UBEZPIECZENIA CYBER: WYZWANIA I SZANSE [ANALIZA]

Ubezpieczenia od ryzyka cybernetycznego to dynamicznie rozwijający się trend, jednak sprawiający dużo problemów ubezpieczycielom. Jak bowiem wycenić ryzyko i prawdopodobieństwo cyberataku? Jak oszacować straty? Z jakich danych skorzystać, skoro większość firm ukrywa fakt, że zostało zaatakowanych? Na te pytania branża ubezpieczeń musi sobie odpowiedzieć - zwłaszcza, że zainteresowanie tym segmentem będzie tylko rosło. Firmy są bowiem coraz bardziej świadome zarówno zagrożeń związanych z atakiem, jak i korzyści, które otrzymają dzięki ubezpieczeniom.

W 2015 r. polski rynek ubezpieczeniowy stał się jednym z elementów kształtującym zarządzanie cyberryzykiem i cyberbezpieczeństwem. Poprzez wprowadzenie tzw. ubezpieczeń ryzyka cybernetycznego (ang. Cyber-Insurance) przedsiębiorstwa po raz pierwszy mają możliwość przenieść część ryzyka związanego z przetrzymywaniem i obróbką cennych danych, atakami hakerów i działaniem systemów informatycznych na ubezpieczyciela. Jak pokazują globalne trendy, coraz więcej podmiotów sięga po tego typu rozwiązanie.

Z drugiej strony ta nowa możliwość zaburza równowagę w cyberbezpieczeństwie stworzoną do pojawienia się ubezpieczyciela. Jakie są więc wyzwania i korzyści płynące z cyber ubezpieczeń? Jaka jest oferta rynkowa takich ubezpieczeń? Czy w przyszłości możemy spodziewać się także cyberubezpieczeń dla osób prywatnych?

Kiedy i gdzie się wszystko zaczęło?

Ubezpieczenia Cyber pojawiły się po raz pierwszy w latach 90. w USA i były to bardziej idee fixe niż prawdziwe rozwiązanie z zakresu zarządzania ryzykiem. Jak trafnie zauważył Frank Addessi w swoim artykule „Cyber Insurance and Personal Data”, oferta ubezpieczyciela dość szybko odzwierciedlała zmiany zachodzące w technologii. Dla przykładu pierwszy samochód wyprodukowano w 1886 r. a pierwsza auto polisa ubezpieczeniowa została zaoferowana dwa lata później. W przeciwieństwie do samochodu, zagrożenie w cyberprzestrzeni istnieje przynajmniej 30 lat, natomiast cyberubezpieczenia dopiero w ostatnich latach zaczęły nabierać znaczenia w formie globalnej.

Obecnie rynek oferuje ubezpieczenie od większości znanych człowiekowi zdarzeń losowych. Sytuacja przypomina trochę totalizatory sportowe, które z pomocą prawdopodobieństwa i statystyki starają się wypracować matematyczną formułę gwarantującą zysk ubezpieczyciela niezależny od wydarzeń losowych. O ile z większością wydarzeń losowych ubezpieczyciel radził sobie dobrze, często jest on bezradny wobec oszacowania ryzyka cyberzagrożeń.

Problem z wyliczeniem zysku i strat – wyzwanie numer 1

Ekonomiczne aspekty cyberprzestrzeni są jednym z najnowszych ukierunkowań ekonomistów w celu wyjaśnienia, ile należy maksymalnie wydać na swoje bezpieczeństwo w sieci tak, aby nie przepłacić.

Obecnie brakuje spójnej formuły wyjaśniającej poziom inwestycji w bezpieczeństwo informacji. Ten problem dotyczy tak samych przedsiębiorstw, jak i ubezpieczyciela.

Jedną z szeroko przyjętych formuł w sektorze prywatnym jest tzw. Return on Investment (ROI). Jak zauważyli Pascal Brangetto i Mari Kert-Saint Aubyn w artykule opublikowanym przez NATO Cooperative Cyber Defence Centre of Excellenceinwestycja w bezpieczeństwo informacji nie może być wyliczona przez formułę ROI, ponieważ a) bezpieczeństwo informacji nie generuje zysku, b) inwestycja w bezpieczeństwo pozwala oszczędzić przedsiębiorstwu finansowych skutków wystąpienia wydarzenia losowego np. cyber ataku, ataku DDOS, kradzieży danych, ransomware itp. Próba zmaterializowania strat będzie dotyczyła zatem trzech wymiarów informacji, tzw. Triadę CIA:

a. Dostępności (availability) – w przypadku ataku na serwer, stronę internetową, infrastrukturę koszt powinien wliczyć straty w produkcji czy usłudze (np. średni zysk stracony poprzez godzinę niedostępności) oraz straty niematerialne takie jak reputacja, zaufanie klienta.

b. Integralność (integrity) – w przypadku ataku koszt powinien wliczyć zniszczenie danych, ich modyfikacje, zmianę ich lokalizacji itp. Dla tej oceny niezbędna jest odpowiednia klasyfikacja-kategoryzacja danych w przedsiębiorstwie zgodnie z oczekiwaniami biznesu.

c. Konfidencyjność (confidentiality) - w przypadku ataku koszt powinien wliczyć kradzież danych, rozpowszechnienie danych dla osób nieupoważnionych. Podobnie jak w integralności potrzebna jest wycena informacji na podstawie ich klasyfikacji.

Proponowana nowa formuła miała by uwzględnić brak generacji zysku przez zabezpieczenie informacji w tzw. ROSI – return on security investment.

ROSI= ((ALE*%risk mitigated)-cost of security) \ cost of security

ALE - Annual Loss Expectancy

Problemem dla większości przedsiębiorstw i ubezpieczycieli pozostaje wyliczenie ALE. ALE można wyliczyć na podstawie historycznych danych statystycznych lub porównania ze średnim ryzykiem branży. Obie koncepcje mają swoje niedostatki:

1. **Dane historyczne** są zazwyczaj bardzo ograniczone, jeśli badamy cyberzjawiska i cyberataki. Niektóre firmy nie doznały żadnych znaczących ataków (bądź są ich nieświadome) na ich Triadę CIA, stąd trudno jest im oszacować potencjalne straty. Po drugie, straty w wyniku ataku z zeszłego roku mogą mieć małe znaczenie w ciągle ewoluującym środowisku cyberzagrożeń. Hakerzy stają się coraz bardziej wyrafinowani (sophisticated), ich wiedza na temat infrastruktury i zabezpieczeń rośnie z roku na rok, podobnie jak sama liczba osób dokonujących ataki cybernetyczne. Jeśli jeden wirus w zeszłym roku mógł spowodować straty w wysokości X, w roku następnym przez modyfikację wirusa straty mogą osiągnąć poziomu 2X czy 3X. Dla przykładu: dane historyczne w dość prosty sposób pomagają przewidzieć ryzyko i straty innych zjawisk losowych. Przez ostatnie 50 lat ubezpieczyciel może przeanalizować, ile osób złamało rękę i jakie odszkodowanie trzeba było im wypłacić. Na podstawie tych danych kształtowana jest cena ubezpieczenia od złamanej ręki, która powinna być wyższa niż statystyczny koszt wypłaty ubezpieczenia na jednego poszkodowanego. W cyberprzestrzeni niemożliwym jest zastosowanie tego samego uproszczenia.

2. **Ryzyko branży –** istnieje dość sporo statystyk pokazujących, ile ataków miało miejsce na daną liczbę przedsiębiorstw. Pytanie: czy możemy im wierzyć? Duża liczba firm decyduje się nie udostępniać informacji o cyberatakach z obawy przed paniką klientów, stratą reputacji itp. Przypuśćmy, że nasza firma sprzedaje książki online – atak na portal może wywołać bardzo różną reakcję i straty, często trudne do przewidzenia i zależne od poziomu zabezpieczeń portalu, polityki reakcji na incydenty, profesjonalizacji personelu, rodzaju przetrzymywanych danych.

Zagrożeniem dla cyberbezpieczeństwa i ubezpieczeń cyber pozostaje zatem problem z wyliczeniem zysków i strat. Może doprowadzić to do dysproporcji w ocenach ryzyka, a w konsekwencji w zawyżonym albo zaniżonym odszkodowaniu.

Teoria transferu ryzyka – wyzwanie numer 2

Występowanie ryzyka jest nieuniknione i nawet przy wysokim poziomie kontroli zawsze pozostaje tzw. Residual risk. Celem każdego przedsiębiorstwa jest sprowadzenie ryzyka do poziomu akceptowanego przez biznes management, co zależy w głównej mierze od teorii apetytu ryzyka czy rodzaju świadczonych usług.

W teorii zarządzania ryzykiem wyróżnia się cztery podejścia:

1. Omijanie (avoidance) – polega na eliminacji ryzyka poprzez nieuczestniczenie w ryzykownych procesach. Zazwyczaj firmy nie mogą sobie pozwolić np. na nieuczestniczenie w wymianie e - maili z kontrahentami, dlatego risk avoidance często jest zagadnieniem teoretycznym.

2. Redukcje (reduction) – polega na aktywnej optymizacji ryzyka poprzez wprowadzenie kontroli np. IPS czy IDS w sieci przedsiębiorstwa

3. Współdzielenie (sharing) – to transfer lub outsourcing ryzyka. Transfer związany jest z ubezpieczycielem, która podejmuje się odpowiedzialności zarządzania ryzykiem w momencie wystąpienia incydentu. Obejmuje to pomoc w zwalczaniu zjawiska losowego, przywrócenie do stanu poprzedniego i wypłata równowartości strat,

4. Akceptacja ryzyka polega na świadomości, że ryzyko istnieje i pogodzenie się z nim. To podejście ma sens, tylko w przypadku jeśli koszt kontroli i redukcji ryzyka przewyższa ewentualne straty wywołane przez incydent.

Z punktu widzenia ubezpieczeń cyber, punkt 3 to kolejne zagrożenie. Przedsiębiorstwa często mylnie rozumieją współdzielenie ryzyka jako jego wyeliminowanie. Ryzyko współdzielone nadal pozostaje ryzykiem, a ubezpieczyciel zobowiązuje się zareagować tylko w przypadku incydentu. Zgodnie z przysłowiem „lepiej zapobiegać, niż leczyć", ubezpieczyciel stwarza w firmie poczucie bezpieczeństwa w cyberprzestrzeni, odsuwając na dalszy plan prewencję i ostrożność w działaniach w środowisku wirtualnym.

Wyobraźmy sobie pracownika firmy udzielającej pożyczki mającego pełną świadomość pokrycia kosztów ewentualnego ataku malware, phishing, socjalnej inżynierii. Poziom ostrożności może być niepoprawnie obniżony przez ubezpieczenie. Transfer ryzyka nie oznacza, że podstawowe środki

prewencji powinny zostać zaniedbane.

Bariery w rozwoju usług ubezpieczeń cyber – wyzwanie numer 3

Rynek ubezpieczeń cyber boryka się z wszelkiego rodzaju barierami: od niemożliwości wyliczenia prawdopodobieństwa zajścia zdarzenia poprzez straty nim spowodowane. Skomplikowany ciąg przyczynowo skutkowy cyber przestrzeni powoduje, ze same ubezpieczenia nie są do końca sprecyzowane i mogą być przyczyną różnych interpretacji, szczególnie jeśli ich pierwowzorem był język angielski (co ma zastosowanie prawie we wszystkich takich firmach).

Zakres ubezpieczeń zazwyczaj jest dość podobny, na przykładzie Ergo Hestia wygląda on następująco:

Powyższa oferta wygląda dość atrakcyjnie i spójnie, lecz trudno powiedzieć, jak przedstawia się ona w praktyce. Brak jest danych statystycznych pokazujących, jakie odszkodowania otrzymały firmy w konkretnych przypadkach.

Przeszkodą w rozwoju rynku cyber ubezpieczeń może być też samo podejście firm. Często ubezpieczają się tylko te firmy, które wyeksponowane są na cyber ataki poprzez rodzaj swej działalności na rynku (finanse, firmy i agencje rządowe przetrzymujące konfidencyjne dane) bądź mają skomplikowaną infrastrukturę informatyczną podatną na atak. Powoduje to z kolei wstrzemięźliwość i obawy samego ubezpieczyciela przed wystawieniem oferty. Im mniej jest firm oferujących cyberubezpieczenia, tym ich koszt średni jest wyższy. Tak zamyka się cały krąg.

Brak danych i statystyk dla ubezpieczeń cyber – wyzwanie numer 4

Na dzień dzisiejszy brak jest solidnych danych statystycznych o ubezpieczeniach cyber. Trudno jest ocenić efektywność ubezpieczeń, skoro nie nastąpiła jeszcze agregacja danych (jak w przypadku USA) bądź istnieje niewystarczająca liczba przypadków do wyciagnięcia wniosków (jak w Polsce).

Portal statista.com jako jeden z niewielu opublikował wykres branży, które najczęściej sięgały po cyberubezpieczenia w 2014 r. w USA. Przodowały firmy związane ze służbą zdrowia, edukacją, energią. Średni poziom ubezpieczeń amerykańskich firm wynosił 32 % w 2014 r.

Bardzo możliwe, ze ubezpieczyciele posiadają dobrze opracowane dane, lecz nie są one udostępniane. Przyszłość niewątpliwie przyniesie pełniejszy obraz trendów i kierunków rozwoju rynków ubezpieczeń cyber.

Dla osób prawnych tak, dla osób fizycznych nie – wyzwanie numer 5

Na dziś w Polsce nie istnieje możliwość ubezpieczenia osoby fizycznej od cyberryzyka. Oferta dotyczy tylko firm, co znacznie ogranicza możliwości rynku. W niektórych państwach, np. USA od paru lat możliwe są ograniczone ubezpieczenia osób fizycznych. Ubezpieczenia te zazwyczaj pokrywają kradzież haseł, loginów, kodów dostępu i związane z tym koszty takie jak prawnicy, przejazdy związane z fizycznym wstawiennictwem, koszty administracyjne w przypadku wymiany dokumentu, patentu, certyfikatu. Podsumowując, zakres usług nie jest szeroki, a oferowane odszkodowanie zazwyczaj nie jest zbyt wysokie.

Ubezpieczenie osób fizycznych od cyberryzyka to zapewne jedno z największych wyzwań przyszłości. Ubezpieczyciel wybiera po pierwsze firmy ze względu na większy popyt niż u osób fizycznych oraz efekt skali, jeśli mówimy o prawdziwej wartości pieniężnej ubezpieczanych danych, procesów, działalności.

Z jednej strony można się z tym zgodzić, z drugiej strony ryzyka ataku na osobę fizyczną i prawną jest bardzo przybliżone. Często hakerzy nie wybierają specyficznego ataku (targeted attack), a hołdują raczej zasadzie „to okazja czyni ich złodziejami". Okazją mogą być wszystkie niezabezpieczone urządzenia podłączone do internetu, bądź wykorzystujące GSM, GPS, Bluetooth.

Aktywność osób fizycznych w cyberprzestrzeni stała się tez porównywalna z aktywnością firm. Jeśli 15 lat temu w Polsce głównie instytucje i firmy przeprowadzały operacje w internecie, dzisiaj może zrobić to każdy ze swojego laptopa, Smartfona itp. od online zakupów, online bankingu, składania formularzy, rozliczeń. Obrót wirtualnego pieniądza przez osobę fizyczną spowodował, ze stała się ona celem ataków hakerów . Dzisiaj kradzież naszych danych może być wykorzystana do wszystkiego. Coraz częściej te same metody są wykorzystywane przy atakach na firmy i osoby fizyczne. Atak ransomware dla osób fizycznych to już normalność.

Pytaniem głównym pozostaje: kto i na ile ceni swoje dane? Podobnie jak w przypadku oceny zysków i strat, jak ocenić włamanie się na nasze konta Facebook? Czy szkoda będzie zależała od sumy godzin, przez które konto nie funkcjonowało, czy ilość rozesłanych fałszywych informacji skutkującą utratą reputacji, czy też publikacją prywatnych zdjęć lub ich usunięciem? Na te pytania ubezpieczyciel jak na razie nie zna odpowiedzi.

Stabilizacja rynku – szansa numer 1

Jedną z ważniejszych korzyści płynących z ubezpieczeń cyber jest stabilizacja rynku. Tak jak każdej innej branży, transfer ryzyka pozwala uporządkować relacje miedzy podmiotami. Ubezpieczenie oznacza zwiększone zaufanie firm, większą współpracę, rozwiązanie problemu zarządzania informacją i ryzykiem przez firmy trzecie (third party risk management).

W coraz bardziej nieprzewidywalnym środowisku cybernetycznym, ubezpieczenie cyber może zapobiec eliminacji podmiotów z rynku w przypadku poważnego ataku i utraty bądź kompromitacji danych. Ubezpieczyciel spełniałby w przyszłości rolę podobną do banku centralnego dla banków komercyjnych i byłby gwarantem funkcjonowania firm w dobie wzmożonych zagrożeń cybernetycznych.

Potencjał jest spory, należy jednakże wypracować skuteczne regulacje prawne, a także pomyśleć o obowiązkowym cyberubezpieczeniu firm oferujących strategiczne usługi : finanse, energia, służba zdrowia. Koszty przywrócenia systemów do ich stanu poprzedniego w przypadku np. ataku DDOS mogłyby być natychmiast poniesione przez ubezpieczyciela, bez względu na kondycję finansową samego przedsiębiorstwa.

Wzrost świadomości bezpieczeństwa danych– szansa numer 2

Pozytywnym efektem pobocznym wejścia ubezpieczyciela na cyberrynek jest wzrost świadomości (ang. awarness raising) w zakresie bezpieczeństwa informacji. W procesie wyceny ryzyka ubezpieczyciel przysyła do firmy ekspertów, którzy badają stan infrastruktury, posiadaną przez firmę dokumentację, zabezpieczenia, kontrole. W idealnej sytuacji ubezpieczyciel powinien także wykonywać pentesty w celu wykrycia podatności (vulnerabilities) i furtek (backdoor) w systemach firmy. Oceny i testy pozwalają na odkrycie i uświadomienie sobie własnych słabości. Zazwyczaj samo świadomość jest pierwszym krokiem do podjęcia strategii obrony przed atakami. Firma, która nie zna swoich podatności, nie może skutecznie się bronić, trudniejszym także jest dla takich firm szybkie reagowanie na cyber-incydenty.

Ubezpieczyciel ponadto zazwyczaj posiada kontakty z dobrze rozbudowaną siecią specjalistów, którzy są w stanie szybko zareagować na incydent – wszak mniejsze straty firmy są obopólną korzyścią

ubezpieczyciela i samej firmy. W tym wypadku ubezpieczyciel stanowi szansę dla biznesu. Może on w porę zareagować na atak bądź skutecznie zminimalizować skutki i przywrócić poprzedni stan danych. Należy jednak pamiętać: ubezpieczenie nie powinno zastąpić prewencji i kontroli ryzyka na poziomie firmy.

Refleksje na przyszłość

W powyższym artykule zilustrowano szanse i wyzwania, jakie niesie ze sobą nowa zastana rzeczywistość, w której firmy coraz częściej sięgać będą po transfer ryzyka w stronę ubezpieczyciela.

Aktualnie wyzwania przeważają nad szansami, jednak myśląc optymistycznie - spora część wyzwań można zamienić w szansy przy odpowiednim wysiłku regulatorów i mechanizmów państwowych.

Największymi szansami cyberubezpieczeń na przyszłość są:

1. **Stabilizacja rynku**

2. **Wzrost świadomości bezpieczeństwa danych**

Elementy, które wymagają dalszych poprawek i opracowań:

1. **Problem z wyliczeniem zysku i strat**

2. **Teoria transferu ryzyka**

3. **Bariery w rozwoju usług cyberubezpieczeń**

4. **Brak danych i statystyk dla cyberubezpieczeń**

5. **Brak ubezpieczeń dla osób prywatnych - fizycznych**

Podsumowując, cyberubezpieczenie jest zjawiskiem nieuchronnym i uzasadnionym względami ekonomicznymi, tak jak każdy inny rodzaj ubezpieczenia. Największym wyzwaniem pozostaje świadomość tego, że cyberryzyko jest nieporównywalne z żadnym innym ryzykiem dotychczas zarządzanym przez firmy i ubezpieczycieli. Skomplikowane relacje miedzy systemami, zabezpieczeniami, podwykonawcami, skomplikowana architektura informatyczna zmuszają nas do zmiany dogmatów i logiki ubezpieczeń.

Paweł Góralski

Czytaj też: Światowy indeks cyberbezpieczeństwa – brakujący element cyberukładanki