JEŚLI TWOJA ORGANIZACJA NIE MA CHMURY OBLICZENIOWEJ….ZMIEŃ ORGANIZACJĘ

Czasami mamy wrażenie, że chmura nie pasuje do aktualnej organizacji cyberbezpieczeństwa. Jeśli tak jest to znaczy, że to prawda. Końcowym wnioskiem nie powinno być odrzucenie chmury jako sposobu na IT, ale zmiana organizacji. Bo właśnie zdobyliśmy dowód na to, że organizacja nie jest dostosowana do wymagań współczesnego świata.

Przykładem niech będzie dyskusja o lokalizacji danych. Wielokrotnie stawiany był znak równości pomiędzy lokalizacją we własnej infrastrukturze a większym bezpieczeństwem. Jednak, jeśli weźmiemy pod uwagę, że intruzi niezauważeni grasują w wewnętrznych sieciach średnio przez ponad 200 dni to tylko niezwykle naiwni lub niezwykle pewni siebie mogą stwierdzić „mnie to nie dotyczy". Jeśli choćby stworzymy listę potencjalnych nowych (NOWYCH!) wektorów ataków to nasze potrzeby budżetowe na cybersec trzeba będzie wielokrotnie zwiększyć. A potem – zakładając, że prosiliśmy i było nam dane – trzeba znaleźć ludzi by wszystko to razem uruchomić i utrzymać. Docieramy wtedy do propozycji chmury, bo wydaje się, że taki sposób realizacji zadań może być skuteczny i bezpieczny. Zamieniana jest wówczas narracja z „bezpieczne, bo u mnie", na „bezpieczne, bo w Polsce". Dlaczego jednak lepiej zabezpieczone dane poza Polską miałyby być bardziej narażone na atak niż słabiej zabezpieczone dane w kraju? Dlaczego globalny atak i połączona z tym utrata funkcjonalności miałaby nie dotyczyć lokalnego dostawcy? Po stronie technicznej taka argumentacja jest wyjątkowo słaba. Prawdziwa przyczyna jest po stronie psychologicznej lub (rzadziej) po stronie prawnej. Po stronie psychologicznej stoi kilka przyczyn. Wszystko dogadam po polsku. Jak będzie pytanie z kierownictwa to informacja, że mamy polskiego dostawcę chmury prawdopodobnie wystarczy. Kiedy przyjdzie kontrola to pewnie też kupią odpowiedź bez dalszych pytań. Jak by się coś działo to my tego dostawcę „zmłotkujemy", a w razie czego to pójdziemy do polskiego sądu. Ten dostawca zapewne będzie mniejszy niż nasza firma, więc to my stawiamy warunki. Z dużym i globalny tak się nie da. A wreszcie ostatni i doskonale zrozumiały, choć nigdy nie wypowiedziany argument: nie muszę nic zmieniać w swojej organizacji, wszystko zostaje po staremu. Spokój decydenta i brak konieczności dodatkowej pracy związanej z wprowadzeniem zmiany przeważają, ale nie mają związku z rzeczywistym bezpieczeństwem.

Czy to co padło powyżej jest zawsze prawdą? Oczywiście nie! Istnieją takie scenariusze i potrzeby, które mogą zapewnić tylko lokalni dostawcy. Raczej mało prawdopodobne by światowy *hyperscaler* chmurowy zgodził się na wprowadzenie jakiegokolwiek sprzętu na teren swojego CPD, na przykład sprzętowego modułu bezpieczeństwa HSM. Taka sytuacja może wynikać z wymagań prawnych, ale jak często się zdarza? Oczywiście *dura lex, sed lex* i nawet jeśli zabezpieczenie informacji będzie słabsze, ale prawodawca w swej mądrości tak nakazał to stosujemy się i już.

Wróćmy zatem do obaw natury prawnej, wyrażanych często przeciw wszelkiej chmurze. Zazwyczaj są słabo udokumentowane i w dużej mierze bazujące na obiegowych przekonaniach. Pierwsze pada

magiczne słowo RODO, ale tutaj niespodzianka, bo Rozporządzenie już w art.1 mówi, że nie zakazuje się i nie ogranicza się swobodnego przepływu danych w UE. Jest jeszcze gorzej z argumentacją, gdy przychodzi do danych nieosobowych – ograniczanie lokalizacji jest zakazane (tak!), a jeśli jakiś kraj chce zostawić zapis z ograniczeniem to tylko do przepisów związanych z bezpieczeństwem narodowym, ale jeszcze trzeba uzyskać notyfikację z Komisji Europejskiej. To jest prawo obowiązujące w Polsce! Ustawa o krajowym systemie cyberbezpieczeństwa (oraz dyrektywa NIS) nie tylko dopuszcza stosowanie chmury dla wsparcia informatycznego usług kluczowych, ale z góry zakłada ich możliwy ponadgraniczny charakter. I tak dalej, przepis po przepisie, ustawa po ustawie.

Prawdziwym problemem jest jednak to, że korzystanie z chmury publicznej i z narzędzi jakie dostawcy z tą chmurą dostarczają wymaga zmiany myślenia o cyberbezpieczeństwie i towarzyszącej mu zmiany w organizacji cyberbezpieczeństwa. Wymagane jest przejście z przekonania, że zasoby jakimi dysponujemy to nasi ludzie (razem z zewnętrznymi konsultantami), nasze narzędzia w naszej infrastrukturze i nasz czas jaki poświęcamy zagadnieniu. Współpraca z dostawcą chmurowym to z jednej strony odciążenie własnych zasobów, ale także wybudowanie umiejętności korzystania z tego co dostawca nam daje, a także komunikacji z tym dostawcą. To jest inny sposób tworzenia i utrzymania cyberbezpieczeństwa niż dotychczas oraz inny sposób pracy ludzi. Celem ostatecznym jednak jest podniesienie bezpieczeństwa w obliczu kolejnych nowych zagrożeń oraz sposobu kształtowania IT w organizacjach.

(lokalizacja była przykładem – taka sama dyskusja dotyczy szyfrowania, dostępu do danych czy innych czynników – ale wnioski są takie same).

Michał Jaworski, Dyrektor Strategii Technologicznej Microsoft Sp. z o.o.

Materiał powstał we współpracy z Microsoft Sp. z o.o.