aut. Andrzej Kozłowski 24.06.2019

HUAWEI WYZNACZA STANDARDY CYBERBEZPIECZEŃSTWA [WYWIAD]

O odmiennym podejściu Huawei do cyberbezpieczeństwa, systemach weryfikacji produktów oraz centrach cyberbezpieczeństwa mówi Rafał Jaczyński, Regional Cyber Security Officer CEE&Nordics,Huawei.

Andrzej Kozłowski: Jak zagwarantować cyberbezpieczeństwo w takiej firmie jak Huawei?

Rafał Jaczyński: Dokładnie tak, jak w każdej innej firmie, z tą subtelną różnicą, że Huawei traktuje ten problem śmiertelnie poważnie.

A inne firmy nie?

Różnie bywało. Powiem o jednej subtelnej różnicy. Kiedy popatrzymy na najlepsze praktyki i standardy cyberbezpieczeństwa, to jedną z pierwszych rzeczy, o których się wspomina jest to, że bezpieczeństwo powinno być wbudowane w procesy firmy. Cyberbezpieczeństwo jest odpowiedzialnością każdego, a bezpieczeństwo w firmie rozpoczyna się w recepcji. Przejdźmy się po prezesach polskich i europejskich firm i popatrzmy na ich cele. Czy tam znajduje się jakikolwiek cel związany z bezpieczeństwem? Wątpię. Nie zdarzyło mi się, żebym coś takiego zobaczył. Zwykle jest tak, że w praktyce bezpieczeństwo spoczywa na barkach jednego Chief Information Security Officera. Toczy on swoją walkę, starając się o środki, przekonując innych. Natomiast niezmiernie rzadko jest tak, że osoby zarządzające firmą ponoszą rzeczywistością odpowiedzialność za cyberbezpieczeństwo.

Czytaj też: Czego powinny spodziewać się polskie firmy w 2019? [RAPORT]

Natomiast Huawei, rozwijając się dynamicznie przez ostatnie 30 lat, traktuje najlepsze praktyki w kwestii cyberbezpieczeństwa dokładnie tak, jak sama nazwa wskazuje – jako podejście rekomendowane przez najlepszych, zasługujące zatem na poważne traktowanie. Skutek jest taki, że corocznie, a nawet 2 razy do roku, prezes każdego lokalnego oddziału musi złożyć do Centrali raport na temat cyberbezpieczeństwa. Taki dokument nie jest opracowywany przez osobę odpowiadającą za cyberbezpieczeństwo, ale robi to prezes, bo za to odpowiada i tej odpowiedzialności nie jest w stanie uniknąć. W razie czego wszystkie problemy i incydenty obciążają go osobiście. Mogę sobie wyobrazić sytuację, że w jakimś kraju w Huawei nie byłoby osoby, która na 100% czasu zajmuje się bezpieczeństwem – ale nie oznacza to, że dany oddział nie zajmowałby się cyberbezpieczeństwem, bo jest ono tak mocno wbudowane w mentalność i w procesy.

Mówiąc o bezpieczeństwie w kontekście Huawei i elementów infrastruktury telekomunikacyjnej. Ostatnio była kolejna informacja jednej z instytucji rządu brytyjskiego o tym, że są problemy z tzw. higieną cyberbezpieczeństwa, czy z pewnymi podstawowymi

zasadami.

To są ciekawe informacje, które warto zawsze umiejscowić w pewnym kontekście, a najlepiej porównując z kimś. Problem polega na tym, że obecnie Huawei nie ma za bardzo z kim się porównać, bo gra w swojej lidze. Żadna inna firma z tej branży nie jest poddana porównywalnemu reżimowi weryfikacji. Jeżeli Rada Nadzorcza naszego Centrum Cyberbezpieczeństwa w Wielkiej Brytanii przygotowuje publiczny raport, w którym wymienia wady i zalety, to nie mamy tego z kim porównać, bo firmy konkurencyjne nie stosują podobnych rozwiązań.

Czytaj też: Brytyjczycy nie zgadzają się z opinią Stanów Zjednoczonych w sprawie Huawei

Te firmy nie mają własnych centrów cyberbezpieczeństwa?

Nie posiadają takich instytucji. Chętnie porównałbym się z tymi firmami, bo widzę jak to jest robione w Huawei, i uważam, że wychodzi to całkiem dobrze. Nie mam niestety takiej możliwości, bo nikt inny nie zaoferował podobnego rozwiązania. A szkoda, bo taka transparentność służy zarówno klientom, jak i poprawia jakość produktów. Wiadomo przecież, że zarówno kod jak i sprzęt trzeba zaimplementować pod względem bezpieczeństwa i przetestować to jeszcze w trakcie rozwoju. Potem trzeba zrobić już tylko rzeczy: testować, testować, testować.

Czytaj też: Huawei otwiera Centrum Przejrzystości i Cyberbezpieczeństwa w Brukseli

Huawei to właśnie robi i nie tylko, dlatego, że chce, ale też musi poddawać się zewnętrznej weryfikacji ze strony państw i firm trzecich. Siłą rzeczy to powoduje, że bezpieczeństwo naszych produktów jest coraz lepsze. Nie boję się powiedzieć, że już teraz jesteśmy, jeśli chodzi o poziom bezpieczenstwa produktów, najlepszą firmą w branży, a będziemy niekwestionowanym liderem, właśnie dlatego, że mamy szanse na tyle sposobów się weryfikować.

Zarzuty stawiane przez brytyjskie instytucje doprowadzą do tego, że Huawei dokona ulepszeń swojego poziomu cyberbezpieczeństwa?

Oczywiście tak będzie. Podam przykład, tam jest mowa o kilkuset błędach bezpieczeństwa. Wolałbym, aby błędów było zero. Natomiast warto sobie zdać sprawę, że produkt, którego dotyczyła analiza, ma ponad 230 milionów linii kodu. Gdyby przyjąć poziom odniesienia do wytwórców masowego oprogramowania, to „przysługiwałoby" nam kilka tysięcy błędów, a jest kilkaset. Jest to dalej za dużo, ale już lepiej i gdyby porównać się z innymi to mogłoby się okazać, że Huawei jest liderem. Druga sprawa to kryteria oceny, które dotyczą rynku brytyjskiego pochodzą ze strony brytyjskich służb państwowych. To nie są wymagania, pod które podlegają firmy komercyjne. One są dużo, dużo wyższe. Owszem, musimy się poprawić aby im sprostać i stąd inwestycja w wysokości 2 miliardów dolarów. Musimy wiele zrobić w tym obszarze i jeśli osiągniemy sukces, to będziemy w stanie spokojnie powiedzieć, że żadna inna firma poza Huawei nie spełnia tych kryteriów.

W Wielkiej Brytanii to rząd współpracując z Huawei dokonuje takiej oceny. Jak wygląda w Polsce współpraca z rządem? W lutym była mowa o możliwości dostępu do kodu źródłowego Huawei.

Druga strona nie podjęła dialogu. W międzyczasie otworzyliśmy nasze centrum w Brukseli, gdzie na zasadach komercyjnych każdy może przyjść, obejrzeć kod i go przetestować, albo może przyprowadzić firmę trzecią z własnymi narzędziami. Oczywiście jest to zrealizowane w taki sposób,

żeby ten kod nie opuścił naszego laboratorium. Jest to w końcu nasza własność intelektualna. Gdybyśmy poszukali firmy, która pozwala na analogiczny poziom przejrzystości w branży, to właściwie takiej nie ma. Dlatego bardzo ciężko jest się z kimś porównać. Ponadto mamy niektóre firmy, które uważają, że produktów pod kątem bezpieczeństwa testować nie warto. Jeden z prezesów pewnego koncernu w Polsce tak powiedział. Początkowo myślałem, że został źle zrozumiany, ale przedstawiciel tej firmy potwierdził mi takie podejście osobiście.

Czytaj też: Polski rząd pozna kody źródłowe Huawei?

Czyli jego zdaniem przy budowie sieci 5G bezpieczeństwo nie będzie ważne?

Trzeba byłoby skierować to pytanie do niego o wytłumaczenie tego stanowiska. Ja to rozumiem w ten sposób, że jego zdaniem polegamy na security by design. W związku z czym tak duża otwartość, jeśli chodzi o udostępnianie kodu, nie jest wskazana. Jego zdaniem testowanie produktów pod kątem bezpieczeństwa nie będzie robiło wielkiej różnicy i ze względu na ochronę praw własności intelektualnej, jego firma nie będzie udostępniała kodu. Osobiście jestem zdziwiony taką postawą, bo uważam, że testowania nigdy za dużo.

Jeżeli każdy może przetestować kod Huawei, to firma nie obawia się kradzieży własności intelektualnej?

Staramy się jednak ograniczać takie ryzyko i nie publikujemy kodu na GitHubie... Dlatego też w naszym centrum w Wielkiej Brytanii nadzór jest bardzo ścisły i pracują tam ludzie, którzy mają prawo dostępu do informacji niejawnych. W Brukseli jest to zorganizowane inaczej, tam ten kod nie opuszcza naszego systemu, a prawa i obowiązki strony reguluje komercyjny kontrakt, który podpisujemy np. z operatorem.

Uważam, że nigdy takich propozycji nie jest za dużo. Świat cyberbezpieczeństwa idzie w kierunku otwartości, im więcej testowania, tym lepszy jest rezultat. Obecnie raczej nikt tego nie kwestionuje. To jest trochę paradoksalne, ale właśnie Huawei jest teraz najbardziej otwartą firmą. Zastosowanie produktów chińskiego producenta jest mniej ryzykowne niż innych przedsiębiorstw, które odmawiają testowania.

Pojawia się taki argument, że testowanie kodów i budowa centrów cyberbezpieczenstwa jest zagrywką PR, bo nie można w krótkim czasie zbadać ileś setek kodu.

W związku z tym można by przyjąć postawę, że nie będziemy robili nic. Idziemy jednak w tym kierunku, że stwarzamy możliwości. Nie ograniczamy naszych klientów w zakresie tego, co oni powinni sprawdzić i nie mówimy, że nie będą w stanie zweryfikować danego sprzętu. Podążamy w drugą stronę i otwieramy się coraz bardziej i wcale nie zakładamy, że nasi klienci nie mają kompetencji czy możliwości przetestowania.

Dając taką możliwość, Huawei wytyczy pewien pozytywny trend dla branży.

Mam taką nadzieje, ponieważ zależy mi, żeby nasze sieci były bezpieczne niezależnie od tego, kto dostarcza tam sprzęt. Chciałbym również, żeby operator, który na koniec dnia odpowiada za bezpieczeństwo sieci, panował nad nią. Zależy mi na tym, żeby trafiały tam rozwiązania, który pewien poziom zaufania spełniają. W związku z czym bardzo chętnie bym widział podobną otwartość ze strony pozostałych dostawców, bo wtedy można przeprowadzić rzeczywiste porównanie oparte na faktach. Wtedy łatwo jest zweryfikować, kto ile ma błędów w odniesieniu do ilości kodu, jaką ten kod ma jakość i jakie mechanizmy zostały zaimplementowane.

W wyniku rozporządzania wykonawczego Donalda Trumpa kilkanaście firm odcięło się od współpracy z Huawei. Czy w jakimś stopniu wpłynie to bezpieczeństwo produktów Huawei?

Rozporządzanie wykonawcze nie wpłynie na bezpieczeństwo produktów firmy ani na bezpieczeństwo klientów. Huawei będzie dostarczał poprawki bezpieczeństwa i usługi wsparcia dla wszystkich istniejących produktów oraz do tych zakupionych w przyszłości. Trzeba też powiedzieć, że Huawei przewidywał takie posunięcie jako duża firma, analizując ryzyka, które wydawały się nieprawdopodobne, ale okazały się realne, po tym jak problemy po nałożeniu amerykańskich sankcji miała chińska firma ZTE. Huawei przez 10 lat przygotowywał się do podobnych scenariuszy. Owszem, żadna taka sytuacja nie pozostaje bez wpływu na przychody. Zawsze trzeba się liczyć, że sprzeda się mniej danego sprzętu lub trzeba będzie zrezygnować z niektórych gałęzi biznesu. Jeśli chodzi o nasze podstawowe produkty, to mamy alternatywy, bądź ta blokada nie wpłynie w dużym stopniu na nasze możliwości. Nie jest to sytuacja łatwa, bo każdy przygotowany plan trzeba wdrożyć i uruchomić, ale nie poddajemy się, a nasi klienci udzielają nam dużego kredytu zaufania.

Czytaj też: Huawei: zawieszenie współpracy nie wpłynie na codzienną działalność