Cyberdefence 24

05.09.2016

WYDATKI NA CYBERBEZPIECZEŃSTWO MUSZĄ WZROSNĄĆ – MÓWIĄ EKSPERCI Z PWC W WYWIADZIE DLA CYBERDEFENCE24

Ostatnim dostrzegalnym trendem jest popularność ataków typu ransomware. Wirus ten jest projektowany specjalnie pod poszczególne instytucje, a jego popularność doprowadziła do tego, że stał się samodzielną gałęzią „biznesu" hakerskiego – mówią w wywiadzie dla portalu Cyberdefence24 Patryk Gęborys, wicedyrektor w zespole Cyber Security oraz Roman Skrzypczyński, ekspert ds. cyberprzestępczości w zespole usług śledczych i zarządzania ryzykiem nadużyć.

Zapraszamy do zapoznania się z pierwszą częścią wywiadu z ekspertami PwC Patrykiem Gęborysem oraz Romanem Skrzypczyńskim.

Andrzej Kozłowski: Czy i jak instytucje państwowe powinny się zaangażować w finansowanie cyberbezpieczeństwa, w szczególności w sektorze MŚP? Czy polskie firmy, które prowadzą działalność biznesową w Państwie Środka, a tym samym są narażone na ataki cyfrowe, powinny od państwa otrzymywać jakąkolwiek pomoc w zakresie cyberbezpieczeństwa? Jak ocenia Pan dotychczasowe działania w tym obszarze?

Roman Skrzypczyński: Na pewno można stwierdzić, że plany Pana Premiera Mateusza Morawieckiego związane z cyberprzestrzenią, idą w dobrym kierunku. Skupiają się one na pobudzaniu innowacyjności między innymi poprzez wykorzystanie dużych agencji rządowych, jak np. Polska Agencja Rozwoju Przedsiębiorczości (PARP). Co ważne, Minister Cyfryzacji już wdraża nowe dokumenty i strategie, które mają regulować ten rynek. Mam nadzieję, że za tym pójdą odpowiednie środki finansowe, do czego służy NCBR i programy przez nie wspierane. To jest realna pomoc państwa, którą należy zintensyfikować, ażeby miała jeszcze większe przełożenie na przedsiębiorców.

AK: Jedna z firm opracowała raport na temat podatności krajów na cyberataki w Unii Europejskiej. Według niego, Polska ma być najbardziej podatnym na cyberataki krajem w UE. Czy Panowie się z tym zgodzą? Czy faktycznie sytuacja wygląda tak źle, skoro nasze straty z tytułu działalności cyberprzestępców są wciąż znacznie mniejsze niż w Holandii czy Niemczech?

RS: Taki wynik jest przede wszystkim efektem wzrostu świadomości, a tym samym szerszej komunikacji firm i instytucji na temat cyberataków. Przez lata tajemnicą poliszynela były ataki na instytucje finansowe, które jednak nigdy nie przyznawały się do tego, że padły ofiarą hakerów. Teraz, kiedy dochodzi do różnych incydentów, nie tylko w instytucjach finansowych, ale także w firmach z innych branż – ich przedstawiciele potrafią nie tylko umiejętnie poinformować o zdarzeniu, ale i odpowiednio nim zarządzić wewnątrz organizacji. Nie chce tutaj dotykać konkretnych zdarzeń, ale widać ewidentną poprawę, że zarówno świadomość, jak i umiejętności zarządzania kryzysem są coraz

lepsze.

AK: Jakbyście Panowie scharakteryzowali krajobraz zagrożeń w Polsce oraz dynamikę ich zmiany? Czy możemy powiedzieć, że inne zagrożenia czyhają na instytucje administracji państwowej, a jeszcze inne na firmy prywatne, czy są on mniej więcej podobne?

RS: Zagrożenia są bardzo zbliżone i nie można ich traktować w podziale na sektory, których dotykają. Wiadomo, że każda z tych instytucji posiada zasoby, które można przejąć w nieuprawniony sposób, a później sprzedać i na tym zarobić, jak np. dane osobowe. Ostatnim widocznym trendem jest wzrost popularności ataków typu ransomware, który dotyka praktycznie wszystkich. Malware tego typu jest specjalnie projektowany pod poszczególne instytucje, a jego popularność doprowadziła, do tego, że stał się samodzielną gałęzią „biznesu" hakerskiego. Nie ma tu różnicy, czy jest to podmiot prywatny czy państwowy. Wszystkie te podmioty są jednakowo narażone, ponieważ posiadają zasoby, na których można zarobić.

Patryk Gęborys: Cele ataku mogą się różnić ze względu na ich kategorię. Pierwszym z nich jest atak powszechny, czyli to co udało się hakerom zainfekować, jest dalej wykorzystywane i proces ten obserwujemy na skrzynkach firmowych i prywatnych. Do ataku może równie dobrze dojść w firmie, szpitalu, urzędzie gminy, czy innej instytucji publicznej. Druga kategoria to ataki precyzyjne, gdzie przestępcy ustalają sobie konkretne cele do osiągnięcia. W przypadku finansowej motywacji ataku, hakerzy próbują uzyskać przelew od konkretnej firmy z wykorzystaniem konkretnych wewnętrznych mechanizmów. Chodzi o typową wiedzę insiderską, kiedy haker wie dokładnie, kto jaką pełni rolę w danej organizacji, kto jest głównym księgowym, kto akceptuje przelewy, kto wypłaca premie – a następnie wykorzystuje tę wiedzę do przestępczych celów. Innym przykładem mogą być instytucje publiczne, które są atakowane, aby uzyskać informacje chronione, albo żeby uzyskać dostęp do infrastruktury krytycznej i mieć możliwość przeprowadzenia akcji sabotażowych. Różnica jest w celach ataków, ale same techniki są w każdym z tych przypadków bardzo podobne.

AK: Jednym z głównych problemów jest ostatnio ransomware. Dlaczego właśnie teraz, przecież jest to narzędzie, które istnieje od wielu lat?

PG: Należy zwrócić uwagę na cykle koniunkturalne cyberprzestępczości. Dość gładko przechodzimy tu z jednej fazy do drugiej i dalej do następnych. W przeszłości była to kradzież kart kredytowych i ten proceder cały czas funkcjonuje i ma się nieźle. Kolejno, cyberprzestępcy skupiali się na „czyszczeniu" kont bankowych, co obecnie również ma miejsce, choć nie jest już tak powszechną praktyką przestępczą. Natomiast najnowszym trendem jest właśnie ransomware. Trudno oszacować skalę tego zjawiska. Podejrzewam, że jest mimo wszystko wciąż nieco mniejsza niż w przypadku pozostałych przestępstw. Jest to po prostu kolejne narzędzie w rękach cyberprzestępców. Powstała cała infrastruktura, którą można wręcz wynająć, aby tworzyć takie ataki.

AK: Czy firmy przeciwko ransomware powinny specjalnie się bronić? Czy to powinna być część większej strategii obrony przed wszystkimi zagrożeniami z cyberprzestrzeni?

RS: Współpraca państwa z sektorem prywatnym jest niezbędna – tutaj łączy wspólny cel, czyli bezpieczeństwo. Bezpieczna cyberprzestrzeń Polski i Europy składa się zarówno z przestrzeni państwowej, jak i prywatnej. Będę się posiłkował tutaj przykładem międzynarodowego operatora telekomunikacyjnego. Jeżeli cieszy się opinią bezpiecznego, to wielce prawdopodobne jest, że instytucje państwowe będą zamawiać właśnie u niego usługi związane z bezpieczeństwem, zapewniając tym samym właściwą ochronę obywatelom. Bezpieczeństwo obywateli tworzy bezpieczeństwo państwa, dlatego kooperacja sektora prywatnego i sektora publicznego jest absolutnie niezbędna.

AK: Może firmy powinny bardziej się skupić na środkach minimalizujących straty, bo cyberatak nastąpi tak czy inaczej?

RS: Niewątpliwie powinien być to jeden z głównych elementów systemu obronnego. Kiedy my pojawiamy się w jakiejś firmie, oznacza to najczęściej, że cyberatak już nastąpił. Na zapewnienia firmy o wysokim poziomie bezpieczeństwa odpowiadamy, że może po prostu w firmie nikt nie wie, nie zdaje sobie sprawy z tego, że padła ofiarą ataku.

AK: Czy nowa dyrektywa Unii Europejskiej NIS wprowadza obowiązek informowania o incydentach?

PG: Nowa dyrektywa wprowadza ten obowiązek i zmienia „zasady gry". Do tej pory mieliśmy przypadki, kiedy dochodziło do przejęcia/ ujawnienia danych osobowych i… nic się z tym później nie działo. Mamy raptem dwa wyroki skazujące dotyczące naruszenia danych osobowych przez ponad 10 lat obowiązywania ustawy. Nowa dyrektywa wprowadza natomiast obowiązek informowania o incydentach. Jeżeli firmy nie zastosują się do nowych przepisów, to grożą im wysokie kary finansowe rzędu 20 mln euro, czy kilku procent przychodów firmy. Dyrektywa wchodzi w życie już za 2 lata, w 2018 roku.

AK: Czy nie jest za mało czasu na jej wprowadzenie?

PG: Firmy mają wystarczająco dużo czasu na przygotowanie oraz na zastanowienie się, na jakie ryzyka są narażone i z jakimi zagrożeniami muszą walczyć. Należy nakreślić scenariusz wydarzeń oraz sposób w jaki dana firma jest zabezpieczana, a także stworzyć plan działania w przypadku incydentu.

AK: Czy ona nie obciąża finansowo szczególnie małych i średnich przedsiębiorstw?

PG: MŚP mają możliwości skorzystania z tańszych, ale wciąż wystarczająco bezpiecznych rozwiązań. Mogą przykładowo użyć rozwiązań chmurowych. Problemem jest natomiast tendencja firm to przechowywania dużej ilości danych na własnych serwerach. Pojawia się tutaj pytanie, czy jest to faktycznie konieczne i opłacalne, w szczególności uwzględniając wzrost wymagań regulacyjnych w tym zakresie.

AK: Jak zdaniem Panów wygląda w Polsce współpraca między sektorem prywatnym a publicznym w zakresie ochrony przed zagrożeniami cybernetycznymi?

PG: Nie jest to jednie kwestia współpracy między sektorem prywatnym a publicznym. Jak pokazuje nasz raport, generalnie polskie firmy niechętnie współpracują. Bez znaczenia jest, czy między sobą, czy z organami administracji publicznej. 42 proc. respondentów zadeklarowało brak współpracy z jakimikolwiek podmiotami zewnętrznymi. Z mojej perspektywy głównym problemem jest tutaj kryzys zaufania, czyli nieufności między różnymi podmiotami. Z drugiej jednak strony mamy pozytywne przykłady takiej współpracy, jak np. grupy branżowe, choćby te skupione wokół CERTu Narodowego, zrzeszające operatorów telekomunikacyjnych czy dostawców usług internetowych.

AK: Z jednej strony firmy ze sobą konkurują, nawet z wykorzystaniem nielegalnych cyberataków, a z drugiej strony powinny ze sobą współpracować w ramach przeciwdziałania zagrożeniom cybernetycznym. Dostrzegam tutaj pewną sprzeczność.

PG: Nie stawiałbym tezy, że każda firma w ramach standardowych metod działania na rynku stosuje cyberataki, to niewielki ułamek firm. Zdecydowana większość z nich jest jednak po tej samej stronie barykady, czyli raczej są narażeni na ataki cyberprzestępców, ale nie ze strony swoich konkurentów. Ponadto należy zauważyć, że sama informacja o incydentach nie daje przewagi konkurencyjnej. Nie jest to informacja biznesowa, więc można połączyć siły w ramach jednego sektora i stawić czoła

atakom. Zresztą widać, że często w ramach jednej branży realizowana jest cała kampania skierowana do różnych podmiotów. W ten sposób cała branża staje się silniejsza. Natomiast zakres dzielenia się informacjami zawsze wymaga decyzji po stronie firmy, do jakiego stopnia chce i może się odsłonić. Nie dając nic w zamian, firmy nie mogą oczekiwać wielkiego wsparcia.

AK: Jak kształtuje się przyszłość cyberbezpieczeństwa w sektorze prywatnym? Czy są Panowie optymistami w tym względzie?

RS: Ja niestety widzę przyszłość w ciemnych barwach. Obecnie znajdujemy się w stanie wojny hybrydowej, a cyberataki są jej ważnym elementem. Ten trend w przyszłości będzie się tylko nasilać. Powstają specjalne oddziały w ramach służb wojskowych, policyjnych i wywiadowczych. Działają one na zlecenie rządów wielu państw i atakują wiele celów, przy czym nie tylko skupiają się na infrastrukturze krytycznej państw, czy na firmach komercyjnych. Zagrożony jest też zwykły obywatel. Moim zdaniem, skala zagrożeń będzie rosła. Dlatego z całą konsekwencją należy przeciwdziałać temu zjawisku.

PG: Nie można mieć wątpliwości, że liczba ataków będzie coraz większa, a one same bardziej złożone i niebezpieczne. W szczególności biorąc pod uwagę nasze rosnące uzależnienie od technologii. Dobrym przykładem jest Internet of Things ze swoimi problemami w obszarze cyberbezpieczeństwa. Mamy przykłady hakowania samochodów, które mają już coraz więcej komunikacyjnych gadżetów podłączonych do globalnej sieci. Zwiększa się dzięki temu pole rażenia cyberataków i firmy, chcąc dalej funkcjonować w przestrzeni biznesowej, będą musiały sobie z tym skutecznie radzić. Istnieje prawdopodobieństwo, że przedsiębiorstwa, które nie uwzględnią w swojej strategii biznesowej zagadnień z zakresu cyberbezpieczeństwa, będą bardziej podatne na ataki, co będzie miało bezpośrednie przełożenie na ich konkurencyjność na rynku.

Czytaj też: Czujnik światła może stać się zagrożeniem dla prywatności użytkowników