Budowanie odporności

Jeśli mamy się czegoś nauczyć z doświadczeń Ukrainy, to utwórzmy polską cyfrową ambasadę dla rejestrów referencyjnych, przygotujmy proste zasady podniesienia poziomu odporności infrastruktury krytycznej i usług kluczowych z pomocą publicznej chmury obliczeniowej.

Michał Jaworski

pracownik polskiego oddziału Microsoftu z najdłuższym, niemal trzydziestoletnim, stażem. Obecnie dyrektor ds. strategii technologicznej (ang. *National Technology Officer*), pełni jednocześnie funkcję członka Zarządu Microsoft sp. z o.o. (od 2013 r.). Wiceprezes Związku Pracodawców Technologii Cyfrowych Lewiatan. Regularnie publikuje w „IT Professional" i „IT w Administracji".

Jeśli wrócił z podróży, to znaczy, że już planuje następną. Najchętniej znalazłby czas na jeszcze jedną książkę lub dłuższy spacer z psem (https://www.linkedin.com/in/mijaworski/).

Estonia była pierwszym krajem, który stworzył podstawy cyfrowej ambasady i wypromował samo pojęcie. Tamtejszy rząd doszedł do wniosku, że funkcjonowanie państwa to nie tylko integralność terytorialna, lecz także świadczenie usług przez to państwo. Procesy cyfryzacji przebiegają w Tallinnie bardzo szybko i objęły niemal każdy obszar życia , dlatego należy zabezpieczyć – równolegle do świata fizycznego – świat cyfrowy. Tłumacząc bardziej obrazowo – bez względu na to, jak szybko tanki mogą zagarnąć terytorium kraju, nadal będzie można cyfrowo dokonać uwierzytelnienia, zarejestrować narodziny, a także zapłacić podatek. W wersji skrajnej państwo będzie działało na rzecz obywateli, nawet jeśli nie będzie kontrolowało nawet piędzi swojej ziemi. W pierwszej chwili trudno zorientować się, dlaczego określono cały projekt jako e-ambasadę, ale kiedy dochodzimy do pojęcia eksterytorialności, klocki zaczynają układać się w spójny obraz.

> *E-ambasada to taka część cyfrowego świata, w której obowiązuje prawo kraju właściciela, choć fizycznie wszystkie dane mogą znajdować się w zupełnie innym kraju.*

Przez wiele lat Estonia była jedynym krajem, który ten koncept realizował, jednak wojna w Ukrainie zmieniła postrzeganie. Litwa kilka tygodni temu wprowadziła podobne założenia dotyczące trzymania danych poza granicami kraju (https://www.linkedin.com/posts/markeviciute_cloud-digitalembassy-datacenters-activity-6930439919773319168-tGnl/?utm_source=linkedin_share&utm_medium=member_desktop_web), zaś Ukraina zmieniła prawo http://www.golos.com.ua/article/357312 w marcu i wówczas, jak to określił Satya Nadella w Davos, rozpoczęła się ewakuacja do chmury.

Nie ma powrotu do papieru

Temat, leżący w Polsce odłogiem przez długie lata, właśnie powrócił. Przyczyny takiego stanu rzeczy znowu wydają się oczywiste, tak jak jasne były przesłanki Estończyków po 2007 r. Pierwsza to rzeczywiste zagrożenie naszego państwa fizyczną agresją. Druga to konstatacja, że niemal wszystkie dziedziny naszego życia nasycone są informatyką i że większość informacji nas dotycząca ma już cyfrową postać. Niepostrzeżenie okazało się, że mamy profil zaufany, elektroniczne konto pacjenta, składamy PIT poprzez sieć, do naszych kont bankowych dostajemy się przez telefon, kupujemy bilety kolejowe w Internecie, uczymy się online, nie potrafimy już czytać papierowych map itd.

Firmy poszły jeszcze dalej – od cyfrowo obsługiwanych magazynów przez logistykę transportu po samą produkcję, zdigitalizowane są łańcuchy dostaw oraz procesy rozliczeń, przez sieć składane są deklaracje podatkowe i jednolity plik kontrolny, kasy fiskalne i terminale obsługujące karty i płatności telefoniczne są wymogiem chwili, dodajmy do tego ZUS i CEIDG, nie wspominając o infoliniach i systemach finansowo-księgowych. Atak cybernetyczny na wybrane elementy tej układanki może prowadzić do katastrofy lub potężnych kłopotów. Co więcej, powrotu do papieru i atramentu nie ma, nikt tego już nie chce.

Dochodzimy zatem do punktu, w którym przestajemy rozważać tylko bezpieczeństwo fizyczne, a wchodzimy na nowy etap – budowania odporności.

Cyfrowa ambasada – jaka i dla kogo?

Jeśli zobaczymy, jak Ukraińcy właśnie przerobili tę lekcję, to może okazać się, że cyfrowa ambasada to zbyt mało, by państwo mogło funkcjonować normalnie. Zacznijmy jednak od niej i zastanówmy się, kto powinien nią być objęty.

Możemy stworzyć rodzaj piramidy istotności różnych organizacji dla państwa, a potem przypisać im różne rozwiązania. Na samym szczycie będą te najważniejsze, referencyjne rejestry państwowe. Wbrew pozorom, nie jest ich aż tak dużo, ani nie są bardzo wielkie. Zaliczylibyśmy do nich PESEL, REGON, NIP, TERYT i zapewne jeszcze kilka innych. To one winny znaleźć się w e-ambasadzie, tak aby stanowić niepodważalną podstawę do potencjalnej odbudowy wszystkich innych systemów. Nie podlega dyskusji, że jedynym dysponentem i zarządzającym tych systemów, bez względu na terytorium, gdzie się znajdują, powinno być państwo polskie. Ich obsługą powinni zajmować się sprawdzeni pracownicy państwowi. Pozostaje pytanie, czym tak naprawdę ta ambasada miałaby być – czy tylko miejscem, gdzie znajdują się kopie danych, a może kopie danych wraz z możliwością odtworzenia systemu, czy jest to zapasowe centrum danych, do którego przełączamy się, jeśli jest taka konieczność. Każdy z tych wyborów niesie dalsze implikacje dotyczące: systemu łączności pomiędzy centralą a ambasadą i jego przepustowości, bezpieczeństwa transmisji danych, wolumenu danych przepływających każdego dnia, obecności personelu w ambasadzie, no i kosztów. Kiedy to wszystko już policzymy, pozostaje jeszcze wybór kraju, któremu chcielibyśmy zaufać. Czy będzie to jeden z naszych sąsiadów w Unii Europejskiej? A może alpejska twierdza w Szwajcarii? A może wybrać się za ocean, byle był w NATO? Wybór wcale nie jest łatwy, koszty wyglądają na potężne, porozumienie z obcym rządem trzeba wypracować, bo przecież ktoś tę ambasadę będzie budował, i zapewnić stabilność zasilania.

Jeśli chcemy mieć pewność, że państwo Polska będzie działało także w momencie największego zagrożenia, to ten koszt warto ponieść. Możemy jednak podejść do tego sprytniej. Wystarczy bowiem – są już takie rozwiązania! – wykorzystać zamknięte w kontenerze przenośne centrum danych. Na co dzień stoi ono w Polsce, nawet tuż obok naszego podstawowego CPD, połączone na stałe bezpiecznym i bardzo szybkim łączem, chronione tymi samymi środkami. Obsługują je nasi ludzie i nie trzeba martwić się ani delegacjami, ani potencjalnym werbunkiem podczas pobytu za granicą. Gdyby były jakieś awarie, to mamy serwis na miejscu. Jeśli – miejmy nadzieję, że właśnie tak będzie – nasze centrum danych zestarzeje się, to można zmienić sprzęt w środku lub nawet wymienić je na całkiem nowe, zaś stare przeznaczyć do innych zadań. Taki stan utrzymujemy, kiedy nie ma zagrożeń. A gdy się pojawiają, kontenerowe centrum doczepiamy do trucka lub pakujemy do Herculesa. Wybrana obsługa jedzie razem z nim i w miejscu docelowym je uruchamia. Wszystko, co potrzebujemy, to wcześniejsza umowa z państwem lub państwami, które zapewnią nam łączność, zasilanie i eksterytorialność. Nasi potencjalni przeciwnicy mogą nawet nie wiedzieć, do którego kraju pojedzie nasze CPD. Przy stałej e-ambasadzie jej lokalizacja i potencjalny atak jest łatwiejszy.

Podstawa piramidy

Cyfrowa ambasada to wierzchołek piramidy, to ta najlepiej opancerzona i chroniona część naszej suwerenności. Cyfrowa rzeczywistość jest jednak dużo bogatsza – chronić przecież trzeba operatorów infrastruktury krytycznej oraz operatorów usług kluczowych. To zaś kilkaset firm i organizacji, przy czym niektóre z nich to potężne instytucje, operujące ogromnymi zasobami danych i setkami aplikacji. Wystarczy wspomnieć, że wśród nich będą operatorzy telekomunikacyjni, banki, firmy energetyczne, a także administracja publiczna i służba zdrowia. Nawet przy najlepszych chęciach nie pomieści ich żadna e-ambasada. Co więcej, wiele z tych podmiotów to firmy prywatne, na co dzień poważnie liczące się z kosztami. Jeśli pojawią się nowe obowiązki, znajdzie to odbicie w wyższych cenach ich usług, które wszyscy zapłacimy.

Chmura publiczna jest już dzisiaj nieźle oswojona przez wiele segmentów rynku, w tym przez rynki regulowane. O licznych migracjach chmurowych podmiotów sektora finansowego mówił ostatnio na Europejskim Kongresie Finansowym sam szef UKNF. Całkiem spore doświadczenia zebrała administracja publiczna, która odkryła ją w czasie pandemii. Pierwsze większe wdrożenia pojawiły się w energetyce, co miało odbicie w wydaniu przez Ministerstwo Klimatu chmurowych wytycznych. Rekomendacje chmurowe dla służby zdrowia były jednymi z pierwszych w Polsce. Chmura nie jest nowością, są ludzie i kompetencje, są wdrożenia. Nikt nie dyskutuje z tym, że rzeczywiste bezpieczeństwo w chmurze publicznej będzie większe niż w rozwiązaniach w infrastrukturze własnej. Dla wszystkich mniejszych i średnich organizacji jest to prawda bezwzględna. Dla dużych najlepsze rezultaty daje synergia cyberbezpieczeństwa chmurowego oraz własnych kompetencji i rozwiązań we własnej infrastrukturze.

Wiadomo jednocześnie, że zasoby dostawców chmurowych bez trudu wchłoną dodatkowe zapotrzebowanie, zaś w standardzie są dostępne konfiguracje zapewniające wyższą odporność, na przykład redundancja pamięci masowych czy serwerów, kopie systemu w kilku centrach jednocześnie czy też kopie w innych regionach. Najprostsze rozwiązanie, czyli backup chmurowy jest na wyciągnięcie ręki. To, czego brakuje, to wyważona i prosta we wdrożeniu regulacja lub wytyczne – dokument, na podstawie którego podmioty obowiązane będą mogły uruchomić proces pozwalający na zabezpieczenie ciągłości działania, a także podnieść bezpieczeństwo przetwarzania. Czy pomogą w tym europejskie certyfikaty chmurowe (EUCS, European Union Certification Scheme), trudno obecnie wyrokować. Czy nowa fala przepisów związanych z cyberbezpieczeństwem, takich jak DORA czy dyrektywy NIS2 i CER, zmienią obraz? Również trudno odpowiedzieć, bo przecież pojawienie się Cybersecurity Act wiele nie zmieniło, a wdrożenie dyrektywy NIS (ustawa o krajowym systemie cyberbezpieczeństwa) przechodziło i przechodzi dalej różne choroby wieku dziecięcego. Co jest także jedną z przyczyn szybkiego procedowania dyrektywy NIS2.

Uważam, że prosty i jasny model wzmocnienia odporności za pomocą chmury warto w Polsce wypracować. To wołanie o prostotę jest niezwykle istotne – dzisiaj potencjalni klienci potrafią przygotować listę kilkuset (tak!) pytań na kilkudziesięciu stronach, starając się wykazać (super) należytą starannością przy wdrażaniu chmury.

Popatrzmy na doświadczenia ukraińskie. Nowe prawo, uchwalone już w trakcie wojny, pozwoliło na migrację danych i systemów do chmur komercyjnych poza terytorium kraju. Szczegółów tych migracji przytomnie nie publikuje się, więc posłużmy się tylko jednym przykładem – Privat Banku, który zdecydował się pod koniec kwietnia 2022 r. przedstawić ogólny opis projektu (*https://english.nv.ua/business/privatbank-moves-all-databases-to-the-cloud-50238052.html*). W ciągu 45 dni przeniesiono 3500 serwerów, ponad 4 petabajty danych i 270 aplikacji. Nad projektem pracowało 460 osób. Można? Można! Pozostaje pytanie, czy trzeba to robić na ostatnią chwilę…