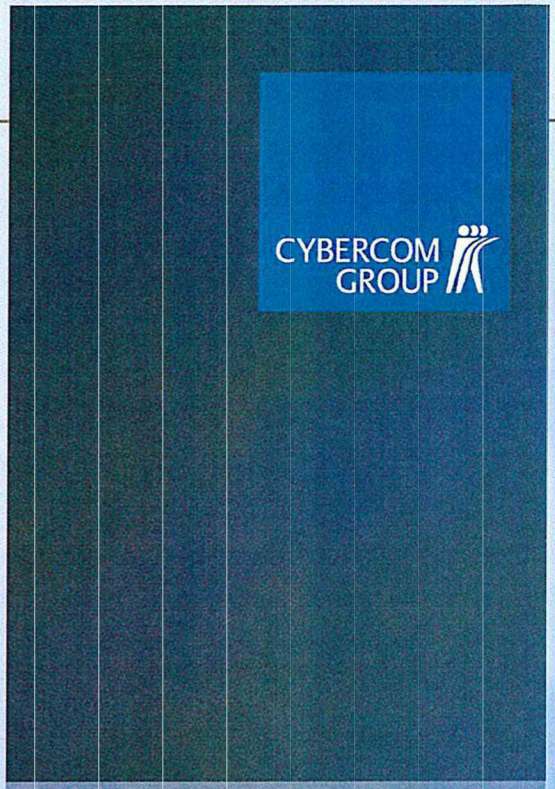



# Opinia rewidenta do spraw szczególnych

(powołanego w trybie art. 85 ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych) dotycząca wyjaśnienia okoliczności związanych z incydentem bezpieczeństwa środowiska teleinformatycznego grupy kapitałowej, gdzie jednostką dominującą jest Kredyt Inkaso S.A. z siedzibą w Warszawie

Adam Wódz

Warszawa, 18.09.2018

# Spis treści

Wyciąg z opinii ..... 3

Przedmiot i zakres badania ..... 10

Materiały i informacje wykorzystane w celu przeprowadzenia badania ..... 11

Ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia ..... 15

Ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów ..... 19

Ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce, na dzień zdarzenia, procedurami wewnętrznymi z zakresu bezpieczeństwa danych ..... 24

Ustalenie, czy audyt bezpieczeństwa informatycznego przeprowadzony przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj A. z siedzibą w Lublinie na zlecenie Spółki obejmował ustalenie okoliczności badanego incydentu ..... 29

Uwagi rewidenta do przebiegu badania ..... 33

## Wyciąg z opinii

Przedmiotem opinii było zbadanie i wyjaśnienie okoliczności związanych z incydentem bezpieczeństwa środowiska teleinformatycznego grupy kapitałowej, gdzie jednostką dominującą jest Kredyt Inkaso S.A. (Spółka), zidentyfikowanym przez osobę pełniącą w Spółce, w dacie zdarzenia, funkcję ABI.

Dokładny przedmiot i zakres badania przez rewidenta obejmował:

a) ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia;
b) ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów, o których mowa w lit. a) powyżej;
c) ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce na dzień zdarzenia procedurami wewnętrznymi z zakresu bezpieczeństwa danych;
d) ustalenie, czy audyt bezpieczeństwa informatycznego przeprowadzony przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie na zlecenie Spółki obejmował ustalenie okoliczności, o których mowa w lit. a) – c) powyżej.

Na podstawie analizy przedstawionych przez Spółkę dokumentów oraz materiału zgromadzonego w aktach niniejszej sprawy, biegły może stwierdzić, że zawierają one informacje dotyczące incydentów związanych z kopiowaniem plików z systemu informatycznego Spółki na urządzenia zewnętrzne w okresie 02-29.02.2016 r. Należy podkreślić, że w Spółce jako generalna zasada niedozwolone było kopiowanie danych na nośniki zewnętrzne, poza wyjątkami zatwierdzonymi uprzednio przez przełożonego Spółki.

Na podstawie przedstawionych dokumentów nie można określić realnej zawartości kopiowanych plików. Kopiowane pliki są wymienione bowiem jedynie z nazwy, jednak ich zawartość / treść nie są załączone do dokumentów. Istnieją jednak przesłanki, które mogą wskazywać, że pliki te mogły zawierać dane poufne dot. Spółki, w tym także dane osobowe:

1. Nazwa plików „kisa_rep" może wskazywać na pochodzenie ich zawartości z serwera *kisa_reporting*, co zostało wskazane w wiadomości e-mail M G w następujący sposób:

„Z nazw plików wynika, że zawierają one dane z serwera *kisa_reporting*, na którym jest hurtownia danych oraz projekty aplikacji."

2. Kopiowanie plików „kisa_rep" miało miejsce dwukrotnie, przy czym dn. 21.02.2016 r. trwało na tyle długo, że można założyć, że pełny plik archiwum „kisa_rep" mógł zawierać ok. 8 GB danych lub więcej. Po wielkości pliku można zatem przyjąć, że mógł on stanowić kopię danych całego środowiska informatycznego.

3. Nazwy plików archiwum TAR „workspaces_backup" wskazują na pochodzenie ich zawartości ze środowisk testowych jakiegoś systemu lub aplikacji w wersjach odpowiednio 103 i 105.

4. W raporcie z audytu bezpieczeństwa systemu informatycznego przeprowadzonego przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie wykazano w pkt. 5, że:
„Zagrożeniem dla poufności danych osobowych dłużników może być (...) stosowanie niezanonimizowanych zbiorów danych w środowiskach testowych". Nie wskazano w tym raporcie jakich konkretnie środowisk testowych może dotyczyć problem, ale tym bardziej może to dotyczyć środowisk związanych z hurtownią danych.

5. W analizowanych logach, przy plikach RAR i TAR brakuje wskazania ścieżki źródłowej tych plików. Nie można zatem jednoznacznie określić z jakiego miejsca zostały one skopiowane. Nie da się także określić, jakie dane zostały uprzednio umieszczone w archiwach RAR i TAR. Rzetelne sprawdzenie tego incydentu wymaga dodatkowych działań związanych z bezpośrednim dostępem do infrastruktury teleinformatycznej Spółki, na co biegły nie uzyskał zgody Spółki, pomimo licznych wniosków w tym zakresie.

6. W szczególności, jeśli w opinii Spółki kopiowanie dotyczyło „kopii środowiska analitycznego do analizy danych finansowych", to rozpoznane w ten sposób pliki RAR i TAR powinny zostać zarchiwizowane zgodnie z obowiązującymi w Spółce procedurami, wynikającymi, np. z Polityki bezpieczeństwa, pkt. 5.4.1 w brzmieniu:
„Aby zapewnić ciągłość działania w przypadku awarii lub katastrofy należy sporządzać awaryjne kopie: danych, instancji systemów informatycznych oraz konfiguracji kluczowych komponentów infrastruktury informatycznej", uszczegółowionymi w załączniku nr 3 do Polityki bezpieczeństwa

dotyczącym Procedury tworzenia kopii zapasowych. Jeśli pliki te podlegały pod procedurę dotyczącą kopii baz danych lub serwerów plikowych to powinny być przechowywane przez okres 10 lat zgodnie z postanowieniami Polityki bezpieczeństwa. **Jeżeli zatem kopie tych plików są dostępne w archiwum (a powinny być zgodnie z wewnętrznymi procedurami), to powinny zostać poddane analizie pod kątem ich zawartości, czego Spółka do tej pory nie zrobiła w ramach żadnego z działań mających na celu zbadanie incydentu – nie wyrażono także zgody na udostępnienie takich plików biegłemu w ramach niniejszego badania. Jeżeli zaś pliki te nie zostały poprawnie zarchiwizowane, to może to stanowić naruszenie polityki bezpieczeństwa Spółki.**

W kontekście zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce na dzień zdarzenia procedurami wewnętrznymi z zakresu bezpieczeństwa danych, bazując na dokumentach i informacjach udostępnionych przez Spółkę biegły ustalił i opiniuje jak poniżej:

1. Procedury wewnętrzne Spółki obejmują blokowanie możliwości użycia wymiennych nośników danych na stacjach roboczych. Wyjątki od tych zasad wymagają zgody przełożonego i są rejestrowane poprzez system zgłoszeń. Zostało to potwierdzone m.in. w pkt. 5 Oświadczenia o przebiegu audytu bezpieczeństwa informatycznego wykonanego przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie. W tej sytuacji postępowanie M G związane z próbą wyjaśnienia incydentów kopiowania danych na nośniki zewnętrzne było zgodne z procedurami Spółki.

2. M G nie została włączona w skład działającego w utajnieniu Zespołu powołanego przez Spółkę, którego celem było zabezpieczenie ciągłości działania Spółki i nie wiedziała o jego funkcjonowaniu. Z kolei P N i inni członkowie Zespołu nie byli świadomi testowego uruchomienia systemu DLP firmy Symantec (przy czym na podstawie analizy historii wiadomości e-mail z dn. 04.03.2018 r. przesłanej przez M G do Prezesa Zarządu Spółki – Pawła Szewczyka, wynika że Dyrektor IT – P N był informowany wcześniej (nie wiadomo jednak kiedy dokładnie) przez pracownika Działu IT – K J „o wdrożeniu na początku roku (2016 – przyp. biegłego) nowej funkcjonalności pakietu zabezpieczającego Symantec, która pozwala kompleksowo monitorować i raportować zdarzenia na stacjach roboczych, wskazując te

które mogą stanowić naruszenie bezpieczeństwa" – e-mail ten został wysłany przez K J do M G z kopią do Pawła Szewczyka i P N ).

Wykryte w ten sposób przez M G incydenty kopiowania danych mogły być efektem działań Zespołu Zadaniowego Spółki, ale nie zostało to nigdy jednoznacznie potwierdzone przez Spółkę. Na tej samej podstawie nie można wykluczyć, że wykryte incydenty nie były powiązane z pracą Zespołu i bez dogłębnej analizy zawartości skopiowanych plików (co zostało biegłemu odmówione w ramach dostępu do infrastruktury teleinformatycznej Spółki) nie można jednoznacznie wykluczyć możliwości skopiowania danych poufnych Spółki (w tym danych osobowych).

3. Sam fakt powołania Zespołu, wyposażenia go w zewnętrzne nośniki danych i umożliwienia kopiowania na nie danych Spółki mógł skutkować celowym lub przypadkowym wyniesieniem wrażliwych danych poza obszar działania Spółki. Wynika to zwłaszcza z cytatu ze Stanowiska Spółki: „Ówczesny Zarząd Spółki stwierdził, że w sytuacji zagrożenia wrogim przejęciem koniecznym było zabezpieczenie określonych danych umożliwiających podjęcie dalszej działalności Spółki nawet poza jej siedzibą".

   Z decyzji nr DPZ 1/01/2016 z dn. 26.01.2016 r. w sprawie powołania Zespołu Zadaniowego nie wynikają szczegółowe zasady jego działania, w szczególności w jaki sposób i gdzie przechowywane miałyby być dyski przenośne powierzone członkom Zespołu w dniach 26.01. – 06.04.2016 r. (do czasu przekazania ostatniego z nich D O – Dyrektorowi Bezpieczeństwa Korporacyjnego Spółki, co zostało udokumentowane w postaci protokołów zdawczo-odbiorczych). Osoby wchodzące w skład Zespołu, które ewentualnie chciałyby działać na szkodę Spółki i wynieść dane poufne Spółki, pozostawały w tym czasie poza kontrolą Spółki.

4. Incydenty związane z kopiowaniem danych wskazane przez M G miały miejsce także poza godzinami pracy, np. w niedzielę wieczorem 21.02.2016 w godz. 21:11-21:26 (P N ), czy w piątek 26.02.2016 w godz. 19:22 – 20:10 (Piotr Podłowski). W opinii biegłego fakt ten może wskazywać na chęć ukrycia przed pracownikami Spółki działań związanych z kopiowaniem danych.

5. Skoro celem działań Zespołu było zabezpieczenie ciągłości działania Spółki, to można zakładać, że skopiowano także dane osobowe przetwarzane przez Spółkę. W pkt. (III) Decyzji Nr DPZ 1/01/2016 w sprawie powołania Zespołu Zadaniowego z dn. 26.01.2016 r. jest wskazane „wykonanie niezbędnych czynności zapobiegawczych przed utratą danych, w szczególności wykonanie i zabezpieczenie w celu zapewnienia ciągłości działania procesów operacyjnych kopii kluczowych zasobów zgromadzonych w systemach informatycznych". Z praktyki biegłego, trudno sobie wyobrazić zabezpieczenie kluczowych zasobów bez uwzględnienia danych wierzycieli obsługiwanych przez Spółkę. W opinii biegłego można przyjąć, że takie dane były kopiowane przez członków Zespołu Zadaniowego.

6. W sytuacji, gdy Zarząd Spółki powołał Zespół Zadaniowy, który funkcjonował w utajnieniu w czasie wystąpienia incydentów wskazanych przez M G , zastanawiający jest fakt braku powiązania tych incydentów z działaniami Zespołu i podjęcie przez Spółkę decyzji o przeprowadzeniu audytu bezpieczeństwa przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie. Członkowie Zespołu, w tym P. N i P. Podłowski, mogli bowiem z łatwością określić, czy proces kopiowania prowadzony przez nich i uwzględniony w logach systemu DLP był realizowany w ramach działań operacyjnych Zespołu, czy też nie. Pomimo tego sam Zespół był inicjatorem konieczności przeprowadzenia audytu bezpieczeństwa, co zostało wskazane w dokumencie „Podsumowanie prac zespołu zadaniowego z dn. 08.04.2016 r.". Jednocześnie Spółka stała i nadal stoi przy stanowisku, że jednym z głównych celów przeprowadzenia audytu przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie było zbadanie incydentów wskazanych przez M G chociażby w stanowisku ówczesnego Prezesa Zarządu Spółki Pawła Szewczyka wyrażonym podczas Nadzwyczajnego Walnego Zgromadzenia Akcjonariuszy Spółki w dn. 05.04.2016 r., zachowanym na nagraniu dołączonym do akt sprawy:

   „W firmie zidentyfikowano rzeczywiście kopiowanie jakichś danych i nie dziewiętnastego, między dziewiętnastym a dwudziestym pierwszym, a dokładnie od dziesiątego lutego i w tej chwili trwa wewnętrzny audyt, który to identyfikuje."

   Na podstawie ww. faktów, w opinii biegłego incydenty wskazane przez M G w mailu z dn. 04.03.2016 r. nie powinny być łączone z pracami Zespołu. W związku z tym, badanie powinno

zostać przeprowadzone w oparciu o dane pochodzące bezpośrednio z systemów IT Spółki, na co jednak biegły, pomimo składanych wniosków, nie uzyskał zgody Spółki.

7. Dodatkowo należy wskazać, że na podstawie analizy nazw i typów kopiowanych plików wskazanych w załącznikach do wiadomości e-mail M G można zauważyć, że pomimo obowiązujących w Spółce procedur, osoby posiadające zgodę przełożonego na korzystanie z portów USB w uzasadnionych przypadkach wykorzystywały ten przywilej także do przenoszenia plików wykraczających poza uzasadniony przypadek, takich jak np. filmy chronione prawem autorskim (Zjawa.2015.PLSUBBED.DVDSCR.XViD.AC3-majorq-LTS.avi – G , czy też wzory haftów (Księżniczka z pieskiem 2.pdf – ). Stanowi to naruszenie wewnętrznych procedur Spółki.

Na podstawie analizy „Oświadczenia o przebiegu audytu bezpieczeństwa informatycznego sporządzonego przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie" biegły stwierdza, że audyt ten nie wykazał jednoznacznych podstaw do stwierdzenia, czy w Spółce doszło, czy też nie doszło do wycieku danych. Audytor nie wykonał wymaganej w takich przypadkach analizy powłamaniowej, a jedynie testy penetracyjne i analizę procedur, na podstawie których nie ma możliwości potwierdzenia lub zanegowania faktu wycieku danych. W szczególności w oświadczeniu audytora brakuje jakiejkolwiek wzmianki o wykonaniu czynności audytowych prowadzących do zbadania incydentu stanowiącego przedmiot niniejszego badania biegłego, takich jak:

a) ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia;
b) ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów, o których mowa w lit. a) powyżej;
c) ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce na dzień zdarzenia procedurami wewnętrznymi z zakresu bezpieczeństwa danych;

Audyt nie wykazał wycieku danych osobowych, lecz jedynie wybrane problemy techniczne i proceduralne. Jest to zgodne z prawdą, ponieważ zakres i rezultaty przeprowadzonego audytu mogły jedynie w wąskim zakresie służyć do dostarczenia odpowiedniego materiału dowodowego

pozwalającego na wykrycie wycieku danych. W czynnościach audytowych zabrakło stosowanych w przypadku podejrzenia wycieku danych procedur związanych z analizą powłamaniową.

Dodatkowo wskazać należy, że firma CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie w opinii biegłego nie jest podmiotem specjalizującym się w badaniach incydentów związanych z bezpieczeństwem danych. Nie wynika to przynajmniej z analizy strony www należącej do tej firmy. Główną działalnością firmy jest projektowanie i wykonywanie kompletnych instalacji sieci LAN, WAN i VPN, pomoc we wdrożeniach i wsparcie techniczne. Żadna z usług wymienionych na stronie firmy nie dotyczy przeprowadzania audytów bezpieczeństwa i testów penetracyjnych, a w szczególności badania incydentów związanych z wyciekiem danych. Z pewnością nie ma wystarczających przesłanek merytorycznych do wyboru tego podmiotu w celu zbadania incydentów związanych z wyciekiem danych, o czym świadczą chociażby istotne zastrzeżenia merytoryczne biegłego do wydanego przez tę firmę Oświadczenia.

## Przedmiot i zakres badania

W związku z postanowieniem z dnia 03.03.2017 roku wydanego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie XIII Wydział Gospodarczy KRS, niniejsza opinia została wykonana w oparciu o projekty uchwał Zwyczajnego Walnego Zgromadzenia spółki pod firmą Kredyt Inkaso Spółka Akcyjna z siedzibą w Warszawie (Spółka) z dnia 29.09.2016 roku oraz z dnia 03.10.2016 roku.

Przedmiotem opinii było zbadanie i wyjaśnienie okoliczności związanych z incydentem bezpieczeństwa środowiska teleinformatycznego grupy kapitałowej, gdzie jednostką dominującą jest Kredyt Inkaso S.A., zidentyfikowanym przez osobę pełniącą w Spółce w dacie zdarzenia funkcję ABI.

Dokładny przedmiot i zakres badania przez rewidenta obejmował:

a) ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia;
b) ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów, o których mowa w lit. a) powyżej;
c) ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce na dzień zdarzenia procedurami wewnętrznymi z zakresu bezpieczeństwa danych;
d) ustalenie, czy audyt bezpieczeństwa informatycznego przeprowadzony przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie na zlecenie Spółki obejmował ustalenie okoliczności, o których mowa w lit. a) – c) powyżej.

Opinia biegłego dotycząca wyników badania poszczególnych ww. zagadnień została szczegółowo przedstawiona w kolejnych punktach niniejszego dokumentu.

## Materiały i informacje wykorzystane w celu przeprowadzenia badania

W celu przeprowadzenia rzetelnego badania biegły wystąpił do Spółki o udostępnienie wszelkich informacji związanych z incydentem, w szczególności dokumentacji wskazanej w § 3 projektu uchwały z dn. 03.10.2016 r., czyli:

a) procedury tworzenia kopii zapasowych baz danych, przechowywania tych kopii i ich niszczenia;
b) ewidencji kopii zapasowych na zewnętrznych nośnikach danych;
c) raportu z audytu bezpieczeństwa systemu informatycznego sporządzonego przez osobę pełniącą w dacie zdarzenia funkcję ABI;
d) raportu z audytu bezpieczeństwa systemu informatycznego przeprowadzonego przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie.

Na wezwanie biegłego z dn. 07.09.2017 r., Spółka udostępniła mu w dniu 20.09.2017 r. informacje w formie wydruków papierowych w liczbie 4.484 stron, zajmujących 3 kartony, zawierające:

a) Pismo informacyjne z 20.09.2017 r. (2 strony);
b) Wyciąg ze spisów zdawczo-odbiorczych (4 strony);
c) Wyciąg z Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (5 stron);
d) Procedurę tworzenia kopii zapasowych (5 stron);
e) Wyciąg z procedur dotyczących przetwarzania danych osobowych obejmujący Procedurę niszczenia dokumentów i nośników informatycznych (4 strony);
f) Wyciąg z Procedury archiwizacji dokumentów (4 strony);
g) Wyciąg z Polityki Bezpieczeństwa Informacji dotyczący Kopii awaryjnych (3 strony);
h) Wydruk obejmujący treść wiadomości e-mail z dn. 04.03.2016 r. przesłanej przez M- G pełniącą do dnia 14.03.2016 r. funkcję ABI w Spółce do Pawła Szewczyka, Prezesa Spółki (3 strony);
i) Wydruk ze zrzutu ekranu obejmujący widok pliku o nazwie „Incydenty 2'16 IT.xls" (1 strona);
j) Wydruk zawartości pliku o nazwie „Incydenty 2'16 IT.xls" (484 strony);
k) Oświadczenie o przebiegu audytu bezpieczeństwa informatycznego sporządzone przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie (2 strony);
l) Wydruk ze zrzutu ekranu obejmujący widok pliku o nazwie „Analiza raportów.xls" (1 strona):

m) Wydruk zawartości pliku „Analiza raportów.xls" (3966 stron).

Dodatkowo Spółka udostępniła biegłemu do badania następujące dokumenty:

1) Kopie pełnych procedur dotyczących bezpieczeństwa, które miały zastosowanie w związku z incydentem, o którym mowa w raporcie z incydentu opracowanym przez Panią M G
   a. Instrukcja zarządzania systemem teleinformatycznym i jego bezpieczeństwem z dnia 16.04.2013 roku wraz z uchwałą Zarządu Spółki dotyczącą jej implementacji;
   b. Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wraz z odpowiednimi uchwałami Zarządu Spółki dotyczącymi jej implementacji oraz zmian;
   c. Polityka Bezpieczeństwa Informacji wraz z odpowiednimi uchwałami Zarządu Spółki dotyczącymi jej implementacji oraz zmian;
   d. Polityka Bezpieczeństwa w zakresie ochrony danych osobowych wraz z odpowiednimi uchwałami Zarządu Spółki dotyczącymi jej implementacji oraz zmian;
   e. Procedura archiwizacji dokumentów z odpowiednią uchwałą Zarządu Spółki dotyczącymi jej implementacji;
   f. Procedury zapobiegające ujawnieniu lub wykorzystaniu informacji stanowiących tajemnicę zawodową wraz z odpowiednią uchwałą Zarządu Spółki dotyczącą jej implementacji;
   g. System klasyfikacji danych finansowych wraz z odpowiednią uchwałą Zarządu Spółki dotyczącą jej implementacji;
2) Wiadomość e-mail od Pani M G z dnia 04.03.2016 r. wraz z załącznikami w formie elektronicznej na płycie CD (**Uwaga biegłego**: na płycie znajdują się jedynie załączniki do wiadomości e-mail, bez samej treści wiadomości e-mail);
3) Kopia dokumentacji dotyczącej powołania Zarządu Zadaniowego pod nazwą „Zabezpieczenie Kluczowych Obszarów Spółki w Sytuacji Nadzwyczajnej:
   a. Decyzja numer DPZ 1/01/2016 z dnia 26.01.2016 r.;
   b. Protokół likwidacji z dnia 12.04.2016 r.;
   c. Wykaz nośników pamięci zewnętrznej przydzielonych członkom Zespołu Zadaniowego;
   d. Protokół zdawczo – odbiorczy z 02.03.2016 r.;
   e. Protokół zdawczo – odbiorczy z 04.03.2016 r.;
   f. Protokół zdawczo – odbiorczy z 08.03.2016 r.;

g. Protokół zdawczo – odbiorczy z 15.03.2016 r.;
h. Protokół zdawczo – odbiorczy z 06.04.2016 r.;
i. Podsumowanie prac Zespołu Zadaniowego z dnia 8.04.2016 r.;
j. Rozwiązanie Zespołu Zadaniowego datowane na 12.04.2016 r.;

4) Wyciąg z protokołu posiedzenia Rady Nadzorczej Spółki nr VI/3/2018 z dnia 04 czerwca 2018 r. obejmujący pkt III .1 porządku obrad tj. „Spotkanie członków Rady Nadzorczej z rewidentem do spraw szczególnych tj. Cybercom Poland sp. z o.o. z siedzibą w Warszawie celem uzyskania wyjaśnień zgodnie z art. 86 ust. 1 ustawy o ofercie publicznej co do przedmiotu badania tj. rzekomego incydentu związanego z wyciekiem danych osobowych.", liczący 5 stron;
5) Wyciąg z protokołu z posiedzenia Rady Nadzorczej Spółki nr IV/5/2016 z dnia 8 sierpnia 2016 r. obejmujący pkt 5 porządku obrad tj. „Prezentacja odpowiedzi przez zaproszone osoby na przekazane pytania oraz dyskusja z zaproszonymi przedstawicielami spółki C.P.U. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie oraz z osobą wykonującą obowiązki ABI w spółce i osobą odpowiedzialną za infrastrukturę techniczną IT w spółce w celu uzyskania dodatkowych informacji z obszaru bezpieczeństwa danych w związku m.in. z przeprowadzonym przez firmę C.P.U. audytem w Spółce", liczący 4 strony;
6) Wyciąg z protokołu z posiedzenia Rady Nadzorczej Spółki nr IV/3/2016 z dnia 17 czerwca 2016 r. obejmujący pkt 4 porządku obrad tj. „Dyskusja oraz podjęcie uchwały w sprawie potrzeby sporządzenia na wniosek Rady Nadzorczej dodatkowej ekspertyzy dotyczącej bezpieczeństwa środowiska informatycznego spółki", liczący 3 strony;
7) Wyciąg z protokołu z posiedzenia Rady Nadzorczej Spółki nr IV/2/2016 z dnia 9 maja 2016 r. obejmujący pkt 11 porządku obrad tj. „Przedstawienie przez Zarząd Spółki informacji na temat wszelkich ewentualnych przypadków naruszenia w Spółce przyjętej polityki bezpieczeństwa danych osobowych lub powszechnie obowiązujących przepisów prawa normujących zasady ochrony przedmiotowych danych, zgłaszanych Zarządowi Spółki przez osoby odpowiedzialne w Spółce w terminie od 1 stycznia 2015 r. udzielanie wyjaśnień wobec ewentualnych przypadków w/w naruszeń wraz ze wskazaniem podjętych przez Spółkę środków zaradczych mających na celu wyeliminowanie możliwości powtarzania się w przyszłości podobnych incydentów", liczący 2 strony.

Biegły wystosował także pytania uszczegóławiające do Zarządu Spółki w piśmie z dn. 19.01.2018 r., na które uzyskał pisemne odpowiedzi Spółki w postaci protokołów, przekazanych podczas spotkań z

Zarządem Spółki w dn. 12.02.2018 r., 30.05.2018 r., 25.06.2018 r. oraz 24.08.2018 r. Biegły spotkał się także z Radą Nadzorczą Spółki w dn. 04.06.2018 r. – co zostało udokumentowane w protokole Rady Nadzorczej z dn. 04.06.2018 r.

Biegły korzystał także z akt sądowych powiązanych ze sprawą i znajdujących się w aktach niniejszej sprawy, w szczególności z dokumentów i nagrań zawartych w aktach o sygnaturze XXIII Gz 776/17 t. XXVIII, t. XXIX, t. XXX, t. XXXI i t. XXXII.

## Ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia

Punktem wyjścia w badaniu dla rewidenta był incydent wskazany w wiadomości e-mail wysłanej w dn. 04.03.2016 r. przez M G pełniącą w tamtym czasie funkcję ABI w Spółce, do Pawła Szewczyka, Prezesa Spółki, z kopią wiadomości do P N (Dyrektor IT) i K J (pracownik Działu IT). Na wniosek biegłego Spółka udostępniła treść tej wiadomości e-mail w postaci wydruku w formie papierowej.

M G informowała w tej wiadomości o wynikach analizy logów otrzymanych z narzędzia DLP firmy Symantec, na podstawie których wskazane były osoby, z których komputerów w okresie 02-29.02.2016 r. zostały skopiowane dane z systemów IT Spółki na nieokreślone nośniki zewnętrzne.

M G informowała m.in. w mailu co następuje:

„Obowiązujące w firmie przepisy wewnętrzne to:

- zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych wypisów, nawet w postaci zaszyfrowanej.
- zabronione jest: przenoszenie informacji uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne nośniki informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne.

(...)

W okresie od 2-19.02.2016 r. zarejestrowano zdarzenia na komputerach menadżerów oraz pracowników IT. Zdarzenia dotyczą przesyłania plików:

- objętych prawami autorskimi – pracownicy IT,

- dokumentów i zestawień firmowych – menadżerowie/samodzielne stanowiska,

- kopie danych

(...)

W raporcie zarejestrowana jest kilkakrotnie operacja kopiowania dużych spakowanych plików danych. (...) Z nazw plików wynika, że zawierają one dane z serwera *kisa_reporting*, na którym jest hurtownia

danych oraz projekty aplikacji. W związku z czym proszę Dyrektora IT (P N z którego komputera były kopiowane te dane – przyp. biegłego) o informacje jaka była/jest zawartość tych plików oraz cel kopiowania na urządzenia zewnętrzne."

Do wiadomości zostały załączone dwa pliki w formacie xlsx, o nazwach „Analiza raportów" oraz „Incydenty 2'16 IT", stanowiące wyciąg z oryginalnych logów systemu Symantec DLP i zawierające, m.in. szczegółowe informacje o dacie i godzinie kopiowania, nazwach kopiowanych plików, ścieżce docelowej oraz źródłowej dla kopiowanych plików oraz przypisanie czynności kopiowania do poszczególnych osób.

Na wniosek biegłego z dn. 07.09.2017 r., Spółka udostępniła pliki załączników w postaci wydruków w formie papierowej w liczbie 4.484 stron. Ponieważ taka forma dokumentacji znacząco utrudniała analizę, biegły w dn. 12.02.2018 r. wystąpił z wnioskiem o uzyskanie oryginalnych plików. Po kilkukrotnych prośbach biegłego o udostępnienie dokumentacji w oryginalnej wersji elektronicznej, Spółka przekazała oba pliki załączników w formie plików xlsx dopiero po rekomendacji uzyskanej przez Radę Nadzorczą Spółki w związku ze spotkaniem z biegłym. Sama wiadomość e-mail w formie elektronicznej nie została dostarczona biegłemu.

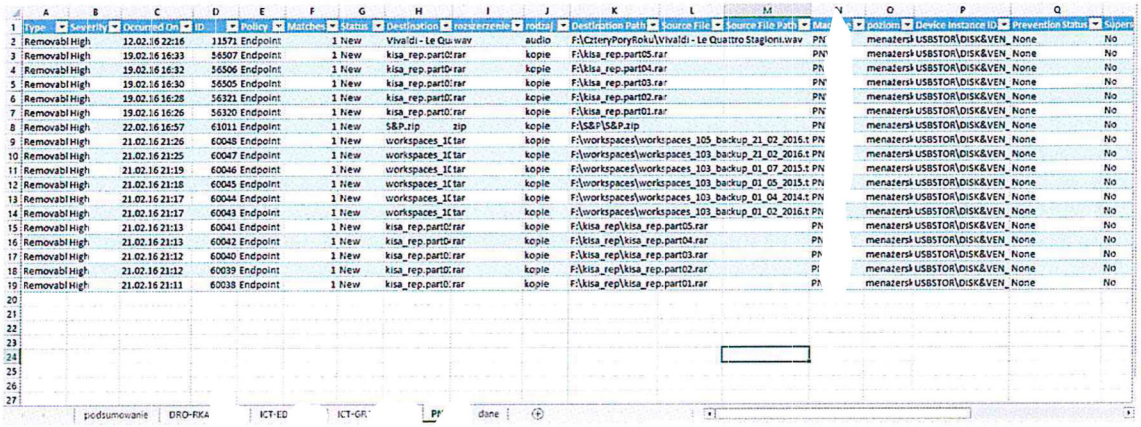
Na pytanie biegłego do Spółki podczas spotkania w dn. 25.06.2018 r. o możliwość udostępnienia oryginalnych logów z systemu Symantec DLP, które stanowiły podstawę analizy przeprowadzonej przez M G biegły uzyskał ustną informację od Wiceprezesa Zarządu Spółki Jarosława Orlikowskiego, z której wynika, że system DLP ten nie został oficjalnie wdrożony w Spółce (M G i K J uruchomili system do testów w lutym 2016 r. bez wiedzy Dyrektora IT P N co wynika m.in. z wypowiedzi Dyrektora IT P N w protokole z posiedzenia Rady Nadzorczej z dn. 08.08.2016 r. – przyp. biegłego) i nie zachowały się oryginalne logi z czasu wystąpienia incydentu, a także ich kopie. Biegły potwierdził, że na podstawie dokumentu *Instrukcji zarządzania systemem teleinformatycznym i jego bezpieczeństwem* pkt 5.3.13 „raporty z monitoringów są przeglądane i przechowywane co najmniej przez 6 miesięcy", a zatem Spółka nie była zobowiązana do przechowywania takich logów dłużej niż do 08.2016 r. (oryginały tych logów mogłyby być przedmiotem badania przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie, jednak w Oświadczeniu o przebiegu audytu bezpieczeństwa informatycznego z dn. 14.04.2016 r. sporządzonego przez tę firmę, brak jest wprost takiej informacji).

Spółka udostępniła także w postaci wydruków papierowych Spisy zdawczo-odbiorcze stanowiące ewidencję nośników (taśm magnetycznych), na których tworzone są kopie zapasowe kluczowych danych z systemów informatycznych i które następnie przechowywane są w archiwum. Spółka poinformowała przy tym biegłego w Piśmie Informacyjnym z dn. 20.09.2017 r., że przekazana dokumentacja to „wyciąg ze spisów obejmujących taśmy magnetyczne dotyczący okresu, w którym miał miejsce rzekomy incydent bezpieczeństwa środowiska teleinformatycznego zidentyfikowany przez osobę pełniącą w Spółce w dacie zdarzenia funkcję ABI". Niestety, biegły nie otrzymał od Spółki dostępu do środowiska teleinformatycznego celem zapoznania się z informacjami zawartymi na nośnikach (taśmach magnetycznych), z uwagi na stanowisko Spółki, iż takie działanie wykraczałoby poza zakres badania, do którego uprawniony jest biegły. Samo przekazanie spisu, bez dostępu do środowiska teleinformatycznego Spółki i przechowywanych w niej kopii zapasowych oraz informacji na nośnikach danych, nie stanowiło dla biegłego wartości w badaniu. Należy zaznaczyć, że biegły występował kilkakrotnie do Spółki z wnioskiem o umożliwienie mu dostępu do infrastruktury IT w celu ustalenia i zweryfikowania informacji i dokumentacji, w tym logów związanych z incydentem, w postaci oryginalnych plików i zapisów w systemach informatycznych, ale Spółka odmówiła, powołując się na przekroczenie zakresu badania biegłego określonego przez Sąd w niniejszej sprawie.

Na podstawie analizy przedstawionych przez Spółkę dokumentów biegły może stwierdzić, że zawierają one informacje dotyczące incydentów związanych z kopiowaniem plików z systemu informatycznego Spółki na urządzenia zewnętrzne w okresie 02-29.02.2016 r. Należy podkreślić, że w Spółce jako generalna zasada niedozwolone było kopiowanie danych na nośniki zewnętrzne, poza wyjątkami zatwierdzonymi uprzednio przez przełożonego Spółki, a zatem zastosowanie przez Spółkę systemu monitorującego zachowania pracowników Spółki, w tym np. zastosowanego przez Spółkę systemu DLP firmy Symantec w celu wykrywania uchybień było jak najbardziej uzasadnione.

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Type | Se | Occurred On | ID | Policy | | Status | Destination | rozszerzenie | Destination Path | Source File | Source File Path | Machine |
| 2 | Removable Storage | High | 21.02.16 21:11 | 60038 | Endpoint | 1 | New | kisa_rep.part01.rar | rar | F:\kisa_rep\kisa_rep.part01.rar | | | PN |
| 3 | Removable Storage | High | 21.02.16 21:12 | 60039 | Endpoint | 1 | New | kisa_rep.part02.rar | rar | F:\kisa_rep\kisa_rep.part02.rar | | | PN |
| 4 | Removable Storage | High | 21.02.16 21:12 | 60040 | Endpoint | 1 | New | kisa_rep.part03.rar | rar | F:\kisa_rep\kisa_rep.part03.rar | | | PN |
| 5 | Removable Storage | High | 21.02.16 21:13 | 60042 | Endpoint | 1 | New | kisa_rep.part04.rar | rar | F:\kisa_rep\kisa_rep.part04.rar | | | PN |
| 6 | Removable Storage | High | 21.02.16 21:13 | 60041 | Endpoint | 1 | New | kisa_rep.part05.rar | rar | F:\kisa_rep\kisa_rep.part05.rar | | | PN |
| 7 | Removable Storage | High | 21.02.16 21:17 | 60043 | Endpoint | 1 | New | workspaces_103_backup_01_02_2016.tar | tar | F:\workspaces\workspaces_103_backup_01_02_2016.t | | | PN |
| 8 | Removable Storage | High | 21.02.16 21:17 | 60044 | Endpoint | 1 | New | workspaces_103_backup_01_04_2014.tar | tar | F:\workspaces\workspaces_103_backup_01_04_2014.t | | | PN |
| 9 | Removable Storage | High | 21.02.16 21:18 | 60045 | Endpoint | 1 | New | workspaces_103_backup_01_05_2015.tar | tar | F:\workspaces\workspaces_103_backup_01_05_2015.t | | | PN |
| 10 | Removable Storage | High | 21.02.16 21:19 | 60046 | Endpoint | 1 | New | workspaces_103_backup_01_07_2015.tar | tar | F:\workspaces\workspaces_103_backup_01_07_2015.t | | | PN |
| 11 | Removable Storage | High | 21.02.16 21:25 | 60047 | Endpoint | 1 | New | workspaces_103_backup_21_02_2016.tar | tar | F:\workspaces\workspaces_103_backup_21_02_2016.t | | | PN |
| 12 | Removable Storage | High | 21.02.16 21:26 | 60048 | Endpoint | 1 | New | workspaces_105_backup_21_02_2016.tar | tar | F:\workspaces\workspaces_105_backup_21_02_2016.t | | | PN |
| 13 | Removable Storage | High | 22.02.16 16:57 | 61011 | Endpoint | 1 | New | S&P.zip | zip | F:\S&P\S&P.zip | | | PN |
| 21 | Removable Storage | High | 19.02.16 16:26 | 56320 | Endpoint | 1 | New | kisa_rep.part01.rar | rar | F:\kisa_rep.part01.rar | | | PN |
| 22 | Removable Storage | High | 19.02.16 16:28 | 56321 | Endpoint | 1 | New | kisa_rep.part02.rar | rar | F:\kisa_rep.part02.rar | | | PN |
| 23 | Removable Storage | High | 19.02.16 16:30 | 56505 | Endpoint | 1 | New | kisa_rep.part03.rar | rar | F:\kisa_rep.part03.rar | | | PN |
| 24 | Removable Storage | High | 19.02.16 16:32 | 56506 | Endpoint | 1 | New | kisa_rep.part04.rar | rar | F:\kisa_rep.part04.rar | | | PN |
| 25 | Removable Storage | High | 19.02.16 16:33 | 56507 | Endpoint | 1 | New | kisa_rep.part05.rar | rar | F:\kisa_rep.part05.rar | | | PN |

*Fragment pliku Analiza raportów.xlsx*



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Type | Severity | Occurred On | ID | Policy | Matches | Status | Destination | rozszerzenie | rodzaj | Destination Path | Source File | Source File Path | Ma | poziom | Device Instance ID | Prevention Status | Super |
| 2 | Removabl | High | 12.02.16 22:16 | 11571 | Endpoint | 1 | New | Vivaldi - Le Qu | wav | audio | F:\CzteryPoryRoku\Vivaldi - Le Quattro Stagioni.wav | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 3 | Removabl | High | 19.02.16 16:33 | 56507 | Endpoint | 1 | New | kisa_rep.part05.rar | | kopie | F:\kisa_rep.part05.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 4 | Removabl | High | 19.02.16 16:32 | 56506 | Endpoint | 1 | New | kisa_rep.part04.rar | | kopie | F:\kisa_rep.part04.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 5 | Removabl | High | 19.02.16 16:30 | 56505 | Endpoint | 1 | New | kisa_rep.part03.rar | | kopie | F:\kisa_rep.part03.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 6 | Removabl | High | 19.02.16 16:28 | 56321 | Endpoint | 1 | New | kisa_rep.part02.rar | | kopie | F:\kisa_rep.part02.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 7 | Removabl | High | 19.02.16 16:26 | 56320 | Endpoint | 1 | New | kisa_rep.part01.rar | | kopie | F:\kisa_rep.part01.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 8 | Removabl | High | 22.02.16 16:57 | 61011 | Endpoint | 1 | New | S&P.zip | zip | kopie | F:\S&P\S&P.zip | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 9 | Removabl | High | 21.02.16 21:26 | 60048 | Endpoint | 1 | New | workspaces_1( | tar | kopie | F:\workspaces\workspaces_105_backup_21_02_2016.t | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 10 | Removabl | High | 21.02.16 21:25 | 60047 | Endpoint | 1 | New | workspaces_1( | tar | kopie | F:\workspaces\workspaces_103_backup_21_02_2016.t | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 11 | Removabl | High | 21.02.16 21:19 | 60046 | Endpoint | 1 | New | workspaces_1( | tar | kopie | F:\workspaces\workspaces_103_backup_01_07_2015.t | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 12 | Removabl | High | 21.02.16 21:18 | 60045 | Endpoint | 1 | New | workspaces_1( | tar | kopie | F:\workspaces\workspaces_103_backup_01_05_2015.t | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 13 | Removabl | High | 21.02.16 21:17 | 60044 | Endpoint | 1 | New | workspaces_1( | tar | kopie | F:\workspaces\workspaces_103_backup_01_04_2014.t | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 14 | Removabl | High | 21.02.16 21:17 | 60043 | Endpoint | 1 | New | workspaces_1( | tar | kopie | F:\workspaces\workspaces_103_backup_01_02_2016.t | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 15 | Removabl | High | 21.02.16 21:13 | 60041 | Endpoint | 1 | New | kisa_rep.part05.rar | | kopie | F:\kisa_rep\kisa_rep.part05.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 16 | Removabl | High | 21.02.16 21:13 | 60042 | Endpoint | 1 | New | kisa_rep.part04.rar | | kopie | F:\kisa_rep\kisa_rep.part04.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 17 | Removabl | High | 21.02.16 21:12 | 60040 | Endpoint | 1 | New | kisa_rep.part03.rar | | kopie | F:\kisa_rep\kisa_rep.part03.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 18 | Removabl | High | 21.02.16 21:12 | 60039 | Endpoint | 1 | New | kisa_rep.part02.rar | | kopie | F:\kisa_rep\kisa_rep.part02.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 19 | Removabl | High | 21.02.16 21:11 | 60038 | Endpoint | 1 | New | kisa_rep.part01.rar | | kopie | F:\kisa_rep\kisa_rep.part01.rar | | PN | | menaterstv | USBSTOR\DISK&VEN_ | None | No |
| 20 | | | | | | | | | | | | | | | | | |
| 21 | | | | | | | | | | | | | | | | | |
| 22 | | | | | | | | | | | | | | | | | |
| 23 | | | | | | | | | | | | | | | | | |
| 24 | | | | | | | | | | | | | | | | | |
| 25 | | | | | | | | | | | | | | | | | |
| 26 | | | | | | | | | | | | | | | | | |
| 27 | | | | | | | | | | | | | | | | | |

podsumowanie | DRO-FKA | ICT-ED | ICT-GR | PP | dane

*Fragment pliku Incydenty 2'16IT.xlsx*

Zawartość plików stanowiących załączniki do badanej wiadomości e-mail pozwala na ustalenie:

- osób, które kopiowały dane (Podłowski, N , Ż , A M K D C ,
- dokładnej daty i godziny kopiowania każdego z plików,
- prawdopodobnej zawartości niektórych z plików (na podstawie rozszerzenia pliku i/lub jego nazwy – np. plików MP3 jako plików muzycznych lub AVI jako plików wideo).

Wskazane pliki xlsx udostępnione biegłemu do badania nie zawierają jednak takich informacji, jak:

- realna zawartość kopiowanych plików (kopiowane pliki są wymienione jedynie z nazwy, jednak ich zawartość / treść nie są załączone do dokumentów),
- wielkość kopiowanych plików (można jedynie domyślać się ich wielkości po różnicach w czasie kopiowania kolejnych plików, co zostało opisane w kolejnym rozdziale niniejszego dokumentu).

Szczegółowe informacje związane z analizą danych przez biegłego zostały przedstawione w kolejnym rozdziale niniejszego dokumentu.

## Ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów

W badanej wiadomości e-mail z dn. 04.03.2016 r. M G zgodnie z obowiązującymi w Spółce procedurami poinformowała ówczesnego Prezesa Zarządu Spółki Pawła Szewczyka, z kopią do przełożonego P N , o wykrytych incydentach kopiowania danych na nośniki zewnętrzne i poprosiła o udzielenie dodatkowych informacji, które były istotne do wyjaśnienia tej okoliczności. W szczególności dotyczyło to wskazanych w wiadomości e-mail plików archiwum RAR i TAR kopiowanych przez samego Dyrektora IT P N

„W raporcie zarejestrowana jest kilkakrotnie operacja kopiowania dużych spakowanych plików danych. (...) Z nazw plików wynika, że zawierają one dane z serwera *kisa_reporting*, na którym jest hurtownia danych oraz projekty aplikacji. W związku z czym proszę Dyrektora IT (P N z którego komputera były kopiowane te dane – przyp. biegłego) o informacje jaka była/jest zawartość tych plików oraz cel kopiowania na urządzenia zewnętrzne."

Dotyczy to następujących plików:

| | |
|---|---|
| 21.02.16 21:11 | kisa_rep.part01.rar |
| 21.02.16 21:12 | kisa_rep.part02.rar |
| 21.02.16 21:12 | kisa_rep.part03.rar |
| 21.02.16 21:13 | kisa_rep.part04.rar |
| 21.02.16 21:13 | kisa_rep.part05.rar |
| 21.02.16 21:17 | workspaces_103_backup_01_02_2016.tar |
| 21.02.16 21:17 | workspaces_103_backup_01_04_2014.tar |
| 21.02.16 21:18 | workspaces_103_backup_01_05_2015.tar |
| 21.02.16 21:19 | workspaces_103_backup_01_07_2015.tar |
| 21.02.16 21:25 | workspaces_103_backup_21_02_2016.tar |
| 21.02.16 21:26 | workspaces_105_backup_21_02_2016.tar |
| 19.02.16 16:26 | kisa_rep.part01.rar |
| 19.02.16 16:28 | kisa_rep.part02.rar |
| 19.02.16 16:30 | kisa_rep.part03.rar |
| 19.02.16 16:32 | kisa_rep.part04.rar |
| 19.02.16 16:33 | kisa_rep.part05.rar |

Biegły wystąpił do Spółki z wnioskiem o udostępnienie wyżej wskazanych plików oraz dalszej wewnętrznej korespondencji na ten temat, w szczególności odpowiedzi Dyrektora IT P N· ale Spółka odmówiła udostępnienia wnioskowanych danych, powołując się na przekroczenie zakresu badania biegłego określonego przez Sąd w niniejszej sprawie.

Na pytanie biegłego w piśmie z dn. 12.02.2018 r. o to, czy przez Spółkę została wykonana analiza rzeczywistej lub domniemanej zawartości plików z rozszerzeniami .rar i .tar i czy ustalono, co znajdowało się w tych plikach, Spółka odpowiedziała w protokole ze spotkania z dn. 30.05.2018 r., iż:

„W wyniku analizy kopiowanych danych ustalono, że wśród danych, które zostały skopiowane nie było baz danych osobowych, lecz były (I) dane analityczne, zagregowane, przeznaczone do modelowego opracowania w oprogramowaniu klasy BI (hurtownia danych), (II) kopie dokumentacji związanej z bieżącą działalnością zespołu obsługi prawnej oraz (III) działu rachunkowości (...)".

W odpowiedzi na pytanie biegłego o działania, jakie zostały wykonane i zlecone przez Spółkę celem wewnętrznego zbadania incydentu, Spółka sprecyzowała informacje w protokole ze spotkania z biegłym z dn. 12.02.2018 r., iż:

„(...) W dniach od 9 do 12 czerwca 2017 roku pracownik działu IT – ekspert bezpieczeństwa informatycznego – dokonał na zlecenie Zarządu identyfikacji na podstawie logów plików kopiowanych przez użytkowników. W wyniku tej identyfikacji pracownik Działu IT stwierdził, że:

1. Piotr Podłowski (Dyrektor Pionu Finansowego/Główny Księgowy Grupy Kapitałowej) kopiował: dokumenty służbowe w formacie plików Office, dokumenty służbowe w formacie pdf, e-maile, baza WASCO (związana z adresami i kodami GUS);
2. P N (Dyrektor IT) wykonywał kopię środowiska analitycznego do analizy danych finansowych (bez danych w bazie i bez danych osobowych) oraz kopiował pliki muzyczne;
3. E Ż ·N (Kierownik Zespołu Obsługi Prawnej, radca prawny) kopiowała: dokumenty służbowe w formacie plików Office, dokumenty służbowe w formacie plików pdf, pliki graficzne (procedury BHP, szkolenia), zdjęcia oraz wiadomości e-mail; (...)".

W ocenie biegłego, po analizie dostarczonych plików i informacji, plikami kopiowanymi na nośniki zewnętrzne, które mogły zawierać (potencjalne) dane osobowe, były pliki archiwum RAR i TAR wskazane w wiadomości e-mail przez M G , a kopiowane z konta P N

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Type | Se | Occurred On | ID | Policy | | Status | Destination | rozszerzenie | Destination Path | Source File | Source File Path | Machine |
| 2 | Removable Storage | High | 21.02.16 21:11 | 60038 | Endpoint | | 1 New | kisa_rep.part01.rar | rar | F:\kisa_rep\kisa_rep.part01.rar | | | PN |
| 3 | Removable Storage | High | 21.02.16 21:12 | 60039 | Endpoint | | 1 New | kisa_rep.part02.rar | rar | F:\kisa_rep\kisa_rep.part02.rar | | | PN |
| 4 | Removable Storage | High | 21.02.16 21:12 | 60040 | Endpoint | | 1 New | kisa_rep.part03.rar | rar | F:\kisa_rep\kisa_rep.part03.rar | | | PN |
| 5 | Removable Storage | High | 21.02.16 21:13 | 60042 | Endpoint | | 1 New | kisa_rep.part04.rar | rar | F:\kisa_rep\kisa_rep.part04.rar | | | PN |
| 6 | Removable Storage | High | 21.02.16 21:13 | 60041 | Endpoint | | 1 New | kisa_rep.part05.rar | rar | F:\kisa_rep\kisa_rep.part05.rar | | | P |
| 7 | Removable Storage | High | 21.02.16 21:17 | 60043 | Endpoint | | 1 New | workspaces_103_backup_01_02_2016.tar | tar | F:\workspaces\workspaces_103_backup_01_02_2016.t | | | P |
| 8 | Removable Storage | High | 21.02.16 21:17 | 60044 | Endpoint | | 1 New | workspaces_103_backup_01_04_2014.tar | tar | F:\workspaces\workspaces_103_backup_01_04_2014.t | | | P |
| 9 | Removable Storage | High | 21.02.16 21:18 | 60045 | Endpoint | | 1 New | workspaces_103_backup_01_05_2015.tar | tar | F:\workspaces\workspaces_103_backup_01_05_2015.t | | | P |
| 10 | Removable Storage | High | 21.02.16 21:19 | 60046 | Endpoint | | 1 New | workspaces_103_backup_01_07_2015.tar | tar | F:\workspaces\workspaces_103_backup_01_07_2015.t | | | P |
| 11 | Removable Storage | High | 21.02.16 21:25 | 60047 | Endpoint | | 1 New | workspaces_103_backup_21_02_2016.tar | tar | F:\workspaces\workspaces_103_backup_21_02_2016.t | | | PN |
| 12 | Removable Storage | High | 21.02.16 21:26 | 60048 | Endpoint | | 1 New | workspaces_105_backup_21_02_2016.tar | tar | F:\workspaces\workspaces_105_backup_21_02_2016.t | | | PN |
| 13 | Removable Storage | High | 22.02.16 16:57 | 61011 | Endpoint | | 1 New | S&P.zip | zip | F:\S&P\S&P.zip | | | PN |
| 21 | Removable Storage | High | 19.02.16 16:26 | 56320 | Endpoint | | 1 New | kisa_rep.part01.rar | rar | F:\kisa_rep.part01.rar | | | PN |
| 22 | Removable Storage | High | 19.02.16 16:28 | 56321 | Endpoint | | 1 New | kisa_rep.part02.rar | rar | F:\kisa_rep.part02.rar | | | P |
| 23 | Removable Storage | High | 19.02.16 16:30 | 56505 | Endpoint | | 1 New | kisa_rep.part03.rar | rar | F:\kisa_rep.part03.rar | | | P |
| 24 | Removable Storage | High | 19.02.16 16:32 | 56506 | Endpoint | | 1 New | kisa_rep.part04.rar | rar | F:\kisa_rep.part04.rar | | | PN |
| 25 | Removable Storage | High | 19.02.16 16:33 | 56507 | Endpoint | | 1 New | kisa_rep.part05.rar | rar | F:\kisa_rep.part05.rar | | | PN |

*Pliki TAR i RAR kopiowane przez P N fragment pliku Analiza raportów.xlsx*

Jak już wspomniano w poprzednim rozdziale, na podstawie analizy wyciągu z logów nie można określić realnej zawartości tych plików. Istnieją jednak pewne przesłanki, które mogą wskazywać, że pliki te mogły zawierać dane poufne dot. Spółki, w tym także dane osobowe:

1. Nazwa plików „kisa_rep" może wskazywać na pochodzenie ich zawartości z serwera *kisa_reporting*, co zostało wskazane w wiadomości e-mail M G w następujący sposób: „Z nazw plików wynika, że zawierają one dane z serwera *kisa_reporting*, na którym jest hurtownia danych oraz projekty aplikacji."

2. Pliki archiwum RAR „kisa_rep" o numerach 01-05 wskazują, że był to jeden bardzo duży plik archiwum RAR podzielony na 5 mniejszych plików. Zazwyczaj taki podział służy ułatwieniu kopiowania dużych plików na nośniki zewnętrzne o mniejszej pojemności lub też przyspieszeniu wykonywania kopii.

3. Kopiowanie plików „kisa_rep" miało miejsce dwukrotnie, przy czym dn. 21.02.2016 r. trwało przynajmniej 3 minuty, a w dn. 19.02.2016 r. przynajmniej 8 minut. Zwłaszcza w tym drugim przypadku prawie każda z części archiwum RAR kopiowała się na nośnik zewnętrzny przez 2 minuty. Biorąc pod uwagę średnią wydajność obecnych komputerów, w ciągu 2 minut można skopiować na nośnik USB plik o wielkości 1 GB. Oznacza to, że pełny plik archiwum „kisa_rep" mógł zawierać ok. 8 GB danych lub więcej. Po wielkości pliku można zatem przyjąć, że mógł on stanowić kopię danych całego środowiska informatycznego.

4. Nazwy plików archiwum TAR „workspaces_backup" wskazują na pochodzenie ich zawartości ze środowisk testowych jakiegoś systemu lub aplikacji w wersjach odpowiednio 103 i 105. Kopiowanie każdego z tych plików także trwało ok. 1 minuty, co pozwala określić ich rozmiar na przynajmniej ok. 512 MB. Przy założeniu, że pliki te zostały kopiowane jeden za drugim w ramach jednej operacji kopiowania (czego nie da się jednoznacznie określić na podstawie analizowanych logów), to skopiowanie pliku *workspaces_103_backup_01_07_2015.tar* trwało 6 minut, co wskazywało by, że plik ten mógłby mieć rozmiar ok. 3 GB.

5. W raporcie z audytu bezpieczeństwa systemu informatycznego przeprowadzonego przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie wykazano w pkt. 5, że:
   „Zagrożeniem dla poufności danych osobowych dłużników może być (...) stosowanie niezanonimizowanych zbiorów danych w środowiskach testowych". Nie wskazano w tym raporcie jakich konkretnie środowisk testowych może dotyczyć problem, ale tym bardziej może to dotyczyć środowisk związanych z hurtownią danych.

6. W analizowanych logach, przy plikach RAR i TAR brakuje wskazania ścieżki źródłowej tych plików. Nie można zatem jednoznacznie określić z jakiego miejsca zostały one skopiowane. Nie da się także określić, jakie dane zostały uprzednio umieszczone w archiwach RAR i TAR. A zatem bazując jedynie na logach nie można jednoznacznie wskazać, że kopiowane pliki zawierały „kopię środowiska analitycznego do analizy danych finansowych (bez danych w bazie i bez danych osobowych)" i wykluczyć, że nie zawierały one danych osobowych. Stanowisko Spółki w tej kwestii jest zatem w opinii biegłego nieuzasadnione, a rzetelne sprawdzenie tego incydentu wymaga dodatkowych działań związanych z bezpośrednim dostępem do infrastruktury teleinformatycznej Spółki, na co biegły nie uzyskał zgody Spółki, pomimo licznych wniosków w tym zakresie.

7. W szczególności, jeśli w opinii Spółki kopiowanie dotyczyło „kopii środowiska analitycznego do analizy danych finansowych", to rozpoznane w ten sposób pliki RAR i TAR powinny zostać zarchiwizowane zgodnie z obowiązującymi w Spółce procedurami, wynikającymi, np. z Polityki bezpieczeństwa, pkt. 5.4.1 w brzmieniu:
   „Aby zapewnić ciągłość działania w przypadku awarii lub katastrofy należy sporządzać awaryjne kopie: danych, instancji systemów informatycznych oraz konfiguracji kluczowych komponentów infrastruktury informatycznej", uszczegółowionymi w załączniku nr 3 do Polityki bezpieczeństwa

dotyczącym Procedury tworzenia kopii zapasowych. Jeśli pliki te podlegały pod procedurę dotyczącą kopii baz danych lub serwerów plikowych to powinny być przechowywane przez okres 10 lat zgodnie z postanowieniami Polityki bezpieczeństwa. **Jeżeli zatem kopie tych plików są dostępne w archiwum (a powinny być zgodnie z wewnętrznymi procedurami), to powinny zostać poddane analizie pod kątem ich zawartości, czego Spółka do tej pory nie zrobiła w ramach żadnego z działań mających na celu zbadanie incydentu – nie wyrażono także zgody na udostępnienie takich plików biegłemu w ramach niniejszego badania. Jeżeli zaś pliki te nie zostały poprawnie zarchiwizowane, to może to stanowić naruszenie polityki bezpieczeństwa Spółki.**

## Ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce, na dzień zdarzenia, procedurami wewnętrznymi z zakresu bezpieczeństwa danych

Należy wskazać, że od początku działań biegłego Spółka stała przy stanowisku, że żaden incydent związany z wyciekiem danych w Spółce nie miał miejsca, np. w pkt. 1 protokołu ze spotkania z dn. 12.02.2018 r.:

„Jakkolwiek doszło do zgłoszenia przez osobę pełniącą funkcję ABI w lutym 2016 r. – M G możliwości zidentyfikowania rzekomego wycieku danych tak po weryfikacji okazało się, iż taki wyciek danych, w szczególności dotyczący danych osobowych, a już na pewno danych dłużników, nie miał miejsca".

Wspomniana wyżej weryfikacja opierała się przede wszystkim na zamówieniu przez Spółkę audytu w firmie CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie (którego wyniki zostały zaopiniowane przez biegłego w następnym rozdziale niniejszego opracowania) oraz wewnętrznego audytu wykonanego przez pracownika Działu IT Spółki w dniach 09-12.06.2017 r. (którego ustalenia zostały zaopiniowane przez biegłego w poprzednim rozdziale niniejszego opracowania). W opinii biegłego żaden z tych audytów nie wykazał, że incydent związany z wyciekiem danych nie miał miejsca.

Dodatkową niejasnością jest stanowisko ówczesnego Prezesa Zarządu Spółki – Pawła Szewczyka wyrażone podczas Nadzwyczajnego Walnego Zgromadzenia Akcjonariuszy Spółki w dn. 05.04.2016 r, zachowane na nagraniu dołączonym do akt sprawy:

„W firmie zidentyfikowano rzeczywiście kopiowanie jakichś danych i nie dziewiętnastego, między dziewiętnastym a dwudziestym pierwszym, a dokładnie od dziesiątego lutego i w tej chwili trwa wewnętrzny audyt, który to identyfikuje."

Szczególnie zaskakujące jest wskazanie daty 10.02.2016 r. jako dokładnej daty rozpoczęcia wykrytego kopiowania danych. W analizie logów systemu DLP załączonej bowiem do wiadomości wysłanej przez M G występują incydenty kopiowania plików od 02.02 do 29.02. 2016 r, w tym także w dniach 09.02 i 11.02.2016 r., ale nie ma ani jednej wzmianki dotyczącej dn. 10.02.2016 r. Wynika z tego, że Spółka mogła posiadać jakieś dodatkowe informacje dotyczące incydentu, które jednak nie

zostały przekazane innym audytorom ani biegłemu w niniejszej sprawie – wszystkie analizy opierały się bowiem o logi wskazane w wiadomości przez M G

W dokumencie „Stanowisko uczestnika w przedmiocie wniosku o wyznaczenie rewidenta do spraw szczególnych" z dn. 25.01.2017 r., załączonym do akt sprawy w t. XXX na stronie 4281, Spółka prezentuje następujące stanowisko:

„(...) prawdopodobnie przyczyną rzekomych doniesień o wycieku danych mogła być wykonywana przez Dyrektora Działu IT P. N multiplikacja oprogramowania (nie zaś danych osobowych) na nośnik zawierający te dane i przekazany Dyrektorowi ds. Bezpieczeństwa, co prawdopodobnie było przez P. M G nieprawidłowo zinterpretowane (...). Dyrektor Działu IT P N posiadał uprawnienia do kopiowania plików na dysk zewnętrzny. Wszelkie dane przechowywane były w specjalnie przygotowanym do tego miejscu. Działanie to wynikało z objętej klauzulą poufności operacji polegającej na zapewnieniu niezakłóconej ciągłości działania Spółki w sytuacji kryzysowej, w którą zaangażowany był m.in. P N "

O działaniach objętych klauzulą poufności operacji polegającej na zapewnieniu niezakłóconej ciągłości działania Spółki w sytuacji kryzysowej biegły został także poinformowany w pkt. 4 Protokołu ze spotkania z dn. 12.02.2018 r., gdzie Spółka wskazała, że został powołany zespół zadaniowy do realizacji Zabezpieczenia Kluczowych Obszarów Spółki w Sytuacji Nadzwyczajnej:

„W okresie poprzedzającym rzekomy incydent, tj. w dniu 26 stycznia 2016 r. powołany został zespół zadaniowy funkcjonujący pod nazwą Zabezpieczenie Kluczowych Obszarów Spółki w Sytuacji Nadzwyczajnej ('Zespół'). Z dokumentacji Zespołu wynika, że określone osoby zostały wyposażone w fizycznie oznaczone nośniki danych w celu zabezpieczenia kluczowych obszarów funkcjonowania Spółki i Grupy Kapitałowej oraz zabezpieczenie ciągłości jej działania w sytuacji nadzwyczajnej jaką było zewnętrzne i wewnętrzne oddziaływanie mniejszościowego akcjonariusza Spółki to jest spółki BEST S.A. (...). Ówczesny Zarząd Spółki stwierdził, że w sytuacji zagrożenia wrogim przejęciem koniecznym było zabezpieczenie określonych danych umożliwiających podjęcie dalszej działalności Spółki nawet poza jej siedzibą."

Na wniosek biegłego Spółka udostępniła dokumenty w formie wydruków związane z działalnością Zespołu. Na ich podstawie biegły stwierdził, że Zespół działał w Spółce od 26.01.2016 r. do 12.04.2016 r.

Bazując na dokumentach i informacjach udostępnionych przez Spółkę biegły ustalił i opiniuje jak poniżej:

8. Procedury wewnętrzne Spółki obejmują blokowanie możliwości użycia wymiennych nośników danych na stacjach roboczych. Wyjątki od tych zasad wymagają zgody przełożonego i są rejestrowane poprzez system zgłoszeń. Zostało to potwierdzone m.in. w pkt. 5 Oświadczenia o przebiegu audytu bezpieczeństwa informatycznego wykonanego przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie. W tej sytuacji postępowanie M G związane z próbą wyjaśnienia incydentów kopiowania danych na nośniki zewnętrzne było zgodne z procedurami Spółki.

9. M G nie została włączona w skład Zespołu i nie wiedziała o jego funkcjonowaniu. Z kolei P N i inni członkowie Zespołu nie byli świadomi testowego uruchomienia systemu DLP firmy Symantec (przy czym na podstawie analizy historii wiadomości e-mail z dn. 04.03.2018 r. przesłanej przez M G do Prezesa Zarządu Spółki – Pawła Szewczyka, wynika że Dyrektor IT – P N był informowany wcześniej (nie wiadomo jednak kiedy dokładnie) przez pracownika Działu IT – K J „o wdrożeniu na początku roku (2016 – przyp. biegłego) nowej funkcjonalności pakietu zabezpieczającego Symantec, która pozwala kompleksowo monitorować i raportować zdarzenia na stacjach roboczych, wskazując te które mogą stanowić naruszenie bezpieczeństwa" – e-mail ten został wysłany przez K J do M G , z kopią do Pawła Szewczyka i P N ).

   Wykryte w ten sposób przez M G incydenty kopiowania danych mogły być efektem działań Zespołu, ale nie zostało to nigdy jednoznacznie potwierdzone przez Spółkę. Na tej samej podstawie nie można wykluczyć, że wykryte incydenty nie były powiązane z pracą Zespołu i bez dogłębnej analizy zawartości skopiowanych plików (co zostało biegłemu odmówione w ramach dostępu do infrastruktury teleinformatycznej Spółki) nie można jednoznacznie wykluczyć możliwości skopiowania danych poufnych Spółki (w tym osobowych).

10. Sam fakt powołania Zespołu, wyposażenia go w zewnętrzne nośniki danych i umożliwienia kopiowania na nie danych Spółki mógł skutkować celowym lub przypadkowym wyniesieniem wrażliwych danych poza obszar działania Spółki. Wynika to zwłaszcza z użytego już wcześniej cytatu ze Stanowiska Spółki: „Ówczesny Zarząd Spółki stwierdził, że w sytuacji zagrożenia wrogim

przejęciem koniecznym było zabezpieczenie określonych danych umożliwiających podjęcie dalszej działalności Spółki nawet poza jej siedzibą".

Z decyzji nr DPZ 1/01/2016 z dn. 26.01.2016 r. w sprawie powołania Zespołu Zadaniowego nie wynikają szczegółowe zasady jego działania, w szczególności w jaki sposób i gdzie przechowywane miałyby być dyski przenośne powierzone członkom Zespołu w dniach 26.01. – 06.04.2016 r. (do czasu przekazania ostatniego z nich D O – Dyrektorowi Bezpieczeństwa Korporacyjnego Spółki, co zostało udokumentowane w postaci protokołów zdawczo-odbiorczych). Osoby wchodzące w skład Zespołu, które ewentualnie chciałyby działać na szkodę Spółki i wynieść dane poufne Spółki, pozostawały w tym czasie poza kontrolą Spółki.

11. Incydenty związane z kopiowaniem danych wskazane przez M G miały miejsce także poza godzinami pracy, np. w niedzielę wieczorem 21.02.2016 w godz. 21:11-21:26 (P N ), czy w piątek 26.02.2016 w godz. 19:22 – 20:10 (Piotr Podłowski). W opinii biegłego fakt ten może wskazywać na chęć ukrycia przed pracownikami Spółki działań związanych z kopiowaniem danych.

12. Skoro celem działań Zespołu było zabezpieczenie ciągłości działania Spółki, to można zakładać, że skopiowano także dane osobowe przetwarzane przez Spółkę. W pkt. (III) Decyzji Nr DPZ 1/01/2016 w sprawie powołania Zespołu Zadaniowego z dn. 26.01.2016 r. jest wskazane „wykonanie niezbędnych czynności zapobiegawczych przed utratą danych, w szczególności wykonanie i zabezpieczenie w celu zapewnienia ciągłości działania procesów operacyjnych kopii kluczowych zasobów zgromadzonych w systemach informatycznych". Z praktyki biegłego, trudno sobie wyobrazić zabezpieczenie kluczowych zasobów bez uwzględnienia danych wierzycieli obsługiwanych przez Spółkę. W opinii biegłego można przyjąć, że takie dane były kopiowane przez członków Zespołu.

13. W sytuacji, gdy Zarząd Spółki powołał Zespół Zadaniowy, który funkcjonował w utajnieniu w czasie wystąpienia incydentów wskazanych przez M G , zastanawiający jest fakt braku powiązania tych incydentów z działaniami Zespołu i podjęcie przez Spółkę decyzji o przeprowadzeniu audytu bezpieczeństwa przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie. Członkowie Zespołu, w tym P. N i P. Podłowski, mogli bowiem z łatwością określić, czy proces kopiowania prowadzony prz z nich i uwzględniony w logach

systemu DLP był realizowany w ramach działań operacyjnych Zespołu, czy też nie. Pomimo tego sam Zespół był inicjatorem konieczności przeprowadzenia audytu bezpieczeństwa, co zostało wskazane w dokumencie „Podsumowanie prac zespołu zadaniowego z dn. 08.04.2016 r.". Jednocześnie Spółka stała i nadal stoi przy stanowisku, że jednym z głównych celów przeprowadzenia audytu przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie było zbadanie incydentów wskazanych przez M G , chociażby w cytowanym już stanowisku ówczesnego Prezesa Zarządu Spółki Pawła Szewczyka wyrażonym podczas Nadzwyczajnego Walnego Zgromadzenia Akcjonariuszy Spółki w dn. 05.04.2016 r., zachowanym na nagraniu dołączonym do akt sprawy:

„W firmie zidentyfikowano rzeczywiście kopiowanie jakichś danych i nie dziewiętnastego, między dziewiętnastym a dwudziestym pierwszym, a dokładnie od dziesiątego lutego i w tej chwili trwa wewnętrzny audyt, który to identyfikuje."

Na podstawie ww. faktów, w opinii biegłego incydenty wskazane przez M G w mailu z dn. 04.03.2016 r. nie powinny być łączone z pracami Zespołu. W związku z tym, badanie powinno zostać przeprowadzone w oparciu o dane pochodzące bezpośrednio z systemów IT Spółki, na co jednak biegły, pomimo składanych wniosków, nie uzyskał zgody Spółki (co zostało wskazane powyżej).

14. Dodatkowo należy wskazać, że na podstawie analizy nazw i typów kopiowanych plików wskazanych w załącznikach do wiadomości e-mail M G można zauważyć, że pomimo obowiązujących w Spółce procedur, osoby posiadające zgodę przełożonego na korzystanie z portów USB w uzasadnionych przypadkach wykorzystywały ten przywilej także do przenoszenia plików wykraczających poza uzasadniony przypadek, takich jak np. filmy chronione prawem autorskim (Zjawa.2015.PLSUBBED.DVDSCr .XViD.AC3-majorq-LTS.avi – G ), czy też wzory haftów (Księżniczka z pieskiem 2.pdf – J ). Stanowi to naruszenie wewnętrznych procedur Spółki.

## Ustalenie czy audyt bezpieczeństwa informatycznego przeprowadzony przez CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj A. z siedzibą w Lublinie na zlecenie Spółki obejmował ustalenie okoliczności badanego incydentu

Na podstawie analizy „Oświadczenia o przebiegu audytu bezpieczeństwa informatycznego sporządzonego przez firmę CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie" biegły stwierdza, że audyt ten nie wykazał jednoznacznych podstaw do stwierdzenia, czy w Spółce doszło, czy też nie doszło do wycieku danych.

Audytor nie wykonał wymaganej w takich przypadkach analizy powłamaniowej, a jedynie testy penetracyjne i analizę procedur, na podstawie których nie ma możliwości potwierdzenia lub zanegowania faktu wycieku danych. W szczególności w oświadczeniu audytora brakuje jakiejkolwiek wzmianki o wykonaniu czynności audytowych prowadzących do zbadania incydentu stanowiącego przedmiot niniejszego badania biegłego, takich jak:

d) ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia;
e) ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów, o których mowa w lit. a) powyżej;
f) ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce na dzień zdarzenia procedurami wewnętrznymi z zakresu bezpieczeństwa danych;

Na podstawie udostępnionych dokumentów biegły opiniuje jak poniżej:

1. Testy penetracyjne nie są metodą pozwalającą na weryfikowanie faktu wycieku danych. Mogą wskazać jedynie luki i podatności istniejące w testowanych systemach informatycznych, za pomocą których osoby niepowołane mogłyby uzyskać dostęp do tych systemów i przetwarzanych przez nie danych lub dokonać innego ataku hackerskiego. Zamówienie usługi polegającej na przeprowadzeniu testów penetracyjnych nie mogło zatem prowadzić do zbadania konkretnych incydentów związanych z bezpieczeństwem danych.

2. Analiza procedur ochrony informacji nie jest metodą pozwalającą na weryfikowanie faktu wycieku danych. Same procedury i procesy mogą być świetnie opisane, ale mogą nie być odpowiednio wdrożone – i właśnie stopień wdrożenia tych procedur oraz dowody ich rzeczywistego funkcjonowania powinny być celem audytu.

3. Odnośnie pkt. 1 Oświadczenia o przebiegu audytu – „Nie stwierdzono wad zabezpieczeń technicznych, które można wykorzystać do zdobycia danych osobowych dłużników poprzez działanie zdalne". Mowa tutaj jedynie o fakcie stwierdzenia wykorzystywania przez klienta infrastruktury IT zabezpieczającej wyłącznie przed atakami z zewnątrz (czyli z Internetu). Sam fakt istnienia takich urządzeń oraz ich poprawnej konfiguracji nie daje możliwości zweryfikowania, czy do faktycznych ataków na dane doszło – nawet takich z zewnątrz. Należałoby zweryfikować rzeczywistą skuteczność tych urządzeń oraz sprawdzić dzienniki ich aktywności w dniach, w których doszło do domniemanego wycieku, ale takich informacji brakuje w oświadczeniu audytora. Punkt ten nie dotyczy w ogóle sytuacji, gdy do ataku może dojść wewnątrz Spółki.

4. Odnośnie pkt. 2 Oświadczenia o przebieg audytu – Błąd w konfiguracji urządzenia RouterBOARD. Opis dotyczy najprawdopodobniej niezabezpieczonego dostępu administracyjnego do sieci bezprzewodowej stworzonej specjalnie na potrzeby działu IT. Opis jest jednak zbyt ogólny, aby określić faktyczne zagrożenie. Nie wiadomo dokładnie jaki był błąd i jaki realnie miał wpływ na bezpieczeństwo poszczególnych sieci i przetwarzanych przez nie dane, choć wskazano, że mógł on dotyczyć bezpośrednio dostępu do sieci, w której „funkcjonują serwery baz danych z danymi osobowymi dłużników". Wiadomo, że błąd został usunięty, więc bez wglądu do dokładniejszej dokumentacji poaudytowej (która nie istnieje lub nie została udostępniona biegłemu) znalezienie źródeł i następstw tego problemu może być już obecnie niemożliwe.

5. Odnośnie pkt. 3 Oświadczenia o przebieg audytu – Domyślne hasło dostępu do urządzenia UPS. Podana informacja nie ma wpływu na bezpieczeństwo danych osobowych.

6. Odnośnie pkt. 4 Oświadczenia o przebieg audytu – Mowa tutaj o tym, że komputery Spółki były zabezpieczone systemem Symantec DLP, który służy do monitorowania ewentualnych wycieków informacji. Z opisu wynika jednak, że system ten nie został poprawnie skonfigurowany, aby dawał możliwość rzetelnej weryfikacji czy wyciek miał miejsce i jakich danych dotyczył. Opis jest zbyt

ogólny, aby wnioskować co dokładnie zostało przeanalizowane i w jakim stopniu. W każdym razie audytor nie potwierdza, że wyciek miał miejsce, ale i równie dobrze nie jest w stanie tego wykluczyć.

7. Odnośnie pkt. 5 Oświadczenia o przebieg audytu – Opis procedur bezpieczeństwa w Spółce. Audytor opisuje dobre praktyki stosowane przez Spółkę w celu ograniczenia ryzyka wycieku danych. Niestety, znowu brakuje opisu w jaki sposób została przetestowana realna skuteczność tych zabezpieczeń. Audytor wskazuje przy tym na zidentyfikowane ryzyko związane z wykorzystaniem niezanonimizowanych danych osobowych dłużników w środowiskach testowych. Nie wiadomo jednak jakich środowisk dotyczy ten problem i czy używanie danych w środowisku testowym wiąże się z jakimś dodatkowym ryzykiem, wynikającym np. z braku zastosowania odpowiednich zabezpieczeń dla tego typu środowisk czy też możliwości dostępu do danych osób do tego niepowołanych.

8. Odnośnie pkt. 6 Oświadczenia o przebieg audytu – Niezgodność polityk z wdrożonymi procedurami. Audytor zauważa, że istnieją odstępstwa od procesów i procedur deklarowanych w dokumentacji bezpieczeństwa, a rzeczywistym ich stosowaniem. Biorąc to pod uwagę tym bardziej właściwe wydaje się zweryfikowanie rzeczywistego bezpieczeństwa systemów i zabezpieczeń wymienionych powyżej.

9. W podsumowaniu audytor stwierdza, że audyt nie wykazał wycieku danych osobowych, lecz jedynie wybrane problemy techniczne i proceduralne. Jest to zgodne z prawdą, ponieważ zakres i rezultaty przeprowadzonego audytu mogły jedynie w wąskim zakresie służyć do dostarczenia odpowiedniego materiału dowodowego pozwalającego na wykrycie wycieku danych. W czynnościach audytowych zabrakło stosowanych w przypadku podejrzenia wycieku danych procedur związanych z analizą powłamaniową.

10. Dodatkowo wskazać należy, że firma CPU s.c. A. Urbanowicz, M. Jastrzębski, P. Ligaj z siedzibą w Lublinie w opinii biegłego nie jest podmiotem specjalizującym się w badaniach incydentów związanych z bezpieczeństwem danych. Nie wynika to przynajmniej z analizy strony www należącej do tej firmy. Główną działalnością firmy jest projektowanie i wykonywanie kompletnych instalacji sieci LAN, WAN i VPN, pomoc we wdrożeniach i wsparcie techniczne. Żadna z usług

wymienionych na stronie firmy nie dotyczy przeprowadzania audytów bezpieczeństwa i testów penetracyjnych, a w szczególności badania incydentów związanych z wyciekiem danych. Z pewnością nie ma wystarczających przesłanek merytorycznych do wyboru tego podmiotu w celu zbadania incydentów związanych z wyciekiem danych, o czym świadczą chociażby istotne zastrzeżenia merytoryczne biegłego do wydanego przez tę firmę Oświadczenia.

## Uwagi rewidenta do przebiegu badania

W związku ze stanowiskiem Spółki, że żaden incydent związany z wyciekiem danych nie miał w Spółce miejsca, biegły miał trudności ze skompletowaniem informacji niezbędnych do rzetelnego wykonania badania. Spółka bardzo literalnie interpretowała postanowienia projektu uchwał Zwyczajnego Walnego Zgromadzenia Akcjonariuszy Spółki, w szczególności mówiące o udostępnieniu biegłemu niezbędnych dokumentów i udostępniła je początkowo wyłącznie w formie papierowej w liczbie ponad 4.000 stron, co znacząco utrudniało analizę dokumentacji. Pomimo wielu wniosków ze strony biegłego do Spółki, w szczególności biegły w piśmie z dnia 11.06.2018 r., po spotkaniu z Radą Nadzorczą Spółki, wskazał wprost jakich informacji i dostępu teleinformatycznego do jakich danych i systemów Spółki potrzebuje w celu prawidłowego i należytego zakończenia badania. W odpowiedzi Spółki, biegły otrzymał jedynie dokumenty w formie papierowej i elektroniczne dwa pliki xlsx pn. „Analiza raportów.xls" oraz „Incydenty 2'16 IT".

W ocenie biegłego dostęp do następujących dokumentów, informacji oraz procedur testowych pozwoli rewidentowi należycie przeprowadzić badanie incydentu bezpieczeństwa informacji:

a) Ustalenie logów przypisanych do urządzeń, za pomocą których wykonano kopie danych oraz danych osób użytkujących te urządzenia – realizacja tego zakresu badania wymaga dostępu do infrastruktury technicznej Spółki przez biegłego ds. szczególnych.

**Procedury testowe do wykonania przez biegłego w środowisku informatycznym Spółki:**

- uzyskanie pełnej zawartości maila od osoby pełniącej funkcję ABI, w którym informowała o możliwości wystąpienia incydentu w jego oryginalnej formie (elektronicznej) wraz z załącznikami;
- ustalenie, jakie konkretnie urządzenia mają być objęte badaniem;
- w miarę możliwości uzyskanie zabezpieczonych logów systemowych pochodzących bezpośrednio z badanych urządzeń;
- uzyskanie oryginalnych logów z systemu DLP w formie elektronicznej;
- weryfikacja oryginalności i integralności otrzymanych logów;

- weryfikacja danych osób użytkujących wskazane urządzenia podczas wystąpienia incydentu;

**Wymagane do badania:**

- dostęp techniczny do wskazanej wiadomości email;
- dostęp techniczny do konsoli zarządzającej systemu DLP;
- dostęp techniczny do repozytorium logów z systemu DLP;
- dostęp techniczny do repozytorium logów z urządzeń;
- dostęp techniczny do informacji o kopiowanych plikach;
- wymagane wsparcie administratora IT Spółki.

b) Ustalenie zakresu oraz rodzaju danych, które zostały skopiowane na zewnętrzne nośniki z logów, o których mowa w lit. a) powyżej – realizacja tego zakresu badania wymaga dostępu do infrastruktury technicznej Spółki przez biegłego ds. szczególnych.

**Procedury testowe do wykonania przez biegłego w środowisku informatycznym Spółki:**

- ustalenie ścieżek źródłowych miejsc, z których zostały skopiowane dane;
- ustalenie nazw kopiowanych plików;
- ustalenie wielkości kopiowanych plików;
- próba odzyskania zawartości kopiowanych plików z momentu wystąpienia incydentu;
- weryfikacja obecnej zawartości plików, które zostały skopiowane podczas incydentu.

**Wymagane do badania:**

- dostęp techniczny do konsoli zarządzającej systemu DLP;
- dostęp techniczny do repozytorium plików, z których były kopiowane dane;
- dostęp techniczny do archiwalnych kopii zapasowych repozytorium plików, z których były kopiowane dane;
- dostęp techniczny do wszelkich informacji o kopiowanych plikach, a w szczególności tych, na podstawie których można by ustalić realną ich zawartość;
- wymagane wsparcie administratora IT.

c) Ustalenie zgodności działań związanych z kopiowaniem danych na zewnętrzne nośniki z obowiązującymi w Spółce na dzień zdarzenia procedurami wewnętrznymi z zakresu bezpieczeństwa danych

**Procedury testowe do wykonania przez biegłego:**

- uzyskanie pełnej wersji papierowej oryginalnych polityk i procedur bezpieczeństwa obowiązujących w Spółce w czasie wystąpienia incydentu;
- uzyskanie pełnej wersji papierowej oryginalnych dokumentów związanych z powołaniem wewnętrznego Zespołu Spółki ds. zbadania incydentu i określających warunki, na których był on uprawniony do kopiowania danych firmowych na nośniki zewnętrzne w czasie wystąpienia incydentu w Spółce;
- uzyskanie informacji o wydaniu Zespołowi nośników zewnętrznych, sposobach zabezpieczenia danych na tych nośnikach oraz późniejszej utylizacji tych nośników;
- wywiady z osobami, które wchodziły w skład Zespołu;
- weryfikacja oryginalności i integralności uzyskanych dokumentów, informacji, polityk i procedur.

**Wymagane do badania:**

- dostęp do repozytorium dokumentacji polityk i procedur bezpieczeństwa;
- dostęp do dokumentacji związanej z istnieniem i uprawnieniami Zespołu działającego w czasie wystąpienia incydentu;
- dostęp do archiwalnych kopii zapasowych dokumentacji polityk, procedur oraz dotyczących pracy Zespołu z okresu wystąpienia incydentu;
- wymagane wsparcie Zarządu w kontakcie z osobami wchodzącymi w skład Zespołu działającego w momencie wystąpienia incydentu.

d) Ustalenie, czy zewnętrzny audyt bezpieczeństwa informatycznego przeprowadzony przez CPU s.c. obejmował ustalenie okoliczności o których mowa w lit. a) - c) powyżej.

**Procedury testowe do wykonania przez biegłego:**

- uzyskanie raportu z audytu bezpieczeństwa w jego oryginalnej formie;

- weryfikacja zakresu przeprowadzonych działań audytowych w oparciu o zachowane dokumenty, logi i informacje zebrane podczas wywiadów z pracownikami IT.

**Wymagane do badania:**

- dostęp techniczny do infrastruktury oraz archiwalnych repozytorium dokumentacji i logów z systemów IT;
- wymagane wsparcie Zarządu w kontakcie z osobami zaangażowanymi w prace audytowe.

Jako że Spółka nie udostępniła w pełni ww. danych, biegły wydał opinię na podstawie przekazanych dokumentów i informacji oraz oparciu o własne wieloletnie doświadczenie zawodowe.

W imieniu Cybercom Poland sp. z o.o.:

Adam Wódz

CISSP QSA ASV