sprawcy czynu, choć jest to jego główny cel, ale również wykazanie, iż zaistniało przestępstwo – to jest czyn o znamionach opisanych w ustawach – wykazując tym samym pokrzywdzonego czynem przestępnym w prowadzonym postępowaniu przygotowawczym.

Wykres 1. Wykres dynamiki zmian liczby przestępstw stwierdzonych, w stosunku do roku 2004.



Źródło: Na podstawie danych z Tabeli 1.

Analizując dynamikę stwierdzonych przestępstw komputerowych w latach 2004 – 2014 wyraźnie widać jej wykładniczy wzrost w ostatnich kilku latach. Sytuacja ta z całą pewnością jest spowodowana rozwojem technologii mobilnych pozwalających na dostęp do sieci m.in. internetowej z wykorzystaniem niewielkich gabarytowo urządzeń typu telefon komórkowy, smartfon, itp. Widać, że przedsiębiorstwa nie posiadały odpowiednich narzędzi zabezpieczających przed tego typu przestępstwami oraz nadal nie posiadają (trend wzrostowy nadal się utrzymuje). Przyczynami wzrostu ujawnionych cyberprzestępstw są (Wiśniewski, 2015):

1. Pojawiające się w mediach informacje o tego typu przestępstwach powoduje wzrost czujności przedsiębiorstw i prowadzi do dodatkowych kontroli, co w efekcie daje większą ich wykrywalność.
2. Duże wymagania prawne w zakresie ochrony danych i monitorowania transakcji, co prowadzi do zwiększania wykrywania cyberprzestępstw.
3. Postęp technologiczny.
4. Aktywność pracowników w sieci poprzez używanie przez nich portali społecznościowych (Facebook, Twitter, LinkedIn itp.), co ułatwia identyfikację osób pracujących w danej organizacji, znajomość ich adresów mailowych, zwyczajów itp. Dzięki temu łatwiejsze jest instalowanie toksycznego oprogramowania na ich komputerach w efekcie zwiększa to zasięg i efektywność cyberprzestępczości.

5. SPOSOBY WYKRYWANIA ANALIZOWANYCH PRZESTĘPSTW I ICH WYBRANE SKUTKI DLA PRZEDSIĘBIORSTW

Według badań firmy PwC przedstawionych w raporcie zatytułowanym „Dlaczego polskie firmy są tak łatwym celem dla cyberprzestępców" (Prezentacja z raportu z badań PWC: „Dlaczego polskie firmy są tak łatwym celem dla cyberprzestępców") cyberprzestępstwo jest identyfikowane na świecie jako „(...) drugie najważniejsze ryzyko mogące zagrozić prowadzonym interesom". Podczas gdy światowe wydatki na walkę z cyberprzestępstwem wynoszą 19%, w Polsce jest to obecnie 10%, wzrastając w roku 2015 z zaledwie 5,5% (Tamże). Zdaniem tego samego raportu, w przyszłości nawet 4% (Tamże) globalnych obrotów mogą wynieść kary za uchybienia w ochronie danych osobowych. Zdaniem firmy PwC w 2015 roku największym zagrożeniem dla firmy w Polsce był jej pracownik – 70%, atak zewnętrznego hakera zidentyfikowało 67% badanych, natomiast na następnych miejscach znalazły się ataki grup zorganizowanych (41%) oraz aktualni dostawcy i wykonawcy firmy (35%) (Tamże). Dodatkowo, mimo rosnącej wagi wykorzystania mediów społecznościowych oraz usług tak zwanej „chmury", połowa (Tamże) polskich przedsiębiorstw nie planuje wprowadzenia oddzielnych strategii poświęconych bezpieczeństwu informacji w tych właśnie usługach.

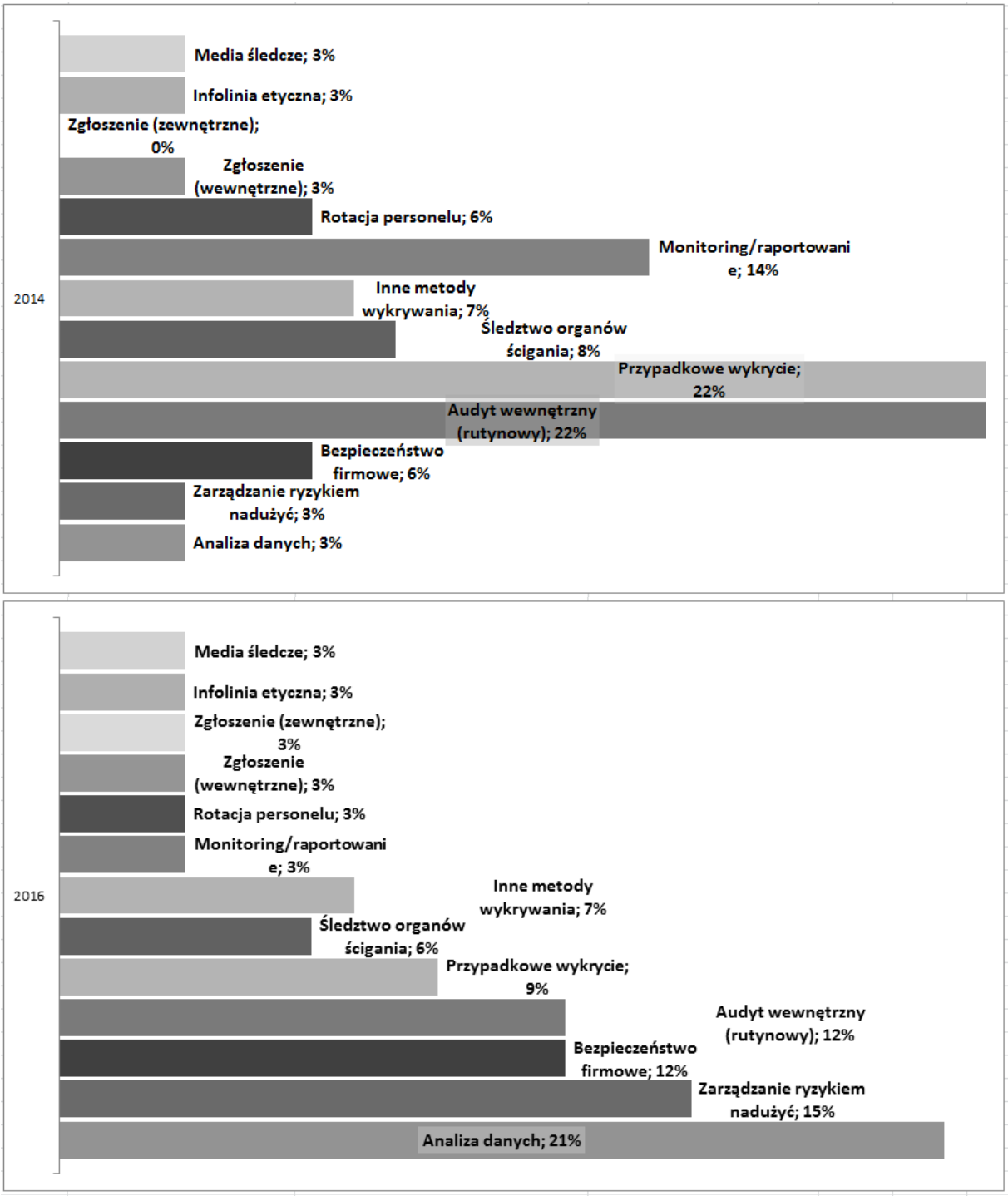
Raport „Badanie przestępczości gospodarczej w Polsce 2016" (Raport „Badanie Przestępczości Gospodarczej w Polsce 2016. Wyniki i kluczowe wnioski, 2016) identyfikuje najczęstsze sposoby wykrywania tego typu nadużyć w Polsce. W roku 2014 były to:

- rutynowy audyt wewnętrzny,
- przypadkowe wykrycie,
- monitoring, raportowanie podejrzanych transakcji.

W roku 2016 rozkład ten uległ zmianie, najczęstszymi sposobami były:

- analiza danych,
- zarządzanie ryzykiem nadużyć,
- bezpieczeństwo firmowe oraz audyt wewnętrzny.

Wykres 2. Najczęstsze sposoby wykrywania nadużyć w Polsce, lata 2014 - 2016



Źródło: Opracowanie własne na podstawie: Raport „Badanie Przestępczości Gospodarczej w Polsce 2016. Wyniki i kluczowe wnioski", Zespół Usług Śledczych i Zarządzania Ryzykiem Nadużyć PwC Polska.

Z danych z tego raportu wynika, że jedna na trzy firmy w Polsce straciła z powodu cyberprzestępstw do dwustu tysięcy złotych, natomiast jedna na pięć odniosła stratę nawet czterech

milionów złotych. Co gorsza, prawie co dziesiąta ankietowana firma nie zna wartości takiej straty.

Z badań przeprowadzonych wśród polskich przedsiębiorców wynika, że ponad połowa cyber-nadużyć popełniana jest przez sprawców zewnętrznych, ale wśród sprawców wewnętrznych pojawia się niepokojąca tendencja – aż 20% takich uchybień jest powodowana przez kadrę menadżerską (Tamże). Statystyczny przestępca to mężczyzna, z wyższym wykształceniem, w wieku od 31 do 40 lat, oraz z 5 letnim stażem pracy (Tamże).

Do najczęstszych konsekwencji wobec sprawców nadużyć wewnętrznych należą zwolnienia, poinformowanie organów ścigania oraz wszczęcie postępowania cywilnego (Raport „Badanie Przestępczości Gospodarczej Polska 2014"). Podobnie dla sprawców zewnętrznych to: poinformowanie organów ścigania, zakończenie współpracy z partnerem oraz wszczęcie postępowania.

W przypadku stwierdzenia przestępstwa sąd wymierza karę przedsiębiorstwu. Granice kary grzywny wyznacza Kodeks karny w art. 33 § 1. „Grzywnę wymierza się w stawkach dziennych, określając liczbę stawek oraz wysokość jednej stawki; jeżeli ustawa nie stanowi inaczej, najniższa liczba stawek wynosi 10, zaś najwyższa 540. oraz art. 33 § 3. stanowiący, że: stawka dzienna nie może być niższa od 10 złotych, ani też przekraczać 2000 złotych (Kodeks Postępowania Karnego, art. 33, § 1). Stąd grzywna może wynosić od 10 złotych do 1.080.000 złotych.

Zamiast obowiązku naprawienia szkody sąd może orzec na rzecz pokrzywdzonego nawiązkę w celu zadośćuczynienia za ciężki uszczerbek na zdrowiu, naruszenie czynności narządu ciała, rozstrój zdrowia, a także za doznaną krzywdę (www.infor.pl). Stąd w zakresie Sądu jest określenie nawiązki za doznaną krzywdę, w którą wliczyć można obecnie wszystko, nawet przejazdy na rozprawę a także utratę anonimowości i tym podobne rzeczy według inwencji skarżącego i przychylności składu orzekającego w Sądzie.

Rządowe Centrum Reagowania na Incydenty Komputerowe – CERT.GOV.PL identyfikuje w swoim raporcie na rok 2014 (Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014) kilka przykładowych zagrożeń z tego okresu. Jedną ze zidentyfikowanych była kampania cyberszpiegowska o nazwie Energetic Bear/Dragon Fly, której celem były europejskie i amerykańskie przedsiębiorstwa energetyczne, firmy z sektora zbrojeniowego, IT oraz agencje rządowe 23 państw (w tym Polski). Dzięki szybkiemu działaniu, współpracy międzynarodowej oraz sprawnemu przekazywaniu informacji i ostrzeżeń wykryto w Polsce kilkaset zarażonych adresów IP, żaden z nich nie okazał się głównym systemem firm lub instytucji państwowej. Głównymi ofiarami okazały się być osoby prywatne oraz firmy nie będące doce-

lową grupą ataku (odpowiednio 84,8% oraz 11,5%), będące prawdopodobnie przypadkowymi lub drugorzędnymi celami cyber-kampanii. Ten przypadek wskazuje, że firmy są narażone także na przypadkowe ataki, które także przynoszą im straty.

Z podobnymi atakami muszą najprawdopodobniej zacząć się liczyć także polskie uczelnie wyższe. Powoli wzrasta poziom ich współpracy firmami sektora publicznego i prywatnego. Jak wykazał atak Energetic Bear/Dragon Fly, także one mogą zostać zaatakowane (uczelnie wyższe stanowiły trzecia pod względem wielkości zainfekowanych grupę) jako ofiary przypadkowe, ale również jako potencjalne medium dostępu do firmy.

PODSUMOWANIE

Przedstawione w niniejszym artykule dane dotyczące przestępczości komputerowej oraz ciągły wzrost poziomu cyfryzacji pozwala wnioskować, że w przyszłości nastąpi dalszy przyrost przestępczość komputerowej, która swym działaniem wpływa na bezpieczeństwo przechowywanych danych przez przedsiębiorców a także obrotu gospodarczego.

Dla przedsiębiorców bardzo istotne jest, że w myśl przepisów Ustawy o Ochronie Danych Osobowych, ustawodawca nie wskazał zwolnienia z odpowiedzialności karnej nawet w przypadku przestępstwa, na przykład naruszenia tajemnicy korespondencji, pozyskania danych objętych ustawową ochroną przez osoby nieuprawnione, itp. Stąd tak istotnym w dzisiejszym coraz bardziej „cyfrowym" świecie jest właściwe zabezpieczanie wszelkich danych, w których posiadaniu znajduje się firma. Należy bezwzględnie stosować zasadę, „przezorny zawsze ubezpieczony" i nie oszczędzać na ochronie danych osobowych. Bardzo wysoka dynamika wzrostu liczby przestępstw komputerowych powinna spowodować konieczność wypracowania narzędzi zarówno technologicznych jak i prawnych, które pozwolą na wyhamowanie dalszego wzrostu liczby tych przestępstw. W przeciwnym razie w niedalekiej przyszłości może to zagrozić bezpieczeństwu prowadzenia działalności gospodarczej. W reakcji na tą sytuację w firmach rośnie znaczenie zespołów ds. cyberbezpieczeństwa, które traktowane jest zdecydowanie szerzej niż tylko to związane z działem IT („Dlaczego polskie firmy są tak łatwym celem dla cyberprzestępców"). Kolejnym sposobem jest wykupienie odpowiedniej polisy jednak w Polsce polisę ubezpieczeniową od cyber-zagrożeń posiada tylko 8% przedsiębiorstw a na świecie według badań PWC – 59% (Tamże). Żeby podnieść poziom bezpieczeństwa można nawiązać współpracę z innymi wyspecjalizowanymi podmiotami w tym zakresie – w PL robi to 45% a w krajach badanych przez PWC - 64%.

Zabezpieczenie przez atakami cyberprzestępców powinno mieć charakter hybrydowy i wielopoziomowy zapewniający holistyczną ochronę całemu przedsiębiorstwu. Strategia takiej obrony powinna mieć następujące elementy (Ochrona przed cyberatakimi – bezpieczeństwo całościowe, Bezpieczny Łańcuch Dostaw - Eurologistics, 6 grudzień 2015 r. – Styczeń 2016):

1. Opracowanie planu zabezpieczeń w zakresie polityki i procedur obejmujących ewaluację i ograniczanie ryzyka a także przywracanie funkcjonowania systemu po awarii.
2. Separacja sieci w efekcie nastąpi podział na strefy, które mają za zadanie ochronę poszczególnych systemów wewnątrz sieci firmowej.
3. Ochrona na granicach sieci blokujące dostęp osobom bez uprawnień poprzez – zapory firewall, weryfikację tożsamości, autoryzację dostępu, sieci VPN, oprogramowanie antywirusowe itp.
4. Segmentacja sieci umożliwiająca ograniczenie zasięgu potencjalnym naruszeniom bezpieczeństwa do jednego segmentu. Realizuję się to przy pomocy przełączników sieciowych i sieci VLAN.
5. Wzmacnianie ochrony urządzeń poprzez zarządzanie hasłami, zdefiniowanie profile użytkowników i zatrzymanie zbędnych procesów.
6. Kontrola aktywności operatora i komunikacji w obrębie sieci oraz regularne aktualizacje oprogramowania.

LITERATURA

1. Kodeks Karny
2. Kozłowski R., Matejun M., The identification of difficulties in using advanced technologies in the implementation of projects. International Journal of Business and Management, Vol. III(4) 2015, DOI: 10.20472/BM.2015.3.4.003, s. 42
3. Latusek – Jurczak D., Pozyskiwanie wiedzy z otoczenia. Wywiad gospodarczy. Relacje z partnerami oparte na wiedzy, w: Jemielniak D. i Koźmiński A.K., Zarządzanie wiedzą, Wydanie II, Oficyna a Wolters Kluwer business, Warszawa 2012
4. Ochrona przed cyberatakimi – bezpieczeństwo całościowe, Bezpieczny Łańcuch Dostaw - Eurologistics, 6 grudzień 2015 r. – Styczeń 2016 r
5. Prezentacja z raportu z badań PWC: „Dlaczego polskie firmy są tak łatwym celem dla cyberprzestępców" za: www.pwc.pl/pl/media/2016/2016-03-01-co-trzecia-firma-w-polsce-pada-ofiara-naduzyc.html w dn. 01.05.2016

6. Raport „Badanie Przestępczości Gospodarczej Polska 2014.”, PwC Polska, Warszawa, Marzec 2014 za: http://www.pwc.pl/pl/biuro-prasowe/assets/pwc_polska_badanie_global_economic_crime_survey_2014_prezentacja.pdf z dn. 01.05.2016
7. Raport „Badanie Przestępczości Gospodarczej w Polsce 2016. Wyniki i kluczowe wnioski”, Zespół Usług Śledczych i Zarządzania Ryzykiem Nadużyć PwC Polska, Warszawa, Marzec 2016 za: www.pwc.pl/pl/media/2016/2016-03-01-co-trzecia-firma-w-polsce-pada-ofiara-naduzyc.html z dn. 01.05.2016
8. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014, Rządowy Zespół Reagowania na Incydenty Komputerowe Cert.Gov.PL, Warszawa, Marzec 2015 za: www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi z dn. 01.05.2016
9. Special Eurobarometer 431 – Data Protection str. 4. Dostęp: www.ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf z dn. 06.04.2016
10. Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny
11. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych
12. Ustawa z dnia 6 czerwca 1997 r - Kodeks Postępowania Karnego
13. Wiśniewski K., Światowe badanie nadużyć gospodarczych. Cyberprzestępstwa, Bezpieczny Łańcuch Dostaw - Eurologistics, 6 grudzień 2015 r. – Styczeń 2016 r.
14. www.foxnews.com/story/2006/07/06/pepsi-alerted-coca-cola-to-stolen-coke-secrets-offer.html z dn. 12.04.2016
15. www.infor.pl/prawo/prawo-karne/wyrok-i-kara/686739,Co-warto-wiedziec-o-nawiazce.html z dn. 01.05.2016
16. www.prawo.egospodarka.pl/64752,Naruszenie-warunkow-i-uniewaznienie-umowy,1,92,1.html z dn. 12.04.2016
17. www.prawo.money.pl/kodeks/pracy/dzial-czwarty-obowiazki-pracodawcy-i-pracownika/rozdzial-ii-obowiazki-pracownika/art-100 z dn. 12.04.2016
18. www.prawo.wiedza.diaboli.pl/kryminalistyka/ z dn. 14.04.2016
19. www.statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63977,Oszustwo-komputerowe-art-287.html z dn. 14.04.2016
20. www.zielona-gora.po.gov.pl/index.php?id=36&ida=2934 z dn. 14.04.2016.