dr Krzysztof Malesa, członek zarządu i dyrektor ds. strategii bezpieczeństwa w Microsoft Polska

Po długo wyczekiwanym upadku żelaznej kurtyny, w historii naszego regionu świata nastąpił chyba najlepszy w dziejach, wręcz arkadyjski okres. Pełni euforii i wiary w bezpieczną przyszłość szybko zapomnieliśmy o bolesnych doświadczeniach ostatnich kilkudziesięciu (może nawet kilkuset) lat.

dr Krzysztof Malesa: Technologia cyfrowa w służbie bezpieczeństwu

dr Krzysztof Malesa, członek zarządu i dyrektor ds. strategii bezpieczeństwa w Microsoft Polska fot. mat. prasowe Microsoft Polska

Nie tylko zresztą my. Wiele państw europejskich (z wyłączeniem Skandynawii) pospiesznie wypłaciło sobie dywidendę od zakończenia zimnej wojny zakładając, że nastał docelowy dla Europy czas długotrwałego pokoju. Zakończył się wyścig zbrojeń, wojska radzieckie opuściły terytorium byłego już Układu Warszawskiego, a NATO w zamian zobowiązało się do redukcji pewnych zdolności i infrastruktury. W zarządzaniu bezpieczeństwem pojawił się biznesowy model skupiony na ciągłości działania, a kwestie przygotowań obronnych państwa i przedsiębiorców zeszły na dalszy plan.

Niestety, historia brutalnie wyrwała Europę z tej błogiej drzemki, zataczając przy okazji koło i wracając do niespokojnych czasów, do których chyba trzeba się będzie przyzwyczaić na dłużej. W dobie transformacji cyfrowej i rozwoju technologicznego ten niepokój uwydatnia się w cyberprzestrzeni, a cyfrowe operacje towarzyszące wojnie przybierają zupełnie inny charakter niż do tej pory.

Wiadomo, że wojna zaczyna się o wiele wcześniej, niż zaczną spadać rakiety i strzelać czołgi. A kiedy się już zacznie, to rozgrywa się na znacznie szerszym obszarze niż tylko pole bitwy. Doskonalone od dziesięcioleci rosyjskie metody dezinformacji i działań hybrydowych, wskutek rozwoju usług cyfrowych i powszechnego dostępu do mediów społecznościowych, są dziś stałym elementem polskiej codzienności. Krajobraz cyberbezpieczeństwa po tegorocznej inwazji na Ukrainę zmienił się na tyle, że należałoby na nowo zdefiniować działania, dzięki którym zapewnimy (celowo używam liczby mnogiej) właściwy poziom cyberbezpieczeństwa Polski.

Porzućcie przedwojenne analizy

Wspólnym mianownikiem większości współczesnych regulacji z obszaru bezpieczeństwa jest działanie w oparciu o analizę ryzyka. Decyzje o wdrażaniu rozwiązań zapewniających bezpieczeństwo powinny być realizowane w sposób adekwatny i proporcjonalny do zidentyfikowanych potencjalnych zagrożeń. Zasada ta jest opisana zarówno w dokumentach krajowych, jak np. Narodowy Program Ochrony Infrastruktury Krytycznej, jak również w szeregu regulacji europejskich, włączając w to dyrektywę NIS określającą zasady zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych na terytorium UE. Również ustawa o krajowym systemie cyberbezpieczeństwa, jako pierwszy obowiązek operatora usługi kluczowej wyraźnie wskazuje systematyczne szacowanie ryzyka oraz zarządzanie nim poprzez wdrożenie odpowiednich i proporcjonalnych do poziomu ryzyka środków.

Wybuch wojny u naszych granic oraz nasilenie działań hybrydowych w Polsce do poziomu skutkującego wprowadzeniem stopni alarmowych BRAVO oraz CHARLIE CRP to okoliczności, wobec których analizę ryzyka należałoby przeprowadzić od nowa. Dotyczy to zresztą nie tylko cyberbezpieczeństwa, ale też kwestii zupełnie fundamentalnych, w których wszyscy, zarówno przedsiębiorcy jak i rządzący, powinniśmy odpowiedzieć sobie na nowo na kilka podstawowych pytań. Czy na pewno chronimy to, co powinniśmy? Czy robimy to we właściwy sposób? Co się wokół nas zmieniło przez ostatnie pół roku?

Zwróćmy uwagę, że analiza ryzyka jest podstawą do wyłaniania krajowej infrastruktury krytycznej. Skoro ryzyko się zmieniło, to może trzeba infrastrukturę krytyczną wyłonić na nowo? Jej właściciele z kolei mają ustawowy obowiązek ochrony tej infrastruktury, poprzez wdrożenie adekwatnych do ryzyka środków. Te środki również wymagają gruntownego przeglądu.

Samozadowolenie bez pokrycia

Tymczasem wiele organizacji żyje przeświadczeniem, że jeśli będą przestrzegać dotychczasowych (czytaj: (przedwojennych) zasad i jeśli dokończą rozpoczęte w zeszłych latach projekty mające na celu zapewnienie bezpieczeństwa swoich sieci i systemów IT, to mogą spać spokojnie. Niestety, trudno się z tym zgodzić.

Po pierwsze, zapewnienie bezpieczeństwa to ciągły proces. W słowniku managera bezpieczeństwa nie ma zwrotu „udało się", a stan samozadowolenia jest dla niego śmiertelnym zagrożeniem. Powinien pozostawać w ciągłym stanie nieufności (o zasadzie Zero Trust za chwilę) spodziewając się ataku w każdej chwili i w każdym miejscu systemu, nie ograniczając się do pilnowania brzegu sieci czy stacji roboczej.

Po drugie, głębokie zmiany w rejestrze ryzyka powodują, że stosowane (lub zaplanowane do wdrożenia) dotychczas środki zaradcze są nieadekwatne do nowych, dodatkowych zagrożeń, które przyniosła ze sobą wojna czy pandemia COVID-19.

Odpowiedzią na wspomniane powyżej nowe ryzyka, które w znacznej mierze wiążą się z działaniami hybrydowymi prowadzonymi w Polsce przez wrogie państwa, powinna być najnowocześniejsza technologia cyfrowa (szczególnie potencjał chmury obliczeniowej wsparty uczeniem maszynowym i sztuczną inteligencją) oraz inne możliwości, które przyniósł ze sobą rozwój techniki. Dobitnie pokazują to doświadczenia z Ukrainy.

E-ambasada

Jak zabezpieczyć krytyczne dane, takie jak rejestry państwowe, w sytuacji, kiedy na serwerownie spadają rakiety i żadne miejsce w kraju nie jest wystarczająco bezpieczne? Odpowiedź wydaje się prosta: przenieść dane tam, gdzie żadna rakieta, klęska żywiołowa czy akt sabotażu ich nie dosięgnie. Ucieczka przed fizycznymi zagrożeniami jest możliwa

dzięki uwolnieniu danych od ich fizycznej lokalizacji i przeniesieniu do chmury obliczeniowej.

Scenariusz ten zrealizowała Estonia, w 2017 roku lokując 10 krytycznych rejestrów w pierwszej na świecie ambasadzie danych w Luksemburgu. Tą samą drogą podążyła Ukraina, która niedługo po wybuchu wojny rozpoczęła ewakuację krytycznych danych do chmury, ze wsparciem cyfrowej technologii Microsoft. Analogiczne decyzje podjęła niedawno Litwa, a i w Polsce temat e-ambasady powoli przebija się do debaty na temat budowania odporności państwa na współczesne zagrożenia. Należy jednak pamiętać, że – tak samo jak w innych obszarach – budowanie odporności jest procesem długotrwałym. Realizacja idei ambasady cyfrowej wymaga przede wszystkim uporządkowania źródeł prawa, przygotowania danych do przeniesienia bądź reduplikacji w nowym środowisku, wymaga wreszcie niełatwej decyzji o zakresie ewentualnej współpracy z dostawcą technologii, która w dzisiejszych czasach może zapewnić wyższy poziom bezpieczeństwa danych niż zasoby administracji publicznej.

Dialog technologiczny

Nie ma innej drogi. Rząd powinien podjąć z dostawcami usług cyfrowych dialog na rzecz zapewnienia bezpieczeństwa Polski w średniej i długiej perspektywie. Tak wydarzyło się w USA, gdzie prezydent Biden, w obliczu nowych cyberzagrożeń, zobowiązał pięciu największych dostawców usług cyfrowych do konkretnych działań i wielomiliardowych inwestycji na rzecz wzmocnienia cyberbezpieczeństwa państwa.

Zobowiązanie Microsoft na najbliższe 5 lat dotyczy inwestycji o wartości 20 miliardów dolarów. Wobec miliarda dolarów rocznie inwestowanych przez Microsoft w cyberbezpieczeństwo, oznacza to czterokrotny wzrost nakładów w tym obszarze. Niezależnie od tego szef Microsoft Satya Nadella zadeklarował niezwłoczne przekazanie 150 mln USD na działania dla wsparcia cyberbezpieczeństwa amerykańskiej administracji

na wszystkich szczeblach. Przywołane kwoty są znaczne, ale z drugiej strony przedstawiciele firm technologicznych zyskali przewidywalnego rządowego partnera do wieloletniej współpracy, w ramach której można budować realną odporność państwa, nie ograniczając się do reaktywnych, pokazowych przedsięwzięć.

Zero trust

Opisane powyżej przykłady wskazują, że na cyberbezpieczeństwo (i w ogóle na bezpieczeństwo) trzeba patrzeć w szerokim kontekście. Dlatego sprowadzanie cyberbezpeczeństwa do kwestii czysto technicznych nie jest właściwe. Koncentrowanie się na wybranych aspektach bezpieczeństwa prowadzi do zaniedbywania pozostałych obszarów czy wręcz do powstawania groźnych luk w zabezpieczeniach. I wszystko jedno w jakim obszarze te luki powstaną – czy będzie to obszar organizacyjny, techniczny, czy związany z czynnikiem ludzkim. Ważne, że podatność taką można wykorzystać do ataku.

Architektura systemów IT jest zazwyczaj rozległa i złożona. Koncentrowanie zabezpieczeń w jednym punkcie nie sprawdza się. Klasyczny antywirus nie wystarczy, bo zapewnia określony poziom ochrony tylko w jednym miejscu. Zgodnie z modelem Zero Trust ochronie powinna podlegać całość środowiska IT: tożsamość, urządzenia końcowe, sieć, dane, aplikacja i infrastruktura.

Elementy, których ochrona nabiera dziś nowego znaczenia, to tożsamość i dane. Dane są bardziej zagrożone niż dotychczas, ponieważ w reakcji na pandemię Covid-19 użytkownicy opuścili kontrolowane środowiska IT i w trybie pracy zdalnej przenieśli się do domów, gdzie poziom ochrony ich danych jest zazwyczaj słabszy niż w korporacyjnej sieci. Z kolei nasilająca się działalność obcych służb, po agresji na Ukrainę uporczywie próbujących uzyskać dostęp do zasobów polskiej administracji, objawia się wzmożonymi kampaniami phishingowymi, kampaniami APT i wieloma innymi metodami na wyłudzenie tożsamości

i uzyskanie dostępu do danych. Dlatego ochrona tożsamości jest elementem krytycznym.

Sześciopak

Polski system ochrony infrastruktury krytycznej opiera się na zasadach z założenia podobnych do modelu Zero Trust. Zakładając, że proces ochrony powinien odnosić się do wszystkich typów zidentyfikowanych zagrożeń, wyróżnia on sześć obszarów, w których należy podjąć działania zapewniające jej bezpieczeństwo. Jest to bezpieczeństwo fizyczne, osobowe, prawne, techniczne, teleinformatyczne oraz plany ciągłości działania. Mówiąc inaczej – w procesie zarządzania ryzykiem należy uwzględnić zagrożenia ze strony intruza, pracownika, konkurencji, technologii, informatyki oraz mieć wdrożony plan ciągłości działania.

Ten tzw. „sześciopak" – nowatorskie polskie podejście do ochrony IK – pozostaje aktualny jako metodologia. Wojna u naszych granic niesie ze sobą natomiast dodatkowe zagrożenia, które można zidentyfikować w każdym z obszarów. Technologia cyfrowa pomaga w obniżaniu poziomu ryzyka w każdym obszarze bezpieczeństwa, nie tylko w teleinformatyce, o której mówi się najczęściej. Dodatkowo, każdy z tych obszarów uległ daleko posuniętej cyfryzacji.

Na przykład – bezpieczeństwo fizyczne może być wspierane przez sztuczną inteligencję Azure analizującą w chmurze zapis z systemu dozoru wizyjnego. Bezpieczeństwo prawne (związane z działalnością innych podmiotów gospodarczych) można wesprzeć sztuczną inteligencją (łatwo i tanio dostępną w chmurze) do wyłapywania niekorzystnych klauzul umownych. Bezpieczeństwo techniczne to optymalizacja procesów technologicznych w oparciu o dane przetwarzane w czasie rzeczywistym na brzegu sieci (edge computing).

Gra zespołowa

Bezpieczeństwo – teleinformatyczne i każde inne – to gra zespołowa. Współdziałanie technologii, ludzi i organizacji to np. cyberhigiena (użytkownicy) wspierana przez technikę (firewalle, SIEM itp.) pozwalająca na skuteczną realizację rozwiązań organizacyjnych opisanych zgodnie z modelem ZERO TRUST w polityce bezpieczeństwa. Wszystkie te trzy aspekty uzupełniają się wzajemnie i są jednakowo istotne. Nota bene – zgodnie z ostatnim raportem Microsoft Digital Defense Report – cyberhigiena pozwala uniknąć 98% zagrożeń.

Co dalej?

Budowanie odporności cyberprzestrzeni jest długotrwałym procesem, który powinien angażować – na zasadzie partnerstwa – administrację publiczną, sektor prywatny (szczególnie globalnych dostawców technologii) oraz społeczeństwo. Z uwagi na wieloletni charakter realizowanych projektów, państwo powinno współpracować z ograniczoną grupą zaufanych dostawców technologii. Jednym z pierwszych tematów takiego dialogu powinna być kwestia ochrony krytycznych zasobów cyfrowych poprzez utworzenie cyfrowej ambasady RP ulokowanej na terytorium sojuszniczego państwa NATO, ale pozostającej w polskiej jurysdykcji.

W krótszej perspektywie planistycznej warto dokonać gruntownego przeglądu posiadanych rejestrów ryzyka lub sporządzić je na nowo i uzupełnić o nowe czynniki towarzyszące wojnie – zgodnie z zasadą Zero Trust. Pomocne tu okażą się ogólnodostępne wytyczne dla operatorów infrastruktury krytycznej i dostawców usług cyfrowych – nawet w organizacjach, które nie zostały ujęte w ww. wykazach.

Po zidentyfikowaniu nowych obszarów ryzyka, w ramach jego analizy, wskazane jest rozważenie szerszego niż dotychczas wykorzystania technologii cyfrowej jako środka mitygującego ryzyko. Niektóre z rozwiązań, które jeszcze pięć lat temu pozostawały

w sferze science-fiction, są już dostępne, tanio i na wyciągnięcie ręki. Korzystajmy z tego, że przyszłość dzieje się już dziś i budujmy odporność, póki mamy na to czas.