Cyberubezpieczenia – ochrona podmiotów leczniczych

KJF | BROKER

Skorzystaj z naszego doświadczenia

Wstęp

Informacje o firmie

- Grupa KJF
- Profil działalności
- Zespół
- Siedziba
- Dział IT

Podstawy prawne – dane osobowe

1. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE L 119/1)
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781)
3. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta
4. Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych (t.j. Dz. U. z 2019 r. poz. 53)
5. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2018 r., poz. 1954)
6. Ustawa z 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2019 r. poz. 869)
7. Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2019 r., poz. 1429)
8. Ustawa z 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2018 r., poz. 2096)
9. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2019 r., poz. 742)
10. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2018 r., poz. 1025)
11. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r., poz. 125)
12. Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej (Dz.U. z 2018 r., poz. 2369)

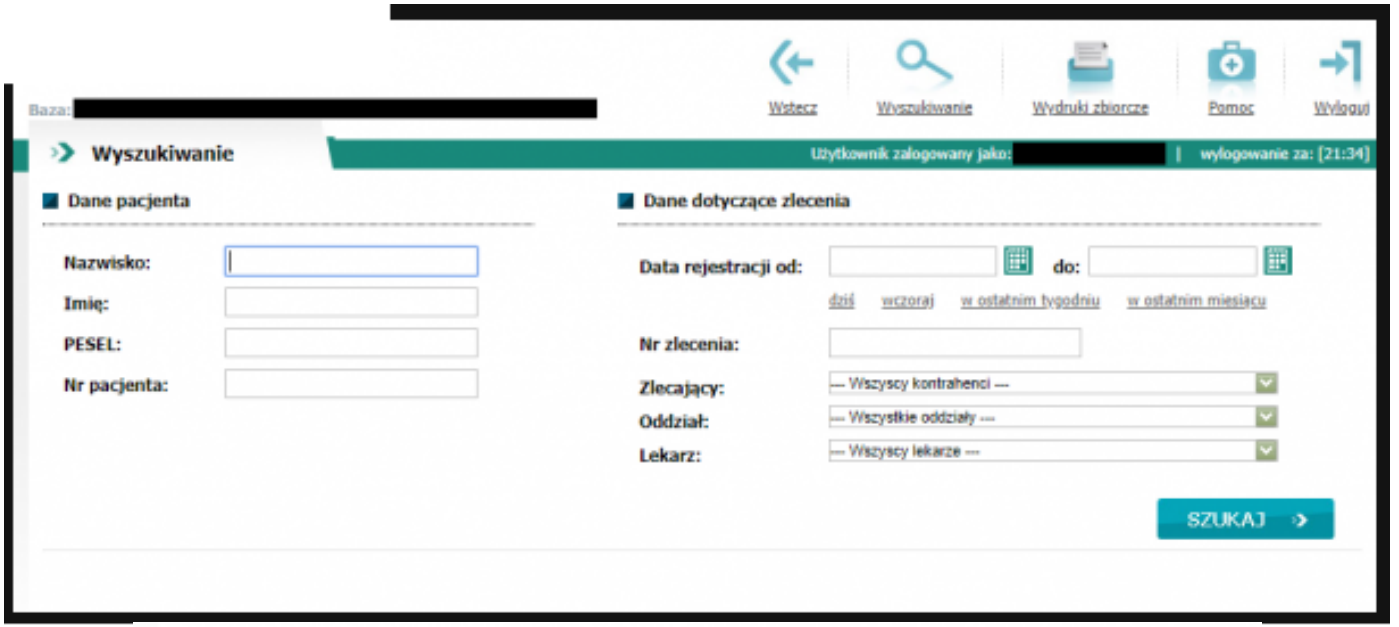
Potencjalne ryzyko cyber w działalności podmiotów leczniczych

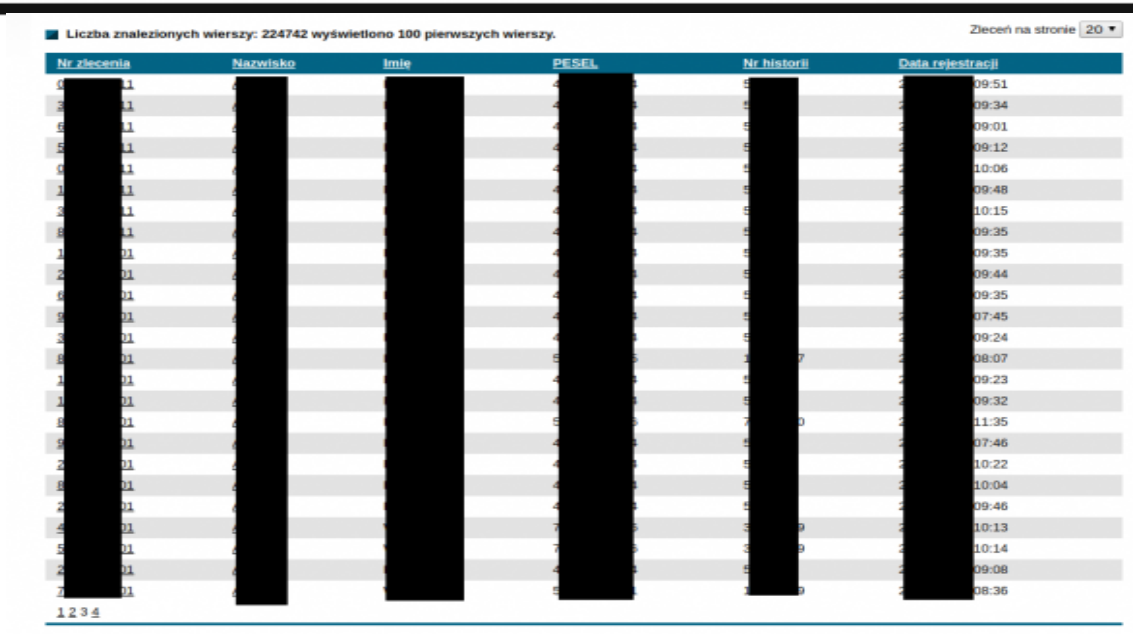
- Wyciek danych z nieumyślnej winy/błędu pracownika
- Celowe działanie pracownika
- ,,Luki” w systemach informatycznych i zabezpieczeniach
- Niewykwalifikowana kadra informatyczna
- Brak procedur
- Wielkość potencjalnej szkody (dane wrażliwe, ogromna ilość rekordów danych)
- Ataki hackerskie
  - Ransomware
  - Phishing
  - DoS
- Kradzieże sprzętu i rejestrów

KJF | BROKER

Wyciek danych - przykłady

Dostęp do danych klientów laboratorium medycznego - 2018





Wyciek danych - przykłady

Dostęp do danych klientów laboratorium medycznego - 2018

BADANIA PŁATNE

Lekarz kierujący: [redacted] Oddział:

Odbiorca wyniku: BADANIA PŁATNE

Pacjent: [redacted]

Data rej: [redacted]

Adres: [redacted]

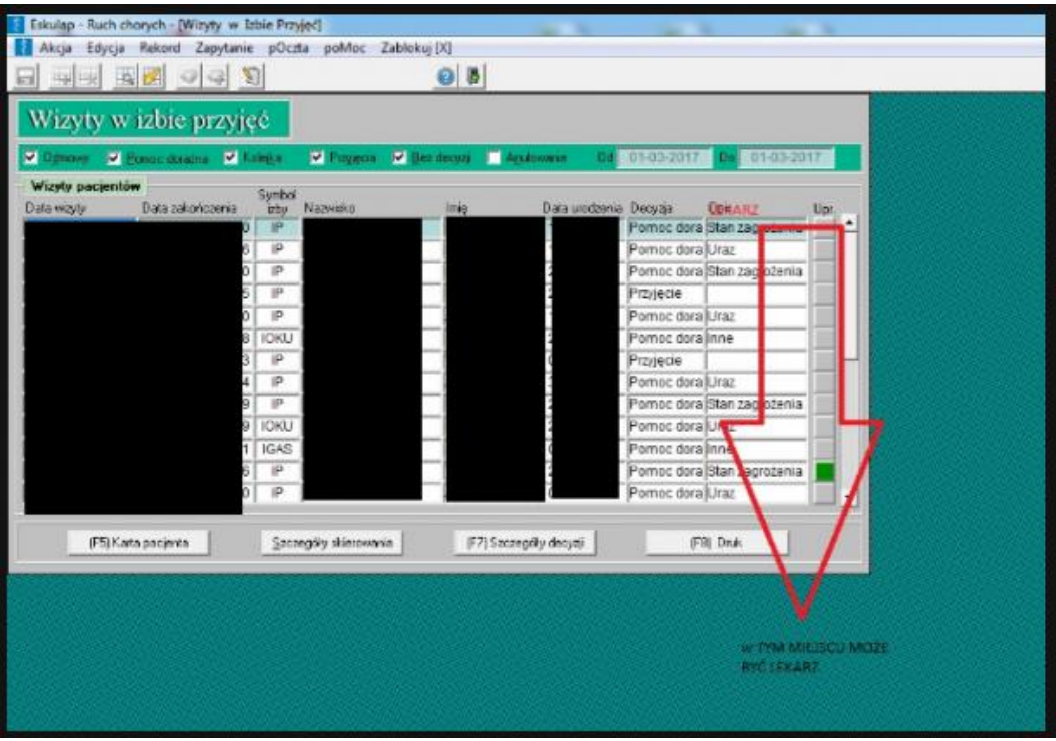
Data ur: [redacted]
PESEL:
Płeć:

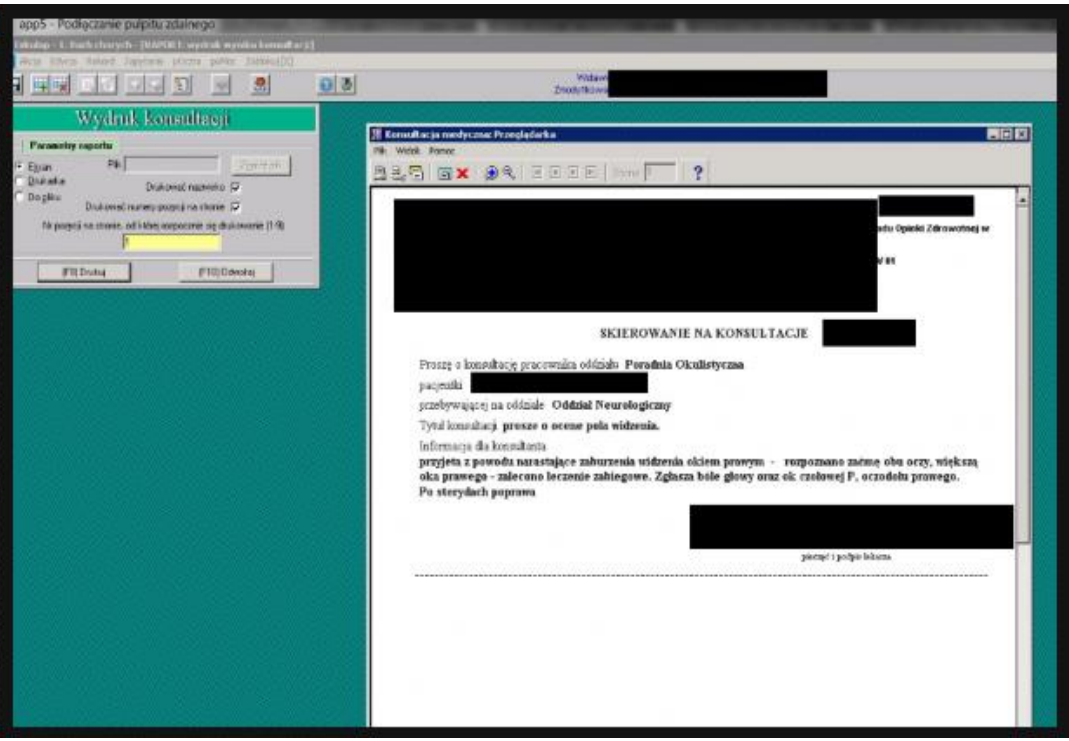
Badanie	Wynik	Jedn.	MIN	MAX	FLAGA
Morfologia krwi (ICD-9: C55)					
Leukocyty	9,94	tys/µl	3,98	10,04	N
Erytrocyty	4,67	mln/µl	3,93	5,22	N
Hemoglobina	15,0	g/dl	11,20	15,70	N
Hematokryt	42,7	%	34,10	44,90	N
MCV	91,4	fl	79,40	94,80	N
MCH	32,1	pg	25,60	32,20	N
MCHC	35,1	g/dl	32,20	35,50	N
Płytki krwi	239	tys/µl	150	400	N
RDW-SD	44,4	fl	36,40	46,30	N
RDW-CV	13,7	%	11,70	14,40	N
PDW	13,0	fl	9,80	16,20	N
MPV	10,90	fl	9,40	12,50	N
P-LCR	31,6	%	19,10	46,60	N
PCT	0,26	%	0	0,40	N
Neutrofile	8,05	tys/µl	2	7	H
Limfocyty	1,37	tys/µl	1	3	N

KJF | BROKER

Wyciek danych - przykłady

Niezabezpieczony dostęp do danych firmy obsługującej HelpDesk programu Eskulap – 2017 r.





KJF | BROKER

Wyciek danych - przykłady

Niezabezpieczony dostęp do serwera SP ZOZ - 2017

IMIE	NAZWISKO	DATAUR	PLEC	PESEL	GRKRWI	RH	KOD	MIEJSCOWOSC	ULICA	NRDOMU	NRMIESZKAN	NRUBEZPIECZENIA
A		-01-19 00:00	K	14	B	2	62-					C
E		-08-19 00:00	K	08	B	2	62-					A
K		-03-19 00:00	K	07	B	2	62-					
M		-02-19 00:00	K	11	B	2	62-					3
A		-11-19 00:00	K	05	B	2	62-					C
M		-11-19 00:00	K	14	B	2	62-					A
D		-11-19 00:00	K	05	B	2	62-					G
B		-11-19 00:00	K	07	B	2	62-					A
N		-08-19 00:00	K	04	B	2	62-					C
M		-04-19 00:00	K	05	B	2	62-					G
A		-06-19 00:00	K	06	B	2	62-					B
M		-03-19 00:00	K	06	B	2	62-					A
A		-11-19 00:00	K	06	B	2	62-					C
A		-07-19 00:00	K	08	B	2	62-					C
A		-07-19 00:00	K	13	B	2	62-					C
E		-01-19 00:00	K	06	B	2	62-					C
E		-01-19 00:00	K	11	B	2	62-					N
S		-03-19 00:00	K	07	B	2	62-					C
IL		-06-19 00:00	K	06	B	2	62-					A
K		-11-19 00:00	K	03	B	2	62-					C
M		-08-19 00:00	K	17	B	2	62-					C
D		-09-19 00:00	K	08	B	2	62-					A
B		-05-19 00:00	M	11	B	2	62-					R
A		-05-19 00:00	K	09	B	2	62-					C
B		-11-19 00:00	K	08	B	2	62-					2
M		-12-19 00:00	K	06	B	2	62-					A
A		-04-19 00:00	K	09	B	2	62-					C
E		-07-19 00:00	K	07	B	2	62-					Z

ODDZIAŁ DZIECIĘCY 2014

Lp.	Imię i nazwisko pacjenta	Data urodzenia	Pesel	Adres	Czynnik chorobotwórczy	Data rozpoznania
91		1 r.			Salmonella	09.03.2016 r.
92		5 r.			Salmonella	18.10.2016 r.
93		4 r.			Salmonella	06.11.2016 r.
94		4 r.			Salmonella	08.11.2016 r.
95		4 r.			Rota dodatni	28.12.2016 r.
96		2 r.			Salmonella	28.12.2016 r.
97		5 r.			Salmonella	30.12.2016 r.
98		4 r.			Salmonella	14.12.2016 r.
99		2 r.			Rota dodatni	15.11.2016 r.
100		6 r.			Rota dodatni	19.11.2016 r.
101		1 r.			Clostridium, Rota	01.01.2017 r.
102		5 r.			Rota dodatni	01.01.2017 r.
103		6 r.			Clostridium	03.01.2017 r.
104		16			Rota dodatni	11.01.2017 r.
105		07			Salmonella	07.01.2016 r.
106		16			Rota dodatni	15.01.2017 r.
107		16			Rota dodatni	19-01-2017
108		11			Rota dodatni	21-01-2017
109					Rota dodatni	22-01-2017
110		12			Rota dodatni	29-01-2017
111		16			Adeno dodatni	04-02-2017
112		16			Rota dodatni	09-02-2017
113		12			Rota dodatni	15-02-2017
114		16			Rota dodatni	18.02.2017 r.
115		6 r.			Rota dodatni	16.02.2017 r.

Wyciek danych - przykłady

Kradzież „Rejestru udostępnionej dokumentacji medycznej” - 2019

• Kradzież przez nieznanego sprawcę Rejestru udostępnionej dokumentacji medycznej w formie papierowej

• Rejestr zawierał dane osób, których dane były udostępniane w okresie 17.11.2018r. do 06.01.2019 r.

• Rejestr zawierał co najmniej następujące dane:

- Imię i nazwisko
- PESEL
- Wzór podpisu

RODO – obowiązki i koszty w przypadku ,,wycieku danych”

- Obowiązki informacyjne poszkodowanych
  - Telefonicznie
  - Listownie
- Obowiązek wprowadzenia postępowania wyjaśniającego i naprawczego
  - Koszty diagnostyczne
  - Koszty wprowadzenia działań naprawczych
- Obowiązek naprawy szkody – odpowiedzialność cywilna wobec osób, których danych wyciekły.
- Postępowanie administracyjne
  - Koszty postępowania administracyjnego
  - Kara administracyjna (do 100 tys. PLN dla podmiotów publicznych)

Kary administracyjne - przykłady

PORTUGALIA - Barreiro

Centro Hospitalar Barreiro Montijo

-Kara administracyjna 400 tys. EUR

-Szeroki dostęp do danych medycznych (296 lekarzy, aktywnych kont 985)

HOLANDIA - Haga

Haga Hospital

-Kara administracyjna 460 tys. EUR (w przypadku braku środków naprawczych 100 tys. EUR co 2 tyg.)

-Brak odpowiednich zabezpieczeń

-Brak monitoringu rejestru upoważnionych do przetwarzania danych osobowych

POLSKA

Morele.net

- Kara administracyjna 2.830.410,00 PLN
- Włamanie i kradzież danych 35 tys. klientów

Dolnośląski Związek Piłki Nożnej

- Kara administracyjna 55.750,50 PLN
- Opublikowanie danych sędziów piłkarskich

Spółka X

- Kara administracyjna 943.000,00 PLN
- Brak informowania klientów o przetwarzaniu danych osobowych

Ubezpieczenie ryzyk cyber

Co to jest? Dla kogo jest przeznaczone?

Ubezpieczenie Cyber umożliwia transfer części ryzyka związanego ze stale rosnącymi zagrożeniami cybernetycznymi na ubezpieczyciela. Polisa ma za zadanie chronić spółkę przed konsekwencjami takich zdarzeń, jak: utrata dostępu do danych, ich naruszenie bądź zniszczenie, ale też finansowe następstwa działania złośliwego oprogramowania typu ransomware czy ryzyka związane z działalnością medialną w sieci.

Ochrona udzielana jest zarówno w odniesieniu do odpowiedzialności ubezpieczonej spółki w stosunku do osób trzecich, które mogą kierować przeciwko niej roszczenia odszkodowawcze w związku z naruszeniem przez nią (lub jej pracowników czy podwykonawców, za których jest prawnie odpowiedzialna) ich prywatności, jak i w odniesieniu do jej straty własnej związanej z zakłóceniem jej działalności, kosztami odzyskania czy odtworzenia utraconych lub zniszczonych danych. Dodatkowo ochrona może być udzielona w zakresie pokrycia kosztów wymuszeń komputerowych. Czynnikami umożliwiającymi uruchomienie polisy są działanie złośliwego oprogramowania, atak hakerski, ale też zaniedbania i błędy ludzkie.

Ubezpieczenie ryzyk cyber

Zakres ubezpieczenia

Koszty poinformowania osób - ochrona obejmuje koszty poinformowania osób, których dane zostały ujawnione, również w sytuacji gdy prawo nie nakłada takiego obowiązku na ubezpieczonego.

Koszty poinformowania regulatora - ochrona obejmuje koszty poinformowania regulatora w przypadku ujawnienia danych osobowych i naruszenia przepisów o ochronie danych osobowych.

Ujawnienie danych osobowych - ochrona obejmuje koszty obrony i odszkodowania za ujawnienie danych osobowych w sposób stanowiący naruszenie przepisów o ochronie danych osobowych.

Koszty postępowania regulacyjnego - ochrona obejmuje koszty obsługi prawnej w przypadku postępowania regulacyjnego związanego z ujawnieniem danych osobowych.

Kary administracyjne - ochrona obejmuje kary administracyjne nakładane przez regulatora w związku z ujawnieniem danych osobowych.

Ujawnienie informacji poufnych - ochrona obejmuje koszty obrony i odszkodowania w przypadku nieuprawnionego ujawnienia lub wykorzystania informacji poufnych otrzymanych od kontrahentów.

Ubezpieczenie ryzyk cyber

Zakres ubezpieczenia c.d.

Wymuszenia - ochrona obejmuje koszty wymuszenia, w tym kwotę okupu w przypadku groźby ujawnienia informacji poufnych otrzymanych od kontrahentów przez ubezpieczonego lub ujawnienia danych osobowych. Ochrona obejmuje też przypadki związane z oprogramowaniem typu ransomware.

Koszty odtworzenia danych - w przypadku utraty lub braku możliwości dostępu do danych ubezpieczonego lub danych, w stosunku do których ubezpieczony pełni funkcję administratora, ubezpieczyciel pokryje koszty odtworzenia danych, jeżeli do takiej utraty doszło m.in. w wyniku wirusa komputerowego, ataku hakerskiego, błędu ludzkiego, awarii zasilania czy przepięcia.

Utrata zysku - ochrona ubezpieczeniowa obejmuje utracone zyski oraz koszty dodatkowe (w tym koszty korzystania z wynajmowanych urządzeń, koszty usług osób trzecich czy dodatkowe koszty personalne), w przypadku gdy dojdzie m.in. do ataku hakerskiego czy działania wirusa komputerowego.

Koszty ochrony dobrego imienia - ochrona obejmuje koszty wynajęcia firmy public relations, której zadaniem będzie ocieplenie medialnego wizerunku ubezpieczonego w związku z wyciekiem danych osobowych

Przykładowe scenariusze

Scenariusz 1 – błąd pracownika

Zdarzenie - Rekruter pracujący dla instytucji opieki zdrowotnej omyłkowo załączył niewłaściwy plik podczas rozsyłania korespondencji do czterech osób ubiegających się o pracę. Plik zawierał pochodzące z działu kadr dane osobowe: 43 000 nazwisk, adresów i numerów dowodów osobistych byłych pracowników. Ubezpieczony zatelefonował na infolinię ubezpieczyciela w celu uzyskania wsparcia. Wyznaczono specjalistę ds. reagowania na incydenty, który zaaranżował usługi prawne w celu uporania się z konsekwencjami związanymi z postępowaniami wszczętymi przez organ regulacyjny.

Potencjalne skutki i koszty:

– Wydatki na obronę związane z podjęciem działań wyjaśniających przez organy regulacyjne - 61 500 EUR

– Koszty obrony oraz ugód z pracownikami, w których przypadku doszło do kradzieży tożsamości- 112 000 EUR

– Wynagrodzenie specjalisty ds. reagowania na incydenty (Incident Managera) - 5 600 EUR

– Koszty powiadomienia osób, których dane zostały ujawnione - 3 400 EUR

– Koszty z tytułu usług monitorowania danych poszkodowanych osób pod kątem kradzieży tożsamości - 14 600 EUR

– Koszty z tytułu porady prawnej – 11 200 EUR **RAZEM: 208 300 EUR**

Wnioski: Błędy ludzkie zdarzają się częściej, niż można by się spodziewać. Nawet z pozoru błahe zaniedbania i pomyłki mogą doprowadzić do poważnych konsekwencji, a w rezultacie do znacznych kosztów czy strat finansowych. Należy zdać sobie sprawę z tego, że zdarzenia cybernetyczne to nie tylko incydenty technologiczne. Wiele odnotowywanych roszczeń wynika z popełnienia bardzo prostych błędów.

Przykładowe scenariusze c.d.

Scenariusz 2 – Atak z wykorzystaniem oprogramowania do wymuszania okupu

Zdarzenie: Pracownik firmy produkującej części do samochodów kliknął złośliwy link w e-mailu. W rezultacie na serwer firmy zostało pobrane złośliwe oprogramowanie, które zaszyfrowało wszystkie informacje. Na komputerze pracownika pojawiła się również wiadomość z żądaniem zapłaty o równowartości 11 200 EUR wyrażonej w bitcoinach w ciągu 48 godzin w celu uzyskania klucza deszyfrującego. Firma skontaktowała się telefonicznie z ubezpieczycielem poprzez infolinię, prosząc o wsparcie. Wyznaczony specjalista ds. reagowania na incydenty zaangażował informatyków śledczych, aby ocenili realność groźby i ustalili, czy firma może uniknąć zapłaty okupu. **Wymuszenie komputerowe** – koszty związane z zakończeniem lub zażegnaniem groźby ujawnienia informacji lub wprowadzenia złośliwego oprogramowania w przypadku niezapłacenia okupu:

– Wynagrodzenie informatyków śledczych z tytułu oceny możliwości przywrócenia danych - 15 700 EUR

– Koszty dochodzenia mającego na celu zlokalizowanie złośliwego oprogramowania, przeanalizowanie wpływu incydentu, poddanie zainfekowanych treści kwarantannie oraz obliczenie strat - 20 100 EUR

– Koszty z tytułu porady prawnej - 7 800 EUR

– Wynagrodzenie specjalisty ds. reagowania na incydenty (Incident Managera) - 6 700 EUR

– **Naruszenie danych** – koszty związane z zastąpieniem utraconych lub zniszczonych danych - 16 800 EUR

RAZEM: 67 100 EUR

Wnioski. Chociaż żądany okup był znacząco niższy niż koszty pokryte z polisy ubezpieczeniowej, policja zaleca niepłacenie okupów w przypadku ataków cybernetycznych. Zapłata okupu nie tylko przyczynia się do finansowania przestępczego procederu, ale także sygnalizuje brak odpowiednich i skutecznych procedur w firmie, jak np. przechowywanie danych zapasowych poza siedzibą firmy i jej siecią. W pewnych sytuacjach zapłata okupu jest jednak najlepszą opcją, dlatego specjaliści ds. reagowania na incydenty mają dostęp do portfela bitcoin i w razie potrzeby mogą z niego skorzystać.

Przykładowe scenariusze c.d.

Scenariusz 3 – Nieuprawniony dostęp

Zdarzenie: Hakerzy bezprawnie uzyskali dostęp do informacji umieszczonych w sieci kuratorium oświaty, wykorzystując nieznaną wcześniej lukę w zabezpieczeniach. Informacje te zawierały nazwiska, adresy e-mail, numery dowodów osobistych oraz numery rachunków bankowych 20 000 byłych i obecnych nauczycieli, a także uczniów. Po licznych zgłoszeniach osób, których dane zostały ukradzione, na temat podejrzanych aktywności w ich skrzynkach e-mailowych dział IT odkrył ślady nieuprawnionego użytkownika w systemie. Ubezpieczony zgłosił się na infolinię Chubb, po czym został wyznaczony specjalista ds. reagowania na incydenty.

Potencjalne koszty:

– Wydatki na obronę związane z podjęciem działań wyjaśniających przez organy regulacyjne w następstwie nieprawidłowego zarządzania prywatnymi danymi - 83 900 EUR

– Koszty obrony oraz ugód związane z roszczeniami osób, w których przypadku doszło do kradzieży tożsamości - 44 700 EUR

– Koszty dochodzenia mającego na celu zlokalizowanie luk w zabezpieczeniach, przeanalizowanie wpływu incydentu oraz obliczenie strat - 89 500 EUR

– Koszty powiadomienia osób, których dane zostały ujawnione – 1 100 EUR

Przykładowe scenariusze c. d.

– Koszty z tytułu usług monitorowania danych poszkodowanych osób pod kątem kradzieży tożsamości - 6 700 EUR

– Koszty zorganizowania i obsługi call center odpowiadającego na pytania poszkodowanych - 10 100 EUR

– Wynagrodzenie ekspertów PR zatrudnionych w celu zminimalizowania wpływu incydentu na reputację - 14 500 EUR

– Koszty z tytułu porady prawnej - 11 100 EUR

– Wynagrodzenie specjalisty ds. reagowania na incydenty (Incident Managera) - 10 000 EUR

RAZEM: 271 600 EUR

Wnioski: Powyższy scenariusz pokazuje, jak ważne jest przechowywanie wrażliwych danych w odpowiednio zabezpieczonej lokalizacji. Oprogramowania wykrywające włamania, szyfrowanie baz danych oraz odpowiednie procesy zabezpieczające przechowywane informacje to niektóre ze sposobów pozwalających odpowiedzialnie dbać o ochronę poufności informacji dotyczących pracowników i klientów.

Bibliografia

1)www.uodo.gov.pl (stan na dzień 15.10.2019 r.)

2)https://strefabiznesu.pl/wyciekly-dane-medyczne-50-tys-pacjentow/ar/12170736 (stan na dzień 12.10.2019 r.)

3)https://www.epiotrkow.pl/news/Z-belchatowskiego-szpitala-skradziono-dane-osobowe,34834 (stan na dzień 15.10.2019 r.

4)https://niebezpiecznik.pl/post/wyszukiwala-wyniki-swoich-badan-wsrod-danych-innych-pacjentow-jak-moga-wyciekac-dane-zdrowotne/ (stan na dzień 13.10.2019 r.)

5)https://www.politykazdrowotna.com/47727,2-mln-zl-kary-dla-szpitala-za-naruszenie-rodo (stan na dzień 12.10.2019 r.)

6)https://niebezpiecznik.pl/post/dane-pacjentow-i-szpitali-wyciekly-z-helpdesku-eskulapa-szpitale-powinny-zmienic-hasla/ (stan na dzień 14.10.2019 r.)

7)https://www.money.pl/gospodarka/rodo-jest-pierwsza-kara-i-od-razu-na-milion-zl-6363323775555713a.html (stan na dzień 14.10.2019 r.)

8)https://www.dutchnews.nl/news/2019/07/hospital-fined-e460000-for-privacy-breaches-after-barbie-case/ (stan na dzień 14.10.2019 r.)

9)Materiały szkoleniowe Chubb European Group SE Spółka Europejska Oddział w Polsce

Dziękujemy za uwagę

Bartosz Horowski – Wiceprezes Zarządu
Krzysztof Skieresz – Dyrektor Oddziału