
Magdalena Czarnecka

OCHRONA PRZED SKUTKAMI CYBERPRZESTĘPCZOŚCI

Przyszłość, która nadchodzi

Być może już za kilka lat oferta polskich towarzystw ubezpieczeń będzie standardowo zawierała ochronę ubezpieczeniową przed wszelkiego rodzaju skutkami cyberprzestępczości – wyspecjalizowane produkty w ramach „cyberubezpieczenia" także na naszym rynku staną się przedmiotem zainteresowania szerokiej rzeszy przedsiębiorstw. Warto zatem przyjrzeć się, o jakich dokładnie ryzykach mówimy i jakie aspekty prawne należy w takim wypadku uwzględnić.


Przemysław Wierzbicki

Coraz więcej firm opiera się w swojej działalności na wykorzystaniu różnorodnych narzędzi informatycznych. Należy założyć, że z biegiem czasu dla dużej części firm brak możliwości korzystania z takich narzędzi lub brak dostępu do sieci względnie danych w formie elektronicznej będzie oznaczał poważne problemy.

Cyberprzestępczość – realne zagrożenie

Niestety, wraz z postępem procesu cyfryzacji gospodarki, wzrastają również specyficzne zagrożenia związane z przestępczością, której narzędziem lub przedmiotem ataku są urządzenia i rozwiązania informatyczne oraz dane w formie elektronicznej (cyberprzestępczość). Pomijam tutaj działanie „tradycyjnych" ryzyk dla działania systemów informatycznych (np.: pożar prowadzący do zniszczenia serwerowni i zgromadzonych tam danych elektronicznych).

Jakkolwiek brak jest danych dotyczących rynku polskiego, to warto zwrócić uwagę, że zgodnie z badaniem przeprowadzonym przez rząd brytyjski[1] w 2014 r., ponad 81% dużych i 60% małych przedsiębiorstw było w 2014 r. poszkodowanych naruszeniem działania systemów informatycznych, przy czym rosnąca część takich naruszeń była wynikiem właśnie cyberprzestępczości. Szacuje się[2], że koszt ponoszony przez brytyjskie firmy z powodu cyberprzestępczości sięga około 27 mld funtów rocznie.

Zgodnie z informacjami prasowymi z lipca 2015 r.[3], Fiat Chrysler został zmuszony do wezwania właścicieli 1,4 miliona wyprodukowanych przez siebie pojazdów do naprawy (aktualizacja oprogramowania zainstalowanego w samochodach), gdyż dwóch hackerów udowodniło możliwość zdalnego przejęcia kontroli nad systemami informatycznymi w Jeep Cherokee zarządzającymi radiem, połączeniami telefonicznymi, klimatyzacją i innymi systemami.

Jednocześnie na poziomie wspólnotowym trwają prace nad dyrektywą Parlamentu Europejskiego i Rady[4], dotyczącą środków służących zapewnieniu wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, w ramach których dyskutuje się nad wprowadzeniem obowiązku dla dużych przedsiębiorstw, świadczących usługi społeczeństwa informatycznego lub wykorzystujących kluczową infrastrukturę w niektórych sektorach gospodarki o istotnym znaczeniu dla całego społeczeństwa, by notyfikowali regulatorowi (i być może także ubezpieczycielowi) o wszelkich incydentach mających istotny wpływ na bezpieczeństwo ich głównych usług.

Można zatem założyć, że w miarę postępu dalszej modernizacji polskiej gospodarki także polskie firmy będą coraz bardziej zagrożone cyberprzestępczością, która w tym momencie nie jest, niestety, traktowana jako istotne zagadnienie, jeśli chodzi o potrzebę ochrony ubezpieczeniowej przez większość przedsiębiorstw. Jednakże należy liczyć się z tym, że w przyszłości także polskie firmy zaczną poszukiwać „szytych na miarę" rozwiązań ubezpieczeniowych.

Następstwa ataku na system informatyczny przedsiębiorstwa

W tym zakresie może to być:

a) kradzież własności intelektualnej lub tajemnic handlowych – nieuprawnione wykorzystanie tych wartości przez inne firmy lub brak możliwości wykorzystania przez poszkodowaną firmę,

b) przerwa w prowadzonej działalności – brak możliwości wykorzystania narzędzi informatycznych (baz danych) niezbędnych w działalności,

c) utrata danych lub utrata systemów informatycznych – konieczność odtworzenia danych lub ponownej instalacji/konfiguracji oprogramowania,

d) konieczność przeprowadzenia dochodzenia oraz analizy „dziur" w systemie ochrony informatycznej,

e) szkody wyrządzone osobom trzecim – w przypadku wykorzystania systemów informatycznych zaatakowanej firmy w celu popełnienia oszustwa lub kradzieży,

f) naruszenie ochrony danych osobowych – ujawnienie lub utrata danych osobowych, które mogą pociągnąć za sobą także roszczenia osób, których dane ujawniono, oraz potencjalne kary ze strony organów regulacyjnych,

g) utrata reputacji,

h) fizyczne uszkodzenia lub zniszczenie aktywów (np. szkody wynikające z nieautoryzowanego wyłączenia urządzeń chłodzących),

i) szkody na osobie – potencjalna możliwość w przyszłości pozbawienia życia lub uszkodzenia ciała, np.: przez roboty będące przedmiotem cyberataku.

Potencjalne szkody

Powszechnie przyjmuje się również, że mówimy w tym zakresie o:

- szkodach (stratach finansowych) po stronie firmy, której systemy informatyczne były przedmiotem cyberataku, w tym:
  - a. wartości utraconych lub uszkodzonych aktywów (np.: przejęcie środków pieniężnych znajdujących się na rachunku bankowym firmy – wskutek wykorzystania technik „łowienia haseł" – ang. *phishing*),
  - b. dodatkowych kosztach lub wydatkach, w tym na:
    - b.i. naprawę lub odtworzenie systemów informatycznych,
    - b.ii. pracę informatyków (włącznie z informatykami śledczymi),
    - b.iii. doradztwo (np.: z zakresu PR, prawne),
  - c. utraconych zyskach (np.: z powodu przerw w działalności, ang. *denial-of-service*),
  - d. szkodach na reputacji,
  - e. karach finansowych (np.: związanych z naruszeniem ochrony danych osobowych),
- (analogicznie do powyższych) szkodach (stratach finansowych) po stronie osób trzecich, w tym:

►

Przyszłość, która nadchodzi

f. szkodach osób trzecich w związku z fizycznym uszkodzeniem lub zniszczeniem aktywów,

g. szkodach wynikających z naruszenia bezpieczeństwa danych, w szczególności szkodach wynikających z ujawnienia danych osobowych (zadośćuczynienie),

h. utraconych zyskach osób trzecich, w tym w związku z przerwami w działalności,

i. konieczności pokrycia dodatkowych kosztów lub wydatków (np.: konieczności pokrycia kosztów wsparcia informatycznego, kosztów odzyskiwania danych).

Jakie produkty ubezpieczeniowe wchodzą w grę?

Odpowiedzią na powyższe ryzyka mogą być:

- w przypadku szkód (strat finansowych) po stronie firmy, której systemy informatyczne były przedmiotem cyberataku – odpowiednio skonstruowane ubezpieczenie mienia, przy czym, z punktu widzenia ubezpieczonego, konieczne jest zwrócenie uwagi na:

a. zakres ochrony ubezpieczeniowej (kwestia szkód wyrządzonych w odniesieniu do systemów i danych elektronicznych),

b. sposób definicji zdarzenia szkodzącego (szkoda wynikła nie tylko z fizycznego oddziaływania na aktywa – np.: w wyniku przekierowania na stronę podszywającą się pod „legalną" stronę, tzw. ang. *pharming*),

c. zakres odszkodowania w przypadku zysków utraconych (w celu ujęcia utraty zysków spowodowanych przez oddziaływanie oprogramowania),

d. kwestię rażącego niedbalstwa lub niezachowania staranności przez poszkodowanego lub jego pracowników (np.: w przypadku ujawnienia poufnych danych przez pracowników wskutek techniki tzw. ang. *spoofing*, skłanianie użytkowników do podawania osobistych danych, które następnie służą do włamania do systemu informatycznego),

e. obowiązki związane ze zgłoszeniem szkody,

f. wykluczenie odpowiedzialności za akty terroru – na wypadek cyberprzestępczości, której można przypisać cechy wykorzystywania jej przez organizacje terrorystyczne,

- w przypadku zaś szkód (strat finansowych) po stronie osób trzecich – odpowiednio skonstruowane ubezpieczenie odpowiedzialności cywilnej, przy czym (oprócz powyższych uwag), z punktu widzenia ubezpieczonego, konieczne jest zwrócenie uwagi na m.in.:

g. wyłączenia odpowiedzialności w przypadku bezprawnego ujawnienia danych osobowych,

h. zakres ochrony ubezpieczeniowej (kwestia szkód wyrządzonych w odniesieniu do systemów i danych elektronicznych przez urządzenia lub systemy informatyczne pozostające pod kontrolą innego przedsiębiorstwa).

Sposoby ograniczenia ryzyka zdarzenia ubezpieczeniowego lub rozmiaru szkody

W zakresie tych zagadnień kluczowe są czynności zabezpieczające, które mogą być podejmowane przez przedsiębiorstwa w celu ograniczenia ryzyka wystąpienia szkody lub ograniczenia jej rozmiaru – w szczególności może to być:

a) stosowanie oprogramowania blokującego próby nieautoryzowanego dostępu (ang. *firewalls* i inne),

b) stosowanie ograniczeń w dostępie do systemów informatycznych, szczególnie w przypadku zdalnego dostępu,

c) staranna konfiguracja sprzętu i oprogramowania, zmniejszająca ryzyko cyberataku,

d) stosowanie ochrony przed tzw. złośliwym oprogramowaniem (ang. *malware*),

e) stosowanie aktualnych wersji oprogramowania, szczególnie oprogramowania antywirusowego.

f) cykliczny audyt bezpieczeństwa sieci (ewentualnie powiązany z uzyskaniem odpowiedniego certyfikatu bezpieczeństwa).

Problemy do rozwiązania dla zakładu ubezpieczeń

Oczywiście, nowy rodzaj ubezpieczenia to także nowe wyzwania i potencjalne problemy do rozwiązania przez zakład ubezpieczeń – w szczególności:

1) trudności w ustaleniu poziomu ryzyka (kwantyfikacji ryzyka) – różnorodność i wielość potencjalnych skutków cyberataku powoduje, że trudno jest skwantyfikować skutki (szkodę) mogące wynikać z cyberataku; przy zrozumiałym braku rozbudowanych danych historycznych i mnogości rozwiązań informatycznych służących ochronie przed cyberatakami – powoduje to trudności w ustaleniu wysokości składki i warunków reasekuracji,

2) trudności w monitorowaniu zmian ryzyka cyberataku – zakład ubezpieczeń może mieć trudność z ustaleniem, na przykład, czy ubezpieczony nie pogorszył swojej polityki IT w sposób powodujący większe ryzyko szkody,

3) problemy z ustaleniem definicji i terminologii – jak wskazują trudności w przyjęciu wcześniej wzmiankowanej dyrektywy Parlamentu Europejskiego i Rady, ustalenie precyzyjnych i wyczerpujących definicji pojęć związanych z cyberprzestępczością jest bardzo trudne i wymaga szczególnej staranności przy formułowaniu ogólnych warunków ubezpieczenia, jak również uwzględnienia porządków prawnych różnych państw,

4) konieczność uwzględnienia w procesie sprzedaży, reasekuracji oraz likwidacji szkód konieczności zapewnienia wsparcia informatycznego dla pracowników zakładu ubezpieczeń (np.: zapewnienie odpowiednio przeszkolonych rzeczoznawców oceniających zakres szkód),

5) konieczność wypracowania standardów oceny systemów zabezpieczeń stosowanych przez klientów.

Jak widać, problemy te nie są bynajmniej nie do przezwyciężenia – wymagają bardziej dostosowania istniejących procesów biznesowych niż tworzenia od podstaw zupełnie nowych procesów.

Podsumowanie – nowa rzeczywistość tuż za rogiem

Nawiązując do powyższych uwag, nie sposób nie zauważyć, że ubezpieczenie od skutków cyberprzestępczości może posiadać wiele zalet dla przedsiębiorców, pozwalając na transfer ryzyka do zakładu ubezpieczeń. Jednocześnie może stanowić ciekawą okazję dla ubezpieczycieli, by poszerzyli ofertę o nowy, dochodowy, produkt. Szacuje się, że w Wielkiej Brytanii koszt ubezpieczenia od cyberprzestępczości jest prawie 2–3-krotnie wyższy niż „standardowego" ubezpieczenia.

Magdalena Czarnecka
paralegal
Przemysław Wierzbicki
partner zarządzający, adwokat
Kancelaria Wierzbicki Adwokaci i Radcowie Prawni Sp.k.

[1] UK Cyber Security Report HM Government

[2] Cost of Cyber Crime, U.K. Cabinet Office and Detica, 2011

[3] http://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking

[4] Projekt dyrektywy Parlamentu Europejskiego i Rady, dotyczącej środków służących zapewnieniu wysokiego poziomu bezpieczeństwa sieci i informacji w ramach Unii z dnia 7 lutego 2013 r., COM(2013) 48 final, 2013/0027 (COD)